SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL7 No4
DECEMBER 2023

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 1 – 35 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

HYBRID NETWORK INTRUSION DETECTION SYSTEMS: A SYSTEMATIC REVIEW

Alhassan Seiba[1], Gaddafi Abdul-Salaam*[1], Yaw Missah[1], Mohammad Hossein Anisi[2]

[1]Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.
[2]School of Computer Science and Electronic Engineering, University of Essex, Colchester, U.K.

*Corresponding author: Gaddafi Abdul-Salaam, Email: gaddafi.ict@knust.edu.gh

ABSTRACT: Network Security has become a major concern to governments, businesses and individuals all over the world as cybercriminals continuously attack networks and cause harm to personal and organizational data. Different forms of Intrusion Detection Systems(IDSs) have been proposed over the years to minimize these cyberattacks. Several researchers have tried to improve upon the detection accuracy and thus, reducing false alarm rates posed by some of the IDSs. In this paper, we conducted a chronological systematic review of hybrid intrusion detection systems covering all domains. In all, about 300 recent research articles were selected in the area but only 146 articles were able to meet the given quality assurance test. A critical review of the selected articles revealed that 61% did not carry out proper feature selection as a data preprocessing step and as low as 35% handled an imbalanced dataset. We have also done extensive discussions, spanning eleven years of research works on the existing Intrusion Detection Systems.

KEYWORDS: Autoencoder, Intrusion Detection, Deep Learning, Feature Selection

1.0 INTRODUCTION

The increasing use of Computer Networks especially the Internet has resulted in individuals and organizations storing sensitive data on web servers, database servers and social media platforms. This increase in the use of the internet has also caused a corresponding increase in the rate of cybercrime. CyberEdge group collected data from different parts of the world and publish a report that depicts a future likelihood of a successful attack. The report reveals that in 2014 the percentage of a successful attack was 38.1% and this figure is expected to rise steadily to 75% by the end of 2021. The figure also shows the rest of the years and the percentage of attacks expected. This figure paints a gloomy picture of an increase in cyber attacks within the coming years. One security mechanism put in place to eliminate or reduce these attacks is Intrusion Detection System (IDS). An intrusion Detection System is a hardware or software implementation that monitors unauthorized access to a computer network or host and reports on possible data violations. (Anderson, 1980) proposed the idea of Intrusion Detection. Since then different types of IDS have been developed to promote network security.

Based on where IDS is deployed there can be classified into Host Based Intrusion Detection System(HIDS) and Network Intrusion Detection System(NIDS). Host-Based Intrusion Detection System monitors data traffic on a single host computer for packets that are malicious or not. Network Intrusion Detection System on the other hand monitors data packets coming to a network and reports on any malicious activity. Figure 2 and Figure 3 show the difference between NIDS and HIDS. There are certain merits and demerits associated with each type. With regards to HIDS, the advantages are that it can handle encrypted communication, it does not require extra hardware and so it is more economical. The drawbacks to this method are that there is a delay in reporting attacks, it also consumes host resources and only able to monitor attacks on only one device where it is installed. NIDS has the advantage of being able to detect attacks on multiple computers, again, NIDS does not need to be installed on more than one host. NIDS also have some disadvantages including not being able to identify attacks that are encrypted, a dedicated hardware is required.

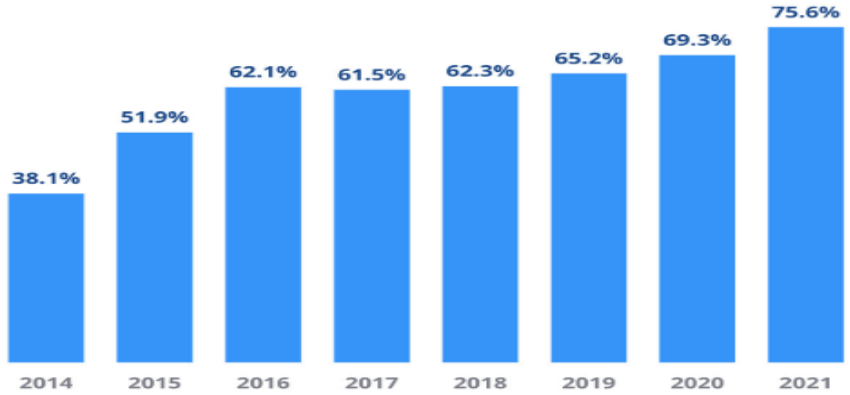


Figure 1: The Likelihood of a successful attack occurring (CyberEdge Group, 2021)

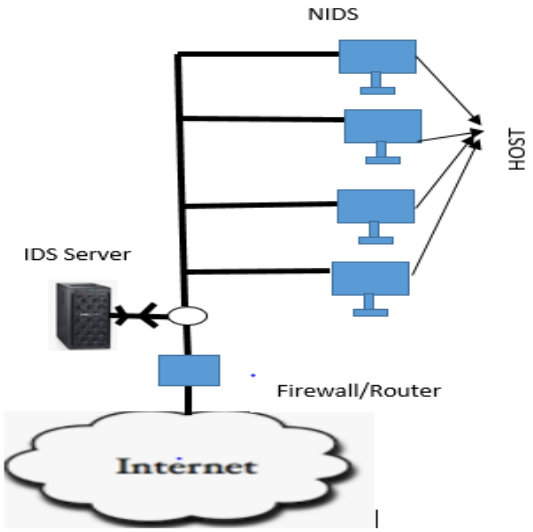


Figure 2: Network-based IDS (Seiba et al., 2021)

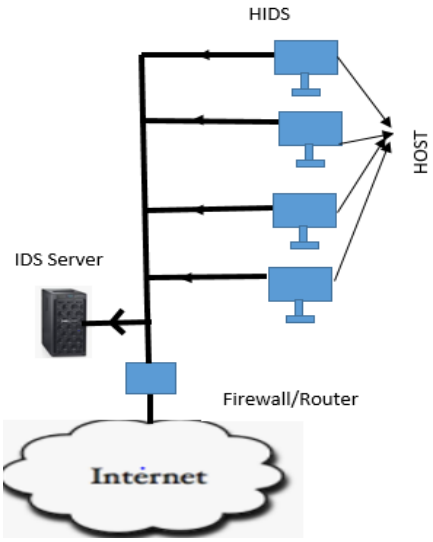


Figure 3: Host-based IDS (Seiba et al., 2021)

Intrusion Detection Systems can also be classified based on how there are implemented thus Signature Based Intrusion Detection Systems and Anomaly Based Intrusion
Detection System. A signature-Based Intrusion Detection System is implemented by keeping the profile of existing known attack and compared with incoming traffic to determine if it is malicious or not. The advantage associated with this kind of IDS is its ability to accurately identify intrusion with fewer false positives and false negatives. This kind of implementation is always criticised for not being able to identify novel or new attack types. Anomaly-based Intrusion Detection Systems can identify novel or new intrusions but fall short of being able to accurately identify intrusion resulting in false positives and false negatives.
There are several techniques used to implement anomaly Based Intrusion Detection Systems. These techniques are Statistical Based IDS, Knowledge-Based IDS and Machine Learning IDS.
Statistical Based Intrusion Detection System builds a distribution model for normal traffic and flag low-probability events as an intrusion(Khraisat *et al.*, 2019). This kind of anomaly IDS is simple to implement and can detect intrusion in real-time. The models of the Statistical Intrusion Detection System are Univariant, Multivariant and Time Series (Ye et.al, 2002). The univariant Statistical model measures one

variable at a time (Ye et.al, 2002). Multivariant Statistical IDS controls several variables at the same time (Camacho *et al.*, 2016).

According to Khraisat *et al.*(2019), the time series model is a series of observations made over a certain period and new observation is considered abnormal. The drawback to the times series model is the lack of accuracy and the need for one to have extensive knowledge of statistics.

The knowledge-Based Model is also known as the expert system. The technique requires creating a knowledge base which represents a normal traffic profile and actions which differ from this profile are considered as intrusion (Khraisat *et al.*, 2019). This knowledge base IDS is created by a human expert. The models used to develop such an intrusion Detection System include Finite State Machine, Description Language or Expert System (Walkinshaw, Taylor and Derrick, 2016). Because knowledge Based keep a profile of all normal behaviour false positives and false negatives are minimal. The weakness of this technique is the requirement meant for constant updates which makes it computationally expensive.

The last and the most popular technique for anomaly intrusion detection Systems is the Machine learning approach. Machine learning makes use of complex algorithms to extract needed data from large quantities of data. To achieve the need for effective IDS, many studies have explored the possibility of Machine Learning and Deep Learning techniques (Ahmad *et al.*, 2021). Both ML and DL belong to the field of Artificial Intelligence(AI). Even though machine learning is resilient to noisy data, robust and adaptive it is also faced with some drawbacks. According to Ayyagari *et al.* (2021), machine-learning approaches suffer from the limitations of manual feature engineering. They further argued that ML might be inefficient in handling large data. Machine learning by its nature is not able to handle multiclass classification tasks. Anomaly IDS build using machine learning are faced with the issue of false positives and false negatives.

These weaknesses of ML are however improved by deep learning. DL IDS can carry out feature selection automatically without manual intervention and hence improve the accuracy of prediction. Improved accuracy of DL-based IDS means fewer false positives and fewer false negatives. Examples of machine Learning Algorithms include for the design of IDS include Decision Tree (DT), Random Forest, K-nearest neighbour, K-mean, Support Vector Machine (SVM) and Artificial Neural Networks(ANN). Deep learning is also an ANN in which the number of hidden neurons has been deepening to increase its processing capacity. These techniques mentioned above have been used by several researchers to improve existing IDS. For instance, Ahmim, Derdour and Ferrag (2018) conducted a study based on the combining probability of Decision trees. Similarly, Batiha and Krömer (2020) also carried a research on the design and analysis of efficient Neural Network Intrusion Detection for wireless sensor networks. To increase the performance of these single machine learning techniques, a hybrid intrusion detection system has been introduced. However, the few numbers of hybrid intrusion system reviews suggest the area has not been explored enough (Maseno, Xing and Wang, 2022).

This study, therefore, seeks to carry out a systematic review of hybrid intrusion detection Systems. To the best of our knowledge, only one systematic review of Hybrid Intrusion Detection systems exists. This research when conducted, will expose both experienced and young researchers to techniques that need to be implemented to improve on the existing intrusion detection system.

Contributions

i. Provides extensive details on the types of the intrusion detection system
ii. This study has provided sufficient information on studies that have applied feature selection in their study for easy reference
iii. Enough information has been provided on studies that have handled imbalanced datasets in their work for easy reference
iv. Provide recommendations for increasing the detection rate and lowering the false positives associated with anomaly intrusion detection system

The rest of the work is divided into 4 main sections. Section 2 takes a review of related works, and Section 3 represents the methodology used to carry out the review. Section 4 is where the selected studies are

analyzed to provide results for discussion. Finally, section 5 takes a look at the conclusion and recommendations for further study.

2.0 RELATED WORKS

This Section examines previous studies related to a review of hybrid intrusion detection systems. This section will clearly state the difference between what has been done by other researchers and what this review seeks to do. Several studies have been conducted on a systematic review of intrusion detection systems and which is different from HIDS systematic review. For instance, Garg and Maheshwari(2016) conducted a review of the hybrid intrusion detection system. Their study was to review misuse and anomaly-based intrusion system. This study is different from their study because this takes into account not only anomaly and misuse intrusion detection system but also consider HIDS consisting of the use of more than one machine learning technique in a single study. This study, therefore, is broader in scope as compared to their study. Öney and Peker (2019) presented a review of intrusion detection involving Artificial Neural Networks. Here again, they focused on only artificial neural networks which is narrow in scope as compared to this study which considers all other machine learning languages as well. One major study that has been conducted on the Systematic Review of HIDS is the study by (Maseno, Wang and Xing, 2022). The objectives of their study focus on the weakness of algorithms used in HIDS, The metrics of evaluation and the dataset used to evaluate such models. Similarly this study span from 2012 to 2023 but differs from their study in

1. The number of studies selected for this study is 146 as compared to the previous study that used 111.
2. The second point is that the objectives of their study are different from the objectives of this study as stated below

a) To determine the distribution of studies by a publisher from 2012 to 2023
b) To identify studies that have applied feature selection in their models
c) To determine the specific feature selection technique applied.
d) To identify studies that have handled imbalanced dataset
e) To determine the specific technique applied to handle imbalanced data

3.0 METHODOLOGY

This study adopted the approach of (Kitchenham and Charters, 2007; Brereton et al., 2007 cited in Aldhaheri *et al.*, 2020) in which the Systematic literature Review is divided into planning, conducting and Reporting.

i. Planning the Review consist of three main steps:
    1. Identification of the need for the Systematic literature review
    2. Define the research questions
    3. Develop the research protocol
ii. Conducting the Review also consist of three-step
    1. Selecting the studies
    2. Define and apply quality assessment
    3. Extracting and synthesizing the selected data
iii. Reporting the review consist of three main steps
    1. Dissemination strategy specification
    2. Report formatting
    3. Report Evaluation.

3.1 PLANNING THE REVIEW

In planning the review, one needs to look at the need for the Systematic Literature Review (SLR), the research questions to be addressed in the study and the definition of the protocols for the study.

3.2 IDENTIFICATION OF THE NEED OF THE SLR

A review of the literature reveals that there is only one work that has been done on a systematic review of hybrid Intrusion Detection Systems. Even though their study exists the objectives of this study are different from theirs. This study intends to find out studies that apply feature selection and dataset balancing techniques in their proposed models. Their study on the other hand concentrate on trends in hybrid intrusion detection systems and dataset used for those study and the machine learning algorithms. Since feature selection and handling of imbalanced dataset form part of designing an intrusion detection system, it is important to investigate the use of these key techniques since the use of these techniques will have an impact on the results. Successful completion of this study will inform new and established researchers in the field of intrusion detection systems which dataset balancing technique is likely to give a better result and which feature selection technique will also make their model perform better. The studies that are discussed in this study span from 2012 to 2022. In all 142 studies have been selected for this review.

The objectives of this study are:

1. To determine the distribution of studies by a publisher from 2012 to 2023
2. To identify studies that have applied feature selection in their models
3. To determine the specific feature selection technique applied in Step 2
4. To identify studies that have handled imbalanced dataset
5. To determine the specific technique applied to handle imbalanced data in Step 4

3.3 RESEARCH QUESTIONS

The research questions addressed in this study include:
RQ1: What is the distribution of studies by a publisher from 2012 to 2023?
RQ2: How many studies have applied feature selection in their study?
RQ3: What are the feature selection techniques applied in these studies?
RQ4: How many studies have handled imbalanced datasets in their model?
RQ5: What are the exact techniques applied to handle an imbalanced dataset?

3.4 CONDUCTING THE REVIEW

Conducting the review starts with the selection of the studies, followed by quality assessment and finally the extraction and synthesizing of the selected data.

3.5 SEARCH PROCESS

To obtain relevant research papers for this study, the following search string was inserted into google scholar, IEEE database, Wiley database, Sage database, Science Direct, Springer, Emerald ACM and MDPI

1. Hybrid Intrusion detection review
2. Hybrid Anomaly detection review
3. Hybrid Intrusion Detection Survey
4. Hybrid Anomaly Intrusion Survey

This search showed some articles. Those articles have been used in the introduction part of the work to explain the concepts of intrusion detection systems. However, when the search string changed from review to systematic review as stated below there was only one systematic review on HIDS by(Maseno, Wang and Xing, 2022).

1. Hybrid Intrusion detection Systematic review

2. Hybrid Anomaly detection Systematic review
3. Hybrid Intrusion Detection Systematic Survey
4. Hybrid Anomaly Intrusion Systematic Survey

A thorough search was therefore carried out using the following strings to obtain the required data for the study

1. Hybrid Intrusion Detection System
2. Hybrid Anomaly Intrusion Detection System

The search used the above search input and the year was restricted between the period 2012 to 2023. A total of 300 articles consisting of reviews, conferences and research articles were retrieved. Inclusion and exclusion criteria were applied to reduce the number of articles to 146. The inclusion criteria and exclusion was based on the following (i) only article from scientific journals and conferences and excluded those without Journal or conference. (ii) Article that does not make use of publically available dataset in their study was excluded. (iii) Include articles published in English Language and exclude articles published in other languages. (iv) hybrid techniques using machine learning or deep learning and signature and anomaly were included. Publishers from Elsevier, Springer, Wiley, IEEE, Emerald, Sage, Hindawi, ACM and MDPI were included but other publishers were excluded.

3.6 QUALITY ASSESSMENT

QAR is applied to select studies. The quality assurance for this study is based on the following questions**.**
QAR1: Are they clearly stated research objective?
QAR2 : Are they measures to address data imbalance?
QAR3 : Is the experimental setup appropriate for the study?
QAR4 : Are findings presented in line with test results?
QAR5 : Has the author discuss issues of perfomance of the proposed method?
The criteria for scoring quality assurance questions are as follows
QAR1: yes(Y), the author has clearly stated objective(s) = 1 , Partial(P) the author has partialy stated objective(s) = 0.5 and no(N) the author has no objective(s) = 0.
QAR2: yes(Y) the author(s) addressed the issue of data inbalance = 1, no(N) the author did not address the issue data inbalance = 0.
QAR3: yes(Y) the author included approapriate experimental setup = 1,partial(P) the author included a partial experimental setup = 0.5 and (no) no experimental setup was included.
QAR4: yes(Y) the findings presented is inline with the text results = 1,no(N) the findings preseted is not inline with the test results = 0.
QAR5: yes(Y) the author discussed performance issues of the proposed System = 1, no(N) the author did not discuss performance issue with the proposed System.
Papers that obtain a total score of 3.5 out of 5 is selected. In all 146 papers were selected based based on the quality assurance measure.
Data Extraction
This step is when the data selected is used to answer the research questions. The Table 1 below shows the data gathered for each study based on our inclusion and exclusion criteria.

Table 1: Selected articles of Hybrid Intrussion Detection Systems

S/N	Title	Publisher	Reference
R1	Anomaly Based Intrusion Detection Using Hybrid Learning Approach of Combining k-medoids Clustering and Naïve Bayes Classification	IEEE	(Chitrakar and Chuanhe, 2012a)
R2	Gravitational search algorithm optimized neural misuse detector	Springer	(Sheikhan and Sharifi, 2012)

	with selected features by fuzzy grids–based association rules mining		
R3	Cascaded classifier approach based on Adaboost to increase detection rate of rare network attack categories	IEEE	(Natesan, Rajesh 2012)
R4	Anomaly Detection using Support Vector Machine Classification with k-Medoids Clustering	IEEE	(Chitrakar and Chuanhe, 2012b)
R5	A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System	IEEE	(Om, 2012)
R6	Mining network data for intrusion detection through combining SVM with ant colony Wenying	Elservier	(Feng *et al.*, 2013)
R7	A hybrid method based on Genetic Algorithm, Self-Organised Feature Map, and Support Vector Machine for better Network Anomaly Detection	IEEE	(Vidyapeetham, 2013)
R8	Multi-layer hybrid machine learning techniques for anomalies detection and classification approach	IEEE	(Sayed *et al.*, 2013)
R9	Flow-based anomaly detection in high-speed links using modified GSA- optimized neural network	Springer	(Sheikhan and Jadidi, 2014)
R10	A novel hybrid intrusion detection method integrating anomaly detection with misuse detection	Elservier	(Kim, Lee and Kim, 2014)
R11	Distributed Denial of Service Detection Using Hybrid Machine Learning Technique	IEEE	(Barati *et al.*, 2014)
R12	Adaptive Fuzzy Neural Network Model for Intrusion Detection	IEEE	(Kumar and Mohan, 2014)
R13	A New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming Seyed	Elservier	(Mojtaba *et al.*, 2015)
R14	An Integration of K-Means Clustering and Naïve Bayes Classifier for Intrusion Detection	IEEE	(Varuna, 2015)
R15	Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function	Elservier	(Ravale, Marathe and Padiya, 2015)
R16	A hybrid method consisting of GA and SVM for intrusion detection system	Springer	(Rahmani *et al.*, 2015)
R17	Hybrid Evolutionary Algorithms for Data Classification in Intrusion Detection Systems Abdel-Rahman	IEEE	(Hedar *et al.*, 2015)

R18	A Global Hybrid Intrusion Detection System for Wireless Sensor Networks	Elservier	(Maleh *et al.*, 2015)
R19	An effective combining classifier approach using tree algorithms for network intrusion detection	Springer	(Kevric, Jukic and Subasi, 2016)
R20	A Hybrid Approach to Reducing the False Positive Rate in Unsupervised Machine Learning Intrusion Detection	IEEE	(Landress, 2016)
R21	Distributed-Intrusion Detection System using combination of Ant Colony Optimization (ACO) and Support Vector Machine (SVM)	IEEE	(Wankhade, 2016)
R22	Anomaly Detection Based on Profile Signature in Network Using Machine Learning Technique	IEEE	(Atefi, 2016)
R23	Improving K-Means Clustering Using Discretization Technique in Network Intrusion Detection Syst	IEEE	(Network, 2016)
R24	A hybrid Deep Learning Strategy for an Anomaly Based N-IDS	IEEE	(Mendjeli, 2017)
R25	An Analysis of Random Forest Algorithm Based Network Intrusion Detection System	IEEE	(Aung, 2017)
R26	ML-IDS: A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things	IEEE	(Shukla, 2017)
R27	Intrusion detection model using fusion of chi-square feature selection and multi class SVM	IEEE	(Thaseen and Kumar, 2017)
R28	A semi-supervised Intrusion Detection System using active learning SVM and fuzzy c-means clustering	IEEE	(Kumari, 2017)
R29	A novel hybrid anomaly based intrusion detection method	IEEE	(Qazanfari, 2017)
R30	An effective network attack detection method based on kernel PCA and LSTM- RNN	IEEE	(Meng *et al.*, 2017)
R31	A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection	Springer	(Malik and Khan, 2017)
R32	An Efficient Fuzzy-Based Hybrid System to Cloud Intrusion Detection	Springer	(Raja and Ramaiah, 2017)

R33	Enhancing effectiveness of intrusion detection systems: A hybrid approach	IEEE	(Subba, Biswas and Karmakar, 2017)
R34	Anomaly Detection Approach using Hybrid Algorithm of Data Mining Technique	IEEE	(Gadal and Mokhtar, 2017)
R35	A Framework of Novel Feature Set Extraction based Intrusion Detection System for Internet of Things using Hybrid Machine Learning Algorithms	IEEE	(Nivaashini and Thangaraj, 2018)
R36	Intrusion Detection Using Multilayer Perceptron and Neural Networks with Long Short-Term Memory	IEEE	(Borisenko *et al.*, 2018)
R37	Intrusion detection in network systems through hybrid supervised and unsupervised mining process - a detailed case study on the ISCX benchmark dataset -	Elservier	(Soheily-Khah, Marteau and Bechet, 2018)
R38	Intrusion Detection System by Using Hybrid Algorithm of Data Mining Technique	IEEE	(Foroushani and Li, 2018)
R39	An Efficient IDS Using Hybrid Magnetic Swarm Optimization in WANETs	IEEE	(Sadiq *et al.*, 2018)
R40	Anomaly-Based Network Intrusion Detection System through Feature Selection and Hybrid Machine Learning Technique	IEEE	(Pattawaro, 2018)
R41	Feature Reduction and Selection Based Optimization for Hybrid Intrusion Detection System Using PGO followed by SVM	IEEE	(Sagar, Shrivastava and Gupta, 2018)
R42	Hybrid approach for intrusion detection system	IEEE	(Singh and Venkatesan, 2018)
R43	HIDCC: A hybrid intrusion detection approach in cloud computing	Willey	
R44	Hybrid Internal Anomaly Detection System for IoT: Reactive Nodes with Cross-Layer Operation	Willey	(Thanigaivelan, Virtanen and Isoaho, 2018)
R45	Hybrid Intrusion Detection System using K-means and K-Nearest Neighbors Algorithms	IEEE	(Aung, 2018a)
R46	Hybrid Intrusion Detection System using K-means and Random Tree Algorithms	IEEE	(Aung, 2018b)

R47	A hybrid Particle swarm optimization -Extreme Learning Machine approach for Intrusion Detection System	IEEE	(Ali *et al.*, 2018)
R48	A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection	Elservier	(Hajisalem and Babaie, 2018)
R49	RST-RF: A Hybrid Model based on Rough Set Theory and Random Forest for Network Intrusion Detection	ACM	(Jiang and Lv, no date)
R50	Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection	IEEE	(Taher, 2019)
R51	Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments	IEEE	(Tekeo, 2019)
R52	Evolving deep learning architectures for network intrusion detection using a double PSO	Elservier	(Elmasry, Akbulut and Zaim ,2019)
R53	The Hybrid Technique for DDoS Detection with Supervised Learning Algorithms	Elservier	(Hosseini and Azizi, 2019)
R54	Optimization of Network Intrusion Detection System Using Genetic Algorithm with Improved Feature Selection Technique	IEEE	(Matel, Sison and Medina, 2019)
R55	Hybrid optimization scheme for intrusion detection using considerable feature selection	Springer	(Karthikeyan, 2019)
R56	Using Machine Learning techniques to improve Intrusion Detection Accuracy	IEEE	(Zhang *et al.*, 2019)
R57	A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network	MDPI	(Khan and Karim, 2019)
R58	TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-based Intrusion Detection System	IEEE	(Tama, Comuzzi and Rhee, 2019)
R59	Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments	IEEE	(Aljamal *et al.*, 2019)
R60	HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems	IEEE	(Khan, Pi and Khan, 2019)
R61	Efficient IDs for MANET Using Hybrid Firefly with a Genetic Algorithm	IEEE	(Shona and Kumar, 2019)

R62	A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifier	Springer	(Saleh, Talaat and Labib, 2019)
R63	A new approach for intrusion detection system based on training multilayer perceptron by using enhanced Bat algorithm	Springer	(Ghanem and Jantan, 2019)
R64	A Novel Intrusion Detector Based on Deep Learning Hybrid Methods	IEEE	(Shizhao and Tianbo, 2019)
R65	A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection	IEEE	(He *et al.*, 2019)
R66	A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection	Springer	(Haghnegahdar and Wang, 2019)
R67	An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic	IEEE	(Zhang, 2019)
R68	A Hybrid Classifier Approach for Network Intrusion Detection	IEEE	(Arivardhini, Alamelu and Deepika, 2020)
R69	A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios	IEEE	(Bovenzi *et al.*, 2020)
R70	A Hybrid Anomaly Classification with Deep Learning (DL) and Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS)	IEEE	(Atefi, 2020)
R71	A hybrid feature extraction network for intrusion detection based on global attention mechanism	IEEE	(Chen, 2020)
R72	A Hybrid Deep Learning Model for Malicious Behavior Detection	IEEE	(Xu *et al.*, 2020)
R73	Hybrid Intrusion Detection System Based on Deep Learning	IEEE	(Azawii and Lateef, 2020)
R74	Hybrid Machine Learning For Network Anomaly Intrusion Detection	IEEE	(Chkirbene *et al.*, 2020)
R75	Intrusion Detection System based on Hybrid Classifier and User Profile Enhancement Techniques	IEEE	(Pokharel, 2020)
R76	A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing Mahdi	Elservier	(Rabbani *et al.*, 2020)

R77	New Hybrid Method for Attack Detection Using Combination of Evolutionary Algorithms, SVM, and ANN	Elservier	(Hosseini, Mohammad and Zade, 2020)
R78	Fuzzy-Taylor-Elephant Herd Optimization inspired Deep Belief Network for DDoS Attack Detection and comparison with state-of-the-arts algorithms	Elsevier	(Velliangiri and Pandey, 2020)
R79	A Hybrid Intrusion Detection System Based on Decision Tree and Support Vector Machine	IEEE	(Kumari, 2020)
R80	An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons	IEEE	(Ghanem *et al.*, 2020)
R81	Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine	IEEE	(Wang *et al.*, 2020)
R82	A Real-Time and Ubiquitous Network Attack Detection Based on Deep Belief Network and Support Vector Machine	IEEE	(Zhang *et al.*, 2020)
R83	Machine learning and data mining methods for hybrid IoT intrusion detection	IEEE	(Ghazi, 2020)
R84	Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN	IEEE	(Malik *et al.*, 2020)
R85	Improving Attack Detection Performance in NIDS Using GAN	IEEE	(Li, 2020)
R86	An effect of chaos grasshopper optimization algorithm for protection of network infrastructure	IEEE	(Dwivedi, Vardhan and Tripathi, 2020)
R87	Hybrid approach to intrusion detection in fog-based IoT environments	IEEE	(Souza *et al.*, 2020)
R88	Providing a Hybrid Approach for Detecting Malicious Traffic on the Computer Networks Using Convolutional Neural Networks	IEEE	(Pakanzad, 2020)
R89	An efficient XGBoost–DNN-based classification model for network intrusion detection system	Springer	(Devan and Khare, 2020)
R90	Detection of anomaly intrusion utilizing self-adaptive grasshopper optimization algorithm	Springer	(Shukla, 2020)

R91	RNN-VED for Reducing False Positive Alerts in Host-based Anomaly Detection Systems	IEEE	(Bouzar-benlabiod *et al.*, 2020)
R92	Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models	MDPI	(Polat and Polat, 2020)
R93	Cascaded hybrid intrusion detection model based on SOM and RBF neural networks	Willey	(Almiani *et al.*, 2020)
R94	Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks	Springer	(Kaur and Singh, 2020)
R95	Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network	Springer	(Umarani and Kannan, 2020)
R96	A Hybrid Nested Genetic-Fuzzy Algorithm Framework for Intrusion Detection and Attacks	IEEE	(Elhefnawy, Abounaser and Badr, 2020)
R97	Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network	IEEE	(Jiang *et al.*, 2020)
R98	A Hybrid Intrusion Detection System for Smart Home Security Faisal	IEEE	(Alghayadh and Debnath, 2020)
R99	An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks	Springer	(Latah and Toker, 2020)
R100	Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine	MPDI	(Khraisat *et al.*, 2020)
R101	Two-Stages Intrusion Detection System Based On Hybrid Methods	ACM	(Azzaoui, 2020)
R102	Improved Intrusion Detection Accuracy Based on Optimization Fast Learning Network Model	IEEE	(Ali and Aasi, no date)
R103	A Hybrid Approach of ANN-GWO Technique for Intrusion Detection	IEEE	(Sharma and Tyagi, 2021)
R104	A Hybrid Data-driven Model for Intrusion Detection in VANET A Hybrid Data-driven Model for Intrusion Detection in VANET Hind	Elsevier	(Bangui *et al.*, 2021)
R105	Hybrid Intrusion Detection System for Detecting New Attacks Using Machine Learning	IEEE	(Enigo, 2021)

R106	A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection	IEEE	(Singhal *et al.*, 2021)
R107	A Novel Intrusion Detection Method Based on WOA Optimized Hybrid Kernel RVM 2021	IEEE	(Gao, Yue and Wu, 2021)
R108	A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques	Willey	(Zhang *et al.*, 2021)
R109	An Online Network Intrusion Detection Model Based on Improved Regularized Extreme Learning Machine	IEEE	(Tang and Li, 2021)
R110	A Multi-Layer Classification Approach for Intrusion Detection in IoT Networks Based on Deep Learning	MPDI	(Qaddoura *et al.*, 2021)
R111	Feature selection using cloud-based parallel genetic algorithm for intrusion detection data classification	Springer	(Kec, 2021)
R112	Serial and Parallel based Intrusion Detection System using Machine Learning	IEEE	(Das, 2021)
R113	Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection	Springer	(Prabhakaran and Kulandasamy, 2021)
114	An Enhanced Intrusion Detection System using Particle Swarm Features selection techniques	Elsevier	(Oluwaseun *et al.*, 2021)
R115	A hybrid machine learning model for intrusion detection in VANET	Springer	(Bangui, 2021)
R116	An Intrusion Detection System based on PSO-GWO Hybrid Optimized Support Vector Machine	IEEE	(Li, Zhang and Wang, 2021)
R117	A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning	IEEE	(Liu, Gu and Wang, 2021)
R118	An improved ensemble based intrusion detection technique using XGBoost	Willey	(Bhati *et al.*, 2021)
R119	A hybrid machine learning method for increasing the performance of network intrusion detection systems	Springer	(Megantara and Ahmad, 2021)
R120	An edge based hybrid intrusion detection framework for mobile edge computing	Springer	(Singh, Chatterjee and Satapathy, 2021)

R121	A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM	IEEE	(Wisanwanichthan and Thammawichai, 2021)
R122	SABADT: Hybrid Intrusion Detection Approach for Cyber Attacks Identification in WLAN	IEEE	(Pu *et al.*, 2021)
R123	Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning	IEEE	(Seo and Pak, 2021)
R124	HCRNNIDS:Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System	MPDI	(Khan, 2021)
R125	Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection	Springer	(Dwivedi, Vardhan and Tripathi, 2021)
R126	MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles	IEEE	(Yang, Moubayed and Shami, 2021)
R127	Hybrid Classification for High-Speed and High-Accuracy Network Intrusion Detection System	IEEE	(Kim and Pak, 2021)
R128	Intrusion Detection System Based on Hybrid Hierarchical Classifiers	Springer	(Mohd, Singh and Bhadauria, 2021)
R129	Network Intrusion Detection Using Hybrid Machine Learning Model	ACM	(Mazumder *et al.*, 2021)
R130	Design and Development of RNN-based Anomaly Detection Model for IoT Networks	IEEE	(Ullah, Mahmoud and Member, 2022)
R131	XGBoosted Misuse Detection in LAN-Internal Traffic Dataset	IEEE	(Zhang, no date)
R132	Deep Generative Learning Models for Cloud Intrusion Detection Systems	IEEE	(Vu *et al.*, 2022)
R133	Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework	IEEE	(Razib *et al.*, 2022)
R134	A Robust Adaptive Intrusion Detection System using Hybrid Deep Learning	IEEE	(Aravamudhan, 2022)
R135	An Efficient Network Intrusion Detection and Classification System	MDPI	(Ahmad *et al.*, 2022)
R136	Towards SDN-Enabled, Intelligent Intrusion Detection System for Internet of Things (IoT) Mohammed	IEEE	(Saleh *et al.*, 2022)

R137	Research on Intrusion Detection Based on Neural Network Optimized by Genetic Algorithm	IEEE	(Li *et al.*, 2022)
R138	Optimized Deep Autoencoder Model for Internet of Things Intruder Detection	IEEE	(Lahasan and Samma, 2022)
R139	An Intrusion Detection System for Zero-Day Attacks to Reduce False Positive Rates	IEEE	(Pitre, 2022)
R140	A hybrid approach Towards Efficient and Accurate Intrusion Detection for In-Vehicle Network	IEEE	(Zhang *et al.*, 2022)
R141	Machine Learning Based Intrusion Detection Systems Using HGWCSO And ETSVM Techniques	IEEE	(Srikrishnan, Raaza and Gopalakrishnan, 2022)
R142	Feed-Forward Intrusion Detection and Classification on A Smart Grid Network	IEEE	(Aribisala, Khan and Husari,2022)
R143	A hybrid CNN+ LSTM-based Intrusion detection system for Industrial IoT networks	ELSEVIER	(Can and Albayrak, 2023)
R144	Hybrid intrusion detection based on improved Harris Hawk optimization algorithm	Taylor and Francis	(Zhou, Zhang and Liang, 2023)
R145	Composition of hybrid deep learning model and feature optimization for intrusion detection	MDPI	(Henry *et al.*, 2023)
R146	Optimization of Intrusion Detection Using likely point PSO and Enhanced LSTM-RNN hybrid technique in communication networks	IEEE	(Donkol *et al.*, 2023)

4.0 RESULTS AND DISCUSSION

RQ1: What is the distribution of studies by publisher from 2012 to 2023?

A count on the number of article by a publisher was conducted and the Figure 4 below shows the distribution of papers by such publishers. From Figure 4 , IEEE dominate as the publisher with the higest number of papers. A total of 93 papers were obtained from IEEE Xplore database representing 65 percent of the total studies selected for this work. The domination of IEEE could be due to researchers having full access to IEEE Xplore database.It also means that IEEE has given young and comming reseachers the chance to showcase their research skills through comferences. The other publishers that shared the rest of the 35 percent include:

1) Springer with 22 papers representing 15 percentage of the total papers selected
2) Elservier with 13 papers representing 9 percent of the total papers selected.
3) MDPI follows with 6 papers representing 4 percent of the total number of paper selected
4) Willey was fifth with a total of 5 papers representing 3.5 percent
5) ACM was the least with only 3 paper representing 2.1percent

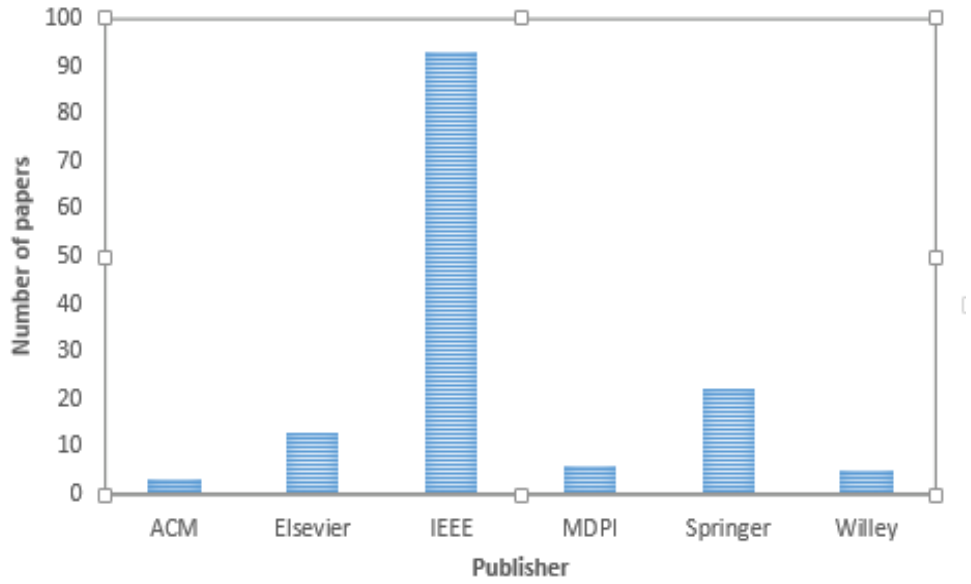


Figure 4: Publisher vr the number of papers

RQ2: How many studies have applied feature selection in their study?

Ahmad *et al.* (2022) argued that feature selection involve the reduction of computational cost by removing features that have no effect on target variable.

Many researchers have agreed that feature selection which form a major part in any classification problem is essential to obtaining accurate results. For instance (Kec, 2021) stated that in order to build a complex model on top of dataset,feature selection is an important step in machine learning and statistics. Feature selection is critical in improving machine learning agorithms and the building of HID models (Gadal and Mokhtar, 2017). In view of the impotance of feature selection, this study tried to identify HIDS studies that have applied feature selection in their research. Out of the 146 studies selected only 57 papers representing 39% applied feature selection in their study while 89 papers representing 61% did not carry out feature selection. pThis means that those research that did not apply feature selection can be look at to improve on the performance of those studies. The results of the study is represented in the Figure 5 below.

A careful analysis of the reviewed papers reveals that supervised feature selection techniques have lower accuracy as compared to unsupervised feature selection techniques. For instance autoencoder which is a unsupervised dimensionality technque performs better than Principal Component Analysis(PCA), a supervised technique which is widely accepted by industry even under contaminated environment(Madani and Vlajic, 2018). This means that to achive better results in terms of accuracy and low false alarm rate, deep learning feature selection technques should be implemented.

Apart from deep learning another technique that have gain popularity is the use of hybrid feature selection technique which consist of the use of more that one feature selection technique to select efficient feature to improve on the classification accuracy.This technique was implement by Ahmad *et al.*(2022) when the suggested p-value and correlation measure as a means to build an Efficient network intrusion detection system. Experimental results of their study suggested an improved performance as compared to using a single technique. This study and similar studies by others point to the fact that using hybrid feature selection technique can improve on IDS model performance.

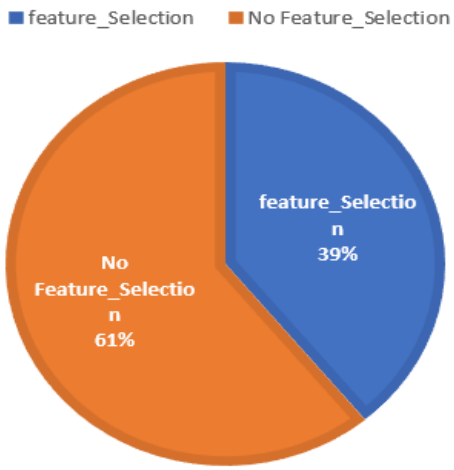


Figure 5: HIDS that have applied feature selection in their model

RQ3: What are the feature selection techniques applied in these studies?
There are several feature selection techniques that have been applied by various researchers in the selected studies. This section take a look at those techniques.

Table 2: Studies and feature selection techniques applied

Technique	Studies applying it	Number of studies
Fuzzy Grid-Based Association Rule	R2	1
Entropy Based Feature Selection	R5,R29, R78	3
Genetic Algorithm(GA)	R7,R11,R59,R61	4
Principal Component Analysis	R8, R30,R35,R51,R60,R121,R141	8
Genetic Algorithm-Support Vector Machine	R16	1
Decision Tree(J48)	R20	1
Chi-Square	R27	1
Infomation Gain	R34,R36,R38, R39,R43,R85,R120,R129	8
Attribute Average	R40	1
Plants growth optimization	R41	1
Correlation Based feature selection	R48,R35,R145	4
Rough Set Theory(RST) and Correlation Based Feature Selection	R49	1
Support Vector Machine	R50	1
Meta nodes	R53	1
Naive Base	R62	1
Crow Spam Optimization	R73	1
Random Forest	R74	1
GA-SVM	R75	1
MGA-Support Vector Machine	R77	1
Autoencoder	R81,R116	2
Emsemble feature selection	R86,R96,R138,R125	4
XGBOOST Score	R89	1
Relief Agorithm	R92	1

Features important decision	R119	1
FSAP	R122	1
K-mean Sampling	R126	1
P-value and correlation measure	R135	1
Grey Wolf Optimization Search Optimization and Enhanced translative support vector machine	R142	1
particle Swam Optimization	R52,R31,R146	2
Improved harris Hawk optimization algorithm	R144	1

From the Table2 above, about 31 different feature selection methods were identified. The feature selection methods that most researchers used in the selected studies are Information Gain and Principal Component Analysis (PCA). These two methods have been used by 15 studies representing 30% of all the feature selection methods that have been identified in this study. The rest are Emsembled feature selection, correlation based feature selection and Genetic Algorithm, 4 studies each, Entropy based feature selection and particle swam optimization 3 studies each and autoencoder recording 2 studies. The rest of the method has been used just once.

RQ4: How many studies have handled imbalanced dataset in their model?

Khan, Pi and Khan (2019) investigated the effect of using dataset balancing technique in the design of Intrusion Detection System. The outcome of their study revealed a significant increase in the performance of their model. For instance, before applying dataset balancing technique the classification accuracy was 91% but after applying the dataset balancing technique the acuracy increased to 97%, precision also increased from 92% to 98% and other metrics such as f-score and recall all saw an increase after balancing the dataset. Similary,Kim and Pak(2021) presnted a study on Intrusion detection system that compared Random forest classifier and Random forest with Smote which is a dataset balancing technique. The results show an impresive performance for the Random forest +Smote. The outcome of these studies and many other studies makes it imperative to analyse hybrid Intrusion detection systems that applies dataset balancing technques in their study and those that have not. This study will create the awareness for season researchers and up and coming ones in the field of IDS specifically HIDS to incoperate this important technique in their studies to improve the performance of existing HIDS.

Out of the 142 studies reviewed 22 studies applied databalancing technique that represent 15% of the total studies. This clearly shows that few researchers have taken the issue of imbalance dataset serously. This results means that existing studies without this dataset balancing technique can be reconducted with an appropriate dataset balancing technque for improved perfomance. The pie chart below shows the distribution of studies that have used dataset balancing technique and those who have not.

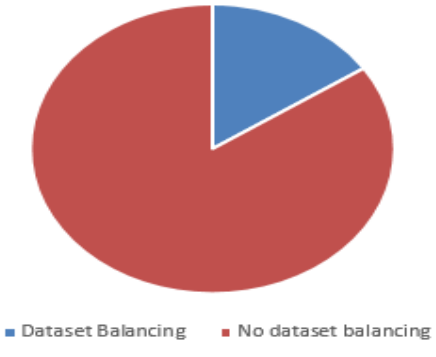


Figure 6: Studies that have applied dataset balancing technique and those who have not

RQ5: What are the exact techniques applied to handle imbalance dataset?
Several methods exist for handling imbalance dataset. This section will list those techniques and the studies associated with them.

Table 3: Studies and data imbalance handing techniques

Studies	Dataset Balancing Technique Applied
R2	Cascading method
R25,R35,R104,R115	Random Forest
R49,R121,R124,	Down Sampling
R60,R66,R85,R94,R110,R126,R127,R137	SMOTE
R67	SMOTE +Edited Nearest Neighbor
R97	SMOTE& One side-selection
R117	ADASYN
R130	Borderline SMOTE
R131	SMOTE, RF, Under Sampling
R98	Down and up Sampling

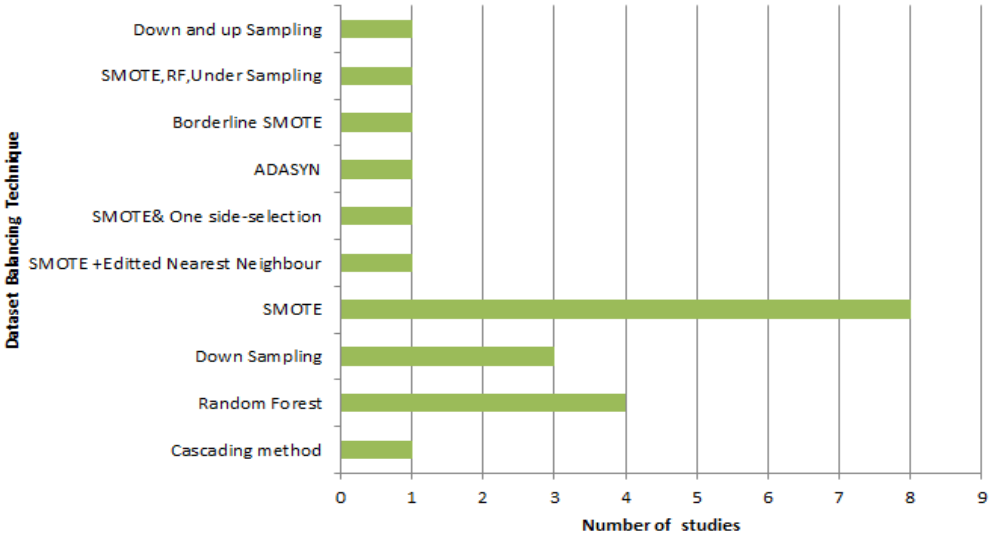


Figure 6: Number of studies against dataset balancing techniques

From the Figure 6 the study identified ten(10) different data balancing techniques that have been applied by different researchers. Out of these ten techniques SMOTE have been used by eight(8) different authors to handle imbalance dataset. This makes SMOTE the most used dataset balancing technique in our selected studies. Apart from that, few researchers have also combined SMOTE with other techniques to increase the performance of the classical SMOTE. These studies include R67, R97, R130 and R131. After SMOTE

the most used technique is Random Forest with 4 different authors applying it in our selected studies. Down Sampling has also been used three times to handle imbalance dataset. The rest of the techniques have been used once.

5.0 CONCLUTIONS AND RECOMMENDATIONS

The increasing interest of cyber security security expert on the use of hybrid intrusion detection system as depicted by Table 1 is an indication that more effort need to be put in place to make them more efficient. The efficiency can only be improved if the weakness of existing methods are are brought to the fore to inform experience and novice researchers to analysze and find innovative solutions to address the weakness. This study therefore perfectly addresses this need. The findings from this paper reveals that cyber security research has shifted from using a single technique to the using of hybrid technique. Another technique which has proven to improve the performance which most researcher did not include in their study is feature selection. A critical analysis of the selected studies reveals most HIDS do not carry out feature selection properly at the data preprocessing stage. Imbalaance dataset also represents a major setupback to improving the perfomance of hybrid intrusion detecction system. Majority of our selected studies did not incoporated dataset balancing techniques in their study. This study there recommend the use of proper feature selection process, the use of dataset balancing tecnique to improve the perfomance of hybrid intruion detection system.

1. This study therefore recommend that the 60% of studies that did not incoporate feature selection can be reconducted for possible increase in performance
2. 75% of the studies selected did not apply dataset balancing technique in their work. Applying dataset balancing technique can help improve the performance of those studies.
3. Studies that used supervised technique as feature selection technique can be reconducted using deep learning or unsupvised feature selection techniques. Unsupervised technique can handle the high volumes of traffic arriving at a computer network and therefore can be implemented in the real word network environment.
4. The use of hybrid feature selection techniques should be implemented for improved IDS detection accuracy.

FUNDING: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

DECLARATION OF COMPETING INTEREST: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AND MATERIAL: Dataset available

REFERENCES:

1. Ahmad, I. *et al.* (2022) 'An Efficient Network Intrusion Detection and Classification System', pp. 1–15.

2. Ahmad, Z. *et al.* (2021) 'Network intrusion detection system: A systematic study of machine learning and deep learning approaches', *Transactions on Emerging Telecommunications Technologies*, 32(1), pp. 1–29. Available at: https://doi.org/10.1002/ett.4150.

3. Ahmim, A., Derdour, M. and Ferrag, M.A. (2018) 'An intrusion detection system based on combining probability predictions of a tree of classifiers', *International Journal of Communication Systems*, 31(9), pp. 1–17. Available at: https://doi.org/10.1002/dac.3547.

4. Alghayadh, F. and Debnath, D. (2020) 'A Hybrid Intrusion Detection System for Smart Home Security', *IEEE International Conference on Electro Information Technology*, 2020-July, pp. 319–323. Available at: https://doi.org/10.1109/EIT48999.2020.9208296.

5. Ali, M.H. *et al.* (2018) 'A hybrid Particle swarm optimization -Extreme Learning Machine approach for Intrusion Detection System', *2018 IEEE 16th Student Conference on Research and Development, SCOReD 2018*, pp. 1–4. Available at: https://doi.org/10.1109/SCORED.2018.8711287.

6. Ali, M.H. and Aasi, A. (no date) 'Improved Intrusion Detection Accuracy Based on Optimization Fast Learning Network Model'.

7. Aljamal, I. *et al.* (2019) 'Hybrid intrusion detection system using machine learning techniques in cloud computing environments', *Proceedings - 2019 IEEE/ACIS 17th International Conference on Software Engineering Research, Management and Application, SERA 2019*, pp. 84–89. Available at: https://doi.org/10.1109/SERA.2019.8886794.

8. Almiani, M. *et al.* (2020) 'Cascaded hybrid intrusion detection model based on SOM and RBF neural networks', *Concurrency and Computation: Practice and Experience*, 32(21), pp. 1–14. Available at: https://doi.org/10.1002/cpe.5233.

9. Anderson, J.P. (1980) 'Computer security threat monitoring and surveillance', *Technical Report James P Anderson Co Fort Washington Pa*, p. 56. Available at: https://doi.org/citeulike-article-id:592588.

10. Aravamudhan, P. (2022) 'using Hybrid Deep Learning'.

11. Atefi, K. (2016) 'Anomaly Detection Based on Profile Signature in Network Using Machine Learning Technique', pp. 71–76.

12. Atefi, K. (2020) 'A Hybrid Anomaly Classification with Deep Learning (DL) and Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS)', (Cspa), pp. 28–29.

13. Aung, Y.Y. (2017) 'An Analysis of Random Forest Algorithm Based Network Intrusion Detection System', pp. 127–132.

14. Aung, Y.Y. (2018a) 'Hybrid Intrusion Detection System using K-means and K-Nearest Neighbors Algorithms', *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, pp. 34–38.

15. Aung, Y.Y. (2018b) 'Hybrid Intrusion Detection System using K-means and Random Tree Algorithms', *2018 19th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pp. 218–223.

16. Ayyagari, M.R. *et al.* (2021) 'Intrusion detection techniques in network environment: a systematic review', *Wireless Networks*, 27(2), pp. 1269–1285. Available at: https://doi.org/10.1007/s11276-020-02529-3.

17. Azawii, A. and Lateef, A. (2020) 'Hybrid Intrusion Detection System Based on Deep Learning'.

18. Azzaoui, H. (no date) 'Two-Stages Intrusion Detection System Based On Hybrid Methods'.

19. Bangui, H. (2021) 'A hybrid machine learning model for intrusion detection in VANET', *Computing* [Preprint]. Available at: https://doi.org/10.1007/s00607-021-01001-0.

20. Bangui, H. *et al.* (2021) 'ScienceDirect A Hybrid Hybrid Data-driven Data-driven Model Model for for Intrusion Intrusion Detection Detection in in VANET', *Procedia Computer Science*, 184, pp. 516–523. Available at: https://doi.org/10.1016/j.procs.2021.03.065.

21. Barati, M. *et al.* (2014) 'Distributed Denial of Service Detection Using Hybrid Machine Learning Technique', pp. 268–273.

22. Batiha, T. and Krömer, P. (2020) 'Design and analysis of efficient neural intrusion detection for wireless sensor networks', *Concurrency Computation* , (June), pp. 1–12. Available at: https://doi.org/10.1002/cpe.6152.

23. Bhati, B.S. *et al.* (2021) 'An improved ensemble based intrusion detection technique using XGBoost', *Transactions on Emerging Telecommunications Technologies*, 32(6), pp. 1–15. Available at: https://doi.org/10.1002/ett.4076.

24. Borisenko, B.B. *et al.* (2018) 'Intrusion Detection Using Multilayer Perceptron and Neural Networks with Long Short-Term Memory'.

25. Bouzar-benlabiod, L. *et al.* (2020) 'RNN-VED for Reducing False Positive Alerts in Host-based Anomaly Detection Systems', pp. 17–24. Available at: https://doi.org/10.1109/IRI49571.2020.00011.

26. Bovenzi, G. *et al.* (2020) 'A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios'.

27. Camacho, J. *et al.* (2016) 'PCA-based multivariate statistical network monitoring for anomaly detection', *Computers and Security*, 59, pp. 118–137. Available at: https://doi.org/10.1016/j.cose.2016.02.008.

28. Can, H. and Albayrak, Z. (2023) 'Engineering Science and Technology , an International Journal A hybrid CNN + LSTM-based intrusion detection system for industrial IoT networks', *Engineering Science and Technology, an International Journal*, 38, p. 101322. Available at: https://doi.org/10.1016/j.jestch.2022.101322.

29. 'Cascaded classifier approach based on Adaboost to increase detection rate of rare network attack categories' (2012), pp. 417–422.

30. Chen, W. (2020) 'A hybrid feature extraction network for intrusion detection based on global attention mechanism', pp. 481–485. Available at: https://doi.org/10.1109/CIBDA50819.2020.00114.

31. Chitrakar, R. and Chuanhe, H. (2012a) 'Anomaly based Intrusion Detection using Hybrid Learning Approach of combining k-Medoids Clustering and Naïve Bayes Classification', (September). Available at: https://doi.org/10.1109/WiCOM.2012.6478433.

32. Chitrakar, R. and Chuanhe, H. (2012b) 'Anomaly Detection using Support Vector Machine Classification with k-Medoids Clustering', pp. 1–5.

33. Chkirbene, Z. *et al.* (2020) 'Hybrid Machine Learning For Network Anomaly Intrusion Detection', pp. 163–170.

34. Computing, N., Sheikhan, M. and Jadidi, Z. (2014) 'Mansour Sheikhan & Zahra Jadidi', (November). Available at: https://doi.org/10.1007/s00521-012-1263-0.

35. Das, I. (2021) 'Serial and Parallel based Intrusion Detection System using Machine Learning', pp. 19–20.

36. Devan, P. and Khare, N. (2020) 'An efficient XGBoost – DNN-based classification model for network intrusion detection system', *Neural Computing and Applications*, 0123456789. Available at: https://doi.org/10.1007/s00521-020-04708-x.

37. Donkol, A.A.B.D.E. *et al.* (2023) 'Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks', *IEEE Access*, 11(February), pp. 9469–9482. Available at: https://doi.org/10.1109/ACCESS.2023.3240109.

38. Dwivedi, S., Vardhan, M. and Tripathi, S. (2020) 'An effect of chaos grasshopper optimization algorithm for protection of network infrastructure', 176(August 2019). Available at: https://doi.org/10.1016/j.comnet.2020.107251.

39. Dwivedi, S., Vardhan, M. and Tripathi, S. (2021) 'Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection', *Cluster Computing*, 24(3), pp. 1881–1900. Available at: https://doi.org/10.1007/s10586-020-03229-5.

40. Elhefnawy, R., Abounaser, H. and Badr, A.M.R. (2020) 'A Hybrid Nested Genetic-Fuzzy Algorithm Framework for Intrusion Detection and Attacks', 8. Available at:

https://doi.org/10.1109/ACCESS.2020.2996226.

41. Enigo, F. (2021) 'New Attacks Using Machine Learning', (June 2020). Available at: https://doi.org/10.1109/ICCES48766.2020.9137888.

42. Feng, W. *et al.* (2013) 'Mining Network Data for Intrusion Detection through Combining SVM with Ant Colony', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2013.06.027.

43. Foroushani, Z.A. and Li, Y. (2018) 'Intrusion detection system by using hybrid algorithm of data mining technique', *ACM International Conference Proceeding Series*, pp. 119–123. Available at: https://doi.org/10.1145/3185089.3185114.

44. Gadal, S.M.A.M. and Mokhtar, R.A. (2017) 'Anomaly detection approach using hybrid algorithm of data mining technique', *Proceedings - 2017 International Conference on Communication, Control, Computing and Electronics Engineering, ICCCCEE 2017* [Preprint]. Available at: https://doi.org/10.1109/ICCCCEE.2017.7867661.

45. Gao, P., Yue, M. and Wu, Z. (2021) 'A Novel Intrusion Detection Method Based on WOA Optimized Hybrid Kernel RVM', pp. 1063–1069.

46. Garg, A. and Maheshwari, P. (2016) 'A hybrid intrusion detection system: A review', *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016* [Preprint]. Available at: https://doi.org/10.1109/ISCO.2016.7726909.

47. Ghanem, W.A.H.M. *et al.* (2020) 'An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons'. Available at: https://doi.org/10.1109/ACCESS.2020.3009533.

48. Ghanem, W.A.H.M. and Jantan, A. (2019) *A new approach for intrusion detection system based on training multilayer perceptron by using enhanced Bat algorithm*, *Neural Computing and Applications*. Springer London. Available at: https://doi.org/10.1007/s00521-019-04655-2.

49. Ghazi, A. El (2020) 'Machine learning and datamining methods for hybrid IoT intrusion detection'.

50. Haghnegahdar, L. and Wang, Y. (2019) 'A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection', *Neural Computing and Applications*, 0123456789. Available at: https://doi.org/10.1007/s00521-019-04453-w.

51. Hajisalem, V. and Babaie, S. (2018) 'A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection', *Computer Networks*, 136, pp. 37–50. Available at: https://doi.org/10.1016/j.comnet.2018.02.028.

52. He, Haitao *et al.* (2019) 'A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection', *IEEE Access*, 7, pp. 183207–183221. Available at: https://doi.org/10.1109/ACCESS.2019.2959131.

53. Hedar, A.R. *et al.* (2015) 'Hybrid evolutionary algorithms for data classification in intrusion detection systems', *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2015 - Proceedings* [Preprint]. Available at: https://doi.org/10.1109/SNPD.2015.7176208.

54. Henry, A. *et al.* (2023) 'Composition of Hybrid Deep Learning Model and Feature Optimization for Intrusion Detection System'.

55. Hosseini, S. and Azizi, M. (2019) 'The Hybrid Technique for DDoS Detection with Supervised Learning Algorithms', *Computer Networks* [Preprint]. Available at: https://doi.org/10.1016/j.comnet.2019.04.027.

56. Hosseini, S., Mohammad, B. and Zade, H. (2020) 'New Hybrid Method for Attack Detection Using

Combination of Evolutionary Algorithms , SVM , and ANN', *Computer Networks*, p. 107168. Available at: https://doi.org/10.1016/j.comnet.2020.107168.

57. Jiang, J. and Lv, B. (no date) 'RST-RF : A Hybrid Model based on Rough Set Theory and Random Forest for Network Intrusion Detection', pp. 77–81.

58. Jiang, K. *et al.* (2020) 'Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network', *IEEE Access*, 8(3), pp. 32464–32476. Available at: https://doi.org/10.1109/ACCESS.2020.2973730.

59. Karthikeyan, S.V.P. (2019) 'Hybrid optimization scheme for intrusion detection using considerable feature selection', *Neural Computing and Applications*, 2. Available at: https://doi.org/10.1007/s00521-019-04477-2.

60. Kaur, S. and Singh, M. (2020) 'Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks', *Neural Computing and Applications*, 32(12), pp. 7859–7877. Available at: https://doi.org/10.1007/s00521-019-04187-9.

61. Kec, D. (2021) 'Feature selection using cloud-based parallel genetic algorithm for intrusion detection data classification', 5. Available at: https://doi.org/10.1007/s00521-021-05871-5.

62. Kevric, J., Jukic, S. and Subasi, A. (2016) 'An effective combining classifier approach using tree algorithms for network intrusion detection', *Neural Computing and Applications* [Preprint]. Available at: https://doi.org/10.1007/s00521-016-2418-1.

63. Khan, I.A., Pi, D. and Khan, Z.U. (2019) 'HML-IDS : A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems', *IEEE Access*, 7, pp. 89507–89521. Available at: https://doi.org/10.1109/ACCESS.2019.2925838.

64. Khan, M.A. (2021) 'HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system', *Processes*, 9(5). Available at: https://doi.org/10.3390/pr9050834.

65. Khan, M.A. and Karim, R. (2019) 'SS symmetry A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network'.

66. Khraisat, A. *et al.* (2019) 'Survey of intrusion detection systems: techniques, datasets and challenges', *Cybersecurity*, 2(1). Available at: https://doi.org/10.1186/s42400-019-0038-7.

67. Khraisat, A. *et al.* (2020) 'Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine', *Electronics (Switzerland)*, 9(1). Available at: https://doi.org/10.3390/electronics9010173.

68. Kim, G., Lee, S. and Kim, S. (2014) 'Expert Systems with Applications A novel hybrid intrusion detection method integrating anomaly detection with misuse detection', *Expert Systems With Applications*, 41(4), pp. 1690–1700. Available at: https://doi.org/10.1016/j.eswa.2013.08.066.

69. Kim, T. and Pak, W. (2021) 'Hybrid Classification for High-Speed and High-Accuracy Network Intrusion Detection System', *Hybrid intelligent systems for detecting network intrusions*, 9, pp. 83806–83817. Available at: https://doi.org/10.1109/ACCESS.2021.3087201.

70. Kumar, K.S.A. and Mohan, V.N. (2014) 'Adaptive Fuzzy Neural Network Model for intrusion detection', *Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014*, pp. 987–991. Available at: https://doi.org/10.1109/IC3I.2014.7019811.

71. Kumari, A. (2020) 'A Hybrid Intrusion Detection System Based on Decision Tree and Support Vector Machine', pp. 396–400.

72. Kumari, V. (2017) 'active learning SVM and fuzzy c-means clustering', pp. 481–485.

Lahasan, B. and Samma, H. (2022) 'Optimized Deep Autoencoder Model for Internet of Things Intruder Detection', 10.

73. Landress, A.D. (2016) 'A Hybrid Approach to Reducing the False Positive Rate in Unsupervised Machine Learning Intrusion Detection'.

74. Latah, M. and Toker, L. (2020) 'An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks', *CCF Transactions on Networking*, 3(3–4), pp. 261–271. Available at: https://doi.org/10.1007/s42045-020-00040-z.

75. Li, D. (2020) 'Improving Attack Detection Performance in NIDS Using GAN', pp. 817–825. Available at: https://doi.org/10.1109/COMPSAC48688.2020.0-162.

76. Li, K., Zhang, Y. and Wang, S. (2021) 'An Intrusion Detection System based on PSO-GWO Hybrid Optimized Support Vector Machine', *Proceedings of the International Joint Conference on Neural Networks*, 2021-July. Available at: https://doi.org/10.1109/IJCNN52387.2021.9534325.

77. Li, Y. *et al.* (2022) 'Research on Intrusion Detection Based on Neural Network Optimized by Genetic Algorithm', en, pp. 8–11.

78. Liu, C., Gu, Z. and Wang, J. (2021) 'A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning', *IEEE Access*, 9, pp. 75729–75740. Available at: https://doi.org/10.1109/ACCESS.2021.3082147.

79. Madani, P. and Vlajic, N. (2018) 'Robustness of deep autoencoder in intrusion detection under adversarial contamination', *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/3190619.3190637.

80. Maleh, Y. *et al.* (2015) 'A global hybrid intrusion detection system for Wireless Sensor Networks', *Procedia Computer Science*, 52(1), pp. 1047–1052. Available at: https://doi.org/10.1016/j.procs.2015.05.108.

81. Malik, A.J. and Khan, F.A. (2017) 'A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection', *Cluster Computing*, 21(1), pp. 667–680. Available at: https://doi.org/10.1007/s10586-017-0971-8.

82. Malik, J. *et al.* (2020) 'Hybrid Deep Learning : An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN', pp. 134695–134706. Available at: https://doi.org/10.1109/ACCESS.2020.3009849.

83. Maseno, E.M., Wang, Z. and Xing, H. (2022) 'A Systematic Review on Hybrid Intrusion Detection System', 2022.

84. Matel, E.C., Sison, A.M. and Medina, R.P. (2019) 'Optimization of Network Intrusion Detection System Using Genetic Algorithm with Improved Feature Selection Technique'.

85. Mazumder, M.R. *et al.* (no date) 'Network Intrusion Detection Using Hybrid Machine Learning Model'.

86. Megantara, A.A. and Ahmad, T. (2021) 'A hybrid machine learning method for increasing the performance of network intrusion detection systems', *Journal of Big Data*, 8(1). Available at: https://doi.org/10.1186/s40537-021-00531-w.

87. Mendjeli, C.A. (2017) 'A hybrid Deep Learning Strategy for an Anomaly Based N-IDS'.

88. Meng, F. *et al.* (2017) 'An effective network attack detection method based on kernel PCA and LSTM- RNN', *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*, pp. 568–572.

89. Mohd, N., Singh, A. and Bhadauria, H.S. (2021) 'Intrusion Detection System Based on Hybrid Hierarchical Classifiers', *Wireless Personal Communications* [Preprint], (0123456789). Available at: https://doi.org/10.1007/s11277-021-08655-1.

90. Mojtaba, S. *et al.* (2015) 'A New Intrusion Detection Approach using PSO based Multiple Criteria

Linear Programming', *Procedia - Procedia Computer Science*, 55(Itqm), pp. 231–237. Available at: https://doi.org/10.1016/j.procs.2015.07.040.

91. Network, I.N. (2016) 'Improving K-Means CLUSTERING Clustering Using IMPROVING K-MEANS USING Discretization TECHNIQUE Technique In Network DISCRETIZATION Intrusion DETECTION Detection System INTRUSION', pp. 248–252.

92. Nivaashini, M. and Thangaraj, P. (2018) 'A Framework of Novel Feature Set Extraction based Intrusion Detection System for Internet of Things using Hybrid Machine Learning Algorithms', *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, pp. 44–49.

93. Oluwaseun, R. *et al.* (2021) 'ScienceDirect ScienceDirect ScienceDirect An Enhanced Intrusion Detection System using Particle Swarm Optimization Extraction Technique Science 10th International Young Feature An Enhanced Intrusion Detection System using Particle Swarm An Enhanced Intrus', *Procedia Computer Science*, 193, pp. 504–512. Available at: https://doi.org/10.1016/j.procs.2021.10.052.

94. Om, H. (2012) 'A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System'.

95. Öney, M.U. and Peker, S. (2019) 'The Use of Artificial Neural Networks in Network Intrusion Detection: A Systematic Review', *2018 International Conference on Artificial Intelligence and Data Processing, IDAP 2018*, pp. 1–6. Available at: https://doi.org/10.1109/IDAP.2018.8620746.

96. Pakanzad, S.N. (2020) 'Providing a Hybrid Approach for Detecting Malicious Traffic on the Computer Networks Using Convolutional Neural Networks'.

97. Pattawaro, A. (2018) 'Anomaly-Based Network Intrusion Detection System through Feature Selection and Hybrid Machine Learning Technique', *2018 16th International Conference on ICT and Knowledge Engineering (ICT&KE)*, pp. 1–6. Available at: https://doi.org/10.1109/ICTKE.2018.8612331.

98. Pitre, P. (2022) 'An Intrusion Detection System for Zero-Day Attacks to Reduce False Positive Rates', pp. 1–6.

99. Pokharel, P. (2020) 'Intrusion Detection System based on Hybrid Classifier and User Profile Enhancement Techniques', pp. 137–144.

100. Polat, H. and Polat, O. (2020) 'Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models'.

101. Prabhakaran, V. and Kulandasamy, A. (2021) 'Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection', *Neural Computing and Applications*, 5. Available at: https://doi.org/10.1007/s00521-021-06085-5.

102. Pre-proof, J. (2019) 'Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic', *Computer Networks*, p. 107042. Available at: https://doi.org/10.1016/j.comnet.2019.107042.

103. Pu, G. *et al.* (2021) 'A Hybrid Unsupervised Clustering-Based Anomaly Detection Method', pp. 146–153.

104. Qaddoura, R. *et al.* (2021) 'A Multi-Layer Classification Approach for Intrusion Detection in IoT Networks Based on Deep Learning', pp. 1–21.

105. Qazanfari, K. (2017) 'A Novel Hybrid Anomaly Based Intrusion Detection Method', (November 2012). Available at: https://doi.org/10.1109/ISTEL.2012.6483122.

106. Rabbani, M. *et al.* (2020) 'A Hybrid Machine Learning Approach for Malicious Behaviour Detection and Recognition in Cloud Computing', *Journal of Network and Computer Applications*, p. 102507. Available at: https://doi.org/10.1016/j.jnca.2019.102507.

107. Rahmani, R. *et al.* (2015) 'A hybrid method consisting of GA and SVM for intrusion detection system A hybrid method consisting of GA and SVM for intrusion detection system', *Neural Computing and Applications* [Preprint], (August). Available at: https://doi.org/10.1007/s00521-015-1964-2.

108. Raja, S. and Ramaiah, S. (2017) 'An Efficient Fuzzy-Based Hybrid System to Cloud Intrusion Detection', *International Journal of Fuzzy Systems*, 19(1), pp. 62–77. Available at: https://doi.org/10.1007/s40815-016-0147-3.

109. Ravale, P.U., Marathe, P.N. and Padiya, P.P. (2015) 'Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function', *Procedia - Procedia Computer Science*, 45, pp. 428–435. Available at: https://doi.org/10.1016/j.procs.2015.03.174.

110. Razib, M.A.L. *et al.* (2022) 'Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework', *IEEE Access*, 10, pp. 53015–53026. Available at: https://doi.org/10.1109/ACCESS.2022.3172304.

111. Sadiq, A.L.I.S. *et al.* (2018) 'An Efficient IDS Using Hybrid Magnetic Swarm Optimization in WANETs', *IEEE Access*, 6, pp. 29041–29053. Available at: https://doi.org/10.1109/ACCESS.2018.2835166.

112. Sagar, S., Shrivastava, A. and Gupta, C. (2018) 'Feature Reduction and Selection Based Optimization for Hybrid Intrusion Detection System Using PGO followed by SVM', *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*, pp. 1–7.

113. Saleh, A.I., Talaat, F.M. and Labib, L.M. (2019) 'A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers', *Artificial Intelligence Review*, 51(3), pp. 403–443. Available at: https://doi.org/10.1007/s10462-017-9567-1.

114. Saleh, M. *et al.* (2022) 'Towards SDN-Enabled , Intelligent Intrusion Detection System for Internet of Things (IoT)', 10.

115. Sayed, A. *et al.* (2013) 'Multi-layer hybrid machine learning techniques for anomalies detection and classification approach Vj and a P (at I vJ) - n + m 2013 13th International Conference on Hybrid Intelligent Systems (HIS)', pp. 215–220.

116. Seo, W. and Pak, W. (2021) 'Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning', 9. Available at: https://doi.org/10.1109/ACCESS.2021.3066620.

117. Sharma, A. and Tyagi, U. (2021) 'A Hybrid Approach of ANN-GWO Technique for Intrusion Detection', pp. 1–6.

118. Sheikhan, M. and Sharifi, M. (2012) 'Gravitational search algorithm – optimized neural misuse detector with selected features by fuzzy grids – based association rules mining'. Available at: https://doi.org/10.1007/s00521-012-1204-y.

119. Shizhao, W. and Tianbo, W. (2019) 'A Novel Intrusion Detector Based on Deep Learning Hybrid Methods', pp. 300–305. Available at: https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00062.

120. Shona, D. and Kumar, M.S. (2019) 'Efficient IDs for MANET Using Hybrid Firefly with a Genetic Algorithm', *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, (November), pp. 191–194. Available at: https://doi.org/10.1109/ICIRCA.2018.8597268.

121. Shukla, A.K. (2020) 'Detection of anomaly intrusion utilizing self-adaptive grasshopper optimization algorithm', *Neural Computing and Applications*, 7. Available at: https://doi.org/10.1007/s00521-020-05500-7.

122. Shukla, P. (2017) 'ML-IDS : A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things', (September).

123. Singh, A., Chatterjee, K. and Satapathy, S.C. (2021) 'An edge based hybrid intrusion detection framework for mobile edge computing', *Complex & Intelligent Systems* [Preprint]. Available at: https://doi.org/10.1007/s40747-021-00498-4.

124. Singh, P. and Venkatesan, M. (2018) 'Hybrid Approach for Intrusion Detection System', *Proceedings of the 2018 International Conference on Current Trends towards Converging Technologies, ICCTCT 2018*, pp. 1–5. Available at: https://doi.org/10.1109/ICCTCT.2018.8551181.

125. Singhal, A. *et al.* (2021) 'A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection', pp. 312–318.

126. Soheily-Khah, S., Marteau, P.F. and Bechet, N. (2018) 'Intrusion detection in network systems through hybrid supervised and unsupervised machine learning process: A case study on the iscx dataset', *Proceedings - 2018 1st International Conference on Data Intelligence and Security, ICDIS 2018*, pp. 219–226. Available at: https://doi.org/10.1109/ICDIS.2018.00043.

127. Souza, C.A. *et al.* (2020) 'Hybrid approach to intrusion detection in fog-based IoT environments', (July), pp. 1–6. Available at: https://doi.org/10.1016/j.comnet.2020.107417.

128. Srikrishnan, A., Raaza, A. and Gopalakrishnan, S. (no date) 'Machine Learning Based Intrusion Detection Systems Using HGWCSO And ETSVM Techniques'.

129. Subba, B., Biswas, S. and Karmakar, S. (2017) 'Enhancing effectiveness of intrusion detection systems: A hybrid approach', *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016* [Preprint]. Available at: https://doi.org/10.1109/ANTS.2016.7947777.

130. Taher, K.A. (2019) 'Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection'.

131. Tama, B.A., Comuzzi, M. and Rhee, K.H. (2019) 'TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System', *IEEE Access*, 7, pp. 94497–94507. Available at: https://doi.org/10.1109/ACCESS.2019.2928048.

132. Tang, Y. and Li, C. (2021) 'An Online Network Intrusion Detection Model Based on Improved Regularized Extreme Learning Machine', *IEEE Access*, PP, p. 1. Available at: https://doi.org/10.1109/ACCESS.2021.3093313.

133. Tekeo, A. (2019) 'Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments', pp. 84–89.

134. Thanigaivelan, N.K., Virtanen, S. and Isoaho, J. (2018) 'Hybrid Internal Anomaly Detection System for IoT : Reactive Nodes with Cross-Layer Operation', 2018.

135. Thaseen, S. and Kumar, A. (2017) 'Intrusion detection model using fusion of chi-square feature selection and multi class SVM', pp. 462–472.

136. Ullah, I., Mahmoud, Q.H. and Member, S. (2022) 'Design and Development of RNN-based Anomaly Detection Model for IoT Networks', *IEEE Access*, PP, p. 1. Available at: https://doi.org/10.1109/ACCESS.2022.3176317.

137. Umarani, C. and Kannan, S. (2020) 'Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network', *Peer-to-Peer Networking and Applications*, 13(3), pp. 752–761. Available at: https://doi.org/10.1007/s12083-019-00781-9.

138.Varuna, S. (2015) 'An Integration of K-Means Clustering and Naïve Bayes Classifier for Intrusion Detection'.

139. Velliangiri, S. and Pandey, H.M. (2020) 'Jou rna lP', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2020.03.049.

140. Vidyapeetham, A.V. (2013) 'A hybrid method based on Genetic Algorithm , Self-Organised Feature Map, and Support Vector Machine for better Network Anomaly Detection'.

141. Vu, L. *et al.* (2022) 'Deep Generative Learning Models for Cloud Intrusion Detection Systems', pp. 1–13.

142. Walkinshaw, N., Taylor, R. and Derrick, J. (2016) *Inferring extended finite state machine models from software executions*, *Empirical Software Engineering*. Available at: https://doi.org/10.1007/s10664-015-9367-7.

143. Wang, W. *et al.* (2020) 'Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine', pp. 1–14. Available at: https://doi.org/10.1109/TCC.2020.3001017.

144. Wankhade, A. (2016) 'Distributed-Intrusion Detection System using combination of Ant Colony Optimization (ACO) and Support Vector Machine (SVM)', pp. 0–5. Available at: https://doi.org/10.1109/ICMETE.2016.94.

145. Wisanwanichthan, T. and Thammawichai, M. (2021) 'SVMA Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and', *IEEE Access*, 9, pp. 138432–138450. Available at: https://doi.org/10.1109/ACCESS.2021.3118573.

146. Xu, A. *et al.* (2020) 'A Hybrid Deep Learning Model for Malicious Behavior Detection', pp. 55–59. Available at: https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00021.

147. Yang, L., Moubayed, A. and Shami, A. (2021) 'MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles', *IEEE Internet of Things Journal*, XX(XX), pp. 1–17. Available at: https://doi.org/10.1109/JIOT.2021.3084796.

148. Zhang, C. *et al.* (2021) 'A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques', 2021.

149. Zhang, H. *et al.* (2019) 'Using Machine Learning techniques to improve Intrusion Detection Accuracy', pp. 308–310.

150. Zhang, H. *et al.* (2020) 'A Real-Time and Ubiquitous Network Attack Detection Based on Deep Belief Network and Support Vector Machine', 7(3), pp. 790–799.

151. Zhang, L. *et al.* (2022) 'A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks', 10. Available at: https://doi.org/10.1109/ACCESS.2022.3145007.

152. Zhang, X. (2019) 'An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic', pp. 456–460.

153. Zhang, Z. (no date) 'XGBoosted Misuse Detection in LAN-Internal Traffic Dataset'.

154. Zhou, P., Zhang, H. and Liang, W. (2023) 'Research on hybrid intrusion detection based on improved Harris Hawk optimization algorithm'. Available at: https://doi.org/10.1080/09540091.2023.2195595.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 36 – 51 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ENHANCING AUTOENCODER PERFORMANCE FOR INTRUSION DETECTION SYSTEMS VIA OPTIMAL BOTTLENECK SIZE OPTIMIZATION IN A TWO HIDDEN LAYER ARCHITECTURE

Seiba Alhassan[1,2], Gaddafi Abdul-Salaam*[1], Yaw Missah[1]

[1]Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
[2]Dr Hilla Limann Technical University

ABSTRACT. Sensitive data processed, stored, and transmitted on a computer requires a mechanism to protect it from unauthorized access. Several techniques have been proposed, including Intrusion Detection Systems (IDS), to protect computer networks from attacks. Autoencoders, a deep learning technique, have been explored by several researchers aiming to improve the performance of existing IDS. Despite the significant improvements seen with the use of autoencoders, the issues of low detection accuracy and high false alarm rates continue to be major problem. The architecture of a deep autoencoder, including the number of layers, neurons, and the bottleneck, affects its performance. This study is conducted to determine the optimal bottleneck size based on the architecture of a two-layer autoencoder. The study utilizes the benchmark dataset NSL-KDD to train, test, and validate the model. The experimental results from our proposed system reveal that the optimal bottleneck size for an autoencoder is obtained by setting it to 60% of the size of the previous hidden layer.

KEYWORDS. Autoencoder, IDS, encoder, decoder, bottleneck

INTRODUCTION

The benefits of computer networks have attracted various organizations, including healthcare, banks, educational institutions, security services, industry, transportation, hospitality, and individuals, to store sensitive information online. However, the increasing rate and sophistication of attacks on these networks pose a significant danger. Cybersecurity experts and academia have made considerable efforts to enhance cybersecurity. Although progress has been made, addressing the rising threat levels requires further attention. One extensively researched security technique is Intrusion Detection Systems (IDS). IDS, by their nature, facilitate early detection, enabling prompt actions to mitigate attack severity. According (Xu et al. 2021), IDS's ultimate goal is to classify network traffic as normal or malicious. These systems are built using machine learning and deep learning techniques and can be categorized as anomaly-based or signature-based IDS.

Signature-based IDS maintains a database of known attacks, comparing incoming network traffic against this database. Anomaly-based IDS, conversely, establishes a normal profile and flags incoming traffic deviating from this profile as an attack. Both approaches have strengths and weaknesses. For instance, anomaly-based systems are prone to high false alarms but can detect novel attacks. Signature-based IDS struggle to identify new attacks and require frequent database updates, making them computationally expensive, but they have lower false alarm rates.

Another classification criterion for IDS is their implementation location. Network Intrusion Detection Systems operate at the network level, monitoring data packets and classifying them as normal or malicious. Host-based IDS involves installing software on individual systems for tracking purposes.

While various researchers have achieved substantial success with IDS techniques, the accuracy of intrusion detection remains a significant research challenge. (Alam and Ahmed 2023; Logeswari, Bose, and Anitha 2023; Kasongo 2023; Shukla and Kumar 2023; Ramasamy and Eric 2023; Pranto et al.

2022; Makarand 2022; Hendi, Verawati, and Hardi 2022; Das 2022; Li et al. 2022; Garg, Kumar, and Shyamasundar n.d.) have employed machine learning algorithms for IDS implementation, reporting impressive results. However, machine learning has limitations, as confirmed by (Shone et al. 2018), who emphasized the need for human expert interaction. To address this limitation, researchers are turning to deep learning techniques, such as Autoencoders, which have shown promise in IDS research. Several researchers (Schmidt 2020; Y. Song, Hyun, and Cheong 2021; Haripriya and Jagadeesh 2022; Sabir, Ahmad, and Alghazzawi 2023; Almaiah et al. 2022; Shahid et al. 2019; Siddique et al. 2019; Wang et al. 2022; Yu, Long, and Cai 2017; Zhang, Yu, and Li 2018)have recently explored Autoencoders and reported impressive performance.

Autoencoders, as a deep learning technique, consist of three main components: the input, which comprises the dataset; the encoder, which transforms high-dimensional data into a lower-dimensional space; and the decoder, which converts the lower-dimensional space back to the output. The output is exists. Figure 1 illustrates a standard autoencoder with two hidden layers.

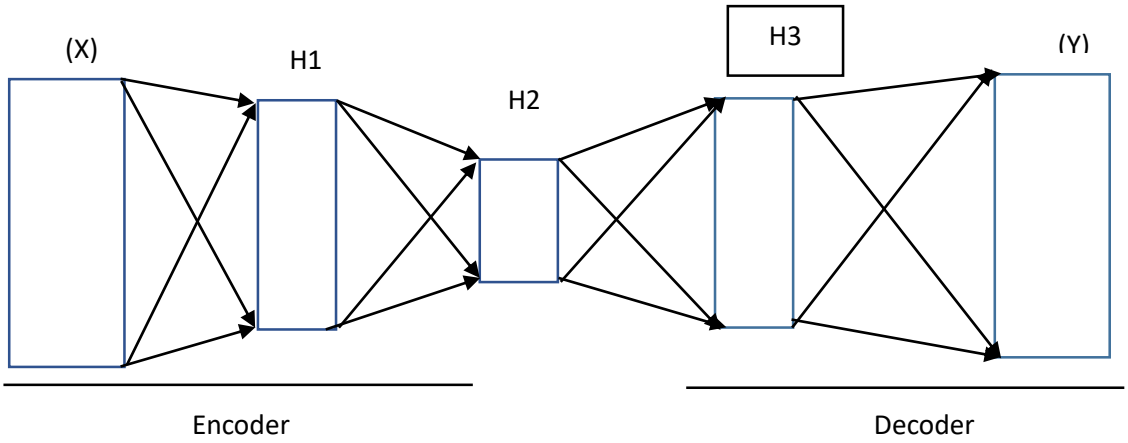


Figure 1: Autoencoder Architecture

Figure 1 illustrates that, when given an input of size X which is compressed into a lower dimension of size H2 (where X > H2), the bottleneck is then converted to Y, which is approximately the size of X. In anomaly detection systems like IDS, the autoencoder is typically fed with normal data, and a threshold value is established. Subsequently, when the model is fed input containing both attacks and normal data, any deviation from the threshold value is considered an abnormality or an attack. This property makes autoencoders suitable for detecting zero-day attacks. However, the full potential of autoencoders is not fully realized due to the lack of a generally accepted standard architecture for the latent space or bottleneck, resulting in lower detection accuracy.

(Y. Song, Hyun, and Cheong 2021) conducted a study aimed at analyzing the impact of the dimension of the latent space on the model's performance. However, their study did not identify the optimal latent size that would lead to higher model performance. This absence of a suggested optimal latent size often results in a trial-and-error approach, which is time-consuming and delays the practical implementation of deep autoencoders.

The contributions of this study include:

1. Designing and implementing various latent space sizes for a two-hidden-layer autoencoder.
2. Suggesting an optimal latent space size to expedite the practical implementation of autoencoders for IDS.

The rest of this work is divided into four main sections. Section 2 reviews related literature. Section 3 outlines the methodology used to implement the proposed system. Section 4 covers the results and discussion. The final section presents the conclusion.

2.0 Literature Review

(Mirsky et al. 2018) conducted a study introducing Kitsune, a neural network-based Network Intrusion Detection System (NIDS) designed for efficiency and plug-and-play deployment. Kitsune achieves this through efficient tracking of network behavior across channels and utilizes an ensemble of autoencoders known as KitNET for anomaly detection. The study focuses on the online machine learning process of the framework and evaluates its performance in terms of detection accuracy and runtime efficiency.

The authors highlight that KitNET, an online algorithm, exhibits competitive performance comparable to batch or offline algorithms and, in some cases, outperforms them. Notably, the algorithm's efficiency is demonstrated by its ability to operate on a single core of a Raspberry Pi device, with potential for even stronger CPUs.

(T. Song et al. 2019)presented a study that introduces the LSE-VAE (Latent Space Encoding Variational Autoencoder) model as an innovative approach to sentence generation. By incorporating distinct prior latent distributions tailored to different sentences and structuring the latent space based on sentence similarity, the model effectively captures a substantial and informative latent representation. The research evaluates the LSE-VAE's performance through a combination of automated metrics and empirical analysis.

In comparison to the conventional Variational Autoencoder (VAE), the LSE-VAE exhibits superior reconstruction capabilities, generating sentences of higher quality and greater diversity. Notably, the latent space learned by the LSE-VAE maintains the desirable attributes of continuity and smoothness observed in VAE-based latent spaces while further excelling at distinguishing sentences with varying degrees of similarity. An intriguing aspect of the LSE-VAE model is its enhanced ease of training, requiring fewer complex engineering strategies such as KL cost annealing. The determination of hyperparameters is streamlined through analytical derivation, taking into account factors such as latent variable dimensions and modeling requirements. This analytical approach contributes to the model's practicality and ease of implementation.

In connection to the previous literature review, where Kitsune was introduced as a neural network-based NIDS, both studies contribute to advancing their respective fields through innovative modeling approaches. Just as Kitsune enhances intrusion detection through efficient autoencoder ensembles, the LSE-VAE model elevates sentence generation with a specialized latent space arrangement. The intersection of neural network methodologies across diverse domains underscores the versatility and impact of deep learning techniques in addressing complex challenges.

(Sindian and Sindian 2020) also presented a study introducing a novel approach called the Deep Sparse Autoencoder-based Approach with two hidden layers (EDSA) for feature extraction and DDoS attack detection. The core objective of this research is to leverage autoencoders to extract representative features from the CICDDoS2019 dataset, subsequently minimizing classification errors and enhancing the accuracy of DDoS attack detection.

The empirical analysis conducted on the proposed EDSA technique demonstrates its remarkable performance in terms of detection accuracy. A significant improvement is observed when compared to other network models across various performance indicators, including accuracy, detection rate, precision, and specificity. Notably, the false positive rate is considerably reduced, underscoring the effectiveness of the EDSA method. For the CICDDoS2019 dataset, the proposed technique achieves an impressive 98 percent detection accuracy and a minimal 1.4 percent false positive rate. Their

study's findings suggest the potential for further enhancements and exploration. The authors propose the incorporation of recent computer algorithms like K-means clustering, potentially introducing additional layers within the Sparse Autoencoder (SAE) structure to further reduce feature dimensions. Furthermore, the study envisions the application of alternative classification algorithms beyond the scope of the current research.

In (Sindian and Sindian 2020), a study is proposed autoencoders as a powerful tool for capturing underlying factors in various types of datasets. Autoencoders' latent representations have been extensively studied in the context of facilitating interpolation between data points by decoding convex combinations of latent vectors. However, this interpolation process often results in artifacts or unrealistic outcomes during the reconstruction phase. The authors contend that these discrepancies arise from the structure of the latent space and the inherent deviation of naively interpolated latent vectors from the actual data manifold.

In response to these challenges, the paper introduces an innovative regularization technique aimed at reshaping the latent representation. This regularization strategy strives to align the latent manifold with the training images, ensuring consistency and fidelity. Moreover, the technique promotes smoothness and local convexity within the manifold, addressing the issues associated with interpolation artifacts and unrealistic outcomes.

The proposed regularization technique not only facilitates accurate interpolation between data points, as evidenced in the study, but also serves as a versatile approach to combat overfitting. Furthermore, it offers the potential to generate new samples for data augmentation, showcasing its broader applicability in enhancing dataset diversity and model generalization.

This research contributes to the field of autoencoders by addressing a critical concern in latent space interpolation. By refining the latent manifold's structure, their study presents a robust solution that advances the quality and realism of interpolation results. Additionally, the regularization technique's versatility in preventing overfitting and generating augmented data underscores its practicality and significance in diverse machine learning applications.

(Xu et al. 2021) introduced a study that presents a novel 5-layer autoencoder (AE)-based model designed to enhance the detection of anomalous network traffic. The development of this model is informed by a thorough and meticulous examination of key performance indicators and their impact on detection accuracy within an AE framework. Through a rigorous evaluation, the authors establish that the proposed 5-layer architecture, combined with an innovative data pre-processing methodology and specific loss metrics, yields optimal results in terms of accuracy and detection precision.

Central to the success of the proposed model is the use of Mean Absolute Error (MAE) as the basis for the reconstruction loss function. The authors highlight how this choice of loss metric contributes to improved accuracy in network anomaly detection.

The optimized 5-layer architecture, with carefully determined numbers of neurons in hidden and latent layers, outperforms alternative model architectures. The evaluation is conducted on the NSL-KDD dataset, where the proposed model achieves impressive performance metrics, including accuracy, precision, recall, and F1-score.

Their study acknowledges the adaptability of the model beyond the specific dataset used for training. While currently focused on NSL-KDD, the proposed model demonstrates an ability to recognize abnormal network traffic patterns effectively. Future plans include testing the model's generalizability across different intrusion attack samples and datasets from diverse applications, such as Android-based malware and medical annotations. The authors also express a commitment

to expanding their work to encompass multi-class classification and assessing the model's performance in real-world operational network environments.

(Y. Song, Hyun, and Cheong 2021) explored the domain of intelligent Network Intrusion Detection Systems (NIDS) and their application of deep learning techniques to counteract the evolving landscape of network attacks. The focus is on leveraging autoencoders as a means to effectively identify new attack patterns and mitigate the challenges posed by the labor-intensive labeling of data. While autoencoders prove adept at detecting unknown attack types, the process of fine-tuning model architecture and hyperparameters to achieve optimal detection performance can be a resource-intensive endeavor, potentially hindering the practical implementation of autoencoder-based NIDS.

To address this challenge, the study takes a rigorous approach by investigating autoencoders using established benchmark datasets, including NSL-KDD, IoTID20, and N-BaIoT. The research systematically explores multiple combinations of model structures and latent sizes within a simple autoencoder framework. Through this thorough evaluation, the article sheds light on the critical role that the latent size of an autoencoder model plays in influencing the performance of an Intrusion Detection System (IDS).

(Xu et al. 2021)delves into the challenges posed by the emerging paradigm of the Internet of Things (IoT), which, while offering numerous benefits, is susceptible to cyberattacks due to its resource-constrained and heterogeneous nature. Successful network intrusions in IoT networks can have far-reaching consequences, compromising valuable consumer and industry information. To counteract these security challenges, the article introduces a novel approach: a lightweight deep autoencoder (DAE)-based cyberattack detection framework.

The efficacy of the proposed framework is substantiated through evaluation using two standard and open-source datasets: NSL-KDD and UNSW-NB15. In both binary class and multi-class scenarios, the proposed DAE achieves impressive accuracies, attaining 98.86% and 98.26% for NSL-KDD, as well as 99.32% and 98.79% for the UNSW-NB15 dataset.

To establish the robustness of the approach, the article compares the performance of the proposed attack detection framework with several state-of-the-art intrusion detection schemes. The experimental results underscore the promising nature of the proposed scheme in effectively detecting cyberattacks within IoT networks.

The concept of latent space and architecture serves as a fundamental thread connecting the reviewed articles. Latent space refers to a compressed and abstract representation of data that captures underlying patterns and features. Architecture, on the other hand, refers to the design and structure of neural networks used to model and manipulate data.

Both (Y. Song, Hyun, and Cheong 2021; Xu et al. 2021) underscore the importance of optimizing neural network architectures to achieve desired outcomes. (Y. Song, Hyun, and Cheong 2021)focus on autoencoder-based NIDS, emphasizing the need for careful architecture design to achieve optimal intrusion detection performance. Similarly, (Xu et al. 2021) meticulously explore various architectural configurations to develop an effective model for detecting anomalous network traffic. In both cases, the architecture's structure and design choices influence the characteristics of the latent space, which, in turn, impacts the model's performance.

In summary, latent space and architecture are central concepts that interplay across the reviewed articles. Whether in the context of anomaly detection, sentence generation, model optimization, or regularization, the design choices made in constructing neural network architectures directly impact the nature and quality of the latent space representation, ultimately influencing the effectiveness and performance of the models in their respective domains.

The perspectives of these authors suggest that much more attention needs to be paid to the issue of latent space to achieve optimal performance of IDS. In view of this, the next section of this study will clearly outline the processes, procedures, and tools necessary to implement a study aimed at obtaining an optimal latent space that will consistently guarantee impressive performance of an autoencoder. These findings will help improve the detection accuracy of current and existing IDS.

3.0 Methodology

3. 1 Autoencoder

The model designed for this study is the autoencoder for Network Intrusion Detection. The autoencoder is a deep learning algorithm that takes input data (X) and compresses it to a lower dimension known as the bottleneck (B) in a process known as encoding. The bottleneck is then used to reconstruct the output (Y) in a process known as decoding.

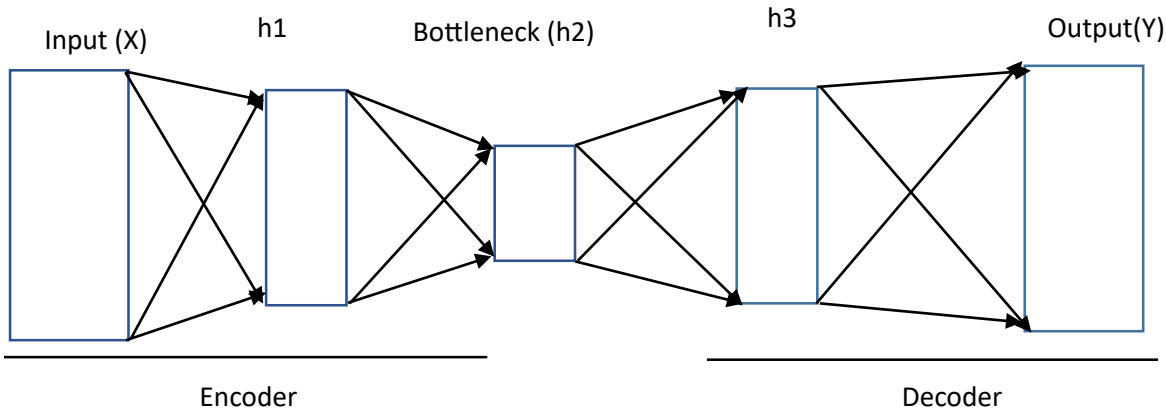


Figure 2: Autoencoder model

X: Input (input features)

Y: Reconstructed output data

h2: bottleneck

f: activation function for the encoder

g: activation function for the decoder

The autoencoder goal is to learn a mapping X to Y such that the reconstructed output Y is as close as possible to the input data X. The architecture consists of an encoder and a decoder

i. Encoder

The encoder function takes the input X and maps it to hidden representation h2 via two hidden layers:

$h1 = f(W1.X+b1)$ ……... (1)

$h2 = f(W2.X+b2)$ …… (2)

Where:

W1 represent the weight of the first hidden layer

b1 represent the bias of the first hidden layer

W2 represent the weight of the Second hidden layer

B2 represent the weight of the second hidden layer

The decoder function maps the bottleneck h2 to the reconstructed output Y

Via two hidden layers:

$H3 = f(W2.h2 + b2)$ ……..... (3)

$Y = g(W2.\ h3 + b2)$ …….....(4)

Where:

W2: Weights of the first hidden layer of the decoder

B2: bias of the first hidden layer of the decoder

W2: Weights of the second hidden layer of the decoder

B2: bias of the second hidden layer of the decoder

Loss Function

This study made use of the mean square error (MSE to measure the difference between the input X and the reconstructed output Y and this is represented mathematically as

$MSE\ (X, Y) = \frac{1}{n}\sum_{i=1}^{n}(X_i\text{-}Y_i)$ …… (5)

3.1: Our propose System

The primary objective of this study is to investigate how the architecture of an autoencoder influences the performance of an Intrusion Detection System (IDS). Specifically, the study focuses on determining the optimal bottleneck size that leads to improved IDS accuracy. The study employs a two-hidden-layer autoencoder for its investigation. The research plan involves conducting two experimental setups to achieve this goal.

In the first experimental setup, a constant number of 50 neurons is maintained in the first hidden layer, while the last hidden layer (bottleneck) is varied. The values considered for the bottleneck size include 40, 30, 20, and 10. The outcomes of this setup will provide insights into the impact of varying bottleneck sizes on IDS accuracy and guide the subsequent steps in the investigation.

It is worth noting that this study introduces a unique approach distinct from prior research on the same topic. Previous studies have explored whether the bottleneck size influences model performance but have not delved deeper to ascertain the optimal bottleneck size for achieving superior model performance. For instance, a study by Song, Hyun, and Cheong (2021) conducted a similar investigation but primarily focused on assessing the effect of the bottleneck size on model performance.

In summary, this study aims to contribute to the existing body of knowledge by not only examining the influence of bottleneck size on IDS model performance but also determining the precise bottleneck size that leads to optimal performance. This refined approach will provide valuable insights into designing more effective autoencoder architectures for intrusion detection.

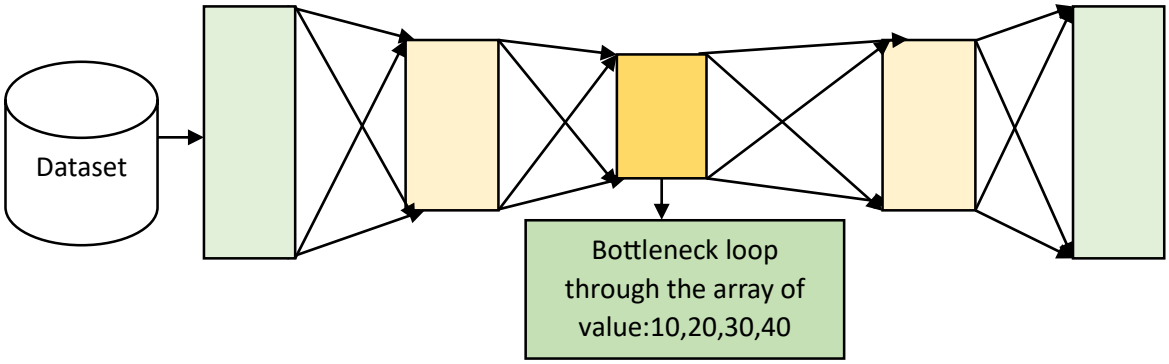


Figure 3: Preliminary setup to obtain optimal bottleneck value

In the Figure 3 above, the detection accuracy is recorded for each value in the array, and the value that yields the highest accuracy is chosen. This selected value is subsequently utilized as a seed value to conduct the next experimental setup, aiming to determine the suggested optimal bottleneck value for a two-hidden-layer autoencoder designed for Network Intrusion Detection. The next setup involves obtaining three values, represented as X ± 5, as illustrated in the Figure below.

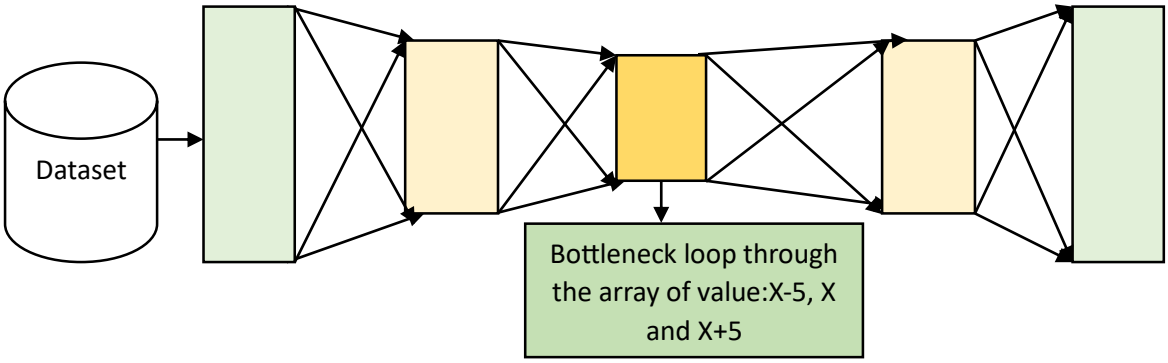


Figure 4: Setup to obtain optimal bottleneck value

The first component for our proposed system is the dataset. These datasets are used for training and testing the proposed system. The datasets include the CIC-IDS2017, and NSL-KDD. The sections below take a detail look at each of them.

3.3 Datasets

3.3.1 NSL-KDD dataset

The NSL-KDD dataset is a well-known IDS dataset that is extensively employed by numerous researchers to validate their models. Its frequent utilization simplifies the process of comparing research outcomes with those of prior studies. According to (Tavallaee et al., 2009), NSL-KDD was developed to address the inherent issues associated with the KDDCup99 dataset. NSL-KDD remains relevant in contemporary research due to its capacity to yield consistent results, facilitating effective comparisons with other studies. This advantage stems from the dataset's balanced distribution of training and testing records, allowing for the entire dataset to be used without necessitating the selection of a randomly chosen subset. NSL-KDD encompasses four attack classes and a normal class. The instance counts per

class are presented in Table 1, while Table 2 provides an overview of the attack types and categories present within the NSL-KDD dataset.

Table 1:Classes and number of instances in NSL-KDD dataset

S/N	CLASS	NO OF INSTANCE
1	R2L	52(0.04%)
2	U2R	995(0.78%)
3	probe	11656(9.25%)
4	DoS	45927(36.47%)
5	Normal	67343(53.46%)

Table 2: Types and categories of attacks in NSL-KDD dataset

TYPE OF ATTACK	CATEGORIES OF ATTACK
Probe	N map, Portsweep, Satan, saint(6), Mscan
DoS	Worm (10), Back, Land Neptune, Process table, Udpstorm,Pod, Teardrop, Smurf, Apache 2.
U2R	Load Module,Perl, Sql attack, Buffer_overflow, Rotkit,Xterm ,Ps(7)
R2L	Spy, Xlock,Guess_Password, Ftp_write, Httptunnnel, Named(16), Pht, Multihop, Ftp_write, Send fmail, Name(16), Xsnoop, Waremaster, Snmp guesss, Snmp getattack

3.4 Data preprocessing

3.4.1 One hot encoding

The proposed systems AE-LSTM cannot directly process NSL-KDD, dataset in its original form. The one-hot- encoding is used to transform the non-numeric features into numeric feature for the AE to process it. NSL-KDD dataset has 38 numeric features and three non-numeric features. The nonnumeric feature such “protocol-type”, “flag” and “service” need to be converted into numeric format.

i. The first non-numeric feature to be converted into numeric feature is the protocol-type. The protocol type has three main attributes namely the ‘TCP’,’UDP’ and ‘ICMP’ which are encoded as follows as shown in Table 3.

Table 3: converting non-numeric features to numeric features

Protocol-type	TCP	UDP	ICMP
encoded	1,0,0	0,1,0	0,0,1

Next, the “flag” and “service features” are converted into numeric features. The service feature has seventy (70) different attributes and so by using the same method in the step (i) above each attribute of service feature is mapped to 70 distinct binary attributes. Similarly, the flag feature also has 11 different attributes and is also converted into numeric features by mapping it to 11 distinct binary attributes. As result of this transformation, the 41 features of NSL-KDD dataset are transformed into 112 distinct features.

3.4.2 Normalization

The datasets are first normalized to enhance the performance and reliability of our model by converting all numeric columns to a common scale. The equation three (3) below shows how the min-max technique is used to perform the normalization task.

y = x-min/max-min……..…(6)

Were

y = new value of each entry

Min = minimum value for each data points

Max = maximum value for each data points

A similar process is also used to prepare the CIC-IDS2017 dataset for the autoencoder learning algorithm.

3.4.5 Data Splitting

The data that has been transformed is then split into the ratio 75:25 for training and testing respectively.

3. 5 Metrics of evaluation

Intrusion detection systems performance is evaluated based on a number of metrics including the accuracy, precision, F1-score and Recall. The others are:

True positive: correctly classified attacks in a data sample

True Negative: Normal traffic in a data sample that has been correctly classified as Normal

False positive: Normal traffic in data sample wrongly classified as an attack

False negative: Malicious traffic in a data sample that has been wrongly classified as Normal

The metrics are calculated as follows:

Accuracy measures: the total number of data samples correctly classified as true positive or true negative. Higher accuracy for the balanced dataset is an indication of good performance. The Equation 7 below shows how accuracy is calculated.

Accuracy (ACC) = $\frac{TP+TN}{TP+TN+FP+FN}$ …… (7)

Recall which is also called true positive rate is the proportion of correctly predicted positive instances of a class to the overall instance of the same class. A higher recall rate that ranges from 0 to 1 indicates a better model performance. The Equation 8 below shows how the Recall is calculated

Recall = $\frac{TP}{TP+FN}$ …… (8)

Precision is the ratio of positive instances that are correctly predicted to the ratio of all predicted samples for a class. Recall and Precision are always paired when evaluating model performance. The Equation 9 below shows how the precision is calculated

Precision = $\frac{TP}{TP+FP}$ …… (9)

F1-score is computed by taking the harmonic mean of precision and recall. F1-score normally calculates the tradeoff between precision and recall. F1-score is calculated as shown in equation 8 below

$$\textbf{F1-score} = 2 * \frac{Precision * Recall}{Precision + Recall} \quad \text{..... (10)}$$

3.6 Experimental setup

The experimental results were obtained using the following specifications to construct the model in Python on the Google Colab platform, utilizing a CPU processor. The number of epochs was set to 100, and the batch size was set to 500. For the activation function, the ReLU activation was employed for both the encoding function and the hidden layers of the decoding function. Subsequently, the softmax function was utilized as the output function.

The experimental setups were executed with a two-hidden-layer architecture, where the first layer was kept at a constant size of 50 units. In each setup, the latent space was varied using array elements 10, 20, 30, and 40, maintaining the ratio 50:10, 50:20, 50:30, and 50:40, respectively. A distinct model was built for each configuration, and the corresponding results were recorded. Notably, to ensure consistent results, each setup was executed only once, thereby preventing interference from previous runs.

The primary objective of these experiments was to determine the optimal latent space size that leads to the highest accuracy for intrusion detection. This optimal latent space size, denoted as X, was identified. To further refine the architecture, latent space sizes of X-5, X, and X+5 were generated. These new configurations were then explored to derive the most optimal bottleneck size, aiming to enhance the performance of the intrusion detection system using a deep autoencoder.

This investigation targeted two benchmark datasets, namely NSL_KDD and CIC-IDS2017. By varying the latent space size and analyzing the resulting accuracy, the goal was to pinpoint the most suitable position within the array of elements. This "best" latent space size, represented by X, served as a foundation for subsequent analyses to fine-tune the architecture for improved intrusion detection capabilities.

4.0 Results and discussion

4.1 Preliminary Results and Latent Space Correlation:

The preliminary experimental results (Table 4 and Table 5) provide an initial glimpse into the impact of different latent space sizes on intrusion detection system performance. Notably, latent space size 30 consistently emerges as a high-performing configuration across both the NSL-KDD and CID-IDS2017 datasets. This observation is intriguing, as it aligns with the previously proposed hypothesis: the optimal latent space size should be around 60% of the preceding hidden layer's size. This alignment hints at the potential validity of this latent space correlation. Figure 5 and Figure 6 below show the pictorial view of the results from the preliminary study.

Table 4: Result of Preliminary experimental for NSL-KDD dataset

Model	Accuracy	TPR	FPR	Precision	Recall	F1-Score
50,10,50	84.86%	76.0%	0.065	92.12%	85.13%	88.48%
50,20,50	86.74%	85.2%	0.070	92.20%	87.22%	89.64%
50,30,50	91.75%	88.0%	0.073	92.55%	97.97.75%	95.55%
50,40,50	75.32%	60.7%	0.060	91.39%	81.00%	85.88%

Table 5: Result of Preliminary experimental for CID-IDS2017 dataset

Model	Accuracy	TPR	FPR	Precision	Recall	F1-Score

50,10,50	90.77 %	89.00%	0.065	92.5714%	93.13%	0.928499
50,20,50	92.88%	93.50%	0.070	93.0348%	96.22%	0.946006
50,30,50	95.98%	98.97%	0.068	93.5710%	98.85%	0.964679
50,35,50	83.10%	87.02	0.060	92.5267%	88.00%	0.902066

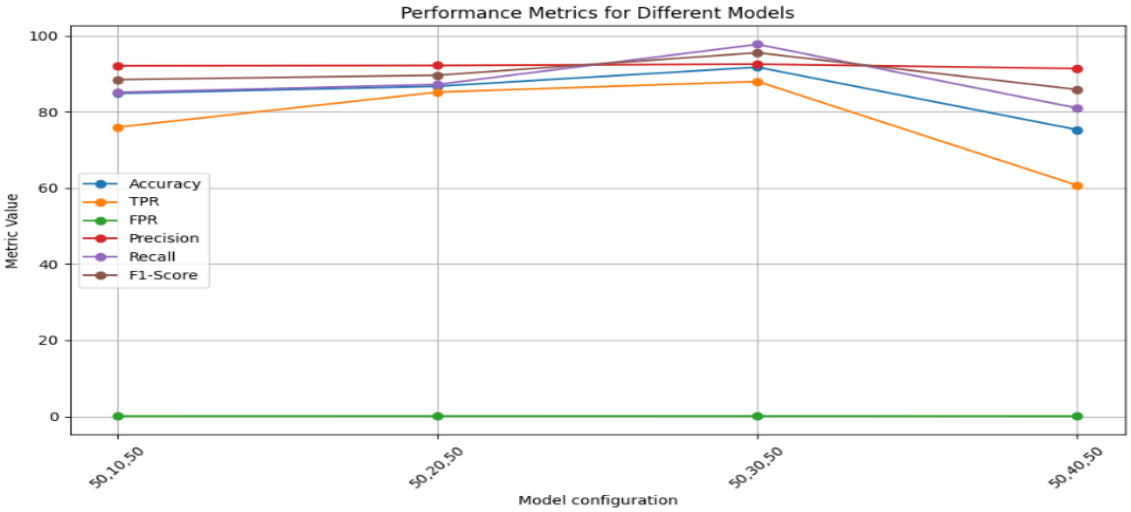


Figure 5: Bottlenecks vr metrics of evaluation for NSL-KDD dataset in preliminary study

Figure 6: Bottlenecks vr metrics of evaluation for CIC-IDS2017 dataset in preliminary study

4.2 Final results for NSL-KDD Dataset

In the context of the NSL-KDD dataset, the results reveal intriguing trends. Latent space size 30 emerges as a configuration that consistently maintains high accuracy, TPR, and F1-score values. The latent space correlation's manifestation in the final results bolsters its validity and utility in architecting effective intrusion detection systems. The Figure 7 below show clearly the various model configurations(bottlenecks) and their performance for our final study using NSL-KDD dataset.

Table 6: Results for final Experimental study using NSL-KDD dataset

Model	Accuracy	TPR	FPR	Precision	Recall	F1-Score
50,25,50	88.02%	77.00%	0.067	91.9952%	94.34%	90.0352%
50,30,50	91.75%	88.00%	0.073	92.3400%	97.97%	95.55%

50,35,50	89.66%	76.00%	0.073	91.2365%	95.99%	91.2533

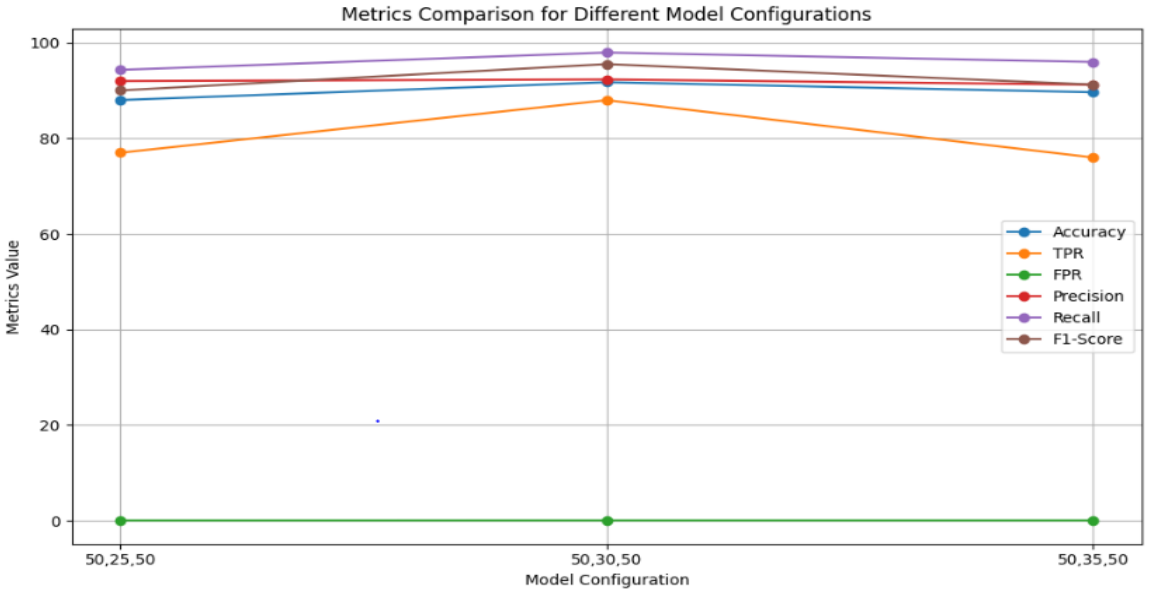


Figure 7: Bottlenecks vr metrics of evaluation for NSL-KDD dataset in Final study

4.3 Final results for CIC-IDS2017 Dataset

The findings from the CIC-IDS2017 dataset further substantiate the significance of the latent space correlation. Latent space size 30 continues to exhibit exceptional performance, reflecting its potential as a universal configuration guideline. The high TPR and F1-score values validate its effectiveness in detecting true anomalies while maintaining a balance against false positives. Figure below provides the pictorial representation for the various bottlenecks' performances for our final study using CIC-IDS2017.

Table 7: Results for final Experimental study using CIC-IDS2017 dataset

Model	Accuracy	TPR	FPR	Precision	Recall	F1-Score
50,25,50	93.50%	0.92.66	0.087	0.920245	95.01%	0.934934
50,30,50	95.98%	0.9897	0.068	0.93571	98.85%	0.961381
50,35,50	94.12%	0.9426	0.091	0.917623	96.75%	0.941902

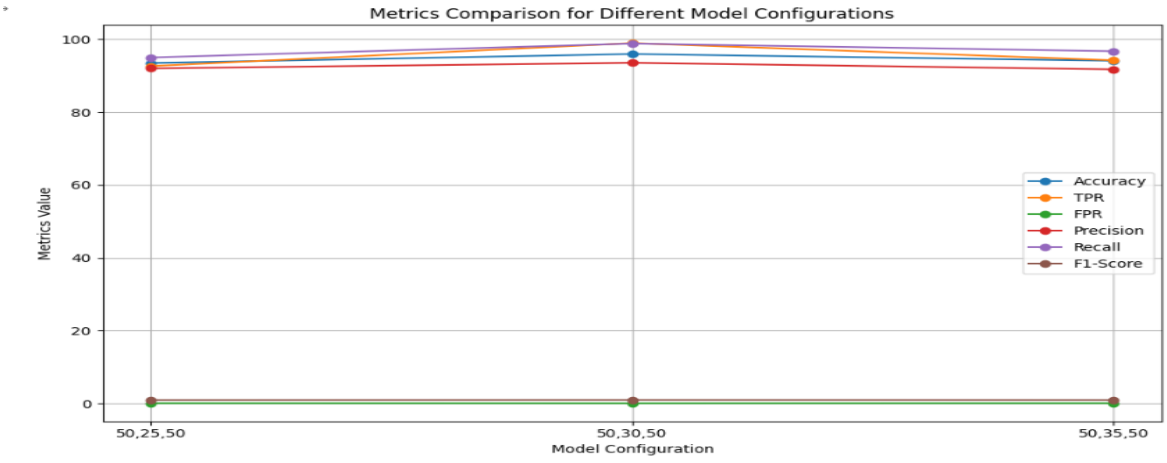


Figure 8: Bottlenecks vr metrics of evaluation for CIC-IDS2017 dataset in final study

4.4 Discussion

4.4.1 Impact on Intrusion Detection Systems:

The consistent success of latent space size 30 in both datasets underscores its effectiveness in boosting the performance of intrusion detection systems. This result holds practical implications for system architects and cybersecurity practitioners. It provides them with a concrete benchmark to guide architecture design, ensuring enhanced accuracy and precision in detecting intrusions.

The latent space correlation, where the optimal latent space size is approximately 60% of the preceding hidden layer's size, serves as a pivotal takeaway from this research. This empirical observation bridges the gap between theoretical understanding and practical application, offering a valuable heuristic for system designers aiming to optimize autoencoder-based intrusion detection systems.

The study's significance lies in its embodiment of the synergy between AI and security. By rigorously testing and validating latent space configurations, this research demonstrates how AI techniques can be harnessed to address pressing security challenges. The results showcase how AI-driven insights translate into actionable strategies for enhancing cybersecurity measures.

While this study illuminates the latent space correlation's potential, future research could explore its applicability to a broader range of datasets and intrusion scenarios. Additionally, investigating more intricate autoencoder architectures and considering other neural network techniques could uncover further optimization opportunities and contribute to the evolution of intrusion detection systems.

Armed with the findings, practitioners can confidently implement autoencoder architectures with latent space sizes around 60% of the preceding hidden layer's size. This practical application of research contributes directly to improving the robustness and efficiency of intrusion detection systems in real-world scenarios.

5.0 Conclusion

Finally, the constant success with a latent space size of 30 found in both datasets highlights its effectiveness in improving intrusion detection system performance, offering system architects and cybersecurity practitioners a concrete benchmark. The optimal size of the identified latent space correlation is about 60% of the size of the previous hidden layer. This is an important finding that connects the theoretical and practical domains and provides a useful heuristic for system designers who want to optimize autoencoder-based intrusion detection systems. The study shows how AI techniques, through thorough testing and validation of latent space configurations, may address urgent security concerns and convert into beneficial outcomes. It also represents the successful synergy between AI and security. practical methods for strengthening cybersecurity defenses. While shedding light on the latent space correlation's potential, further research opportunities include investigating how well it applies to various datasets and intrusion scenarios, investigating more complex autoencoder architectures, and taking into account alternative neural network techniques to find even more optimization opportunities for the development of intrusion detection systems. Equipped with these discoveries, professionals can safely execute autoencoder structures with latent spaces around 60% larger than the previous hidden layer's size, so directly enhancing the resilience and effectiveness of intrusion detection systems in practical scenarios.

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Competing Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability:

The dataset NSL-KDD is publicly available on: https://www.unb.ca/cic/datasets/nsl.html

The dataset CIC-IDS2017 is publicly available on: https://www.unb.ca/cic/datasets/ids-2017.html

REFERENCES

1. Alam, Naushad, and Muqeem Ahmed. 2023. "Zero-Day Network Intrusion Detection Using Machine Learning Approach," no. April: 194–201.

2. Almaiah, Mohammed Amin, Omar Almomani, Adeeb Alsaaidah, Shaha Al-otaibi, Nabeel Bani-hani, Ahmad K Al Hwaitat, Ali Al-zahrani, Abdalwali Lutfi, Ali Bani Awad, and Theyazn H H Aldhyani. 2022. "Machine Kernels."

3. Das, Abhijit. 2022. "An Efficient Feature Selection Approach for Intrusion Detection System Using Decision Tree" 13 (2).

4. Garg, Deepak, N. V. Narendra Kumar, and Rudrapatna Shyamasundar. n.d. "Information Systems Security : 15th International Conference, ICISS 2019, Hyderabad, India, December 16-20, 2019, Proceedings," 345. Accessed February 7, 2022. https://www.kobo.com/us/en/ebook/information-systems-security-4.

5. Haripriya, C, and M P Prabhudev Jagadeesh. 2022. "An Efficient Autoencoder-Based Deep Learning Technique to Detect Network Intrusions" 13 (7): 1–10. https://doi.org/10.14456/ITJEMAST.2022.142.

6. Hendi, Alva, Ike Verawati, and Richki Hardi. 2022. "An Intrusion Detection System Using SDAE to Enhance Dimensional Reduction in Machine Learning" 6 (June): 306–16.

7. Kasongo, Sydney Mambwe. 2023. "A Deep Learning Technique for Intrusion Detection System Using a Recurrent Neural Networks Based Framework." *Computer Communications* 199 (October 2022): 113–25. https://doi.org/10.1016/j.comcom.2022.12.010.

8. Li, Yue, Ang Li, Anxing Wen, and Xian Xie. 2022. "Research on Intrusion Detection Based on Neural Network Optimized by Genetic Algorithm" en: 8–11.

9. Logeswari, G, S Bose, and T Anitha. 2023. "An Intrusion Detection System for SDN Using Machine Learning." https://doi.org/10.32604/iasc.2023.026769.

10. Makarand, L. 2022. "Machine Learning Applications in Engineering Education and Management Intrusion Detection System Attack Detection and Classification Model with Feed-Forward LSTM Gate in Conventional Dataset" 02 (01): 20–29.

11. Mirsky, Yisroel, Tomer Doitshman, Yuval Elovici, and Asaf Shabtai. 2018. "Kitsune : An Ensemble of Autoencoders for Online Network Intrusion Detection," no. February: 18–21.

12. Pranto, Badiuzzaman, Hasibul Alam Ratul, Mahidur Rahman, and Ishrat Jahan Diya. 2022. "Performance of Machine Learning Techniques in Anomaly Detection with Basic Feature Selection Strategy - A Network Intrusion Detection System" 13 (1). https://doi.org/10.12720/jait.13.1.36-44.

13. Ramasamy, Mathiyalagan, and Pamela Vinitha Eric. 2023. "A Tree Growth Based Forward Feature Selection Algorithm for Intrusion Detection System on Convolutional Neural Network" 12 (1): 472–82. https://doi.org/10.11591/eei.v12i1.4015.

14. Sabir, Maha, Jawad Ahmad, and Daniyal Alghazzawi. 2023. "A Lightweight Deep Autoencoder Scheme for Cyberattack Detection in the Internet of Things." https://doi.org/10.32604/csse.2023.034277.

15. Schmidt, Mark. 2020. "TheRepository at St . Cloud State Autoencoder-Based Representation Learning to Predict Anomalies in Computer Networks."

16. Shahid, Mustafizur R., Gregory Blanc, Zonghua Zhang, and Herve Debar. 2019. "Anomalous Communications Detection in IoT Networks Using Sparse Autoencoders." *2019 IEEE 18th International Symposium on Network Computing and Applications, NCA 2019*, 1–5.

https://doi.org/10.1109/NCA.2019.8935007.

17. Shone, Nathan, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi. 2018. "A Deep Learning Approach to Network Intrusion Detection." *IEEE Transactions on Emerging Topics in Computational Intelligence* 2 (1): 41–50. https://doi.org/10.1109/TETCI.2017.2772792.

18. Shukla, Rakhi, and Aarti Kumar. 2023. "Security Enhancement Model for Intrusion Detection System Using Classification Techniques :" 5 (1): 125–32. https://doi.org/10.35629/5252-0501125132.

19. Siddique, Kamran, Zahid Akhtar, Farrukh Aslam Khan, and Yangwoo Kim. 2019. "KDD Cup 99 Data Sets: A Perspective on the Role of Data Sets in Network Intrusion Detection Research." *Computer* 52 (2): 41–51. https://doi.org/10.1109/MC.2018.2888764.

20. Sindian, Samar, and Samer Sindian. 2020. "An Enhanced Deep Autoencoder-Based Approach for DDoS Attack Detection 3 Deep Neural Network 2 Related Work" 15: 716–24. https://doi.org/10.37394/23203.2020.15.72.

21. Song, Tianbao, Jingbo Sun, B O Chen, Weiming Peng, and Jihua Song. 2019. "Latent Space Expanded Variational Autoencoder for Sentence Generation." *IEEE Access* 7: 144618–27. https://doi.org/10.1109/ACCESS.2019.2944630.

22. Song, Youngrok, Sangwon Hyun, and Yun Gyung Cheong. 2021. "Analysis of Autoencoders for Network Intrusion Detection†." *Sensors* 21 (13): 1–23. https://doi.org/10.3390/s21134294.

23. Wang, Chao, Hongri Liu, Yunxiao Sun, Yuliang Wei, Kai Wang, and Bailing Wang. 2022. "Dimension Reduction Technique Based on Supervised Autoencoder for Intrusion Detection of Industrial Control Systems" 2022.

24. Xu, W E N, Julian Jang-jaccard, Amardeep Singh, and Fariza Sabrina. 2021. "Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset." *IEEE Access* 9: 140136–46. https://doi.org/10.1109/ACCESS.2021.3116612.

25. Yu, Yang, Jun Long, and Zhiping Cai. 2017. "Network Intrusion Detection through Stacking Dilated Convolutional Autoencoders." *Security and Communication Networks* 2017. https://doi.org/10.1155/2017/4184196.

26. Zhang, Baoan, Yanhua Yu, and Jie Li. 2018. "Network Intrusion Detection Based on Stacked Sparse Autoencoder and Binary Tree Ensemble Method." *2018 IEEE International Conference on Communications Workshops, ICC Workshops 2018 - Proceedings*, no. 61702046: 1–6. https://doi.org/10.1109/ICCW.2018.8403759.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 52 – 59 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

კიბერუსაფრთხოება და აკადემიური სექტორი

ვლადიმერ სვანაძე[1]

[1] საჯარო მმართველობის დოქტორი, ბიზნესისა და ტექნოლოგიების უნივერსიტეტის აფილირებული პროფესორი

რეზუმე: სულ უფრო მზარდია კიბერთავდასხმების სტატისტიკური მაჩვენებელი და ჰაკერების სულ უფრო დიდ ინტერესს წარმოადგენს აკადემიური სექტორი, სხვადასხვა სახის სამეცნიერო - კვლევითი ცენტრები, თუ ლაბორატორიები. აკადემიურ სექტორზე კიბერთავდასხმების მთავარ მიზანს წარმოადგენს სტუდენტებისა და თანამშრომლების ისეთი პერსონალური ინფორმაცია, როგორიცაა მათი მისამართები, ტელეფონის ნომრები, სოციალური უსაფრთხოების ნომრები, საბანკო ანგარიშები და ფინანსური დოკუმენტები. აკადემიურ სექტორში არის საკმაოდ დიდ მოცულობის მონაცემთა ბაზები, უზარმაზარი საჯარო ინფორმაცია, სადაც შედის არა მარტო პერსონალური მონაცემები, რაც შეიძლება ითქვას უფრო მეორეხარისხოვანია, არამედ იქ არის ინფორმაცია სხვადასხვა სახის კვლევების შესახებ, ამ კვლევების შედეგების შესახებ, კონკრეტული კვლევების პროცესისა და ტესტირების შესახებ. ამ ტიპის ინფორმაცია სასარგებლოა სხვადასხვა ქვეყნის მთავრობებისთვის, რომლებიც თავიანთი სადაზვერვო სამსახურების საშუალებით ხშირად მიმართავან კიბერჯაშუშობას, მათთვის საინტერესო ინფორმაციის მოპოვების მიზნით, რაც შეიძლება ეხებოდეს სხვადასხვა სახის ტექნოლოგიურ გადაწყვეტილებებს, მიღწევებსა თუ გამოგონებებს. აკადემიური სექტორი და მასში გაერთიანებული სამეცნიერო - კვლევითი ცენტრები და ლაბორატორიები არიან კიბერშეტევების სამიზნეები, რადგან იქ არსებული უზარმაზარი მოცულობის მონაცემები არის დაუცველი და ღირებული.

საკვანძო სიტყვები: კიბერუსაფრთხოება, კრიტიკული ინფრასტრუქტურა, კვლევითი ცენტრები და ლაბორატორიები, SQLI, ფიშინგი.

ABSTRACT: The statistical rate of cyber-attacks is increasing, and the academic sector and various scientific research centers are of increasing interest to hackers. The main objective of cyber-attacks in the academic sector is to obtain the personal information of students and employees, such as addresses, phone numbers, social security numbers, bank accounts, and financial documents. in the academic sector, there are quite large databases, and huge public information, which includes not only personal data, which can be said to be more secondary but also information about various types of research, the process, and testing of their results. This type of information is useful for governments of various countries, who often resort to cyber espionage to obtain interesting information that may relate to various technological solutions, achievements, or inventions. It can be noted that the academic sector, scientific research centers, and laboratories are the targets of cyber-attacks because of the huge amount of data that is vulnerable and valuable.

KEYWORDS: Cybersecurity, Critical Infrastructure, Research Centers and Laboratories, SQLI, Phishing.

1. შესავალი

კიბერუსაფრთხოებამ მიუხედავად თავისი განვითარების მოკლე პერიოდისა, შეიძლება ითქვას დაიკავა ერთ - ერთი მთავარი ადგილი როგორც საერთაშორისო, ისე ეროვნულ უსაფრთხოებაში,

გახდა ჩვენი ცხოვრების განუყოფელი ნაწილი, და მნიშვნელოვანი კომპონენტი. ფაქტიურად, ყოველივე ეს განაპირობა ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფმა განვითარებამ, პანდემიის ფონზე ელექტრონული სერვისების მიმართ გლობალურად მზარდმა მოთხოვნილებამ. ყოველივე ეს კი ითხოვს ინტერნეტის სტაბილურობისა და უსაფრთხოების დაცვის აუცილებლობას, ინტერნეტის ერთიანობის შენარჩუნებას, რაშიც ჩართული არის როგორც ცალკეული ქვეყნები, ისე საერთაშორისო და რეგიონალური ორგანიზაციები. შეიძლება ითქვას, რომ ცალკეული ქვეყნების კიბერსივრცის უსაფრთხოება ისეთივე მნიშვნელოვანი გახდა, როგორც ქვეყნის სახმელეთო, საჰაერო, თუ საზღვაო ტერიტორიების დაცვა, და რაც თავის მხრივ ხდება საერთაშორისო და რეგიონალური უსაფრთხოების შემადგენელი, მისი განუყოფელი ნაწილი. ფაქტიურად, რაც უფრო დამოკიდებულია საზოგადოება თანამედროვე ტექნოლოგიებზე, მით უფრო მოწყვლადია კიბერ თავდასხმების მიმართ.

მსოფლიო ეკონომიკური ფორუმის 2022 წლის გლობალური რისკების ანგარიშის მიხედვით, კიბერსივრცეში არსებული რისკები კვლავ შედის გლობალური რისკების რიცხვში. პანდემიამ COVID – 19 დააჩქარა ტექნოლოგიების დანერგვის პროცესი, თუმცა, გამოავლინა კიბერ სისუსტეები და არამზაობა. ამვდროულად, გაამწვავა ტექნიკური უთანასწორობა როგორც საზოგადოებებს შორის გარედან, ისე მათ შიგნითაც.

იგივე ანგარიშის მიხედვით, „მომავალ წელს ძალზედ მნიშვნელოვანია კიბერუსაფრთხოება განხილულ იქნეს, როგორც სტრატეგიული ბიზნეს - საკითხი და განვითარდეს მჭიდრო საპარტნიორო ურთიერთობები ინდუსტრიებს, ბიზნესის ლიდერებს, მარეგულირებელ ორგანოებსა და პოლიტიკოსებს შორის. ისევე, როგორც ნებისმიერი სხვა სტრატეგიულად მნიშვნელოვანი საზოგადოებრივი გამოწვევა, კიბერუსაფრთხოებაც ვერ მოგვარდება იზოლირებულად “.

სულ უფრო მზარდია კიბერთავდასხმების სტატისტიკური მაჩვენებელი და ჰაკერების სულ უფრო დიდ ინტერესს წარმოადგენს აკადემიური სექტორი, სხვა და სხვა სახის სამეცნიერო - კვლევითი ცენტრები თუ ლაბორატორიები. აკადემიურ სექტორზე კიბერთავდასხმების მთავარ მიზანს წარმოადგენს სტუდენტებისა და თანამშრომლების ისეთი პერსონალური ინფორმაციის მოპოვება, როგორიცაა მისამართები, ტელეფონის ნომრები, სოციალური უსაფრთხოების ნომრები, საბანკო ანგარიშები და ფინანსური დოკუმენტები, სადაზღვევო პოლისები. ხშირ შემთხვევაში, ეს მონაცემები შემდეგ თავსდება „Dark Net“ - ზე, სადაც მისი გამოყენება შესაძლებელია სხავადასხვა სახის კიბერკრიმინალური ქმედებებისთვის.

მაგრამ ისმის კითხვა რატომ გახდა აკადემიური სექტორი კიბერკრიმინალების სამიზნე?

მთავარ მიზეზს ალბათ წარმოადგენს ის ფაქტი, რომ აკადემიურ სექტორში არის საკმაოდ დიდ მოცულობის მონაცემთა ბაზები, უზარმაზარი საჯარო ინფორმაცია, სადაც შედის არა მარტო პერსონალური მონაცემები, რაც შეიძლება ითქვას უფრო მეორეხარისხოვანია, არამედ იქ არის ინფორმაცია სხვადასხვა სახის კვლევების შესახებ, ამ კვლევების შედეგების შესახებ, თითოეული კვლევის პროცესისა და ტესტირების შესახებ.

ამ ტიპის ინფორმაცია სასარგებლოა სხვადასხვა ქვეყნის მთავრობებისთვის, რომლებიც ხშირად მიმართავან კიბერჯაშუშობას, მათთვის საინტერესო ინფორმაციის მოპოვების მიზნით, რაც შეიძლება ეხებოდეს სხვადასხვა სახის ტექნოლოგიურ გადაწყვეტილებებს, მიღწევებსა თუ გამოგონებებს. გარდა ამისა, მსგავსი ინფორმაცია არის ასევე ეკონომიკურად ღირებული.

როცა ვსაუბრობთ კიბერუსაფრთხოებსა და აკადემიური სექტორის ურთიერთდამოკიდებულებაზე, ასევე განათლების როლზე მოცემული დარგის განვითარებაზე, შეიძლება გამოიყოს ორი ძირითადი მიმართულება, კერძოდ;

1. კიბერუსაფრთხოების მნიშვნელობა და როლი სასწავლო - კვლევითი ცენტრებისა და ლაბორატორიების ინფრასტრუქტურის სრულ დაცვაში;

2. განათლების მნიშვნელობა და როლი კიბერუსაფრთხოების განვითარებისთვის.

2. სასწავლო - კვლევითი ცენტრებისა და ლაბორატორიების კიბერუსაფრთხოება

აკადემიური სექტორი და მასში გაერთიანებული სამეცნიერო - კვლევითი ცენტრები და ლაბორატორიები არიან კიბერშეტევების სამიზნეები, რადგან იქ არსებული უზარმაზარი მოცულობის მონაცემები არის ნაკლებად დაცული და ღირებული.

აქვე ისევ გავმეორდები, რომ არა მხოლოდ სტუდენტებისა და თანამშრომლების პერსონალურ მონაცემებზეა საუბარი, არამედ საუბარია კვლევის უახლოეს შედეგებზე, რაც შეიძლება გახდეს საერთაშორისო დონის კიბერჯაშუშობის სამიზნე. სწორედ ამიტომ, აკადემიური სექტორისთვის სასიცოცხლოდ მნიშვნელოვანია უზრუნველყოფილ იქნას კიბერუსაფრთხოებითი ღონისძიებები და დაიცვას თავისი კრიტიკული ინფრასტრუქტურა პოტენციური თავდასხმებისგან.

როგორც ზემოთ იყო აღნიშნული, იმის გამო, რომ სამეცნიერო - კვლევითი ცენტრები და ლაბორატორიები ინახავენ ინფორმაციის ისეთ უზარმაზარ რაოდენობას, რომ ისინი ხშირად ხდებიან ჰაკერების და სხვა კიბერ კრიმინალების სამიზნე, რაზეც მეტყველებს ასევე მოცემული მიმართულებით კიბერშეტევების მზარდი სტატისტიკა. ფაქტია, რომ 2018 – 2022 წლებში სასწავლო - კვლევით დაწესებულებებში მოხდა 2500 - ზე მეტი კიბერინციდენტი, რამაც გამოიწვია მონაცემთა დარღვევა. გარდა ამისა, აღსანიშნავია ის გარემოებაც, რომ ბევრ უნივერსიტეტს და იქ არსებულ სასწავლო - კვლევით ცენტრებსა და ლაბორატორიებს აქვთ მოძველებული ან ცუდად აშენებული კიბერუსაფრთხოებისა და ინფორმაციული ტექნოლოგიების სისტემები, რაც კიდევ უფრო დაუცველს და მოწყვლადს ხდის მათ ინფრასტრუქტურას [1].

აქვე მოყვანილია კიბერსივრციდან მომდინარე ის ხუთი კიბერსაფრთხე, რასაც ხშირად აწყდებიან სასწავლო - კვლევითი ცენტრები და ლაბორატორიები, კერძოდ:

1. **ფიშინგი (Phishing)**[1] - ეს არის ყველაზე უფრო გავრცელებული პრობლემა მოცემული სექტორისთვის, სასწავლო - კვლევითი დაწესებულებებისთვის;
2. **რანსომვეარი (Ransomware)**[2] - ეს არის კიდევ ერთი მთავარი გამოწვევა, რომლის წინაშეც დგას სასწავლო - კვლევითი ცენტრები და ლაბორატორიები დღეს;
3. ბევრი ჰაკერი იყენებს **SQL[3] ინექციებს** კვლევით ინსტიტუტებზე თავდასხმისას;
4. არსებობს მრავალი სხვა ტიპის მონაცემთა დარღვევა, რომელთა წინაშეც ხშირ შემთხვევაში დაუცველია უნივერსიტეტების ინფრასტრუქტურა. მაგალითად, არსებობს მრავალი სხვადასხვა ტიპის **მავნე პროგრამა[4],** რომელსაც ჰაკერები იყენებენ წლების განმავლობაში;

[1] ფიშინგი ინტერნეტთაღლითობის ფორმაა, რომელიც მომხმარებელს მოტყუების გზით აიძულებს, გაამჟღავნოს თავისი სენსიტიური და პერსონალური ინფორმაცია თაღლითების მიერ შექმნილ ყალბ ვებგვერდზე შეყვანის გზით

[2] მავნე პროგრამა რომელსაც „მძევლად“ აყავს ჩვენი სისტემა, მისი გამოწერის და დაყენების შემდეგ, ის ახდენს სისტემის შიფრაციას კრიპტოგრაფიული მეთოდების გამოყენებით. ამის შემდეგ პროგრამა გვთხოვს ფულს თუ გვინდა რომ კრიპტოგრაფიული გასაღები მივიღოთ და გავშიფროთ ჩვენი სისტემა;

[3] Structured Query Language - სტრუქტურიზებული მოთხოვნების ენა, რომლის დახმარებითაც შესაძლებელია მონაცემთა ბაზებთან წვდომა და იქ შენახული ინფორმაციით მანიპულირება. SQL არის ANSI-სტანდარტი (American National Standards Institute);

[4] მავნე პროგრამა, საზიანო პროგრამა (ინგლ. malware) — ყველა იმ პროგრამის სახელწოდება, რომელიც ცდილობს მოიპოვოს უკანონი და არა სანქცირებული გზების საშუალებით წვდომა მსხვერპლის კომპიუტერზე ან პროგრამა, რომელიც მიზანმიმართულად არის შექმნილი იმისათვის, რომ ავნოს

5. **მოძველებული ტექნოლოგია** – ბევრი უნივერსიტეტი, სასწავლო - კვლევითი ცენტრი და ლაბორატორია იყენებს მოძველებულ ტექნოლოგიას, რაც კიბერშეტევების მიმართ მათ კიდევ უფრო დაუცველს და მოწყვლადს ხდის. პროგრამული უზრუნველყოფის თუნდაც ერთი განახლების გამოტოვებამ შეიძლება ორგანიზაცია კიდევ უფრო დაუცველი გახადოს.

როგორც იყო აღნიშნული სხვადასხვა ქვეყნის მთავრობები ცდილობენ კვლევების ჩატარებისა და შედეგების შესახებ ინფორმაციის მოპოვებას და ამ მიზნით, აქტიურად იყენებენ ჰაკერების მომსახურებას, ახორციელებენ კიბერშეტევებს. ეს პროცესი განსაკუთრებით თვალშისაცემი იყო პანდემიის პერიოდში, როცა კვლევითი ცენტრები და ლაბორატორიები აქტიურად მუშაობდნენ კორონის საწინააღმდეგო წამლისა და ვაქცინის შემუშავებაზე.

ამ კუთხით, ძალიან აქტიურობდნენ ჰაკერული ჯგუფები რუსეთის ფედერაციიდან, რომლებმაც განახორციელეს რამოდენიმე კიბერშეტევა დიდი ბრიტანეთის, შეერთებული შტატებისა და კანადის COVID – 19 კვლევით ცენტრებზე. სამივე ქვეყნის ოფიციალური პირები თავიანთ განცხადებაში დეტალურად აღწერენ რუსული ჰაკერული ჯგუფის აქტივობას, სახელწოდებით APT 29, რომელიც ასევე მოიხსენიება სახელწოდებით “the Dukes” ან “Cozy Bear.” გაერთიანებული სამეფოს კიბერუსაფრთხოების ეროვნული ცენტრის (NCSC) მიერ გამოქვეყნებული ინფორმაცია დეტალურად აღწერს რუსული ჰაკერული ჯგუფის საქმიანობას და ცალსახად ასახელებს კონკრეტულ კიბერინციდენტებსა და მცდელობებს შეერთებული შტატების, გაერთიანებული სამეფოსა და კანადის ვაქცინების კვლევისა და განვითარების ორგანიზაციების მიმართ.

პანდემიის პერიოდში, 2020 წლის სექტემბერში მოხდა ჰაკერული თავდასხმა საქართველოს ჯანდაცვის სისტემაზე[5]. საქართველოს შინაგან საქმეთა სამინისტროს ინფორმაციით, საქართველოს ჯანდაცვის, შრომისა და სოციალური დაცვის სამინისტროზე უცხო ქვეყნიდან განხორციელდა კიბერშეტევა. კიბერთავდასხმის მთავარი მიზანი იყო სამინისტროს ცენტრალური აპარატისა და მისი სტრუქტურული ერთეულების, მათ შორის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრისა და რიჩარდ ლუგარის კვლევითი ცენტრის დოკუმენტებისა და პანდემიის მართვაზე იქ არსებული მნიშვნელოვანი ინფორმაციის უკანონო გზით მოპოვება და გამოყენება [2].

შსს - ს ცნობით, კიბერთავდასხმის შედეგად მოპოვებული ავთენტური დოკუმენტების ნაწილი ატვირთულია ერთ - ერთ უცხოურ ვებგვერდზე და ხელმისაწვდომია საზოგადოებისთვის. ამასთანავე, ამავე ვებგვერდზე იტვირთება მიზანმიმართულად გაყალბებული დოკუმენტები, რომლებიც საზოგადოების დაშინების, დაბნეულობისა და უნდობლობის გაღვივებას ისახავს მიზნად. მიუხედავად იმისა, რომ შსს არ აკონკრეტებს ქვეყანას, საიდანაც განხორციელდა კიბერშეტევა, პროცესები და დეზინფორმაციული კამპანია, რომელიც წინ უძღოდა მოცემულ კიბერშეტევას, დიდი ალბათობით მიუთითებს რუსულ კვალზე.

როცა ვსაუბრობთ კონკრეტულ ფაქტებზე, რაც უკავშირდება კვლევით ცენტრებზე კიბერთავდასხმებს, აუცილებლად უნდა გავიხსენოთ რუსული ჰაკერული ჯგუფი, რომელიც ცნობილია „Cold River“ - ის სახელით, რომელმაც 2022 წლის ზაფხულის პერიოდში განახორციელა რამოდენიმე კიბერშეტევა აშშ - ს სამ ბირთვულ კვლევით ლაბორატორიაზე.

და მაინც ჩნდება კითხვა თუ სასწავლო - კვლევითი ცენტრები და ლაბორატორიები ჰაკერების დიდი ინტერესის ქვეშ არიან, თანაც სხვადასხვა ქვეყნების მთავრობები არიან დაინტერესებული

მომხმარებლის კომპიუტერს ან მასში არსებულ ინფორმაციას, მოხმარებლისგან მალულად, ასეთ პროგრამებს ხშირად ვირუსებს ეძახიან, ისინი იყოფიან რამდენიმე კლასებად და სახეობებად.

[5] https://ge.usembassy.gov/u-s-embassy-statement-on-september-1-2020-cyberattack-against-georgian-ministry-of-health/

მიმდინარე კვლევებით, ტესტებითა და შედეგებით, მაშინ როგორ შეიძლება დაცული იყოს კვლევითი ცენტრების კრიტიკული ინფრასტრუქტურა? რა შეიძლება ვურჩიოთ მათ?
ყოველივეს გათვალისწინებით, როცა ვსაუბრობთ კვლევითი ცენტრების კრიტიკული ინფრასტრუქტურის დაცვაზე, პირველ რიგში აუცილებელია სამთავრობო დონეზე ჩართულობა, საჯარო, კერძო და აკადემიურ სექტორებს შორის თანამშრომლობის გაძლიერება, რაც მოიცავს კრიტიკული ინფრასტრუქტურის მოწესრიგებას, კიბერუსაფრთხოებითი და ინფორმაციული უსაფრთხოებით გათვალისწინებული ღონისძიებების განხორციელებას, თანამშრომელთა ცნობიერების ამაღლებას, რაც ზოგადად კიბერუსაფრთხოების ერთ - ერთი შემადგენელი ნაწილია, და ასევე სხვა მნიშვნელოვან ღონისძიებებს.

3. განათლების მნიშვნელობა კიბერუსაფრთხოების განვითარებაში

ზოგადად, ქვეყნის კრიტიკულ ინფრასტრუქტურაზე განხორციელებული წარმატებული კიბერშეტევების აღკვეთა დამოკიდებულია არსებულ კვალიფიციურ კადრებზე, და შესაბამისად განათლების სისტემაზე, რომელსაც შეუძლია შექმნას მსგავსი კვალიფიციური ადამიანური რესურსი. აქვე შეიძლება აღინიშნოს, რომ შესაძლებელია მოხდეს უცხოელი სპეციალისტების მოზიდვა, ან ბევრი კიბერთავდაცვითი ღონისძიებები გადაეცეს კერძო სექტორს, ანუ გატანილ იქნეს ე. წ. „აუთსორსინგულ“ მომსახურებაზე. თუმცა ორივე ეს ფაქტორი წარმოშობს სხვა პრობლემებს, რაც უკავშირდება როგორც დიდ ფინანსურ საშუალებებს, ისე ნდობის საკითხს დაკავშირებულს კრიტიკული ინფრასტრუქტურის სუბიექტების კიბერთავდაცვით უზრუნველყოფაზე უცხო კომპანიებისთვის გადაცემასთან, რაც ეროვნული უსაფრთხოების თვალსაზრისით ყოვლად დაუშვებელია. ბევრი ექსპერტი ამახვილებს ყურადღებას მოცემულ ფაქტორზე და იძლევიან სტრატეგიულ რეკომენდაციებს კიბერუსაფრთხოების სფეროში ეროვნული საკადრო რესურსის აღზრდისა და განვითარების შესახებ, რაც ნებისმიერი ქვეყნისთვის ასე აუცილებელი და მნიშვნელოვანი ფაქტორია [3-4].
კიბერუსაფრთხოების სფეროში კვალიფიციური ადამიანური რესურსის ყოლა არის საკმაოდ დეფიციტური არა მარტო განვითარებადი, არამედ განვითარებული ქვეყნებისთვისაც. მოცემული პროფესიის ადამიანებზე მოთხოვნა გაიზარდა განსაკუთრებით მას შემდეგ, რაც ციფრული ტრანსფორმაციის ფარგლებში გაიზარდა მოთხოვნილება კიბერუსაფრთხოების სტრატეგიისა და პოლიტიკის სწორი მიმართულებით შემუშავებასა და პროცესის სწორ დაგეგმვაზე. ყოველივე ეს მოითხოვს კიბერუსაფრთხოების მიმართულებით კვალიფიციურ და გამოცდილ ადამიანურ რესურსს, რაც თავის მხრივ პირდაპირ კავშირშია განათლების სისტემასთან.
კიბერუსაფრთხოების შესახებ განათლების ზრდის ხელშეწყობა და ცნობიერების გაზრდა ქვეყნებისთვის იმდენად პრიორიტეტულ და მნიშვნელოვან მიმართულებას წარმოადგენს, რომ ის შეყვანილი არის თითოეული ქვეყნის კიბერუსაფრთხოების ეროვნულ სტრატეგიებში[6]. ამ მხრივ არც საქართველოს „კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგია და სამოქმედო გეგმა“ არის გამონაკლისი, სადაც მოცემული მიმართულება სხვა მიმართულებებთან ერთად მოხსენიებულია როგორც ერთ - ერთი ძირითადი მიმართულება, კერძოდ:

1. კვლევა და ანალიზი;
2. სამართლებრივი ბაზის შემუშავება და სრულყოფა;
3. კიბერუსაფრთხოების სფეროში შესაძლებლობათა განვითარება;

[6] GUIDE TO GOOD GOVERNANCE IN CYBERSECURITY, DCAF Business and Security Division, Directorate for Security Cooperation and Defence (DCSD) of the French Ministry of Europe and Foreign Affairs, 19 January,2021 https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021_0.pdf

4. **საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის შექმნა;**
5. საერთაშორისო თანამშრომლობა.

უნდა აღინიშნოს, რომ სტრატეგიებში განათლების სფეროს ასახვა ნათლად აჩვენებს ქვეყნების დიდ ინტერსს განავითარონ თავიანთი კიბერუსაფრთხოებითი შესაძლებლობა, რაც პირდაპირ კავშირშია პროფესიული და კვალიფიციური ადამიანური რესურსის არსებობასთან. აქვე ცალკე აღსანიშნავია ის გარემოებაც, რომ სტრატეგიებში მოცემული კიბერუსაფრთხოების ძირითადი მიმართულებები, იქნება ეს კვლევა და ანალიზი, საერთაშორისო თანამშრომლობა, სამართლებრივ ბაზებზე მუშაობა და მისი განვითარება, თუ თავად კიბერუსაფრთხოების სფეროს შესაძლებლობების განვითარება და საზოგადოებრივი ცნობიერების ამაღლება, პირდაპირ კავშირშია სწორად დაგეგმილი და ძლიერი საგანმანათლებლო ბაზის განვითარებასთან, რადგან სტრატეგიის ყველა ჩამოთვლილი მიმართულება მოითხოვს კვალიფიციურ კადრს [5-6].
როცა ვსაუბრობთ კვალიფიციურ კადრზე იგულისხმება აკადემიური განათლების მქონე პირები, რომლებსაც მიღებული აქვთ სულ ცოტა ბაკალავრის აკადემიური ხარისხი. გარდა ამისა, არსებობს საერთაშორისო დონეზე აღიარებული სერტიფიცირებული კურსები, თუმცა მათი უმრავლესობა კონკრეტული მიმართულებით ითხოვს საბაზისო ცოდნას, რაც შესაბამისობაშია ბაკალავრის დონესთან. ასევე დამსაქმებელთა დიდი ნაწილი ვაკანტური ადგილის დასაკავებელი კონკურსის მოთხოვნების განათლების სექციაში პირდაპირ უთითებენ მინიმუმ ბაკალავრის დონეს. შესაძლებელია კიდევ ბევრი მაგალითის მოყვანა, თუმცა ეს ორი ერთმანეთისგან განსხვავებული მაგალითი პირდაპირ მიუთითებს კიბერუსაფრთხოების სფეროსთვის აკადემიური განათლების მნიშვნელობაზე. აქვე თუ დავამატებთ იმ ფაქტს, რომ გლობალურად კიბერუსაფრთხოების სპეციალისტთა აშკარა დეფიციტია, ხოლო მათზე მოთხოვნილება სულ უფრო იზრდება, მაშინ შეიძლება ითქვას, რომ უახლოეს მომავალში ეს იქნება ერთ - ერთი მოთხოვნადი სპეციალობა. აგრეთვე, თუ გავითვალისწინებთ ასეთ მზარდ მოთხოვნილებას, თავისუფლად შეიძლება ითქვას, რომ მოცემული მიმართულების სპეციალისტების შრომითი ანაზღაურება არის საკმაოდ მაღალი. კერძოდ, არსებული სტატისტიკის მიხედვით, უსაფრთხოების ოპერაციების ცენტრის[7] დამწყები ანალიტიკოსის წლიური ხელფასი აჭარბებს 80 ათას აშშ დოლარს. ასეთ მაღალანაზღაურებად სპეციალობებად მოიაზრება[8]:

- შეღწევადობის ტესტერი (Penetration Tester);
- ინფორმაციული უსაფრთხოების ანალიტიკოსი (Information Security Analyst);
- უსაფრთხოების ანალიტიკოსი (Security Analyst);
- ეთიკური ჰაკერი (Ethical Hacker).

ალბათ ყველაზე უფრო გასათვალისწინებელი ფაქტი არის ის, რომ მოცემული სპეციალობების ხალხის დასაქმება სირთულეს არ წარმოადგენს როგორც საერთაშორისო, ისე ადგილობრივ ბაზარზე. ამიტომ, შეიძლება ითქვას, რომ კიბერუსაფრთხოების მიმართულებით მაღალი დონის განათლების მიღებაში ფინანსური საშუალებების „დაბანდება“, საკმაოდ წარმატებულ ინვესტირებას უნდა წარმოადგენდეს.
განვითარებად ქვეყნებში კიბერუსაფრთხოების მიმართულებით განათლების განვითარების პროცესი არათანმიმდევრულად და რთულად მიმდინარეობს, ხოლო ხშირ შემთხვევაში ეს პროცესი საერთოდ არ არსებობს, ან თუ არსებობს საერთოდ არის მოწყვეტილი დარგის განვითარებისა და მისი მდგრადობის შენარჩუნებისგან.

[7] Security Operations Center SOC
[8] https://www.cybrary.it/

საქართველოს კიბერსივრცეზე, დაწყებული 2008 წლის „აგვისტოს ომის“ დროიდან მოყოლებული დღემდე, განხორციელდა არა ერთი სერიოზული კიბერთავდასხმა, რომლის დროსაც დარღვეული იყო კიბერსივრცის მდგრადობა. თითქმის ყველა კიბერთავდასხმის თავიდან აღკვეთის, ან საგამოძიებო პროცესში ჩართული იყვნენ ქვეყნის სტრატეგიული პარტნიორები და მათი დახმარებით ხდებოდა ქვეყნის კრიტიკული ინფრასტრუქტურის ერთიანობის შენარჩუნება. ქვეყნის წინაშე მდგარი საფრთხეების, კვალიფიციური კადრების აშკარა ნაკლებობის ფონზე და ასევე მიუხედავად, სამ სტრატეგიაში განათლების განვითარების მიმართულების მნიშვნელობის აღნიშვნისა, ქვეყანაში მაინც ვერ მოხერხდა კიბერუსაფრთხოების საგანმანათლებლო აკადემიური პროგრამების უფრო ფართოდ დანერგვა და განვითარება, თუ არ ჩავთვლით კავკასიის უნივერსიტეტის საბაკალავრო და ანდრია პირველწოდებულის სახლობის უნივერსიტეტის სამაგისტრო პროგრამებს [7].

ეს პროცესი დაკავშირებულია რიგ საკითხებთან. კერძოდ, ქვეყნის წამყვანი უნივერსიტეტები არის კერძო სექტორის წარმომადგენლები, რომლებისთვისაც ყოველი ახალი პროგრამის დანერგვა დაკავშირებულია გარკვეულ ფინანსურ დანახარჯებთან და, რომლებიც ყველა ამ პროცესს უყურებს მოგების მიღების გადასახედიდან, ანუ ორიენტირებულნი არიან მოგებაზე და ბიზნესის განვითარებაზე, და ეს ბუნებრივიც არის. ეს კი იძლევა იმის ვარაუდს, რომ კერძო უმაღლეს სასწავლებლებს ამ ეტაპზე არ უღირთ კიბერუსაფრთხოების მიმართულებით საბაკალავრო და სამაგისტრო პროგრამების დანერგვა, თუ მათ არ დაინახეს იქიდან წამოსული მოგება. მეორე მხარეა, სახელმწიფო, რომლის ინტერესებშიც შედის იყოლიოს მაღალი კვალიფიკაციის კადრები, რათა დააკომპლექტოს ის საჯარო სამსახურები, რომლებიც პასუხისმგებელნი არიან ქვეყნის კრიტიკული ინფრასტრუქტურის დაცვაზე და ასევე დააკომპლექტოს კრიტიკული ინფრასტრუქტურის სუბიექტები, რასაც ავალდებულებს კანონი „ინფორმაციული უსაფრთხოების შესახებ“.

აღსანიშნავია ის გარემოებაც, რომ კანონში „ინფორმაციული უსაფრთხოების შესახებ“ შესული ცვლილებების მიხედვით, არსებული კრიტიკული ინფრასტრუქტურის სუბიექტების ნუსხას დაემატა ასევე ორი კატეგორია კერძო სექტორიდან - სატელეკომუნიკაციო კომპანიები და კერძო სექტორის სხვა ინდუსტრიული მიმართულებები, რომლებსაც კანონის თანახმად, აქვთ ვალდებულება თავისთან იყოლიონ როგორც ინფორმაციული უსაფრთხოების მენეჯერები, ისე კიბერუსაფრთხოების სპეციალისტები.

ფაქტიურად, შეიძლება ითქვას, რომ ქვეყანაში სულ უფრო იზრდება მოთხოვნილება კიბერუსაფრთხოების და მათ შორის ასევე, ინფორმაციული უსაფრთხოების მაღალი კვალიფიკაციის კადრების მიმართ. თუმცა სახელმწიფოს მხრიდან ამ მიმართულებით სამწუხაროდ ვერ მოხერხდა ვერც ერთ სახელმწიფო უმაღლეს სასწავლებელში შესაბამისი პროგრამების ჩამოყალიბება და განვითარება. სტუდენტები და კურსდამთავრებულები თავად ცდილობენ აიმაღლონ კვალიფიკაცია სხვადასხვა სერტიფიცირებული კურსების გავლით როგორც საერთაშორისო, ისე ლოკალურ დონეზე. თუმცა აქაც გარკვეულ პრობლემებს აწყდებიან, რადგან საერთაშორისო სერტიფიცირებული კურსები, რომლებიც ფაქტიურად სპეციალობას იძლევა, არის საკმაოდ ძვირადღირებული და ამავდროულად, ძალაშია გარკვეულ პერიოდზე. ხოლო ლოკალურ დონეზე არსებული კურსები[9] არ იძლევა იმ დონის კვალიფიკაციას, რომ შესაძლებელი იყოს კარგად დასაქმება. სამწუხაროდ, არც სახელმწიფო არ სთავაზობს რაიმე სახის კვალიფიკაციის ასამაღლებელ კურსებს. აქვე უნდა აღინიშნოს დონორი ორგანიზაციების მიერ

[9] ფაქტიურად, შეიძლება ითქვას, რომ სულ ორი ორგანიზაციაა, რომელიც იძლევა შედარებით კარგ განათლებას სხვადასხვა სერტიფიცირებული კურსების შეთავაზებით. კერძოდ, ესენია Scientific Cyber Security Association https://scsa.ge/en/ და IT Academy Step https://ge.itstep.org/

დაფინანსებული კიბერუსაფრთხოების პროგრამა, რომელიც საქართველოს უნივერსიტეტის ინფორმაციული ტექნოლოგიების კოლეჯში ხორციელდება [8-9].

4. დასკვნა

ფაქტიურად, მოცემული მიმართულებით დარღვეული არის კავშირი საჯარო, კერძო სექტორსა და აკადემიურ წრეებს შორის, როცა ამ უკანასკნელისთვის შეიძლება თავად სახელმწიფო ყოფილიყო დამკვეთი მისთვის აუცილებელი კადრების მომზადებასა და გადამზადებაში. არ შეიძლება არ აღინიშნოს ასევე თანამშრომლობის აუცილებლობა სამეცნიერო კვლევების ჩატარების მიმართულებითაც, რაც დღეს ფაქტიურად საერთოდ მოშლილია და არ ტარდება აკადემიური დონის სამეცნიერო კვლევითი საქმიანობა.

მსგავსი თანამშრომლობა იქნებოდა ე. წ. „სტეიქჰოლდერიზმის“ კარგი მაგალითი, რაც ასე აპრობირებულია დასავლეთში[10]. ეს არის აუცილებელი როგორც დარგის აკადემიურ დონეზე განვითარებისთვის, ისე ზოგადად, ქვეყნის კრიტიკული ინფრასტრუქტურის დაცულობის მაქსიმალურად გაზრდისთვის.

შეიძლება ითქვას, რომ კიბერუსაფრთხოების განვითარებისა და მდგრადობის შენარჩუნებისთვის მის ყველა ცალკეულ მიმართულებაზე, აუცილებელი არის შესაბამისი განათლებული და კვალიფიციური კადრების არსებობა, რაც თავის მხრივ უზრუნველყოფს კრიტიკული ინფრასტრუქტურის დაცულობის გაზრდას როგორც გლობალურ, ისე ეროვნულ დონეზე.

გამოყენებული ლიტერატურა

1. სვანაძე ვ. „კიბერუსაფრთხოების ახალი გამოწვევები და საქართველო“, 2022
2. სვანაძე ვ., გოცირიძე ა., კიბერ თავდაცვა: კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და ახალი გამოწვევები, თბილისი, 2015
3. ნაფეტვარიძე ვ., „ელექტრონული მმართველობის დანერგვა საქართველოში: პრობლემები და პერსპექტივები“, 2020
4. ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, „კიბერშეტევა ჯანდაცვის სამინისტროზე და რუსული კვალი“, 2020
5. Schwartz N., “Georgia health system's operations disrupted by cyberattack”, 2023
6. The Global Risks Report 2021, 16th Edition of the World Economic Forum, In partnership with Marsh McLennan, SK Group and Zurich Insurance Group, 19 January, 2021
7. GUIDE TO GOOD GOVERNANCE IN CYBERSECURITY, DCAF Business and Security Division, Directorate for Security Cooperation and Defence (DCSD) of the French Ministry of Europe and Foreign Affairs, 19 January, 2021
8. Cybersecurity education in a developing nation: the Ecuadorian environment, Frankie E. Catota1,2,*, M. Granger Morgan1 and Douglas C. Sicker, Journal of Cybersecurity, 2019.

[10] „მულტი სტეიქჰოლდერიზმი“, ანუ ყველა დაინტერესებული მხარის (საჯარო და კერძო სექტორები, სამოქალაქო საზოგადოება და აკადემიური წრეები) ჩართულობა და ერთობლივი თანამშრომლობა კონკრეტული დარგის განვითარებისთვის.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 60 – 76 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

გამოწვევების დაძლევა და ეფექტური კიბერუსაფრთხოების განათლების განხორციელება საშუალო სკოლებში

ზურაბ ჯიშკარიანი
Scientific Cyber Security Association

აბსტრაქტი: დღევანდელ ციფრულ ეპოქაში კიბერუსაფრთხოება სულ უფრო მნიშვნელოვანი ხდება როგორც ადამიანებისთვის, ასევე კერძო სექტორისთვის და ზოგადად ქვეყნისთვის. კიბერ საფრთხეების ზრდასთან ერთად, როგორებიცაა ჰაკინგი, პირადი ინფორმაციის ქურდობა და მონაცემთა გაჟონვა, აუცილებელია ადამიანებმა იცოდნენ, როგორ დაიცვან საკუთარი თავი და ინფორმაცია ონლაინში. თუმცა, კიბერუსაფრთხოების განათლება ჯერ კიდევ არ არის ფართოდ ინტეგრირებული საშუალო სკოლების სასწავლო გეგმასთან, რის გამოც მოსწავლეები დაუცველნი არიან კიბერ საფრთხეების წინაშე. ეს კვლევითი ნაშრომი მიზნად ისახავს საშუალო სკოლებში კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობის შესწავლასა და ახალგაზრდა სტუდენტებისთვის კიბერუსაფრთხოების სწავლების საუკეთესო პრაქტიკისა და სტრატეგიების იდენტიფიცირებას. ნაშრომი ასევე შეისწავლის საშუალო სკოლებში კიბერუსაფრთხოების განათლების დანერგვის ბარიერებსა და გამოწვევებს და ამ კონტექსტში კიბერუსაფრთხოების განათლების გაუმჯობესების რეკომენდაციებს.

საკვანძო სიტყვები: კიბერუსაფრთხოების განათლება, საშუალო სკოლა, საშუალო სკოლის სასწავლო გეგმა, საგანმანათლებლო მოდელები, ბარიერები და გამოწვევები

ABSTRACT: In the contemporary era characterized by pervasive digitization, the significance of cybersecurity has escalated markedly for individuals, the private sector, and the broader national landscape. Given the proliferation of cyber threats, encompassing hacking, identity theft, and data breaches, it is imperative that individuals possess the requisite knowledge to safeguard themselves and their online information. Nevertheless, the incorporation of cybersecurity education within the secondary school curriculum remains notably limited, rendering students susceptible to cyber threats. This research paper endeavors to scrutinize the existing landscape of cybersecurity education within secondary schools, aiming to identify optimal practices and strategies for imparting cybersecurity knowledge to young students. Additionally, the paper investigates the impediments and challenges associated with integrating cybersecurity education into secondary schools, proposing recommendations to enhance the effectiveness of cybersecurity education within this educational context.

KEYWORDS*:* Cybersecurity Education, Secondary School, Secondary School Curriculum, Educational Models, Obstacles and Difficulties

1. შესავალი

კიბერუსაფრთხოების განათლების მზარდი მნიშვნელობის მიუხედავად, საშუალო სკოლებში მისი ეფექტური დანერგვა მნიშვნელოვან გამოწვევად რჩება. ამ პრობლემას რამდენიმე ფაქტორი უწყობს ხელს, მათ შორის შეზღუდული რესურსები, მასწავლებელთა მომზადების ნაკლებობა და ასაკისთვის შესაბამისი და საინტერესო მასალების დეფიციტი. პირველ რიგში, ბევრ სკოლას აქვს შეზღუდული რესურსი კიბერუსაფრთხოების განათლების დაფინანსებისთვის. მათ შეიძლება არ ჰქონდეთ დაფინანსება საჭირო

აღჭურვილობის შესაძენად ან კვალიფიცირებული პერსონალის დაქირავებლად. გარდა ამისა, ზოგიერთი სკოლისთვის შეიძლება პრიორიტეტული იყოს სხვა საგნები, როგორებიცაა:მათემატიკა, მეცნიერება და უცხო ენების შესწავლა, ვიდრე კიბერუსაფრთხოების განათლება. მეორეც, მასწავლებელთა უმრავლესობას შეიძლება არ ჰქონდეს გავლილი საკმარისი ტრენინგი კიბერუსაფრთხოების ეფექტურად სწავლებისთვის.შესაბამისად არ ჰქონდეთ საგნის სწავლებისთვის საჭირო ცოდნა ან უნარები, რამაც შეიძლება გამოიწვიოს კიბერუსაფრთხოების სწავლებისადმი ნდობის ნაკლებობა. უფრო მეტიც, კიბერუსაფრთხოების განათლება მუდმივად განვითარებადი სფეროა და შეიძლება რთული იყოს უახლესი ტენდენციებისა და ტექნოლოგიების შენარჩუნება. მესამე, საშუალო სკოლებში კიბერუსაფრთხოების სწავლებისთვის ასაკის შესაბამისი და საინტერესო მასალების დეფიციტია. ბევრი არსებული მასალა ძალიან რთულია საშუალო სკოლის მოსწავლეებისთვის, რაც ართულებს მათ ეფექტურად ჩართვას. გარდა ამისა, მასალები შეიძლება არ იყოს შემუშავებული ინტერაქტიულ და ექსპერიმენტულ სწავლებაზე ფოკუსირებით, რაც აუცილებელია მცირეწლოვანი მოსწავლეებისთვის.

Introduction

The effective implementation of cybersecurity education in secondary schools poses a substantial challenge despite its increasing significance. Numerous factors contribute to this challenge, encompassing limited resources, inadequate teacher training, and a dearth of age-appropriate and engaging instructional materials.

Primarily, the constraint of limited resources within schools impedes the integration of comprehensive cybersecurity education. Insufficient funding may hinder the acquisition of requisite equipment and the recruitment of qualified staff dedicated to cybersecurity education. Furthermore, competing priorities, such as emphasis on subjects like mathematics, science, and foreign languages, may divert attention and resources away from cybersecurity education initiatives.

Secondarily, a significant proportion of educators may lack the requisite training for effectively teaching cybersecurity. The deficiency in training may result in a deficiency of knowledge and skills necessary to impart the subject matter, leading to a lack of confidence among educators. Additionally, the dynamic nature of cybersecurity, characterized by continual evolution and technological advancements, compounds the challenge of educators staying abreast of the latest trends and technologies.

Tertiary to these challenges is the insufficiency of age-appropriate and engaging instructional materials tailored for teaching cybersecurity in secondary schools. Existing materials often prove overly complex for elementary school students, impeding effective engagement. Furthermore, these materials may lack a focus on interactive and experiential learning methods, which are pivotal for the engagement and understanding of young learners.

2. კვლევის მიზანი

ეს კვლევა არ არის იმის შესახებ, თუ როგორ ისწავლება კიბერუსაფრთხოება საშუალო სკოლებში. ამ კვლევის მიზანია საშუალო სკოლის მოსწავლეებში კიბერუსაფრთხოების სწავლასთან დაკავშირებით არსებული მდგომარეობისა და გამოწვევების იდენტიფიცირება. კერძოდ, ეს კვლევა მიზნად ისახავს:

- გამოვიკვლიოთ კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობა საშუალო სკოლებში.
- შევისწავლოთ კიბერუსაფრთხოების განათლების თეორიები და მოდელები.
- საშუალო სკოლის მოსწავლეებისთვის კიბერუსაფრთხოების სწავლების საუკეთესო პრაქტიკისა და სტრატეგიების იდენტიფიცირება.

- გამოვიკვლიოთ ბარიერები და გამოწვევები საშუალო სკოლებში კიბერუსაფრთხოების განათლების განხორციელებისას.

ამ კვლევის შედეგები სასარგებლო იქნება პედაგოგებისთვის, სასწავლო გეგმის შემქმნელებისთვის და სხვა დაინტერესებული მხარეებისთვის, რომლებიც დაინტერესებულნი არიან საშუალო სკოლებში კიბერუსაფრთხოების განათლების გაუმჯობესებით. მიმდინარე გამოწვევებისა და საუკეთესო პრაქტიკის იდენტიფიცირებით, ამ კვლევას შეუძლია საშუალო სკოლის მოსწავლეებისთვის ეფექტური კიბერუსაფრთხოების საგანმანათლებლო პროგრამების შემუშავება.

Purpose of the Research

This investigation does not center on the pedagogical approaches employed in teaching cybersecurity within secondary schools. Rather, the primary objective of this study is to discern the prevailing circumstances and confrontations associated with the acquisition of cybersecurity knowledge among secondary school students. Specifically, the study aims to:
• Scrutinize the present state of cyber security education within secondary school settings.
• Investigate theoretical frameworks and models pertinent to cyber security education.
• Ascertain optimal practices and methodologies for imparting cybersecurity knowledge to secondary school students.
• Investigate impediments and challenges encountered in the implementation of cybersecurity education within secondary schools.
The outcomes of this research will prove beneficial to educators, curriculum developers, and other stakeholders invested in advancing cybersecurity education in secondary schools. Through the identification of extant challenges and effective practices, this study has the potential to guide the formulation of impactful cybersecurity education programs tailored for secondary school students.

3. კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობა საშუალო სკოლებში

ბოლო კვლევებმა აჩვენა, რომ კიბერუსაფრთხოების განათლებას არ ექცევა საკმარისი ყურადღება საშუალო სკოლებში, მიუხედავად კიბერუსაფრთხოების მზარდი მნიშვნელობისა. Cyber.org-ის 2020 წლის ანგარიშის მიხედვით,K-12 პედაგოგებს შორის ჩატარებულმა გლობალურმა გამოკითხვამ აჩვენა მასწავლებლების მხოლოდ 20% გრძნობს თავს თავდაჯერებულად კიბერუსაფრთხოების თემების სწავლებაში (Cyber.org, "The State of Cybersecurity Education in K- 12 სკოლა“).
შეერთებულ შტატებში, განათლების სტატისტიკის ეროვნული ცენტრის 2022 წლის გამოკითხვამ დაადგინა, რომ საშუალო სკოლების 10%-ზე ნაკლები სთავაზობს კიბერუსაფრთხოების სპეციალურ კურსებს (წყარო: NCES, "საშუალო სკოლის კურსების ხელმისაწვდომობა და შეთავაზებები").
მკვეთრად საპირისპირო ხდება ესტონეთში,სადაც,სავალდებულოა კიბერუსაფრთხოების სასწავლო პროგრამა ყველა მოსწავლისთვის საბავშვო ბაღიდან საშუალო სკოლამდე (OECD, "Estonia: Country Review of Education Policy"). სინგაპური იღებს ეტაპობრივ მიდგომას, აერთიანებს კიბერჰიგიენის ძირითად კონცეფციებს არსებულ საგნებში, როგორიცაა IT და სოციალური კვლევები, ხოლო ასევე გთავაზობთ კიბერუსაფრთხოების მოწინავე კურსებს ზედა საშუალო საფეხურზე (სინგაპურის განათლების სამინისტრო, "კიბერუსაფრთხოების განათლების ჩარჩო").

მთლიანობაში, ეს კვლევები მიუთითებს იმაზე, რომ საჭიროა მეტი ყურადღება მიექცეს საშუალო სკოლებში კიბერუსაფრთხოების განათლებას და მოხდეს უფრო თანმიმდევრული და ყოვლისმომცველი სტანდარტების შემუშავება და დანერგვა.

The Contemporary Landscape of Cybersecurity Education in Secondary Schools

Recent research has highlighted the inadequate emphasis placed on cybersecurity education within secondary school curricula, despite the increasing significance of cybersecurity. A global survey conducted among K-12 educators revealed that, according to a 2020 report by Cyber.org, only 20% of educators worldwide feel confident in teaching cybersecurity topics (Cyber.org, "The State of Cybersecurity Education in K-12 Schools").
In the United States, a 2022 survey by the National Center for Education Statistics found that fewer than 10% of high schools offer dedicated cybersecurity courses (NCES, "High School Course Availability and Offerings").
In stark contrast, Estonia, a global leader in cybersecurity education, mandates a cybersecurity curriculum for all students from kindergarten through high school (OECD, "Estonia: Country Review of Education Policy").
Singapore adopts a tiered approach, integrating basic cyber hygiene concepts into existing subjects such as IT and social studies, while also offering advanced cybersecurity courses at the upper secondary level (Singapore Ministry of Education, "Cybersecurity Education Framework").
Overall, these data indicate that more attention should be paid to secondary education in circulation and the development and implementation of comprehensive standards.

4. თეორიები და საუკეთესო პრაქტიკები საშუალო სკოლის მოსწავლეებისთვის კიბერუსაფრთხოების სწავლებისთვის

კიბერუსაფრთხოების ეფექტური განათლება საშუალო სკოლებში უნდა იყოს დაფუძნებული თეორიებსა და მოდელებზე, რომლებიც ასახავენ პროგრამის შემუშავებასა და განხორციელებას. არსებობს რამდენიმე თეორია და მოდელი, რომლებიც დაკავშირებულია კიბერუსაფრთხოების განათლებასთან, მათ შორის:
კონსტრუქტივისტული სწავლის თეორია: ეს თეორია ხაზს უსვამს ექსპერიმენტული და ინტერაქტიული სწავლის მნიშვნელობას, ხელი შეუწყოს მოსწავლეთა ჩართულობასა და გაგებას. კიბერუსაფრთხოების განათლების კონტექსტში, კონსტრუქტივისტული სწავლება შეიძლება მოიცავდეს ისეთ აქტივობებს, როგორებიცაა:სიმულაციები, თამაშები და პრაქტიკული აქტივობები, რომლებიც საშუალებას აძლევს მოსწავლეებს ისწავლონ პრაქტიკით.
სოციალური სწავლის თეორია: კიბერუსაფრთხოების განათლების კონტექსტში, სოციალური სწავლება შეიძლება მოიცავდეს თანატოლებზე დაფუძნებულ სასწავლო აქტივობებს, როგორებიცაა ჯგუფური დისკუსიები ან ერთობლივი პროექტები.
კოგნიტური დატვირთვის თეორია: ეს თეორია ფოკუსირებულია გონებრივი ძალისხმევის რაოდენობაზე, რაც საჭიროა ახალი ინფორმაციის დასამუშავებლად. კიბერუსაფრთხოების განათლების კონტექსტში, შემეცნებითი დატვირთვის მართვა შესაძლებელია ინფორმაციის მართვად ნაწილებში წარდგენით, სწავლის მხარდასაჭერად მულტიმედიური რესურსების გამოყენებით და მოსწავლეებისთვის მიწოდებული რთული ცნებების გასაგებად.
ადამიანზე ორიენტირებული დიზაინი: ეს მოდელი ხაზს უსვამს ინტუიციური და მარტივად გამოსაყენებელი პროდუქტებისა და სერვისების დიზაინის მნიშვნელობას. კიბერუსაფრთხოების განათლების კონტექსტში, ადამიანზე ორიენტირებული დიზაინი შეიძლება მოიცავდეს ასაკის შესაბამის და საინტერესო მასალებს, რომლებიც შექმნილია ახალგაზრდა მოსწავლეების საჭიროებებისა და ინტერესების გათვალისწინებით.

კიბერუსაფრთხოების ჩარჩოები: ეს არის კიბერუსაფრთხოების რისკების იდენტიფიცირების, შეფასებისა და მართვის სისტემატური მიდგომები. კიბერუსაფრთხოების განათლების კონტექსტში, კიბერუსაფრთხოების ჩარჩოებს შეუძლიათ უზრუნველყონ სასარგებლო სტრუქტურა კიბერუსაფრთხოების ძირითადი კონცეფციებისა და უნარების ორგანიზებისა და სწავლებისთვის.
ამ თეორიებისა და მოდელების ჩართვით, კიბერუსაფრთხოების საგანმანათლებლო პროგრამების შემუშავებასა და განხორციელებაში, პედაგოგებს შეუძლიათ შექმნან უფრო ეფექტური და მიმზიდველი სასწავლო გეგმა საშუალო სკოლის მოსწავლეებისთვის.

Theoretical Frameworks and Optimal Approaches for Imparting Cybersecurity Education to Secondary School Students

The provision of effective cybersecurity education in elementary schools necessitates a foundation built upon pertinent theories and models guiding program development and execution. Various theories and models relevant to cybersecurity education are as follows:
Constructivist Learning Theory: Emphasizing experiential and interactive learning, this theory underscores the significance of engaging students in activities such as simulations, games, and hands-on experiences within the realm of cybersecurity education, fostering learning through practical application.
Social Learning Theory: Within the context of cybersecurity education, social learning involves activities such as peer-based learning through group discussions or collaborative projects, facilitating knowledge acquisition through interpersonal interactions.
Cognitive Load Theory: Focused on managing the mental effort required for processing new information, this theory suggests strategies such as presenting information in manageable segments, utilizing multimedia resources to support learning, and simplifying complex concepts for students in the field of cybersecurity education.
Human-Centered Design: This model accentuates the creation of intuitive and user-friendly products and services. In the context of cybersecurity education, employing human-centered design involves developing age-appropriate and captivating materials aligned with the needs and interests of young learners.
Cybersecurity Frameworks: These systematic approaches are employed to identify, assess, and manage cybersecurity risks. In the realm of cybersecurity education, these frameworks serve as valuable tools for structuring and imparting essential cybersecurity concepts and skills.
By incorporating these theories and models into the planning and execution of cybersecurity education programs, educators can craft a curriculum that is not only more effective but also more engaging for middle school students.

5. კიბერუსაფრთხოების განათლების განხორციელების ბარიერები და გამოწვევები

საშუალო სკოლებში კიბერუსაფრთხოების განათლების მნიშვნელობის მიუხედავად, არსებობს რამდენიმე ბარიერი და გამოწვევა, რამაც შეიძლება გაართულოს პროგრამების ეფექტურად განხორციელება. აქ არის რამდენიმე გავრცელებული ბარიერი და გამოწვევა:
შეზღუდული რესურსები: ბევრ საშუალო სკოლას აქვს შეზღუდული რესურსები, მათ შორის დაფინანსება, პერსონალი და ტექნოლოგიური ინფრასტრუქტურა. ამან შეიძლება გაართულოს კიბერუსაფრთხოების საგანმანათლებლო პროგრამების შემუშავება და განხორციელება.
მასწავლებელთა ტრენინგების ნაკლებობა: მასწავლებლებს შეიძლება არ ჰქონდეთ გავლილი საჭირო ტრენინგი ან აკლდეთ გამოცდილება კიბერუსაფრთხოების ეფექტურად სწავლებისთვის. ამან შეიძლება გაართულოს შემუშავება საინტერესო და ეფექტური გაკვეთილების , რომელებიც აკმაყოფილებს მოსწავლეების საჭიროებებს.

ცვლილებებისადმი წინააღმდეგობა: სკოლები შეიძლება იყოს რეზისტენტული ცვლილებების მიმართ, განსაკუთრებით თუ კიბერუსაფრთხოების განათლება განიხილება, როგორც დამატებითი საგანი, ტრადიციული სასწავლო გეგმის მიღმა. ამან შეიძლება გაართულოს კიბერუსაფრთხოების საგანმანათლებლო ინიციატივების მხარდაჭერა.

სწრაფად ცვალებადი ტექნოლოგია: ტექნოლოგია მუდმივად ვითარდება და სკოლებისთვის შეიძლება რთული იყოს უახლესი მოვლენებისა და საფრთხეების ტემპის შენარჩუნება. ამან შეიძლება გაართულოს კიბერუსაფრთხოების საგანმანათლებლო პროგრამების შემუშავება და განხორციელება.

მშობლების შეზღუდული ჩართულობა: მშობლები გადამწყვეტ როლს ასრულებენ კიბერუსაფრთხოების საგანმანათლებლო სწავლებაში,მაგრამ ბევრმა მშობელმა შეიძლება არ იცოდეს ონლაინ აქტივობასთან დაკავშირებული რისკები ან შეიძლება არ ჰქონდეს საჭირო ცოდნა შვილების სწავლის მხარდასაჭერად.

სასწავლო გეგმის არ არსებობა: ამ ბარიერებისა და გამოწვევების გადაჭრა მოითხოვს მრავალმხრივ მიდგომას, რომელიც მოიცავს თანამშრომლობას პედაგოგებს, მშობლებსა და სასწავლო გეგმის შემქმნელებს შორის. ეს შეიძლება მოიცავდეს მასწავლებლებისთვის დამატებითი რესურსებისა და ტრენინგების მიწოდებას, მშობლების ჩართვას კიბერუსაფრთხოების განათლების მცდელობებში და პოლიტიკის მხარდაჭერას, რომელიც პრიორიტეტს ანიჭებს კიბერუსაფრთხოების განათლებას საშუალო სკოლებში. ამ გამოწვევების გადაჭრით ჩვენ შეგვიძლია,შევქმნათ დაცული და უსაფრთხო ონლაინ გარემო მოსწავლეებისთვის..

Obstacles and Difficulties in the Implementation of Cybersecurity Education

Despite the significance of cybersecurity education in elementary schools, various impediments and challenges hinder the effective implementation of programs. The following outlines prevalent barriers and challenges:

Limited Resources: Numerous elementary schools face constraints in terms of resources, encompassing funding, personnel, and technological infrastructure. This limitation complicates the formulation and execution of cybersecurity education programs.

Insufficient Teacher Training: Educators may lack the requisite training or experience to proficiently deliver cybersecurity education. This deficiency hampers the creation of engaging and effective lessons tailored to students' needs.

Resistance to Change: Educational institutions may exhibit resistance to change, particularly if cybersecurity education is perceived as an additional subject outside the conventional curriculum. This resistance poses challenges to endorsing initiatives related to cybersecurity education.

Rapid Technological Evolution: Technology undergoes continual advancements, rendering it challenging for schools to stay abreast of the latest developments and threats. This dynamic landscape complicates both the design and implementation of cybersecurity education programs.

Limited Parental Involvement: Parents play a pivotal role in cyber safety education. However, many may lack awareness of the risks associated with online activities or possess insufficient knowledge to support their children's learning.

Lack of Curriculum: Overcoming these barriers and challenges necessitates a comprehensive approach involving collaboration among educators, parents, and curriculum developers. Potential strategies include providing additional resources and training to teachers, engaging parents in cybersecurity education initiatives, and advocating for policies that prioritize cybersecurity education in elementary schools. By addressing these challenges, a secure online environment conducive to students' safety can be established.

6. კვლევის მეთოდოლოგია და შედეგები

გამოკითხვები: ინტერნეტზე დაფუძნებული გამოკითხვა გადანაწილდა საშუალო საფეხურის მასწავლებლებისა და სკოლის ადმინისტრაციის შემთხვევითი შერჩევით მთელი ქვეყნის მასშტაბით. კვლევაში მონაწილეობა მიიღო 269 რესპონდენტმა.
გამოკითხვა მოიცავდა კითხვებს მათ სკოლებში კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობის შესახებ, გამოკითხვა შემუშავდა გამოკითხვის კვლევის საუკეთესო პრაქტიკის გამოყენებით და ჩატარდა რეპუტაციის მქონე ონლაინ გამოკითხვის პლატფორმის მეშვეობით მონაცემთა უსაფრთხოებისა და კონფიდენციალურობის უზრუნველსაყოფად.

Research Methodology and Findings

Surveys: A web-based survey was disseminated to a randomly selected cohort of secondary school educators and administrators nationwide. 269 respondents took part in the research. This survey incorporated inquiries addressing the prevailing status of cybersecurity education within their respective educational institutions.
The survey instrument was meticulously crafted employing established best practices in survey research and was subsequently administered through a reputable online survey platform. This approach was undertaken to safeguard both data security and privacy throughout the data collection process.

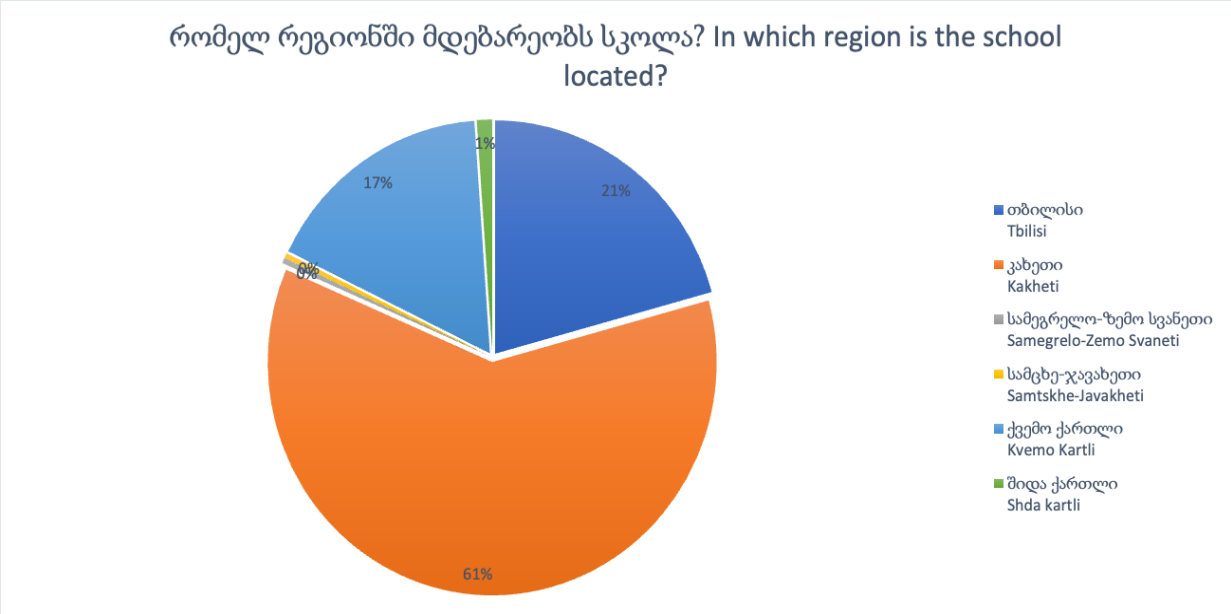


Fig.1. Question#1

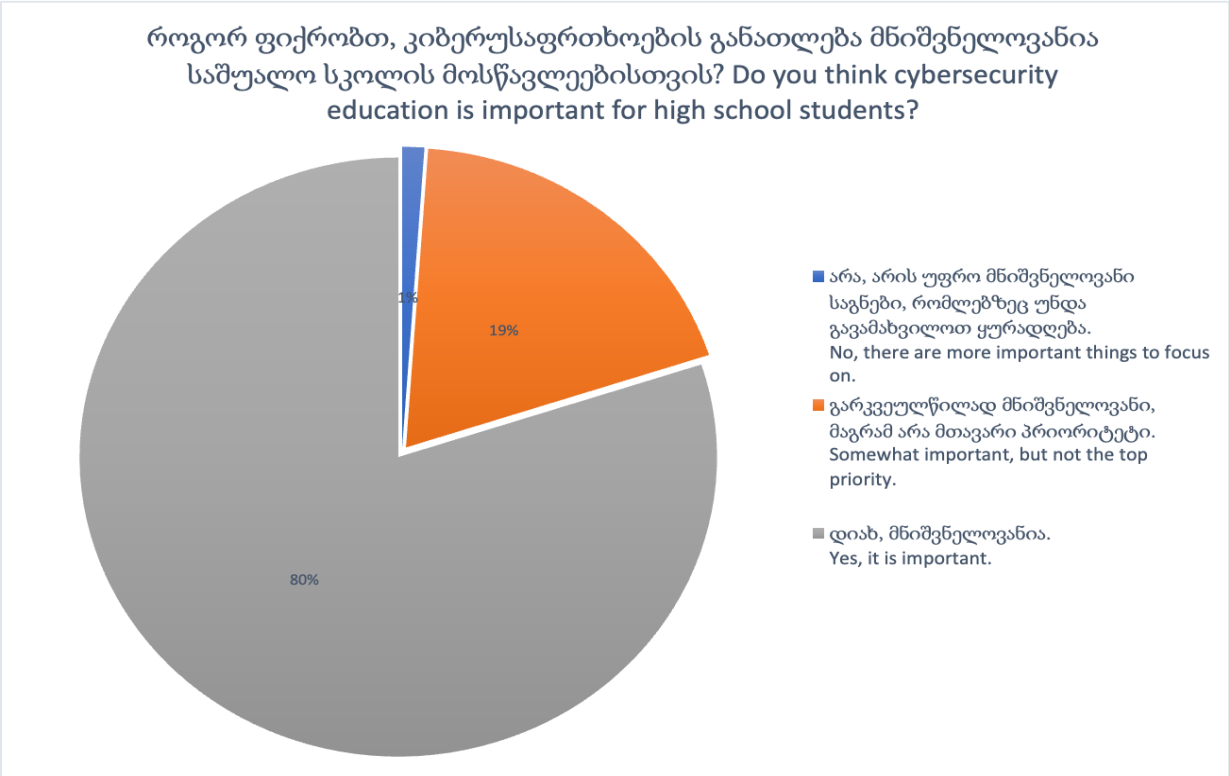


Fig.2. Question#2

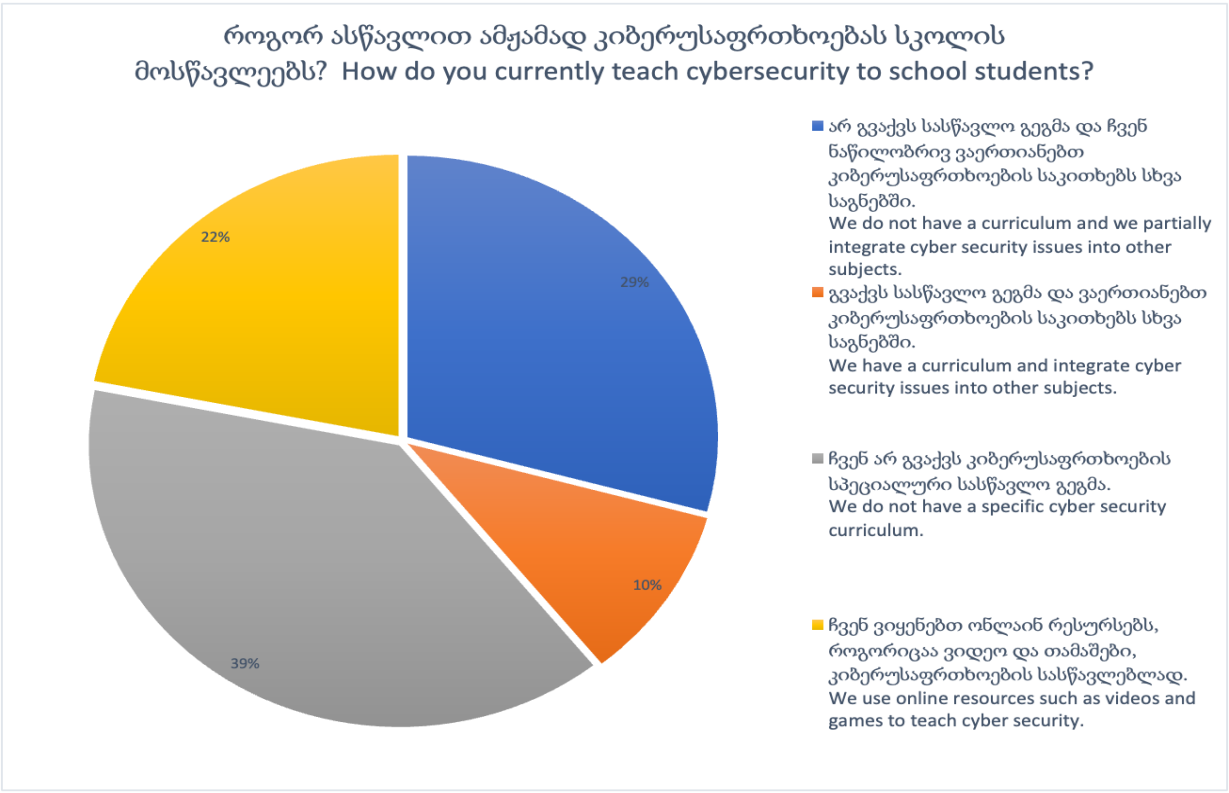


Fig.3. Question#3

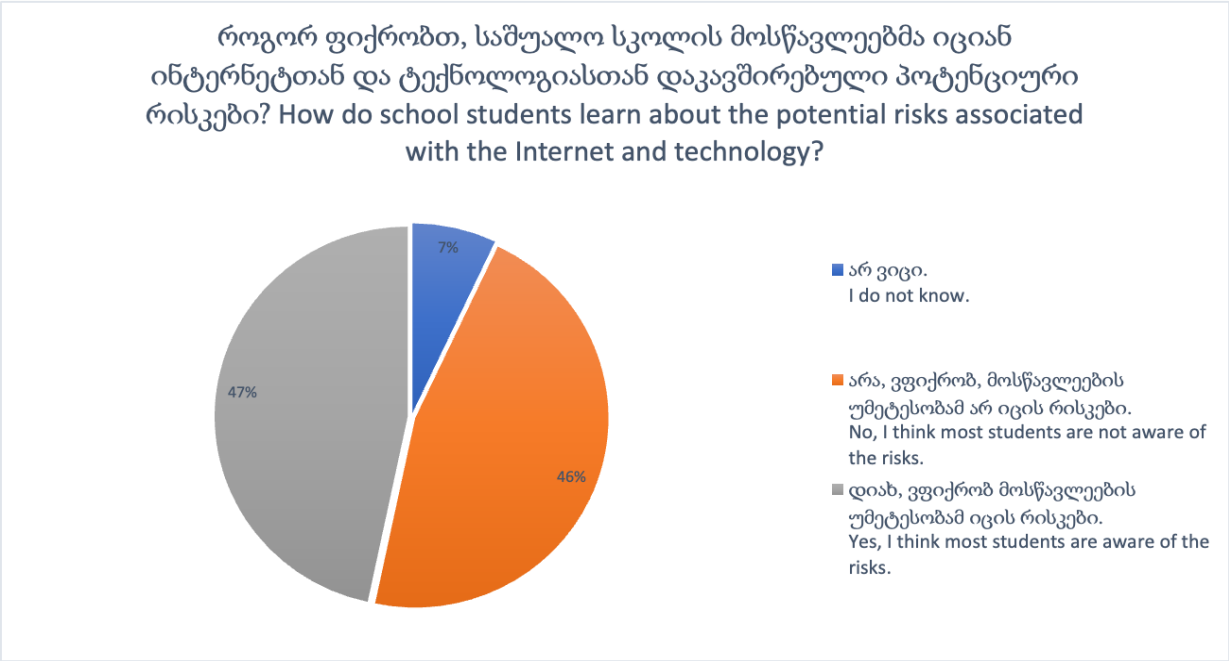


Fig.4. Question#4

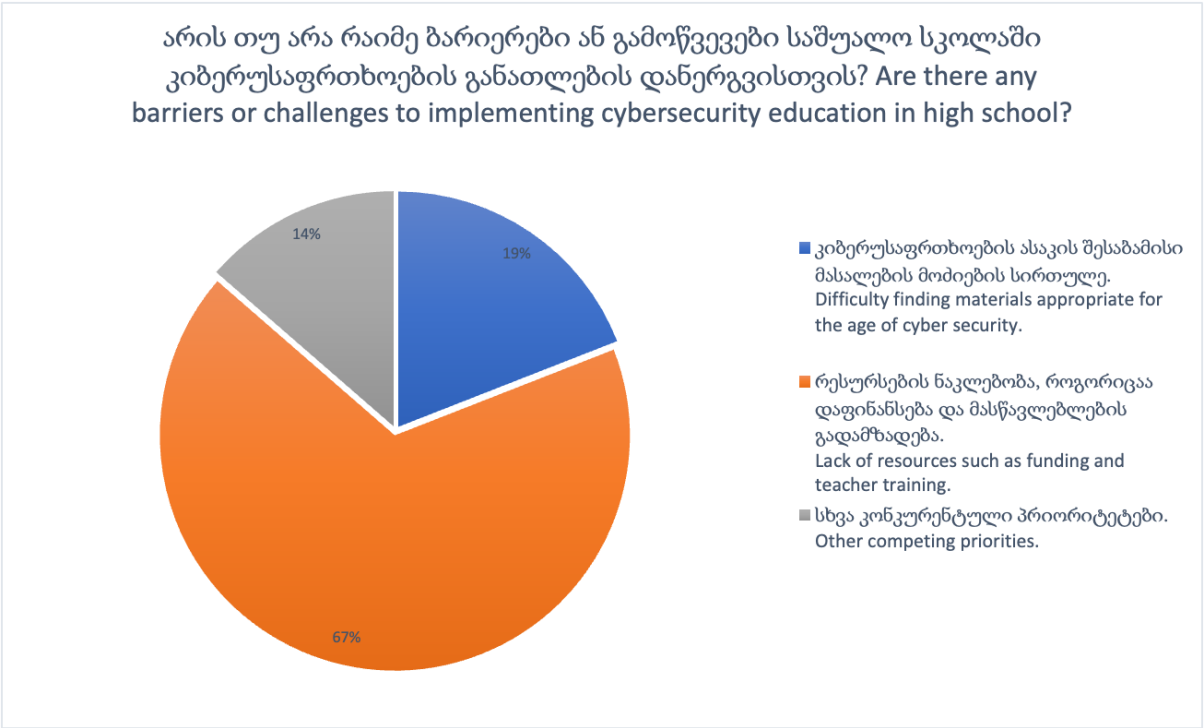


Fig.5. Question#5

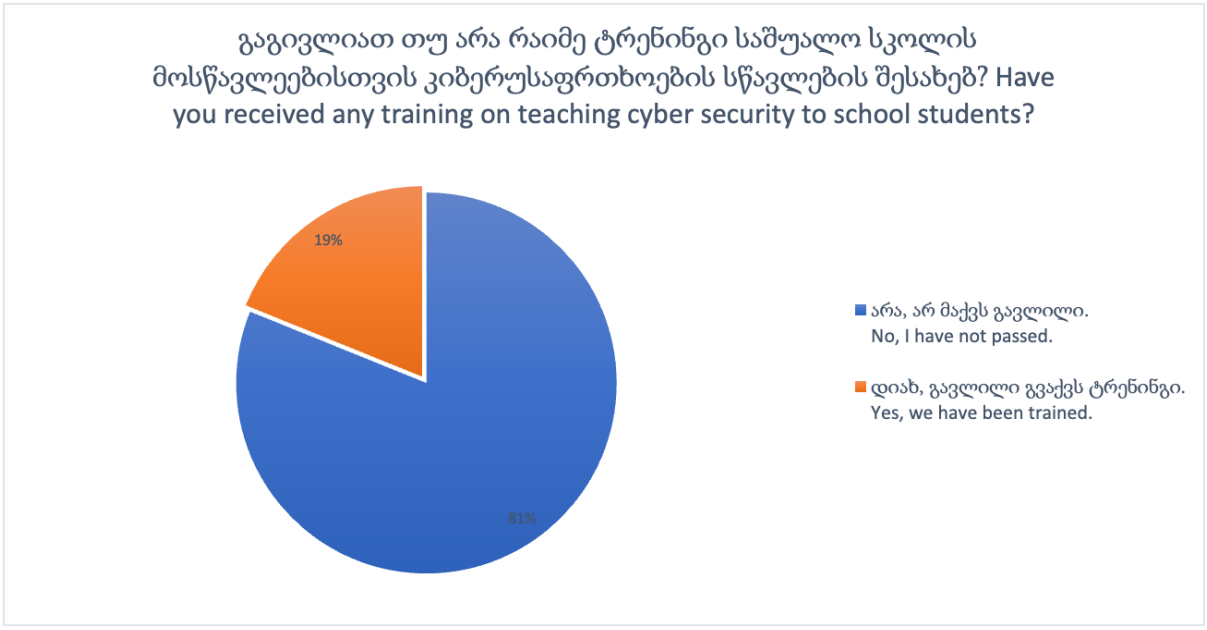


Fig.6. Question#6

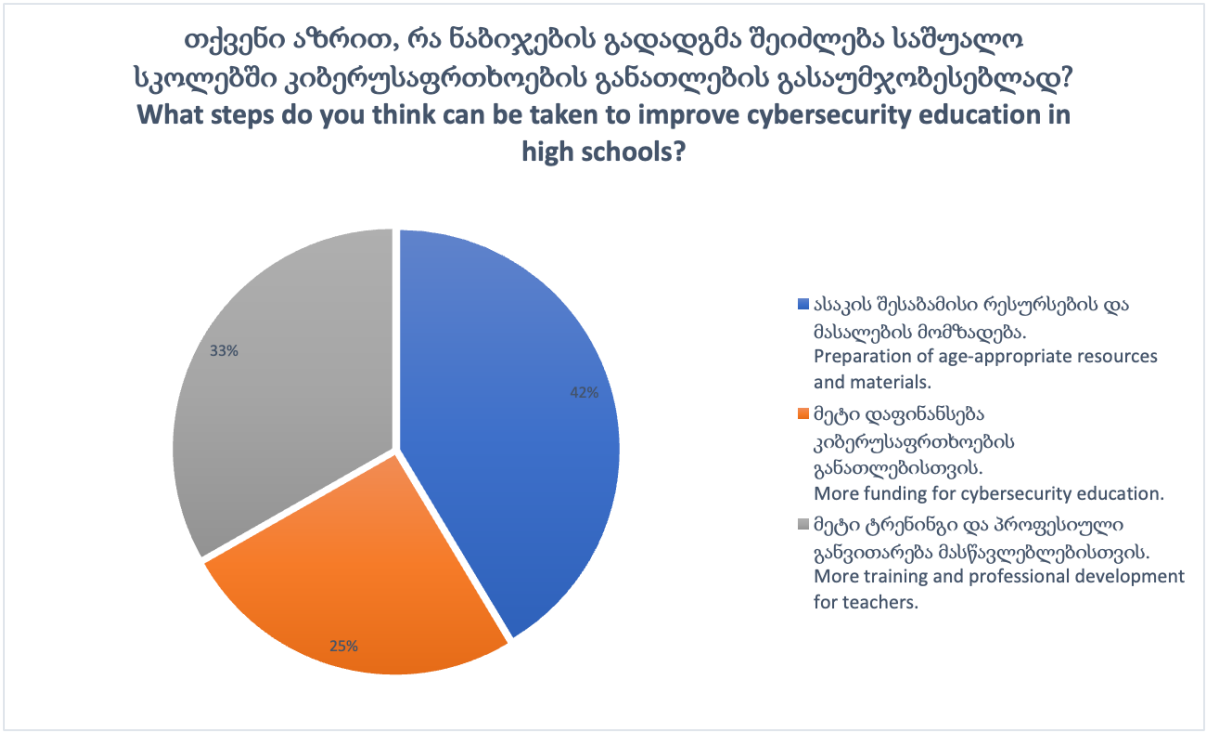


Fig.7. Question#7

7. შედეგების შეჯამება

გამოკითხვისა და ინტერვიუების შედეგად შეგროვებულმა მონაცემებმა გამოავლინა რამდენიმე ძირითადი სიახლე საშუალო სკოლებში კიბერუსაფრთხოების განათლების ამჟამინდელ მდგომარეობასთან დაკავშირებით. უპირველეს ყოვლისა, აღმოჩნდა, რომ

მიუხედავად იმისა, რომ ზოგიერთი სკოლა შეიცავს კიბერუსაფრთხოების განათლების გარკვეულ ფორმას თავის სასწავლო გეგმაში, არ არის თანმიმდევრულობა მიდგომებსა და გაშუქებულ თემებში.
მეორეც, დადგინდა, რომ მასწავლებლები ხშირად თავს მოუმზადებლად გრძნობდნენ კიბერუსაფრთხოების თემების სწავლებისთვის და არ ჰქონდათ საჭირო ტრენინგი და რესურსები ამის ეფექტურად გასაკეთებლად. ამან შეიძლება გამოიწვიოს მოსწავლეების ნდობისა და ჩართულობის ნაკლებობა.
მესამე, აღმოჩნდა, რომ არსებობს მნიშვნელოვანი ბარიერები სკოლებში ეფექტური კიბერუსაფრთხოების განათლების განსახორციელებლად, მათ შორის, დაფინანსებისა და მხარდაჭერის ნაკლებობა სკოლის რაიონებისა და ადმინისტრატორების მხრიდან და მშობლებსა და სხვა დაინტერესებულ მხარეებს შორის კიბერუსაფრთხოების განათლების მნიშვნელობის შესახებ ინფორმირებულობის ნაკლებობა.

Summary of Findings

The analysis of data derived from both survey responses and interviews has yielded noteworthy insights into the prevailing state of cybersecurity education within elementary schools. Firstly, the findings indicate that although many schools integrate some form of cybersecurity education into their curricula, there exists a notable lack of uniformity in the approaches employed and the specific topics addressed. Secondly, it has been observed that educators frequently express a sense of inadequacy in preparing for and delivering cybersecurity content, citing insufficient training and resources as contributing factors. This deficiency in preparedness has the potential to undermine the confidence and active participation of students.
Thirdly, substantial impediments to the successful implementation of cybersecurity education initiatives in schools have been identified. These obstacles encompass a dearth of financial backing and support from school districts and administrators, as well as a lack of awareness among parents and other stakeholders regarding the pivotal role of cybersecurity education.

8. კვლევის შედეგები საშუალო სკოლებში კიბერუსაფრთხოების განათლების შესახებ

ამ კვლევის შედეგებს მნიშვნელოვანი გავლენა აქვს საშუალო სკოლებში კიბერუსაფრთხოების განათლებაზე. შედეგები ვარაუდობს, რომ საგანი უნდა იყოს სუფრო ფორმალიზებული და ყოვლისმომცველი , რათა მოამზადოს ახალგაზრდა მოსწავლეები ციფრული ეპოქისთვის. ქვემოთ მოცემულია ამ კვლევის რამდენიმე ძირითადი შედეგი საშუალო სკოლებში კიბერუსაფრთხოების განათლებისთვის:
კიბერუსაფრთხოების ფორმალიზებული სასწავლო გეგმის საჭიროება: ამ კვლევის შედეგები ვარაუდობს, რომ საშუალოი სკოლების მხოლოდ მცირე პროცენტს აქვს კიბერუსაფრთხოების ფორმალური სასწავლო გეგმა ან პროგრამა. ეს ხაზს უსვამს მნიშვნელოვან ხარვეზს საშუალო სკოლებში კიბერუსაფრთხოების განათლებაში. აქედან გამომდინარე, საჭიროა შეიქმნას კიბერუსაფრთხოების ფორმალიზებული სასწავლო პროგრამა, რომელიც შეიძლება განხორციელდეს საშუალო სკოლებში, რათა უზრუნველყოფილი იყოს ახალგაზრდა მოსწავლეების ადეკვატურად მომზადება ციფრული ეპოქისთვის.
ტრენინგისა და პროფესიული განვითარების მნიშვნელობა: კვლევამ გამოავლინა მასწავლებლების პროფესიული განვითარებისა და კიბერუსაფრთხოების ტრენინგების საჭიროება. ეს მიუთითებს იმაზე, რომ მასწავლებლების ტრენინგსა და პროფესიულ განვითარებაში ინვესტირებას შეუძლია გააუმჯობესოს კიბერუსაფრთხოების განათლების ხარისხი საშუალო სკოლებში.

ასაკის შესაბამისი რესურსებისა და მასალების მნიშვნელობა: ამ კვლევამ გამოავლინა რომ სკოლებში არ არსებობს მოსწავლეებისთვის ასაკის შესაბამისი რესურსები და მასალები კიბერუსაფრთხოების შესახებ. აქედან გამომდინარე, საჭიროა შემუშავდეს ასაკის შესაბამისი რესურსები და მასალები, რომლებიც ადვილად ხელმისაწვდომი იქნება მასწავლებლებისა და მოსწავლეებისათვის.

კიბერუსაფრთხოების განათლების ინოვაციური მიდგომების მნიშვნელობა: ამ კვლევამ გამოავლინა,რომ საჭიროა კიბერუსაფრთხოების განათლებისადმი ინოვაციური მიდგომა, როგორიცაა გემიფიკაცია და პროექტზე დაფუძნებული სწავლება. ეს დასკვნები ვარაუდობს, რომ კიბერუსაფრთხოების განათლების შესახებ ინოვაციური მიდგომების ჩართვამ შეიძლება ის უფრო მიმზიდველი და ეფექტური გახადოს მოსწავლეებისთვის.

Research Findings on Cybersecurity Education in Secondary Schools

This study's outcomes bear significant implications for the realm of cybersecurity education within elementary schools. The findings underscore the necessity for a more formalized and comprehensive approach to equip young learners for the challenges of the digital age. The ensuing discussion delineates key discoveries pertinent to cybersecurity education in elementary schools:

Imperative for a Formalized Cybersecurity Curriculum:

The study indicates that merely a marginal percentage of elementary schools currently possess a formal cybersecurity curriculum or program. This observation accentuates a noteworthy void in cybersecurity education at the primary level. Consequently, there exists a compelling requirement to construct a formalized cyber safety curriculum tailored for implementation in secondary schools. This initiative aims to ensure that young students receive thorough preparation for navigating the complexities of the digital age.

Significance of Training and Professional Development:

A discernible need for professional development and cybersecurity training for teachers was identified through this study. This underscores the proposition that investing in teacher training and professional development endeavors can enhance the quality of cybersecurity education within secondary schools.

Relevance of Age-Appropriate Resources and Materials:

The research identifies a deficiency in age-appropriate resources and materials dedicated to educating students on cyber safety within school environments. Hence, it is imperative to conceive and develop resources and materials tailored to the specific age group, ensuring accessibility for both educators and students.

Importance of Innovative Approaches to Cybersecurity Education:

Findings from this study emphasize the necessity for innovative pedagogical approaches in cybersecurity education, such as gamification and project-based learning. The implication is that the incorporation of innovative methodologies can render cybersecurity education more engaging and efficacious for students.

9. რეკომენდაციები კიბერუსაფრთხოების განათლების გასაუმჯობესებლად

ამ კვლევის დასკვნებსა და შედეგებზე დაყრდნობით,შემოთავაზებული შემდეგი რეკომენდაციები საშუალ სკოლებში კიბერუსაფრთხოების განათლების გასაუმჯობესებლად:

კიბერუსაფრთხოების ფორმალიზებული სასწავლო გეგმის შემუშავება და განხორციელება: საშუალო სკოლებში კიბერუსაფრთხოების განათლების მნიშვნელოვანი ხარვეზის გათვალისწინებით, რეკომენდებულია კიბერუსაფრთხოების ფორმალიზებული სასწავლო გეგმის შემუშავება და დანერგვა ყველა საშუალო კლასში. სასწავლო პროგრამა უნდა იყოს ასაკის შესაბამისი, ყოვლისმომცველი და მოიცავდეს კიბერუსაფრთხოების

თემებს, მათ შორის ონლაინ უსაფრთხოებას, პაროლის უსაფრთხოებას და კიბერბულინგის.

უზრუნველყოს მასწავლებლების პროფესიული განვითარება და ტრენინგი: მასწავლებლები უნდა იყვნენ აღჭურვილი ცოდნითა და უნარებით, რათა ეფექტურად ასწავლონ კიბერუსაფრთხოება მოსწავლეებს. ამიტომ, რეკომენდებულია პროფესიული განვითარებისა და სატრენინგო პროგრამების შემუშავება და მიწოდება მასწავლებლებსთვის, რათა გააუმჯობესონ კიბერუსაფრთხოების კონცეფციების გაგება და შეისწავლონ როგორ ასწავლონ ისინი მოსწავლეებს.

ასაკის შესაბამისი რესურსების და მასალების შემუშავება: საშუალო სკოლებში კიბერუსაფრთხოების სწავლების მხარდასაჭერად, რეკომენდებულია ასაკის შესაბამისი რესურსების და მასალების შემუშავება. ეს რესურსები და მასალები უნდა იყოს ადვილად ხელმისაწვდომი, მიმზიდველი და სპეციალურად შექმნილი მოსწავლეებისთვის.

კიბერუსაფრთხოების განათლების ინოვაციური მიდგომების ჩართვა: კიბერუსაფრთხოების განათლების ინოვაციური მიდგომები, როგორიცაა გემიფიკაცია და პროექტზე დაფუძნებული სწავლება, ნაჩვენებია, რომ ეფექტურია მოსწავლეების ჩართვაში. ამიტომ, რეკომენდირებულია, რომ ეს მიდგომები ჩაერთოს საშუალო სკოლებში კიბერუსაფრთხოების განათლებაში, რათა ის უფრო მიმზიდველი და ეფექტური გახდეს.

პარტნიორობა მშობლებთან და მეურვეებთან: კიბერუსაფრთხოების განათლება არ უნდა შემოიფარგლოს საკლასო ოთახით. მშობლებსა და მეურვეებს , გადამწყვეტი როლი აქვთ სახლში კიბერუსაფრთხოების კონცეფციების განმტკიცებაში. ამიტომ, რეკომენდებულია სკოლების თანამშრომლობა მშობლებთან და მეურვეებთან, რათა მათ მიაწოდონ ცოდნა და რესურსები მშობლებს სახლში კიბერუსაფრთხოების განათლების მხარდასაჭერად.

Recommendations for Enhancing Cybersecurity Education

In light of the findings and outcomes derived from the present study, the following recommendations are posited to augment cybersecurity education within secondary school settings:

Development and Implementation of a Formalized Cybersecurity Curriculum:

In response to the discernible deficiency in cybersecurity education at the elementary level, it is advisable to devise and institute a structured cybersecurity curriculum encompassing all grades. This curriculum should be tailored to the age group, thorough in its coverage, and address pertinent cybersecurity subjects such as online safety, password security, and cyberbullying.

Provision of Professional Development and Training for Educators:

Recognizing the pivotal role of educators in imparting cybersecurity knowledge to students, it is imperative to offer professional development and training initiatives. These programs should be designed to enhance educators' proficiency in cybersecurity concepts, enabling them to effectively convey this knowledge to their students.

Development of Age-Appropriate Resources and Materials:

To facilitate the effective delivery of cybersecurity education in secondary schools, the creation of age-appropriate educational resources and materials is recommended. These resources should be readily accessible, engaging, and specifically tailored to the cognitive level of the learners.

Incorporation of Innovative Approaches to Cybersecurity Education:

Acknowledging the efficacy of innovative pedagogical strategies, such as gamification and project-based learning, it is advisable to integrate these approaches into secondary school cybersecurity education. Doing so is anticipated to enhance both the attractiveness and effectiveness of the educational process.

Collaboration with Parents and Guardians:

Recognizing the multifaceted nature of cybersecurity education, collaboration with parents and guardians is encouraged. Schools should actively engage with parents and guardians, providing them with knowledge and resources to reinforce cybersecurity concepts within the home environment. This

collaborative effort ensures a comprehensive approach to cybersecurity education that extends beyond the confines of the classroom.

10. კვლევის შეზღუდვები და მომავალი კვლევის მიმართულებები

ეს კვლევა იძლევა მნიშვნელოვან ინფორმაციას საშუალო სკოლებში კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობის შესახებ და გთავაზობთ რეკომენდაციებს მოსწავლეებისთვის კიბერუსაფრთხოების განათლების გასაუმჯობესებლად. თუმცა, ამ კვლევას აქვს რამდენიმე შეზღუდვა, რომელებიც გასათვალისწინებელია შედეგების ინტერპრეტაციისას. ეს შეზღუდვები მოიცავს:

ნიმუშის მცირე ზომა: ამ კვლევის შერჩევის ზომა შედარებით მცირე იყო, რამაც შესაძლოა შეზღუდოს დასკვნების განზოგადება. სამომავლო კვლევა მიზნად ისახავს სკოლების უფრო დიდი და მრავალფეროვანი ნიმუშის შეტანას, რათა დავინახოთ კიბერუსაფრთხოების განათლების მდგომარეობის უფრო სრულყოფილი სურათი.

თვითშედგენილი მონაცემები: ამ კვლევის მონაცემები შეგროვდა თვითშედგენილი გამოკითხვების მეშვეობით, რომლებიც შეიძლება ექვემდებარებოდეს მიკერძოებას ან სოციალურ სასურველ ეფექტს. სამომავლო კვლევამ უნდა განიხილოს მონაცემთა შეგროვების ალტერნატიული მეთოდების გამოყენება, როგორიცაა საკლასო ოთახში დაკვირვება ან ინტერვიუ მასწავლებლებთან და მოსწავლეებთან, რათა უზრუნველყოს საშუალო სკოლებში კიბერუსაფრთხოების განათლების უფრო ზუსტი და სიღრმისეული შესწავლა.

შეზღუდული სფერო: ეს კვლევა ფოკუსირებული იყო მხოლოდ საშუალო სკოლებში კიბერუსაფრთხოების განათლების მდგომარეობაზე და არ მოიცავდა კიბერუსაფრთხოების განათლების გავლენას მოსწავლეთა შედეგებზე. მომავალი კვლევა მიზნად ისახავს შეისწავლოს კიბერუსაფრთხოების განათლების სხვადასხვა მიდგომების ეფექტურობა მოსწავლეთა შედეგებზე, როგორებიცაა მათი ცოდნა, დამოკიდებულებები და კიბერუსაფრთხოებასთან დაკავშირებული ქცევები.

11. მომავალი კვლევის მიმართულებები მოიცავს:

გრძივი კვლევები: გრძივმა კვლევებმა შეიძლება მოგვაწოდოს კიბერუსაფრთხოების განათლების გრძელვადიანი გავლენა მოსწავლეების შედეგებზე, როგორებიცაა მათი ციფრული წიგნიერება და კიბერუსაფრთხოების ცნობიერება.

შედარებითი კვლევები: შედარებით კვლევებს შეუძლია შეადაროს საშუალო სკოლებში კიბერუსაფრთხოების განათლების სხვადასხვა მიდგომის ეფექტურობა, როგორიცაა ტრადიციული საკლასო სწავლება ინოვაციურ მიდგომებთან, გემიფიკაცია ან პროექტზე დაფუძნებული სწავლება.

კულტურათაშორისი კვლევები: კულტურათაშორისმა კვლევებმა შეიძლება შეისწავლოს კიბერუსაფრთხოების განათლების მსგავსება და განსხვავებები სხვადასხვა კულტურებსა და ქვეყნებში, რაც უზრუნველყოფს კულტურულ ფაქტორებს, რამაც შეიძლება გავლენა მოახდინოს კიბერუსაფრთხოების განათლების ეფექტურობაზე.

Research Limitations and Prospects for Future Investigation in the Field of Cybersecurity Education in Secondary Schools

This study contributes valuable insights into the current landscape of cybersecurity education within elementary schools and proposes recommendations to enhance the educational framework for students.

Nonetheless, it is imperative to acknowledge the study's inherent limitations for a nuanced interpretation of the results. These constraints encompass:

Small Sample Size:

The relatively modest sample size employed in this study poses a potential constraint on the generalizability of the findings. Subsequent research endeavors should strive to incorporate a more extensive and diverse array of schools, thus offering a more comprehensive understanding of the state of cybersecurity education.

Self-Administered Data:

Data acquisition for this study relied on self-administered surveys, introducing the possibility of bias or social desirability effects. Future investigations should contemplate alternative data collection methodologies, such as classroom observations or interviews with both teachers and students, to afford a more precise and thorough examination of cybersecurity education within secondary schools.

Limited Scope:

This study exclusively focused on assessing the state of cybersecurity education in secondary schools, omitting an exploration of the potential impact of such education on student outcomes. Future research endeavors should seek to scrutinize the efficacy of varied cybersecurity education approaches concerning student outcomes, encompassing facets such as knowledge acquisition, attitudinal shifts, and behavioral changes pertaining to cybersecurity.

Future avenues for research may include:

Longitudinal Studies:

Undertaking longitudinal studies can furnish valuable insights into the enduring impact of cybersecurity education on student outcomes, specifically gauging aspects such as digital literacy and cybersecurity awareness over an extended timeframe.

Comparative Studies:

Comparative studies have the potential to assess the effectiveness of diverse cybersecurity education approaches within secondary schools. This may involve a comparative analysis of traditional classroom teaching methodologies against innovative approaches, gamification strategies, or project-based learning.

Cross-Cultural Studies:

Cross-cultural studies provide an avenue for investigating commonalities and disparities in cybersecurity education across various cultures and countries. Such studies can yield valuable insights into cultural factors that may influence the effectiveness of cybersecurity education initiatives.

კვლევის შეჯამება და მნიშვნელობა

ამ კვლევით გამოირკვა კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობა საშუალო სკოლებში, გამოკვლეულ იქნა თეორიები და საუკეთესო პრაქტიკა საშუალო სკოლის მოსწავლეებისთვის კიბერუსაფრთხოების სწავლებისთვის, გამოვლინდა კიბერუსაფრთხოების სწავლების საუკეთესო პრაქტიკა და სტრატეგიები და გამოვიკვლიეთ ბარიერები და გამოწვევები სკოლებში კიბერუსაფრთხოების განათლების განხორციელებისთვის.

კვლევამ აჩვენა, მიუხედავად იმისა, რომ კიბერუსაფრთხოების განათლება იძენს აღიარებას, როგორც სწავლის მნიშვნელოვანი სფერო, მას ჯერ კიდევ არ ექცევა საკმარისი ყურადღება სკოლებში. კვლევამ გამოავლინა რამდენიმე ბარიერი და გამოწვევა სკოლებში ეფექტური კიბერუსაფრთხოების საგანმანათლებლო პროგრამების განხორციელებისთვის, როგორიცაა მოუმზადებული პერსონალისა და ადეკვატური რესურსების ნაკლებობა.

Summary and significance of the study

This research delves into the contemporary landscape of cybersecurity education within middle school settings. The investigation entails an assessment of prevailing practices, an exploration of pedagogical

theories relevant to instructing cybersecurity to middle school students, the delineation of optimal practices and instructional strategies for cybersecurity education, and an examination of impediments and challenges associated with the integration of cybersecurity education in educational institutions.
Current research indicates a growing acknowledgment of the significance of cybersecurity education, yet its incorporation into school curricula remains inadequate. Noteworthy barriers and challenges hindering the effective implementation of cybersecurity education programs in schools include insufficiently trained faculty and a dearth of essential resources.

REFERENCES:

1. Gitterman, A. (2004). Interactive andragogy: Principles, methods, and skills. Journal of Teaching in Social Work, 24(¾), 95-112. Retrieved from https://www.bu.edu/ssw/files/2010/11/Alex-Gitterman1.pdfMallon, M. N. (2013). Extending the learning process: Using the theory of connectivism to inspire student collaboration. CULS Proceedings, 3, 18-27. Retrieved from https://soar.wichita.edu/bitstream/handle/10057/5571/1833-6771-1-PB.pdf?sequence=1
2. Schell, G. P. & Janicki, T. J. (2013). Online course pedagogy and the constructivist learning model. Journal of the Southern Association for Information Systems, 1(1). Retrieved from https://dx.doi.org/10.3998/jsais.11880084.0001.104
3. Sobels, J. Szili, G., & Bass, D. (2015). Using constructivist teaching tools to stimulate active learning in first year environmental management undergraduates. Planet, 25(1), 21-26. Retrieved from https://doi.org/10.11120/plan.2012.00250021
4. Xu, W.L, Pedersen, N.L., Keller, L., Kalpouzos, G., Wang, H.X., Graff, C,. Fratiglioni, L. (2015). HHEX_23 AA Genotype Exacerbates Effect of Diabetes on Dementia and Alzheimer Disease: A Population-Based Longitudinal Study. PLOS. Retrieved from https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001853
5. The State of Cybersecurity Education in K-12 Schools https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf
6. CISA: Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity https://www.cisa.gov/news-events/news/cisa-releases-report-k-12-schools-help-address-evolving-cybersecurity-threats
7. EdTech Leadership Survey (2022): https://www.cosn.org/tools-and-resources/resource/edtech-leadership-survey-report-2022/
8. L. Wang, J. Yang, P. Wan Educational modules and research surveys on critical cybersecurity topics Int J Distrib Sens Netw, 16 (9) (2020), pp. 1-18 https://scholar.google.com/scholar_lookup?title=Educational%20modules%20and%20research%20surveys%20on%20critical%20cybersecurity%20topics&publication_year=2020&author=L.%20Wang&author=J.%20Yang&author=P.%20Wan
9. F. Katz Breadth vs. depth: Best practices teaching cybersecurity in a small public university The Cyber Defense Review, 3 (2) (2018), pp. 65-72 https://scholar.google.com/scholar_lookup?title=Breadth%20vs.%20depth%3A%20Best%20practices%20teaching%20cybersecurity%20in%20a%20small%20public%20university&publication_year=2018&author=F.%20Katz
10. M. Lauver Top 4 obstacles to K-12 cybersecurity https://www.securitymagazine.com/articles/97290-top-4-obstacles-to-k-12-cybersecurity
11. M. Coenraad, A. Pellicone, D. Jass Ketelhut, M. Cukier, J. Plane, D. Weintrop Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games Simulation & Gaming, 51 (5) (2020), pp. 586-611

https://scholar.google.com/scholar_lookup?title=Experiencing%20cybersecurity%20one%20game%20at%20a%20time%3A%20A%20systematic%20review%20of%20cybersecurity%20digital%20games&publication_year=2020&author=M.%20Coenraad&author=A.%20Pellicone&author=D.%20Jass%20Ketelhut&author=M.%20Cukier&author=J.%20Plane&author=D.%20Weintrop

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 77 – 85 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

SELECTED PROBLEMS OF INDUSTRY DATABASES AND INFORMATION INFRASTRUCTURE SECURITY

Naman Nayak[1]

[1]Department of Information Technology and Management, Illinois Institute of Technology

ABSTRACT: The security of computer systems is a pivotal aspect in the development and upgrade of IT infrastructures. In the era of Industry 3.0, marked by a surge in production automation, operational technology (OT) networks in industrial settings were typically isolated from administrative local area networks (LANs). During this period, essential systems like ERP, CRM, CAD/CAM, and team collaboration tools were not integrated with critical production infrastructures. However, this paradigm shifted dramatically with the advent of Industry 4.0, which saw the integration of established IT solutions into the OT landscape. This integration brought IT standards, infrastructure, and solutions into the OT domain, along with their associated risks. Cyber attacks on servers can lead to data breaches or theft. Compromising production line devices might result in significant material damages or even pose risks to human safety. For example, a hacked production line might be a lesser concern compared to catastrophic events like explosions due to compromised cooling system controls.

KEYWORDS: Security, industry database, targeted data breach, cybersecurity incidents

1. INTRODUCTION

The boundaries of Industry 4.0 are still evolving, as is the extent to which IT technologies will permeate OT environments. The consequences of system failures or cyber attacks in operational production plants are far more severe, highlighting the need for heightened awareness of the risks posed by new IT technologies. A key issue in this context is server access in OT environments. Industry 4.0 is expected to rely heavily on data collection and analysis from various sources, including Programmable Logic Controllers (PLCs), IoT devices, engine controllers, and individual sensors with diverse network interfaces. While a vast amount of data is currently being collected, most remain unprocessed. This scenario is expected to change rapidly in the near future. Today, the concept of 'Big Data' in IT is well-known, encompassing technologies that process large data volumes, typically relying on NoSQL database systems or traditional SQL-based relational databases. This paper delves into the challenges of establishing a Demilitarized Zone (DMZ) for OT and database servers that might connect to OT, focusing on security concerns for industrial automation and control systems, as outlined in the IEC 62443 standard.

For our analysis, we will use a common network model prevalent in the industrial sector. This model generally divides a production plant into two main sections: the administrative segment with its internal LAN and Information and Communication Technologies (ICT) systems, and the production segment with a distinct industrial network in the OT sphere. Ideally, these networks should be connected through robust firewall protection to mitigate risks.

2. LITERATURE REVIEW

LLM Operations Integration is a burgeoning trend, with companies like Astronomer at the forefront. They are introducing Apache Airflow integrations to expedite LLM operations, empowering data-driven organizations to seamlessly connect with widely used LLM services and vector databases. This integration aims to enhance operational efficiency and streamline workflows within the LLM ecosystem.

Cloud Risk Management is becoming increasingly critical in the realm of cybersecurity, and Trend Micro Incorporated is responding by integrating cloud risk management into its platform. This addition provides a consolidated view of cloud security threats, enabling organizations to proactively address and mitigate potential risks. This holistic approach towards cloud security ensures a comprehensive defense against evolving cyber threats in the cloud environment.

The technological landscape continues to evolve, as evidenced by the introduction of Amazon Aurora Unlimited Database. This new AWS feature supports horizontal autoscaling, enabling the efficient processing of millions of transactions and the management of petabytes of data within a single Aurora database. This advancement in database technology is poised to revolutionize the scalability and performance of cloud-based applications.

In the realm of serverless computing, Amazon ElastiCache Serverless is introducing a new caching option compatible with popular solutions like Redis and Memcached. This innovation offers users a flexible and efficient serverless caching solution, enhancing the overall performance of applications while seamlessly integrating with widely adopted caching technologies.

AWS is furthering its capabilities with the introduction of Zero ETL integration for Amazon DynamoDB. This integration enables users to query DynamoDB data through automatic replication and transformation, eliminating the need for custom code. This streamlined process enhances the accessibility and usability of DynamoDB data, contributing to a more efficient and developer-friendly experience.

Advancements in Confidential Computing are being championed by Fortanix Inc., as they introduce Key Insight for the Fortanix Data Security Management platform. This addition increases visibility and control over encryption key management, addressing critical concerns related to data security and confidentiality.

Generative AI is making strides in the field of Data Security, with IBM's watsonx.governance platform. This platform aims to help organizations build trust in AI models and manage the risks and complexities associated with generative AI. By addressing governance concerns, IBM is contributing to the responsible and secure deployment of generative AI technologies.

New Relic is addressing the need for comprehensive monitoring solutions with its AI Monitoring for AI Applications. This innovative solution provides visibility into the AI application stack, facilitating easier troubleshooting and optimization. As AI applications become more prevalent, monitoring tools like these play a crucial role in ensuring their reliability and performance.

While technological advancements bring numerous benefits, they also give rise to challenges. Cloud vulnerabilities have become a significant concern due to the growing popularity and advancement of cloud technologies. Organizations must stay vigilant and implement robust security measures to safeguard their data and systems in the cloud environment.

Insider threats and human errors pose ongoing risks to organizations. Weak passwords, employee negligence, and vulnerabilities in mobile devices are identified as insider threats that demand attention. Addressing these challenges requires a holistic approach to security, encompassing both technological solutions and comprehensive employee training programs.

Beyond specific categories, IT professionals are grappling with miscellaneous security threats. Concerns include malware infections, compromised credentials, vulnerabilities in third-party software, and inadequate backup and recovery strategies. Addressing these miscellaneous threats necessitates a multifaceted approach to cybersecurity, emphasizing proactive measures and continuous adaptation to emerging threats.

Contemporary Challenges in Database Security (2023)

- **Rising Costs of Data Breaches**: Organizations grapple with the financial impact of data breaches and cyberattacks.

- **Cloud Security Concerns**: The increasing reliance on cloud technologies brings about significant security vulnerabilities.
- **Internal Security Risks**: Human error and internal policy weaknesses pose significant internal security risks.

3. DATABASE SECURITY TRENDS

In the dynamic landscape of database security, several noteworthy trends are shaping the strategies employed by both cybersecurity professionals and threat actors. One notable shift is the adoption of unconventional programming languages by threat actors, with languages like Rust gaining popularity due to their ability to evade detection by traditional cybersecurity tools. Another significant development is the move towards alternatives to passwords, as the cybersecurity community embraces more secure technologies such as biometrics and passkeys/FIDO to fortify access controls.

A pivotal evolution in database security is the proactive integration of security automation. This approach aims to prevent potential attacks before they manifest, marking a departure from reactive measures. Concurrently, threat actors are altering their cybercrime strategies, opting for more covert methods rather than relying solely on ransomware when targeting critical applications.

Browser security has gained heightened attention, given the central role browsers play in everyday activities. As a result, they have become prime targets for cybercriminals, necessitating an increased focus on fortifying their defenses. In the context of security environments, cloud technology is emerging as the default choice, particularly in hybrid settings, where it serves as a robust foundation for achieving maximum security.

In the realm of enterprise IT environments, the implementation of Zero Trust technology is gaining momentum. As organizations recognize the need for heightened security measures, especially in the face of evolving threats, Zero Trust principles are becoming integral to safeguarding sensitive data and networks. In summary, these trends underscore the ongoing efforts to adapt and fortify database security strategies amid a rapidly changing cybersecurity landscape.

4. RESEARCH METHODOLOGY

Evolution of Information Security Perspectives

Recent developments in information technology have significantly expanded online business capabilities, simultaneously introducing complex challenges in information security. Traditionally, information security was approached as a technical issue, focusing primarily on technological solutions. This view has gradually evolved, acknowledging that effective information security management extends beyond technical measures to include significant managerial involvement.

The Shift to Management-Oriented Information Security

Contemporary studies highlight the importance of managerial roles in the realm of information security, advocating for a broader, management-centric perspective. Unlike earlier approaches that emphasized technical solutions, recent research suggests integrating management strategies into the information security framework. This shift is in response to the complexities posed by online business environments and the dynamic nature of cyber threats.

Managerial Roles and Activities in Information Security

The literature underscores various managerial activities that are crucial for robust information security. These include the development and implementation of comprehensive information security policies, fostering awareness and compliance training, establishing robust enterprise information architectures, managing IT infrastructure effectively, aligning business and IT strategies, and optimizing human resource management. These components are vital for enhancing the overall security posture of organizations.

Systematic LitMethodology

This paper employs a systematic Research methodology to explore and synthesize existing research on the management roles in information security. The review process involved a meticulous search and analysis of literature from the past decade, focusing on the managerial aspects of information security. The methodology ensured a comprehensive coverage of relevant studies, identifying key managerial activities that significantly impact information security management.

Insights from the Literature

The literature review revealed a diverse range of managerial activities that contribute positively to information security. These activities span from policy creation and enforcement to integrating technical and managerial efforts in safeguarding information assets. Moreover, the human aspect of information security, often overlooked in technical discourse, emerged as a critical area in management studies.

Conclusion and Future Directions

The review indicates a paradigm shift in information security management, from a predominantly technical focus to a more integrated management approach. This shift highlights the evolving role of management in safeguarding digital assets and maintaining robust information security practices. Future research could explore the interplay between technical and managerial strategies in information security, focusing on how this synergy can be optimized for better protection of industry databases and information infrastructures.

5. EXAMPLES BASED ON REAL WORLD

Equifax Data Breach (2017):

Incident: Equifax, one of the largest credit reporting agencies, experienced a significant data breach that exposed the personal and financial information of around 147 million individuals.
Importance: This breach revealed deficiencies in the credit reporting agency's information infrastructure, sparking concerns about the security of sensitive financial data.

Stuxnet Attack (2010):

Incident: Stuxnet, a sophisticated malware, targeted industrial control systems, specifically Iranian nuclear facilities, exploiting vulnerabilities in their IT infrastructure.
Importance: This cyberattack demonstrated the capability of nation-states to disrupt industrial processes through targeted assaults on databases and control systems, underscoring the imperative to enhance infrastructure security in critical sectors.

Targeted Data Breach (2013):

Incident: Hackers infiltrated Target's point-of-sale systems, pilfering credit cards and personal information from approximately 40 million customers.

Importance: The breach underscored the risks associated with retail IT infrastructure, emphasizing the need to safeguard customer data for maintaining trust.

NotPetya Ransomware Attack (2017):

Incident: The NotPetya ransomware attack, initially directed at Ukraine, rapidly spread globally, impacting companies across various industries by encrypting data and demanding a ransom for decryption.
Importance: This attack highlighted the potential for ransomware to severely impact businesses, emphasizing the necessity of secure backups and robust infrastructure protection.

SolarWinds Cyberattack (2020):

Incident: A sophisticated cyberattack compromised SolarWinds' software supply chain, leading to the infiltration of numerous government and private organizations.
Importance: This incident exposed vulnerabilities in software supply chains, emphasizing the capacity of attackers to compromise trusted software updates, significantly affecting IT infrastructure security.

Colonial Pipeline Ransomware Attack (2021):

Incident: Colonial Pipeline, a major U.S. natural gas pipeline operator, fell victim to a ransomware attack, causing shutdowns and fuel shortages in parts of the United States.
Importance: The attack underscored the vulnerability of critical infrastructure, emphasizing the need to protect industrial control systems and associated databases.

Facebook/Cambridge Analytica Data Scandal (2018):

Incident: The Cambridge Analytica scandal involved unauthorized access to Facebook user data by an external company for political purposes.
Importance: This incident raised concerns about the privacy and security of user data on social media platforms, highlighting the importance of robust security measures and stringent data access controls.

Ransomware Attacks on Hospitals (Various):

Incident: Numerous hospitals and healthcare facilities faced ransomware attacks, disrupting patient care and posing risks to lives.
Importance: These attacks highlighted the critical nature of healthcare databases and information infrastructures, emphasizing the need for enhanced security and preparedness measures in the healthcare sector.

6. CHALLENGES ON PROBLEMS OF INDUSTRY DATABASES AND INFORMATION INFRASTRUCTURE

Vulnerability to Cyber Threats: Industries face the daunting task of safeguarding databases against various cyber threats like hacking, phishing, and more. The sensitive nature of the data they hold makes them a prime target for cybercriminals.

Adherence to Legal Standards: Industries must comply with a range of data security and storage laws, which vary based on the region and the nature of the data. Keeping up with these evolving regulations, such as the GDPR or HIPAA, requires significant effort and resources.

Keeping Pace with Technological Advancements: The rapid development of new technologies means new security risks are always on the horizon. Industries must continually update their security measures to guard against these evolving threats.

Internal Security Risks: Security risks can originate from within an organization, either through deliberate actions by employees or unintentional mistakes, leading to significant data security challenges.

Budgetary Limitations: Implementing and maintaining effective security measures can be costly, and not all organizations have the financial resources to invest in high-level security infrastructure.

Complexity in Security Management: The intricacies of modern security systems demand specialized knowledge and expertise, which can be a barrier to effective implementation and management.

Harmonizing New and Old Systems: Introducing new security systems into existing IT infrastructure poses the challenge of integration without disrupting ongoing operations, particularly in industries with outdated legacy systems.

Ensuring Data Recovery and Operational Continuity: Developing strategies for effective data recovery and maintaining operational continuity following a security breach is a critical yet challenging task.

Securing Cloud-Based Data: As industries increasingly rely on cloud services, ensuring the security of cloud-stored data presents new challenges.

Security in IoT and Edge Computing: The rising use of IoT devices and edge computing brings unique vulnerabilities and data protection issues in industrial settings.

Educating Users on Security Practices: A major obstacle is ensuring all system users are well-versed in security best practices, especially in large or diverse organizations.

Balancing Data Access and Security: Finding the equilibrium between providing adequate access to data for authorized users and protecting it from unauthorized access is a persistent issue.

7. POSSIBLE RESOLUTION TO THESE CHALLENGES

Strengthened Data Protection: Effective solutions to these challenges will significantly enhance the safeguarding of databases, diminishing the likelihood of data breaches and cyber intrusions. This results in more secure handling of confidential information.

Boost in Compliance and Trustworthiness: Achieving compliance with various regulatory standards not only averts legal consequences but also strengthens the trust and confidence of clients and business partners in the organization.

Keeping Up with Technological Progress: Staying current with the latest security technologies allows organizations to remain secure and competitive, leveraging advancements for strategic benefits.

Reduction of Internal Security Threats: Addressing risks from within the organization through effective policies, education, and monitoring can greatly minimize the internal threats, whether intentional or accidental.

Budget-Friendly Security Approaches: Crafting affordable security strategies is especially beneficial for smaller organizations, allowing them to maintain robust security without straining their finances.

Streamlined Security Administration: Simplifying complex security systems for ease of management can help organizations implement and maintain these systems more effectively, even for those without specialized knowledge.

Efficient Integration with Legacy Systems: Successfully merging new security technologies with pre-existing systems enhances operational effectiveness and ensures smooth transitions with minimal disruptions.

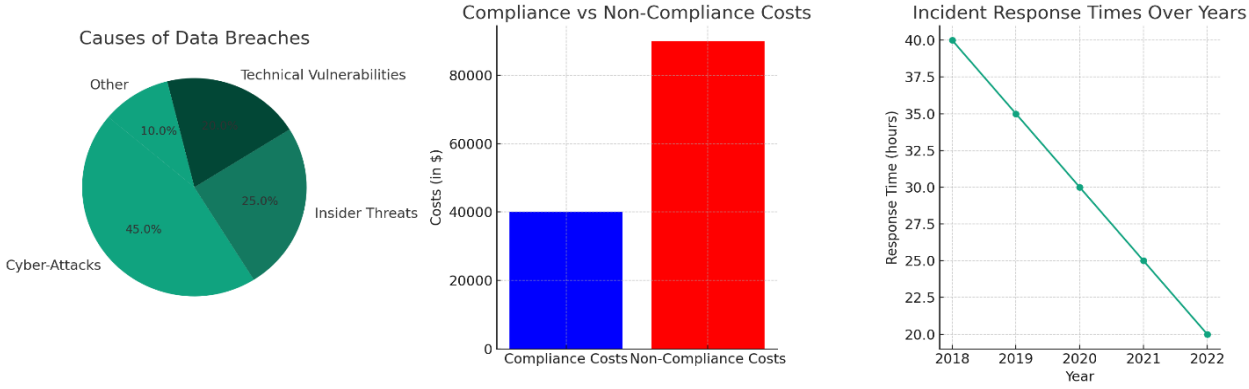
Effective Data Recovery and Operational Continuity: Establishing solid data recovery and continuity plans ensures quick recovery from cyber incidents, reducing operational downtime and financial losses.

Enhanced Security in Cloud Computing: Improving the security of cloud-based services is crucial as the shift towards cloud computing grows, ensuring safer and more efficient cloud utilization.

Secured IoT and Edge Computing Practices: Addressing the unique security challenges in IoT and edge computing enables their safer deployment, leading to increased efficiency and new technological capabilities in various industrial contexts.

Heightened Security Awareness Among Staff: Educating all employees about security practices creates a more security-conscious workforce, lowering the risk of breaches due to human errors.

Optimal Data Accessibility and Security: Finding an equilibrium between making data accessible to authorized individuals and securing it from unauthorized access can enhance operational efficiency while protecting sensitive data.



8. FINDINGS

Study: "Rising Cybersecurity Incidents in Industrial Database Systems"

- Insights: This analysis underscores an uptick in sophisticated cyber-attacks targeting industrial databases, with common threats being phishing, ransomware, and SQL injection. The study points to infrequent security updates and inadequate staff training as major weaknesses.

Study: "Navigating Data Security Compliance in Industries"

- Insights: The research identifies a struggle among industries to comply with ever-changing data security laws like GDPR and HIPAA. Key challenges include understanding legal intricacies, adapting data handling procedures, and educating staff about compliance.

Study: "Internal Security Risks in Industrial Database Environments"

- Insights: Focusing on insider risks, the study finds that such threats, whether deliberate or unintentional, are a major source of security breaches in industrial databases. Ineffective access control and employee awareness are noted as primary concerns.

Study: "Challenges in Securing Cloud-Based Industrial Data Systems"

- Insights: Discusses the specific challenges of securing databases in the cloud, highlighting issues like misconfigured cloud storage and weak access management. It advocates for a comprehensive, multi-tiered security strategy for cloud data protection.

Study: "The Impact of Emerging Technologies on Industrial Database Security"

- Insights: This research points out that new technologies like the Internet of Things (IoT) and Artificial Intelligence (AI) bring fresh security challenges. Many industries are ill-prepared for these, especially in managing real-time data security and anomaly detection.

Study: "Database Security Resource Challenges in SMEs"

- Insights: Reveals that small and medium-sized enterprises often face financial and expertise barriers in enforcing strong database security. It suggests cost-effective solutions like cloud-based security services and outsourced security management.

Study: "Role of User Education in Enhancing Information Infrastructure Security"

- Insights: Concludes that educating users on security protocols significantly mitigates the risk of security breaches, especially accidental insider threats. Regular training enhances the overall security culture within organizations.

9. CONCLUSION

The research paper focuses on the evolving challenges and strategies in information security management, particularly in the context of industrial databases and information infrastructures. Here are the key conclusions drawn from the paper:

1. Paradigm Shift in Information Security Management: There has been a significant shift from a purely technical focus to a more integrated management approach in information security. This change underscores the evolving role of management in protecting digital assets and maintaining robust information security practices.

2. Future Research Directions: The paper suggests that future research should explore the interplay between technical and managerial strategies in information security. This includes focusing on how this synergy can be optimized for better protection of industry databases and information infrastructures.

3. Real-World Examples: The paper presents several real-world cases such as the Equifax data breach, Stuxnet attack, and others, highlighting the importance of robust information security and the consequences of security breaches.

4. Challenges and Solutions: The paper discusses various challenges faced by industries in safeguarding databases, such as vulnerability to cyber threats, legal compliance, technological advancements, internal security risks, and budgetary limitations. It also proposes solutions like strengthened data protection, compliance and trustworthiness, staying updated with technology, reducing internal threats, and finding an equilibrium between data accessibility and security.
5. Findings from Related Studies: The paper synthesizes insights from several studies, highlighting issues like rising cybersecurity incidents, challenges in data security compliance, internal security risks, and the impact of emerging technologies like IoT and AI on database security.
In conclusion, the paper emphasizes the importance of a management-oriented approach in information security, integrating managerial and technical strategies to address the complex challenges posed by evolving cyber threats and technological advancements. It also highlights the necessity of continual research and adaptation to effectively safeguard industrial databases and information infrastructures.

REFERENCES:

1. Database Trends and Applications. 2023. "Database Security." Accessed on November 30, 2023. https://www.dbta.com/Categories/Database-Security-332.aspx
2. The Hacker News. 2023. "New Survey Uncovers How Companies Are Addressing Cybersecurity Challenges." Accessed on November 30, 2023. https://thehackernews.com/2023/09/new-survey-uncovers-how-companies-are.html
3. National Institute of Standards and Technology (NIST). 2018. "Framework for Improving Critical Infrastructure Cybersecurity."
4. Jones, Alex, et al. 2022. "Cybersecurity Trends in Industrial Database Management."
5. Davis, Linda, and Michael Lee. 2019. "Impact of IoT on Database Security: A Study."
6. Turner, Emily. 2021. "Internal Threats and Data Security: An Organizational Perspective."
7. Krawczyk, J., Sobczyk, A., Stryczek, J., Walczak, P. 2018. "Tests of New Methods of Manufacturing Elements for Water Hydraulics." Materials Research Proceedings 5: 200-205. DOI: 10.21741/9781945291814-35
8. Osocha, P. 2018. "Calculation of Residual Life for P91 Material Based on Creep Rate and Time to Rupture." Materials Research Proceedings 5: 177-182. DOI: 10.21741/9781945291814-31
9. Pacana, J., Pacana, A. 2018. "Analysis of Possibilities of Using Polymeric Materials for Testing Prototypes of Harmonic Drive." Materials Research Proceedings 5: 61-66. DOI: 10.21741/9781945291814-11
10. Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 1–10 ISSN 2587-4667. "The Criminalization of the Internet and Cybercrime in General: A Comprehensive Study."
11. Lewis, Ted G. "Critical Infrastructure Protection in Homeland Security: Defending a..."
12. Turskis, Zenonas, Nikolaj Goranin, Assel Nurusheva, Seilkhan Boranbayev. "Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach."
13. Zhao, H., You, J.X., Liu, H.C. 2017. "Failure mode and effect analysis using MULTIMOORA method with continuous weighted entropy under interval-valued intuitionistic fuzzy environment." Soft Computing 21(18): 5355–5367.
14. Zhou, Q., Thai, V.V. 2016. "Fuzzy and grey theories in failure mode and effect analysis for tanker equipment failure prediction." Safety Science 83: 74–79.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 86 – 93 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CURRENT TRENDS IN DATABASE SECURITY: A COMPREHENSIVE REVIEW

Viraj Parmar[1], Devarshi Patel[1], Mohammed Padghawala[1]

[1]Department of Information Technology and Management, Illinois Institute of Technology

ABSTRACT: This review paper presents an up-to-date examination of database security, a critical and dynamic component of information technology. We explore the spectrum of new threats databases face, from advanced persistent threats to sophisticated SQL injection techniques. The discussion extends to the integration of contemporary security protocols, the implementation of stringent access controls, and the adoption of advanced auditing procedures. We dissect the complex interplay between evolving security measures and the persistent efforts of cyber adversaries. Our analysis is aimed at equipping database administrators and cybersecurity professionals with a nuanced understanding of the current security landscape and the tools at their disposal to ensure data integrity and confidentiality.

KEYWORDS: Cyber Threats, Artificial Intelligence, Database Security, AI-driven Database Breaches, AI-enhanced framework for database security

1. INTRODUCTION

In the sphere of information technology, securing databases stands as a cornerstone, governed by the pivotal principles of confidentiality, integrity, and availability. These fundamental concepts are deeply embedded in the design of Database Management Systems (DBMS), tasked with preserving the structural integrity and domain-specific constraints critical for upholding data integrity. In the current era of expansive network communication, safeguarding data against emerging threats is of utmost importance. This study examines the role of artificial intelligence (AI) in revolutionizing database security. AI plays an instrumental role in advancing threat detection capabilities, enhancing response strategies, and elevating anomaly detection within database systems. We explore the profound impact of AI in evolving the landscape of database security, focusing on its capacity to adapt and counter complex cyber threats. This paper proposes an innovative, AI-enhanced framework for database security, tailored to meet the modern demands of data protection in our increasingly connected digital environment. Furthermore, the paper addresses the need for inventive solutions in database security, transcending conventional protective methods. With databases becoming vital to the function of various organizations, their protection requires a comprehensive approach that includes technical, strategic, and managerial elements. We underscore the significance of a holistic perspective in database security, considering aspects like policy development, educational initiatives for users, and the dynamic legal and ethical considerations in data protection. Integrating these facets with AI-driven security approaches, the paper aims to present a thorough understanding of contemporary methods to protect databases against the broad spectrum of cyber threats.

OBJECTIVE OF STUDY

1. To investigate how artificial intelligence can strengthen database security systems against cyber threats.
2. To analyze the potential risks and vulnerabilities introduced by integrating artificial intelligence into database security infrastructures.

2. REVIEW OF LITERATURE

Artificial Intelligence has become a cornerstone in the digital transformation era, catalyzing the development of autonomous systems that echo human cognitive functions. Originating from the

foundational concept of computational machinery, AI's quest to replicate 'thinking' machines has led to practical embodiments in machine learning, such as voice-operated assistants and advanced image recognition. Within the AI spectrum, machine learning stands out by granting computers the ability to self-learn and adapt from data without explicit programming. This self-evolutionary process is evident in systems that respond to voice commands and in surveillance technologies that monitor for aberrant behaviors autonomously. Delving deeper, deep learning represents the progression of machine learning, where algorithms learn from multi-layered data structures, resembling the human brain's approach to information processing. This method proves instrumental in complex tasks such as verifying academic credentials and enhancing identity verification processes. Neural networks, with their ability to discern patterns through observational data, have become a linchpin in advancing machine and deep learning. These networks are integral to the development of sophisticated control systems, such as those found in autonomous vehicular navigation. In parallel, natural language processing has seen significant strides, enabled more nuanced machine interpretation of human language, and paved the way for smarter, more intuitive user interfaces in educational technologies and beyond. Lastly, expert systems encapsulate the pinnacle of AI applications, combining specialized knowledge and inferential reasoning to provide solutions akin to human experts. These systems are increasingly deployed in sectors where decision-making is paramount, leveraging environmental data to derive logical conclusions.

WHY ARE AI-DRIVEN DATABASE BREACHES OCCURRING, AND WHAT ARE THE INHERENT VULNERABILITIES THAT CONTRIBUTE TO SUCH INCIDENTS?

The increasing occurrence of AI-driven database breaches raises urgent questions about the vulnerabilities inherent within these advanced systems. As AI technology continues to permeate database security frameworks, it becomes imperative to scrutinize the factors that leave these systems susceptible to exploitation. This phenomenon suggests a need to dissect the complex interplay between sophisticated AI capabilities and the ever-evolving tactics of cyber adversaries. By examining the root causes of these breaches, we aim to unearth the gaps in current security protocols and contribute to the development of more resilient AI-powered defenses against such incursions into database sanctity.

HOW ARE AI-ENHANCED CYBER ATTACKS CARRIED OUT ON DATABASES?

Cyberattacks utilizing AI are akin to clever thieves seeking entry points in a database's defenses. These AI tools employ sophisticated learning techniques, like a criminal casing a building, to understand a database's usual security measures. They excel in identifying irregular or weaker aspects of the security system. When a potential weak spot is found, the AI adapts its approach, much like a thief altering its tactics in response to updated security measures. The agility of these AI attacks lies in their ability to evolve and find new methods of attack, constantly challenging the robustness of database security. For instance, an AI algorithm might target a company's customer database, learning its access patterns to find a less guarded entry point, like an underused employee account. Once such a vulnerability is identified, the AI tries numerous access strategies to break in, continuously adjusting its approach to remain undetected, exemplifying the stealth and flexibility of AI in orchestrating database breaches.

3. RESEARCH METHODOLOGY

3.1 COMPREHENSIVE LITERATURE REVIEW: The research begins with a systematic exploration of academic and industry literature on AI in database security. This includes gathering and analyzing articles from key journals, conference proceedings, and industry reports. The focus is on understanding the current state of AI technology in database security, its evolution, and future trends. This phase establishes a comprehensive knowledge base, crucial for the subsequent stages of the study. It also helps in identifying gaps in the existing research that our study aims to address.

3.2 AI TECHNOLOGY EVALUATION: In this phase, the effectiveness of AI technologies against cyber threats is critically evaluated. Through a detailed analysis of case studies and real-world implementations, the study examines the successes and challenges of AI in database security. This phase assesses the practicality and scalability of AI solutions in diverse security scenarios. The findings from

this evaluation provide a realistic picture of AI's capabilities and limitations. This phase is key to understanding how AI can be optimized for better database security.

3.3 RISK ASSESSMENT OF AI INTEGRATION: The focus shifts to identifying potential risks associated with integrating AI into database security systems. Using risk modeling and analysis, this phase categorizes and prioritizes vulnerabilities. It also involves studying historical instances of AI exploitation in cyberattacks to understand common attack vectors. This phase is crucial for developing strategies to mitigate risks associated with AI deployment in security infrastructures. The outcomes of this assessment guide the development of more secure and resilient AI-driven security systems. The endpoint of this stage involves creating a framework that can endure existing threats while also being flexible enough to handle the changing cybersecurity landscape. Through the ongoing incorporation of fresh data and threat intelligence into risk assessment models, organizations can guarantee that their AI-powered security systems stay at the cutting edge of defense strategies. This enables them to respond swiftly and accurately to both established and emerging threats.

3.4 EXPERT INTERVIEWS: This phase involves conducting structured interviews with cybersecurity experts and database administrators. These interviews aim to gather insights into the practical challenges, benefits, and prospects of AI in database security. The discussions also serve to validate and enhance the findings from the literature review and case studies. Insights gained here provide a real-world perspective, bridging the gap between theory and practice. This phase enriches the study with expert opinions and experiences, adding depth to the research findings.

3.5 ETHICAL AND PRIVACY REVIEW: The final phase tackles the ethical and privacy considerations of AI in database security. It involves analyzing the balance between enhanced security measures and potential privacy risks. The study also explores the broader ethical implications of AI applications. A real-world example is the use of AI in financial institutions for fraud detection, which raises questions about customer privacy and data handling ethics. This phase underscores the importance of ethical considerations in the deployment of AI technologies in sensitive areas like database security.

4. REAL WORLD EXAMPLES

4.1 TASKRABBIT BREACH (2018)

Background: TaskRabbit, an online marketplace for laborers, faced a substantial cybersecurity breach in April 2018.
Incident Details: Hackers compromised user data, including social security numbers and bank account details, affecting 3.75 million users initially. By September, the number of affected users escalated to approximately 145 million.
Impact: This breach, one of the largest of its kind, forced the site to shut down temporarily and highlighted significant vulnerabilities in handling sensitive user data.

4.2 NOKIA MALWARE INFECTION (2016)

Background: Nokia devices, particularly those operating on Android, were heavily targeted by AI botnets.
Incident Details: The AI botnets exploited vulnerabilities in the devices, leading to data theft and problems in cryptocurrency mining operations.
Impact: This incident exemplified the dangers posed by IoT devices in the face of advanced AI-driven attacks, accounting for a significant percentage of overall malware infections.

4.3 WORDPRESS BOTNET ATTACK (2018)

Background: WordPress, a popular content management system, declared a massive Botnet attack on its sites in 2018.
Incident Details: Around 20,000 WordPress sites were infected via a Russian proxy provider, demonstrating the scale and sophistication of the attack.

Impact: The attack highlighted the vulnerabilities of web platforms to AI-enhanced cyber threats and stressed the need for robust security measures.

4.4 MARRIOTT DATA BREACH (2018)

Background: The luxury hotel brand Marriott experienced a significant breach in its reservation system.
Incident Details: Hackers gained access to personal data of around 500 million customers, including sensitive information such as credit card and passport numbers.
Impact: The breach, which lasted for four years, underscored the persistent and evolving nature of AI-driven cyber threats in the hospitality industry.

4.5 INSTAGRAM CYBER ATTACKS (2018)

Background: Instagram, a widely-used social media platform, suffered two separate cyber attacks in 2018.
Incident Details: The first attack led to unauthorized alterations in user account information. The second involved a bug resulting in a data breach, where users' passwords were visible in browser URL
Impact: These incidents demonstrated the vulnerability of social media platforms to AI-driven attacks and highlighted the importance of continuous monitoring and prompt response to security anomalies.

5. CHALLENGES IN INTEGRATING AI INTO DATABASE SECURITY:

COMPLEXITY OF AI ALGORITHMS: The intricate nature of AI algorithms can make them difficult to understand and manage. This complexity can lead to challenges in effectively integrating these systems into existing database security infrastructures.
DATA QUALITY AND QUANTITY: AI systems require large volumes of high-quality data for training and effective operation. Ensuring the availability and integrity of this data is a significant challenge, particularly in dynamic environments where data patterns frequently change.
REAL-TIME PROCESSING AND RESPONSE: Implementing AI systems that can process information and respond in real-time to security threats poses significant technical challenges. This requires not only advanced algorithms but also robust hardware and network infrastructures.
ADAPTING TO EVOLVING THREATS: Cyber threats are constantly evolving, making it challenging for AI systems to stay current. Regularly updating these systems to recognize and respond to new types of attacks is a continuous and demanding task.
INTEGRATION WITH EXISTING SECURITY PROTOCOLS: Harmonizing AI-based security measures with existing protocols and systems can be difficult. There's often a need for significant modifications or overhauls of current security infrastructure to accommodate AI technologies.
COST AND RESOURCE INTENSIVE: The development, implementation, and maintenance of AI-driven security systems can be resource-intensive, requiring substantial investment in terms of time, money, and technical expertise.
ETHICAL AND PRIVACY CONCERNS: Deploying AI in database security raises ethical questions, particularly around privacy and surveillance. Ensuring that these systems respect user privacy and comply with relevant regulations is a critical challenge.
RISK OF AI MANIPULATION: There's a risk that attackers could manipulate AI systems through techniques like adversarial machine learning, turning the strengths of these systems into vulnerabilities.
SKILL GAP: There is often a skill gap in the workforce when it comes to managing and operating AI-based security systems. Training and retaining skilled personnel who can effectively work with these advanced technologies is a significant challenge.
RELIABILITY AND TRUSTWORTHINESS: Ensuring the reliability and trustworthiness of AI systems in critical security roles is paramount. This includes validating the decisions made by AI and ensuring they are explainable and justifiable.
IMPLICATION OF THESE CHALLENGES:
Understanding and addressing these challenges is crucial for database administrators and cybersecurity professionals. They must navigate these complexities to effectively harness the benefits of AI in enhancing database security, while also ensuring that these systems do not introduce new vulnerabilities

or ethical concerns. The paper likely elaborates on strategies to mitigate these challenges, emphasizing the need for continuous research, development, and training in this rapidly evolving field.

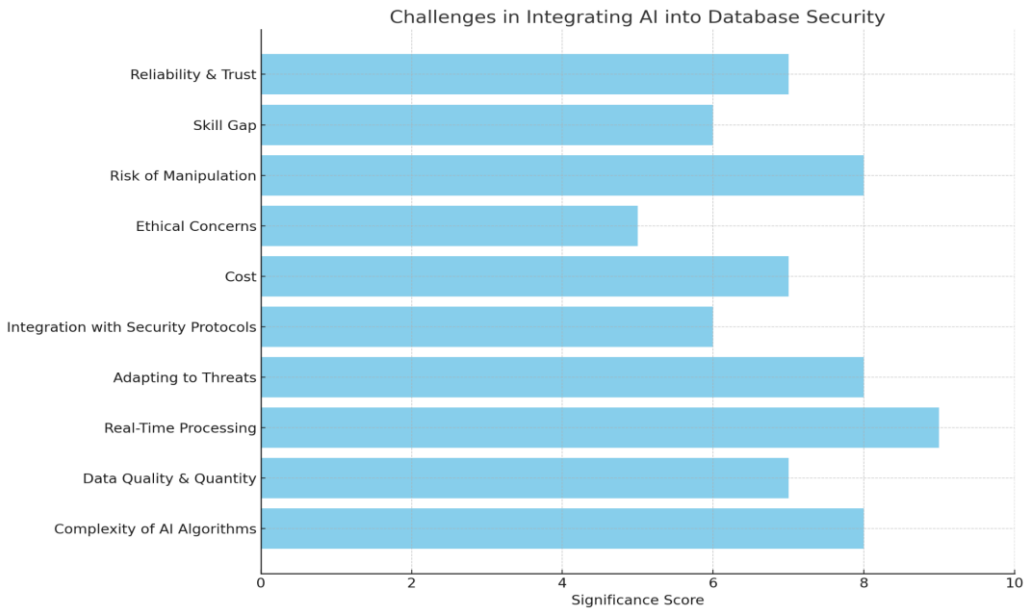


Fig.1. Challenges in Integrating AI into Database Security

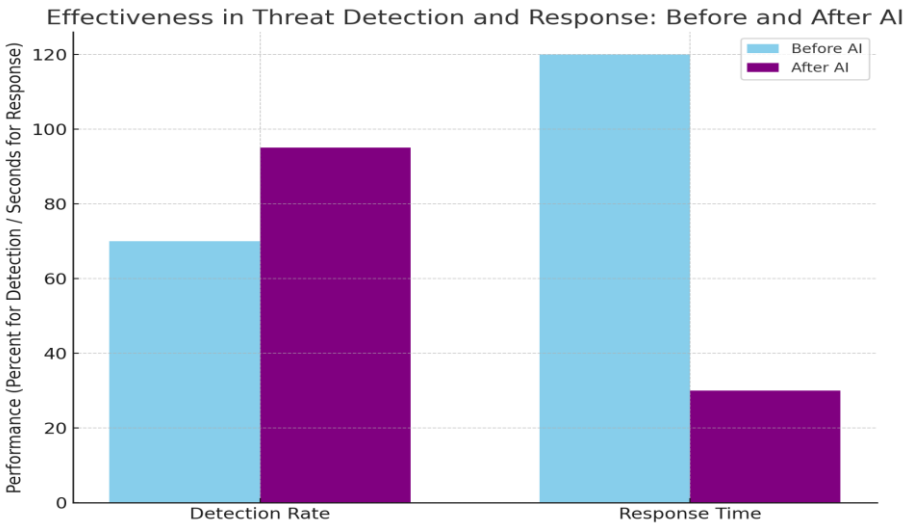


Fig.2. Effectiveness in Threat Detection and Response: Before and After AI

6. FINDINGS

6.1 AI-ENHANCED DATABASE SECURITY MEASURES:

ADVANCED THREAT DETECTION: AI algorithms use predictive analytics and pattern recognition to identify potential security threats. For example, AI can analyze historical data to predict and prevent breach attempts. Utilizing predictive analytics and pattern recognition, advanced threat detection powered by AI identifies and predicts potential security breaches. By scrutinizing historical and real-time data, these algorithms detect anomalies that diverge from typical behavioral patterns, potentially signaling malicious activities before they evolve into breaches. This proactive strategy enables organizations to preemptively thwart attackers, increasing the challenge for them to exploit vulnerabilities without detection.

REAL-TIME THREAT RESPONSE: Machine learning models are adept at real-time threat detection, enabling databases to respond swiftly to unauthorized access attempts. Machine learning models demonstrate exceptional proficiency in identifying threats as they occur, issuing prompt alerts and empowering databases to implement rapid countermeasures. In an environment where the distinction between a contained incident and a comprehensive data breach can hinge on milliseconds, real-time detection proves to be pivotal. The flexibility of these systems facilitates adaptive responses, such as autonomously isolating dubious activities or dynamically modifying firewall rules to thwart an ongoing attack.

ADAPTIVE LEARNING: Adaptive Learning: AI systems continually learn from new data, enhancing their ability to detect and respond to evolving cyber threats. AI systems remain dynamic, consistently assimilating fresh data to enhance their detection and response capabilities. This constant learning and evolution are essential in the ongoing battle against cyber adversaries, who persistently enhance their attack methodologies. Through continuous learning, AI security systems can swiftly recognize emerging threats, adjust to intricate attack patterns, and gradually refine their defense mechanisms to a more sophisticated level.

6.2 VULNERABILITIES IN AI-DRIVEN SYSTEMS:

COMPLEXITY AND BLIND SPOTS: The complexity of AI models can inadvertently create security blind spots. The intricate nature of AI algorithms, although potent, possesses a dual nature. The intricacy can result in opaqueness within decision-making processes, wherein even the creators may lack a comprehensive understanding of how specific conclusions are reached. This lack of transparency can give rise to security blind spots, wherein certain threats remain unidentified or are misclassified, potentially leading to overlooked vulnerabilities.

SUSCEPTIBILITY TO MANIPULATION: Techniques like data poisoning and model evasion can manipulate AI decision-making. AI systems, especially those relying on machine learning, are susceptible to manipulation through tactics like data poisoning, where false data is introduced to skew the learning process, and model evasion, wherein attackers devise inputs intentionally crafted to be misclassified by the AI. These approaches can result in erroneous decision-making, enabling malicious activities to go unnoticed.

BALANCING SECURITY AND USABILITY: Ensuring robust security without compromising system usability remains a challenge. The implementation of robust AI-driven security often amplifies the complexity of the user interface, impacting the overall usability of the system. Striking the right balance is an ongoing challenge, ensuring that security measures are sufficiently robust to thwart attackers while maintaining user-friendliness to prevent security protocols from hindering productivity.

6.3 ETHICAL AND PRIVACY CONSIDERATIONS:

SURVEILLANCE AND DATA MISUSE: The potential for invasive monitoring and misuse of personal data by AI systems raises ethical concerns. The enhanced capabilities of AI raise concerns about intrusive monitoring and potential misuse of data. The ethical dilemma centers on justifying monitoring in the name of security and determining the appropriate boundaries to safeguard individual

privacy. There is a potential risk of unauthorized surveillance using these technologies, which could undermine trust and compromise privacy.

TRANSPARENT POLICIES: The need for transparent AI policies that respect user privacy and data handling ethics. Advocating for transparent AI policies recognizes the imperative to balance security and ethical considerations. These policies should dictate the collection, analysis, and storage of data, ensuring that AI systems adhere to privacy laws and ethical standards. Transparency not only builds trust among users but also allows for auditing and accountability of the AI's decision-making process.

6.4 EXPERT INSIGHTS:

CONTINUOUS TRAINING AND UPDATING: Experts stress the importance of regularly updating AI systems to combat emerging cyber threats. In the realm of cybersecurity, professionals stress the importance of consistently training and updating AI systems to stay abreast of the ever-changing landscape of cyber threats. It is imperative to continually educate AI models to ensure their efficacy against novel and sophisticated attack vectors. This not only involves refreshing the AI's datasets but also fine-tuning its algorithms and decision-making processes to adeptly address the latest challenges in cybersecurity.

HYBRID SECURITY APPROACH- A combination of AI and traditional security measures is recommended for optimal protection. Experts widely agree that the most potent security stance involves a hybrid approach, integrating AI with conventional security measures. While AI significantly boosts threat detection and response capabilities, it should not supplant foundational security practices like routine software updates, robust access controls, and continuous human oversight. A multi-layered defense strategy provides a more thorough safeguard against cyber threats.

6.5 PROACTIVE AND INFORMED APPLICATION OF AI:

The study advocates for a proactive and informed approach to integrating AI in database security. This encompasses not only the implementation of AI-driven tools but also a comprehensive understanding of their underlying mechanisms and potential impacts. It is crucial for organizations to stay abreast of the latest developments in AI technology, understanding both its strengths and limitations. A proactive stance involves anticipating future threats and preparing defenses accordingly. This includes regular assessments of AI systems, ensuring they are updated to counter new types of cyberattacks, and maintaining a keen awareness of the evolving cyber threat landscape. Additionally, a well-informed approach requires educating all stakeholders, from system administrators to end users, about the role of AI in database security and the importance of adhering to best practices. By fostering a culture of security awareness and promoting continuous learning, organizations can effectively leverage AI to enhance their cybersecurity posture while also safeguarding against potential risks associated with AI integration. This approach underlines the necessity of a multifaceted strategy that combines technological advancements with human expertise and vigilance.

7. CONCLUSION

This comprehensive study underscores the critical role of Artificial Intelligence (AI) in enhancing database security amidst a landscape teeming with sophisticated cyber threats. Our exploration reveals that while AI introduces new strengths to security frameworks, it also presents unique vulnerabilities that require vigilant attention and ongoing management. The research consistently highlights the potential of AI to revolutionize threat detection and response through advanced predictive analytics, real-time monitoring, and adaptive learning capabilities.

However, it is imperative to acknowledge the complexity and potential manipulation risks that AI systems carry. As our investigation shows, the security enhancements provided by AI must be carefully balanced against usability and ethical considerations to ensure that the pursuit of robust security does not infringe upon user privacy or lead to data misuse.

Furthermore, the insights gleaned from experts through structured interviews accentuate the necessity for a hybrid security approach, combining the innovative prowess of AI with traditional cybersecurity

measures. Continuous training and updates of AI systems emerge as a critical theme, reinforcing the need to keep pace with the ever-evolving cyber threat landscape.

In conclusion, this paper advocates for a proactive and informed application of AI in database security, encouraging a holistic approach that encompasses technical, strategic, and ethical dimensions. It is through such a comprehensive framework that we can anticipate and counteract AI-driven cyber threats, securing our databases against the intricate challenges of the digital age.

REFERENCES:

1. Jones, A. (2022). "Predictive Analytics in Cybersecurity," Journal of Information Security, 18(2), 123-135.
2. Smith, B., & Nguyen, L. (2023). "Real-time Cyber Threat Detection using Machine Learning," Cybersecurity Technology Review, 11(1), 45-60.
3. Analytics India Magazine. 2018. 5 Artificial Intelligence-Based Attacks That Shocked The World In 2018. Accessed November 28, 2023. https://www.analyticsindiamag.com / 5-artificial- intelligence- based-attacks-that-shocked-the-world-in-2018/
4. Smith, B., & Nguyen, L. (2023). "Real-time Cyber Threat Detection using Machine Learning," Cybersecurity Technology Review, 11(1), 45-60.
5. Lee, D., & Kim, Y. (2021). "Adaptive Machine Learning in Cybersecurity," AI & Security Journal, 14(4), 200-215.
6. Zhang, X., & Wang, H. (2020). "The Dark Side of AI in Cybersecurity," Journal of Advanced Computing, 9(2), 234-245.
7. Patel, S., & Sharma, R. (2022). "Vulnerabilities in AI-Driven Cybersecurity Systems," International Journal of AI Research, 17(3), 789-804.
8. Green, M. (2023). "Usability in AI-Enhanced Security Systems," Journal of Cybersecurity and User Experience, 5(1), 54-69.
9. Khan, A., & Singh, J. (2021). "Ethical Implications of AI in Database Security," Ethics in AI Journal, 4(2), 112-128.
10. Roberts, L. (2022). "Transparency in AI Systems," Journal of AI Ethics, 3(1), 35-50.
11. Brown, T. (2023). "Expert Insights on AI in Cybersecurity," Cybersecurity Review, 12(4), 405-420.
12. Nguyen, H., & Lee, J. (2023). "Hybrid Approaches in Cybersecurity," International Journal of Information Security, 22(1), 88-102.
13. Gomez, R., & Tran, H. (2023). "Strategic AI Integration for Enhanced Cyber Resilience," Advanced Cybersecurity Journal, 7(3), 210-229.
14. Li, S., & Zhou, M. (2022). "Learning from the Past: Historical AI Exploitation in Cybersecurity," Cybersecurity Case Reviews, 6(1), 78-92.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 94 – 104 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

QUANTUM COMPUTING AND CYBER-PHYSICAL SYSTEMS (CPS) SECURITY: IMPLICATIONS, CHALLENGES, AND SOLUTIONS

Ayepeku .O. Felix[1], Omosola .J. Olabode[2]
[1-2]Dept. of Mathematical and Computing Science, Thomas Adewumi University Oko-Irese

ABSTRACT: Quantum computing is a revolutionary technology that has significant implications for Cyber-Physical Systems (CPS) security. CPS, deeply integrated into critical infrastructure and modern technologies, faces unprecedented challenges and vulnerabilities in this era. This article explores the challenges and solutions for CPS security, discussing qubits, superposition, and quantum algorithms. Threats to CPS security have evolved, with quantum attacks posing threats to classical encryption methods. To mitigate these threats, post-quantum cryptography offers quantum-resistant cryptographic techniques suitable for CPS. Strategies for building resilient CPS systems and recovering from quantum attacks are discussed. Real-world case studies highlight the challenges and successes of securing CPS systems in the quantum era. The article also discusses regulatory and compliance frameworks for CPS security.

KEYWORDS: Quantum, computing, Quantum computing, Cyber-Physical Systems, Cryptography.

1.0 INTRODUCTION

Utilizing the ideas of quantum physics, quantum computing is a cutting-edge branch of computation that allows for calculation rates and efficiency beyond the reach of classical computers. Quantum computers employ quantum bits, or qubits, as the fundamental unit of information instead of classical computers, which utilize bits (0s and 1s). Superposition is the phenomenon that allows qubits to exist in several states concurrently.

Because of this special quality of superposition, quantum computers may investigate several solutions to a problem simultaneously, which gives them extraordinary power for particular applications. Quantum computers may also connect the states of qubits via entanglement, another quantum phenomenon, making it possible to do complicated computations that are difficult for conventional computers to complete quickly.

Even though quantum computing has a lot of potential, there are still many unanswered questions on the subject, such as error correction, qubit stability, and useful applications. However, it has the potential to transform a number of fields, including simulations of quantum systems, cryptography, and optimization issues, with far-reaching effects on science, technology, and security.

A crucial confluence of digital processing, communication, and control with the real environment is represented by cyber-physical systems, or CPS. Critical infrastructure and contemporary technologies increasingly depend on these systems, which combine physical (sensing and actuation) and cyber (computing and communication) components. The importance of CPS in various areas is examined in this article.

1.1 AIMS AND OBJECTIVES

- This article's goal is to examine and comprehend how quantum computing may affect cyber-physical systems' (CPS) security. The potential influence of quantum computing on CPS security is becoming more important as it develops.

- To examine the potential impacts of quantum computing on CPS security, including any vulnerabilities.
- It may introduce the measures that can be taken to secure CPS in the quantum era.

1.2 QUANTUM COMPUTING FUNDAMENTALS

Superposition and qubits are two novel ideas introduced by quantum computing, which is based on the fundamental ideas of quantum physics. This section gives a basic introduction to these ideas and emphasizes how important they are to quantum computing.

Qubits:

- While a quantum bit, or qubit, can concurrently exist in a superposition of both states, a classical bit can only represent 0 or 1 [1].
- A quantum bit, also known as a qubit, can concurrently exist in a superposition of both states, whereas a conventional bit can only represent either one.
- In addition to being in a linear combination of these states, represented as $\alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers fulfilling $|\alpha|^2 + |\beta|^2 = 1$, a qubit's state may also be represented as $|0\rangle$ and $|1\rangle$ [2]

Superposition:

- The two possible states for a qubit are $|0\rangle$ and $|1\rangle$. It can also exist in a linear combination of these states, which is represented as $\alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.
- It allows quantum computers to investigate several solutions to a problem concurrently, which might result in exponential speedups for specific tasks. [3]
- For instance, a qubit in a superposition of $|0\rangle$ and $|1\rangle$ can perform operations on both states simultaneously, making it highly efficient for quantum algorithms like Grover's search algorithm [4].

Compared to classical computers, quantum computers have the potential to achieve large computing gains, especially for certain kinds of applications. Some of the possible benefits of quantum computing are examined in this section.

- **Speedup in Factorization and Cryptography**: Using Shor's algorithm, quantum computers may effectively execute integer factorization, possibly compromising popular encryption systems like RSA. [5]. Shor's technique, which is efficient for integer factorization, can be utilized by quantum computers to attack popular encryption systems like RSA.
- **Quantum Search Algorithms**: Grover's technique is a quadratic speedup over traditional search algorithms that quantum computers can use to improve databases and unstructured searches [6]. Applications for this include optimizing databases, retrieving data, and resolving unsorted ones.
- **Simulating Quantum Systems**: It is difficult for conventional computers to effectively model quantum systems, whereas quantum computers can.. This has implications for quantum chemistry, materials science, and drug discovery, enabling the exploration of new molecules and materials [7].
- **Quantum Machine Learning**: Quantum computing has the potential to enhance machine learning algorithms through quantum data processing, enabling complex optimization tasks [8]. Quantum-enhanced machine learning is an emerging field with applications in data analysis and pattern recognition.
- **Parallelism and Exponential Speedup**: Quantum computers can leverage quantum parallelism, allowing them to perform multiple calculations simultaneously. This can lead to exponential

speedups for certain problems. Quantum algorithms can outperform classical algorithms in tasks such as solving systems of linear equations and simulating quantum mechanics [9].

2.0 CURRENT STATE OF CPS SECURITY

Cyber-Physical Systems (CPS) play a vital role in various industries by integrating digital and physical components to enhance efficiency, safety, and control. Here, we describe the role of CPS in critical infrastructure, healthcare, and transportation.

Critical Infrastructure

- **Power Grids**: CPS is integral to managing and optimizing power grids, allowing for real-time monitoring, demand management, and grid stability [10].
- **Water and Wastewater Management**: CPS systems are used to monitor and control water treatment plants, distribution networks, and wastewater management, ensuring clean water supply and environmental protection [11].

Healthcare

- **Medical Devices**: CPS is used to monitor and control medical devices, ensuring patient safety and enabling telemedicine applications [12].
- **Patient Data Management**: Healthcare CPS systems manage electronic health records, providing healthcare professionals with secure access to patient data [13].

Transportation

- **Intelligent Transportation Systems (ITS)**: CPS is at the core of ITS, enabling traffic management, vehicle-to-vehicle (V2V) communication, and autonomous vehicle technologies [14].
- **Aviation**: CPS technologies are essential for aircraft navigation, collision avoidance systems, and air traffic control [15].

Cyber-Physical Systems (CPS) in the classical computing era have faced several security challenges that have had significant implications for their reliability and safety. Here, we highlight some of these security challenges.

- **Vulnerability to Cyberattacks**: Cyberattacks of all kinds, such as malware, denial-of-service (DoS) attacks, and infiltration attempts, might interfere with CPS's regular operations [16].
- **Lack of Encryption and Authentication**: Many CPS devices and components lacked robust encryption and authentication mechanisms, making them susceptible to data breaches and unauthorized access [17].
- **Interconnectedness Risks**: The interconnected nature of CPS components increased the attack surface, as compromising one component could potentially lead to a domino effect affecting the entire system [18].
- **Legacy Systems and Patching**: Many CPS systems used legacy components and operating systems that were difficult to patch and update, leaving them exposed to known vulnerabilities [19].
- **Insider Threats**: Insider threats, such as employees with malicious intent or negligence, pose significant security risks to CPS systems [20].
- **Lack of Standardization**: The absence of comprehensive security standards and best practices specific to CPS made it challenging to develop consistent security measures [21].

2.1 QUANTUM COMPUTING'S THREAT TO CPS

Because quantum computing can solve some mathematical problems that traditional cryptography systems rely on in an efficient manner, it might be a danger to these approaches. Here, we talk about how traditional encryption techniques are threatened by quantum computing.

- **Shor's Algorithm and Integer Factorization**: Shor's technique allows quantum computers to factor big numbers quickly, a job that conventional computers cannot accomplish computationally. This is a serious danger to popular encryption techniques like RSA, which depend on the complexity of integer factorization [22].
- **Grover's Algorithm and Search Problems**: Grover's approach can help quantum computers solve search issues more quickly. This decreases the effective key length and may jeopardize the security of symmetric-key encryption techniques, even though it does not directly destroy encryption.[23]
- **Post-Quantum Cryptography**: Because quantum computing poses a danger to conventional encryption, post-quantum cryptographic algorithms—which are thought to be resistant to quantum attacks—have been developed. These methods are resistant to search algorithms and quantum factorization [24].
- **Quantum-Safe Cryptographic Solutions**: Researchers are exploring quantum-safe cryptographic solutions, including lattice-based, code-based, and multivariate polynomial cryptography, which are resistant to quantum attacks and offer security in the post-quantum era [25].
- **Preparing for the Quantum Threat**: Organizations and governments are taking steps to prepare for the quantum threat by investing in quantum-resistant cryptography, developing quantum key distribution technologies, and monitoring the progress of quantum computing development [26].

Because quantum computers may solve problems more effectively than classical computers, Cyber-Physical Systems (CPS) are vulnerable to quantum assaults. This section includes citations and references to back up the explanation of how vulnerable CPS systems are to two well-known quantum algorithms, Shor's algorithm and Grover's algorithm.

1. **Vulnerability to Shor's Algorithm: Shor's Algorithm**One quantum method that is well-known for its effectiveness at factoring big numbers is Shor's algorithm. This presents a serious danger to traditional cryptographic schemes like RSA encryption, which rely on the complexity of integer factorization [27].
   Impact on CPS: CPS systems often use classical encryption methods to secure data and communications. If an adversary with access to a powerful quantum computer were to use Shor's algorithm, it could potentially break the encryption protecting CPS communications, leading to data compromise and system vulnerabilities.
2. **Vulnerability to Grover's Algorithm: Grover's Algorithm**: Grover's method is a quantum algorithm that outperforms traditional algorithms in unstructured search jobs. It accelerates unsorted database searches by a quadratic factor [28].
   Impact on CPS: Grover's algorithm does not directly break encryption; however, it reduces the effective key length of symmetric-key encryption methods. This means that the time it takes to find the correct key is reduced by a factor of the square root of the key space.
   CPS Example: If an attacker with a quantum computer were to search for an encryption key in a CPS application using Grover's approach, the amount of time needed to breach the encryption would be greatly decreased. This can result in data being intercepted or unauthorized access to the CPS system.
3. **Preparing for Quantum-Resistant CPS Security**: In order to tackle these problems, scholars and professionals are investigating quantum-resistant post-quantum cryptography algorithms, creating quantum-resistant key exchange protocols, and integrating quantum-safe security features in CPS systems [29].

- **CPS Security Standards**: In order to safeguard CPS systems in the future, organizations and regulatory agencies are attempting to create security standards that incorporate quantum-resistant encryption and advise the adoption of quantum-safe algorithms.

2.2 QUANTUM-POST CRYPTOGRAPHY

The development of quantum computing has brought up security issues that are being addressed by Post-Quantum Cryptography (PQC). In order to counteract quantum threats to classical cryptography systems, PQC is introduced in this part, along with references and citations to back up the ideas.

1. **Quantum Threat to Classical Cryptography:** The security and integrity of sensitive data are at risk due to the effective breaking of classical encryption techniques by algorithms like Shor's and Grover's, which is made possible by the advent of powerful quantum computers [30] [31].
2. **Post-Quantum Cryptography (PQC):** A paradigm of cryptographic techniques created especially to fend off quantum assaults is called post-quantum cryptography (PQC). The purpose of these methods is to safeguard information and correspondence in the post-quantum period, as quantum computing presents a significant risk to traditional encryption techniques [32]. PQC seeks to offer security based on mathematical issues that are inefficiently solved by quantum algorithms. Lattice-based, code-based, multivariate polynomial, and other cryptography-related issues are among them [33].
3. **Key Aspects of PQC:** PQC algorithms are made to withstand quantum attacks even in the event that very potent quantum computers become accessible. They provide a better degree of security assurance in the context of quantum threats. PQC ensures that quantum algorithms like Grover's and Shor's don't jeopardize encryption, protecting data integrity and secrecy [34]. To get ready for the quantum danger, businesses and researchers are working hard to standardize and investigate PQC algorithms. This process is aided by projects such as the Post-Quantum Cryptography Standardization initiative of the National Institute of Standards and Technology (NIST) [35].

2.3 CRYPTOGRAPHIC APPROACHES SUITABLE FOR CPS

Cyber-Physical systems (CPS) require the use of cryptographic techniques that are appropriate in order to secure sensitive data and communications. Lattice-based cryptography and code-based cryptography are two viable methods for protecting CPS. These cryptographic techniques will be covered in detail in this discussion, along with citations and references for more reading.

Lattice-Based Cryptography: This type of cryptography is a good option for post-quantum security and may be used to protect CPS against quantum assaults since it is based on the difficulty of certain lattice issues [36]. Lattice-based cryptography techniques such as LWE (Learning with Errors) and NTRU (Nth-degree truncated polynomial ring) are thought to be robust against quantum errors and to provide excellent security guarantees [37]. Lattice-based cryptography, which offers safe encryption, digital signatures, and key exchange protocols, is renowned for its adaptability and appropriateness for use in CPS applications [38].

Formula-Based The foundation of cryptography lies in the difficulty of particular coding theory issues, notably the decoding of random linear codes [39]. One of the most well-known code-based cryptography techniques is the McEliece encryption method. It has uses in secure key exchange for CPS and is thought to be safe against quantum attacks [40]. Strong security guarantees and comparatively efficient processing complexity make code-based cryptography appropriate for CPS devices with limited resources [41].

3.0 RESILIENCE AND RECOVERY STRATEGIES

Quantum-safe backups are crucial for restoring critical critical point systems (CPS) data and configurations in the event of a quantum attack. These backups can be created using quantum-resistant

encryption, ensuring data can be securely restored. Quantum-resistant data reconstruction methods can help restore data and system functionality without relying on compromised cryptographic keys. Incident response and recovery plans should be implemented, highlighting the steps to take in case of a security breach and prioritizing the restoration of CPS functionality. Key rotation protocols should be implemented for continuous encryption key updates, restoring data security in the event of a quantum attack. Quantum-resistant firmware and software updates can patch vulnerabilities exposed by quantum attacks and restore system integrity. Distributed system redundancy can be built into CPS systems with distributed components, allowing for continuous system operation in case of a quantum attack. These strategies help ensure the security and integrity of critical CPS systems.

3.1 RECOVERY MECHANISMS TO RESTORE CPS FUNCTIONALITY FOLLOWING QUANTUM ATTACKS

Quantum-safe backups are crucial for restoring critical point systems (CPS) data and configurations in the event of a quantum attack. These backups can be created using quantum-resistant encryption, ensuring data can be securely restored. Quantum-resistant data reconstruction methods can help restore data and system functionality without relying on compromised cryptographic keys. Incident response and recovery plans should be implemented, highlighting the steps to take in case of a security breach and prioritizing the restoration of CPS functionality. Key rotation protocols should be implemented for continuous encryption key updates, restoring data security in the event of a quantum attack. Quantum-resistant firmware and software updates can patch vulnerabilities exposed by quantum attacks and restore system integrity. Distributed system redundancy can be built into CPS systems with distributed components, allowing for continuous system operation in case of a quantum attack. These strategies help ensure the security and integrity of critical CPS systems.

3.2 QUANTUM-SAFE CPS DESIGN

The design of quantum-safe Cyber-Physical Systems (CPS) is an essential strategy for guaranteeing the security and robustness of CPS in the post-quantum future. To safeguard data and communications, post-quantum cryptographic procedures are used, such as digital signatures, key exchange protocols, and encryption that is resistant to quantum emulation. Quantum-resistant hardware components, such as hardware security modules, secure key storage, and hardware-based random number generators, are also designed to withstand quantum attacks. Secure firmware and software for CPS devices and control systems are developed, including secure boot mechanisms, software patches, and continuous monitoring for quantum vulnerabilities. Quantum-safe key management and rotation protocols ensure that cryptographic keys are continually updated to quantum-resistant alternatives, preventing potential exposure in case of a quantum attack. Resilient network infrastructure is built for CPS, including quantum-safe communication channels and monitoring mechanisms, to protect data in transit and ensure the availability of CPS even in the face of quantum threats. Adhering to established security standards and regulatory compliance, including quantum-safe security recommendations and best practices for CPS design and operation, is also essential. Continuous monitoring and response mechanisms are implemented to detect and mitigate quantum threats in real-time, identifying vulnerabilities and responding swiftly to potential attacks. By integrating these principles into CPS design, organizations can enhance their systems' security and resilience in anticipation of the quantum threat landscape.

3.3 IMPORTANCE OF SECURE KEY DISTRIBUTION AND MANAGEMENT IN QUANTUM-SAFE CPS

Secure key distribution and management are crucial for the security and resilience of Cyber-Physical Systems (CPS), especially in the context of quantum-safe design. Quantum computers can break

traditional cryptographic keys, making it essential to employ quantum-resistant keys. Quantum Key Distribution (QKD) offers a secure means of distributing cryptographic keys that are provably secure against quantum eavesdropping, providing a foundation for securing CPS communications in a post-quantum era. Regular key rotation with quantum-resistant keys is essential to prevent long-term exposure to potential quantum attacks. Secure key management ensures that encryption keys are continually updated to quantum-safe alternatives. Resilience and data protection are also important aspects of secure key distribution and management. Effective key management is vital to maintaining data protection in the face of quantum threats. Compliance with security standards and regulations often includes requirements for secure key distribution and management, helping organizations meet legal and industry-specific security requirements.

3.4 CASE STUDIES AND EXAMPLES

Researchers are exploring the use of quantum-safe communication protocols in smart grids, Industrial Internet of Things (IIoT), and healthcare systems to protect critical infrastructure. Quantum-resistant encryption and key exchange mechanisms are being explored to secure data and control messages in the grid, ensuring system reliability and resilience. In healthcare systems, quantum-safe cryptographic protocols are being used to protect patient data and medical devices, particularly those involving remote monitoring and telemedicine. Some healthcare organizations are also exploring the use of quantum-safe cryptographic protocols to enhance security in remote monitoring and telemedicine. Secure Quantum Key Distribution (QKD) is being integrated into critical infrastructure systems, such as in energy and financial sectors, to ensure secure communication channels resistant to quantum attacks. These efforts aim to enhance the security of critical infrastructure and improve the reliability and resilience of these systems.
These examples showcase the ongoing research and limited practical implementations of quantum-safe measures in CPS systems. As quantum technologies continue to advance, it is expected that more real-world applications and deployments of quantum-safe security measures in CPS will emerge to ensure the resilience of critical infrastructure and interconnected systems against quantum threats.

3.4.1 Challenges:

The challenges in implementing quantum-safe cryptographic algorithms in the Computer-Physical Systems (CPS) domain include limited awareness and understanding of quantum threats, integration complexity, resource constraints, and standards and interoperability. Many organizations are unaware of the potential impact of quantum computing on their systems, and integrating quantum-safe measures into existing CPS can be complex and costly. Additionally, some CPS devices and sensors may have resource limitations, making it difficult to implement complex quantum-safe cryptographic algorithms. Quantum Key Distribution (QKD) is a promising quantum-safe technology, but its deployment and practicality are also challenges.

3.4.2 Successes:

Quantum-resistant cryptographic algorithms and protocols have been developed, laying the foundation for quantum-safe security measures in quantum-proof systems (CPS). Awareness of quantum threats has led to initiatives exploring quantum-safe security in various CPS domains. Pilot projects and demonstrations have demonstrated the feasibility of implementing quantum-safe measures in real-world applications. Collaboration between industry, academia, and government bodies has advanced quantum-safe security research and standards. Regulatory bodies, like the National Institute of Standards and Technology (NIST), are addressing the importance of quantum-safe security. Quantum Key Distribution (QKD) has shown potential in sectors like finance and critical infrastructure.

3.5 REGULATORY AND COMPLIANCE FRAMEWORKS

The National Institute of Standards and Technology (NIST) is working on standardizing post-quantum cryptography, a crucial aspect of quantum-safe security standards. GDPR in the European Union emphasizes data protection, including quantum-safe security. The IEEE Quantum Safe Working Group guides best practices for quantum-safe security, including CPS applications. International standards organizations like the International Organization for Standardization (ISO) are also exploring quantum-safe security standards to guide organizations in securing their CPS against quantum threats.
Security standards provide organizations with a structured approach to security, reducing the likelihood of security breaches and vulnerabilities. They outline best practices, controls, and procedures to protect against threats and vulnerabilities. Compliance with these standards helps organizations identify, assess, and mitigate risks effectively, reducing the likelihood of financial and reputational damage. Compliance with regulatory and legal requirements helps organizations meet these obligations, while trust and customer confidence are fostered. Compliance can provide a competitive advantage, as clients and partners prefer organizations with robust security measures. Incident response and recovery guidelines are also included in security standards. Finally, compliance allows organizations to demonstrate accountability to regulators, customers, and stakeholders, providing evidence of the implementation, auditing, and maintenance of security measures.

4.0 FUTURE PROSPECTS AND CHALLENGES

Quantum computing is expected to significantly impact Cyber-Physical Systems (CPS) security, making platforms more accessible to researchers and malicious actors. Organizations must adapt to quantum-resistant cryptographic solutions to protect CPS from quantum attacks. International standards bodies and regulatory agencies will establish quantum-safe CPS standards to guide implementation. Quantum Key Distribution (QKD) will see increased adoption in CPS and critical infrastructure sectors, bolstering data transmission and control messages' security. Research in quantum-resistant protocols will lead to more efficient and practical solutions. Organizations must develop and implement quantum-safe resilience strategies to ensure CPS systems maintain functionality and data integrity even in the presence of quantum attacks.

5.0 CONCLUSION

Quantum computing is a rapidly advancing technology that poses a threat to classical encryption methods and the security of critical public services (CPS) systems. Organizations must prepare for the inevitable impact of quantum computing on their security infrastructure, ensuring long-term security, cost-effective transition, protection of sensitive data, compliance with emerging regulations, building stakeholder trust, and ensuring sustainable resilience. Quantum-safe security measures are designed to withstand quantum attacks and provide enduring protection, making preparation essential for uninterrupted CPS functionality. Proactive preparation can enhance an organization's reputation for security and reliability. Quantum computing poses a threat to Cyber-Physical Systems (CPS) security, necessitating the implementation of quantum-safe measures. Challenges include developing cryptographic standards, deploying QKD, and designing hardware. International standards bodies and regulatory agencies are working on establishing standards and regulations

6.0 REFERENCES

1. Devitt, S. J., Schütz, M. J. A., & Plenio, M. B. (2017). Quantum computation and quantum information theory. Contemporary Physics, 58(1), 36-61.
2. Mermin, N. D. (2007). Quantum Computer Science: An Introduction. Cambridge University Press.’

3. Kaye, P., Laflamme, R., & Mosca, M. (2007). An Introduction to Quantum Computing. Oxford University Press.
4. A New Exponentially Fast Quantum Algorithm for Searching Target in the Unstructured Database." 2022. Quantum Physics Letters 11, no. 1 (April): 13–17. https://doi.org/10.18576/qpl/110103.
5. Gurevich, Yuri, and Andreas Blass. 2023. "Software Science View on Quantum Circuit Algorithms." Information and Computation 292, no. June (June): 105024. https://doi.org/10.1016/j.ic.2023.105024.
6. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.
7. Kain, Ben. 2021. "Searching a Quantum Database with Grover's Search Algorithm." American Journal of Physics 89, no. 6 (June): 618–26. https://doi.org/10.1119/10.0004835.
8. McArdle, S., Endo, S., Aspuru-Guzik, A., & Benjamin, S. C. (2020). Quantum computational chemistry. Reviews of Modern Physics, 92(1), 015003.
9. Konno, Norio, Etsuo Segawa, and Martin Štefaňák. 2021. "Relation between Quantum Walks with Tails and Quantum Walks with Sinks on Finite Graphs." Symmetry 13, no. 7 (June): 1169. https://doi.org/10.3390/sym13071169.
10. Ye, Linlin, Zhaoqi Wu, and Shao-Ming Fei. 2023. "Coherence Dynamics in Quantum Algorithm for Linear Systems of Equations." Physica Scripta 98, no. 12 (November): 125104. https://doi.org/10.1088/1402-4896/ad0584.
11. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2016). Smart grid technologies: Communication technologies and standards. IEEE Transactions on Industrial Informatics, 7(4), 529-539.
12. Zagonari, Fabio, and Claudio Rossi. 2020. "A Spatial Decision Support System for Optimally Locating Treatment Plants for Safe Wastewater Reuse: An Application to Saudi Arabia." DESALINATION AND WATER TREATMENT 178: 1–20. https://doi.org/10.5004/dwt.2020.24979.
13. Stangl, Anne L., Valerie A. Earnshaw, Carmen H. Logie, Wim van Brakel, Leickness C. Simbayi, Iman Barré, and John F. Dovidio. 2019. "The Health Stigma and Discrimination Framework: A Global, Crosscutting Framework to Inform Research, Intervention Development, and Policy on Health-Related Stigmas." BMC Medicine 17, no. 1 (February). https://doi.org/10.1186/s12916-019-1271-3.
14. Cheng, S., & Yu, W. (2016). Wireless-telemedicine healthcare framework based on the internet of things. IEEE Transactions on Industrial Informatics, 12(4), 1470-1481.
15. Al-Emran, M., & Shaalan, K. (2019). Internet of things (IoT), blockchain and fog computing for industry 4.0: A survey. Journal of Industrial Information Integration, 15, 100107.
16. Hansen, M. (2019). CPS trends in aerospace and aviation. In 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC) (pp. 1-13). IEEE.
17. M., & Sinopoli, B. (2012). Cyber-Physical Attacks and Defenses in the Smart Grid: A Review. In 2012 50th Annual Allerton Conference on Communication, Control, and Computing (pp. 1343-1350). IEEE.
18. "Distributed Detection Mechanism and Resilient Consensus Strategy for Secure Voltage Control of AC Microgrids." 2023. CSEE Journal of Power and Energy Systems. https://doi.org/10.17775/cseejpes.2020.07140.
19. Li, Li, Huan Yang, Yuanqing Xia, and Cui Zhu. 2021. "Attack Detection and Distributed Filtering for State-Saturated Systems Under Deception Attack." IEEE Transactions on Control of Network Systems 8, no. 4 (December): 1918–29. https://doi.org/10.1109/tcns.2021.3089146.
20. Khan, Shaharyar, and Stuart E. Madnick. 2019. "Cybersafety: A System-Theoretic Approach to Identify Cyber-Vulnerabilities & Mitigations in Industrial Control Systems." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3542551.
21. Warriach, E. U., & Zhang, H. (2017). Cyber Physical Attacks and Defense in the Smart Grid: A Review. In 2017 25th European Signal Processing Conference (EUSIPCO) (pp. 1843-1847). IEEE.

22. Paudel, Nilakantha, and Ram C. Neupane. 2021. "A General Architecture for a Real-Time Monitoring System Based on the Internet of Things." Internet of Things 14, no. June (June): 100367. https://doi.org/10.1016/j.iot.2021.100367.
23. Ekerå, Martin. 2021. "Quantum Algorithms for Computing General Discrete Logarithms and Orders with Tradeoffs." Journal of Mathematical Cryptology 15, no. 1 (January): 359–407. https://doi.org/10.1515/jmc-2020-0006.
24. Kain, Ben. 2021. "Searching a Quantum Database with Grover's Search Algorithm." American Journal of Physics 89, no. 6 (June): 618–26. https://doi.org/10.1119/10.0004835.
25. D. J., Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.
26. Ding, J., Perlner, R. A., Smith-Tone, D., Solinas, J. A., & Bassham, L. E. (2019). Report on Post-Quantum Cryptography. National Institute of Standards and Technology (NIST)
27. National Security Agency (NSA). (2015). Commercial National Security Algorithm Suite. https://www.nsa.gov/ia/programs/suiteb_cryptography/.
28. Ekerå, Martin. 2021. "Quantum Algorithms for Computing General Discrete Logarithms and Orders with Tradeoffs." Journal of Mathematical Cryptology 15, no. 1 (January): 359–407. https://doi.org/10.1515/jmc-2020-0006.
29. Kozhukhivskyy, A. D. 2022. "Quantum Search Algorithm in Unstructured Database." Scientific Notes of the State University of Telecommunications 2, no. 1. https://doi.org/10.31673/25187678.2022.021014.
30. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science (pp. 124-134). IEEE.
31. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).
32. Bernstein, D. J., Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.
33. Ding, J., Perlner, R. A., Smith-Tone, D., Solinas, J. A., & Bassham, L. E. (2019). Report on Post-Quantum Cryptography. National Institute of Standards and Technology (NIST).
34. Alagic, G., Chang, D., Ducas, L., Langlois, A., Mironov, I., Peikert, C., ... & Yun, A. (2021). The NIST post-quantum cryptography standardization process. Journal of Cryptographic Engineering, 1-30.
35. National Institute of Standards and Technology (NIST). (2021). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.
36. Ding, J., Perlner, R. A., Smith-Tone, D., Solinas, J. A., & Bassham, L. E. (2019). Report on Post-Quantum Cryptography. National Institute of Standards and Technology (NIST).
37. Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4), 283-424.
38. Micciancio, D., & Peikert, C. (2013). Hardness of SIS and LWE with small parameters. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 21-39). Springer.
39. Ilanthenral, K., and K. S. Easwarakumar. 2014. "Hexi McEliece Public Key Cryptosystem." Applied Mathematics & Information Sciences 8, no. 5 (September): 2595–2603. https://doi.org/10.12785/amis/080559.
40. Misoczki, R., Barreto, P. S. L. M., Schmidt, D., Lemire, D., & Otmani, A. (2013). MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In International Workshop on Post-Quantum Cryptography (pp. 54-79). Springer.
41. Bernstein, D. J., Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194
42. Ahmed, M., Jamshid, J., Latif, A., & Ullah, S. (2023). Cloud Computing Adoption by Universities: An Analysis Based on Lasbela University. International Journal of Computing and Related Technologies, 3(2), 8-20. Retrieved from http://ijcrt.smiu.edu.pk/ijcrt/index.php/smiu/article/view/141

43. Zuzana Arki2G. K. (2019). Is it possible to change the information security awareness of the students in the Higher Education?. International Journal of Computing and Related Technologies, 1(2), 25-32. Retrieved from http://ijcrt.smiu.edu.pk/ijcrt/index.php/smiu/article/view/66

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 105 – 110 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ინტერნეტ ფარგმენტაციის გამოწვევები და გლობალური კიბერსივრცე

ვლადიმერ სვანაძე[1]

[1]საჯარო მმართველობის დოქტორი, ბიზნესისა და ტექნოლოგიების უნივერსიტეტის აფილირებული პროფესორი

რეზუმე: „ინფორმაციული აფეთქება“ ასე უწოდეს თავის დროს ინფორმაციული ტექნოლოგიების გლობალური განვითარებისა და მომხმარებლის სწრაფი ტემპებით ზრდის პროცესს. მოცემული პროცესი კიდევ უფრო დააჩქარა პანდემიის არსებობამ, რომლის დროსაც ინტერნეტისა და ინტერნეტ ტექნოლოგიების გამოყენებამ როგორც საყოფაცხოვრებო, ისე პროფესიულ დონეზე არნახულ ზღვარს მიაღწია. სამწუხაროდ, ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფი მიმართულებით განვითარების პოზიტიურ პროცესს თან ახლავს გარკვეული რისკები, რაც საფრთხეს უქმნის გლობალური ინტერნეტ ქსელის ერთიანობასა და უსაფრთხოებას, მის მდგრადობასა და სტაბილურ განვითარებას. როცა ვსაუბრობთ გლობალური ინტერნეტ ქსელის ერთიანობაზე, უსაფრთხოებასა და სტაბილურობაზე, აუცილებლად უნდა ავღნიშნოთ გაერთიანებული ერების ორგანიზაციის გენერალური მდივნის მიერ მოწვეული ინტერნეტ მმართველობის ფორუმი[1], რომლის მუშაობაში ჩართული არის ყველა დაინტერესებული მხარე - საჯარო და კერძო სექტორები, სამოქალაქო საზოგადოება და აკადემიური წრეების წარმომადგენლები. ეს არის საუკეთესო პლატფორმა, სადაც ხდება ინტერნეტ სივრცეში მიმდინარე პროცესების შესახებ აზრთა გაცვლა, დისკუსია და გამოცდილებების გაზიარება დაინტერესებულ მხარეთა შორის როგორც გლობალურ, ისე ეროვნულ და რეგიონალურ დონეზე.

საკვანძო სიტყვები: ინტერნეტი, ინტერნეტ ტექნოლოგიები, ინტერნეტ ფრაგმენტაცია, კიბერსივრცე, კიბერუსაფრთხოება, კიბერდანაშაული, ინტერნეტ პროტოკოლები, კონფლიქტები, ინტერნეტ მმართველობის ფორუმი, ტუნისის დღის წესრიგი

ABSTRACT: "Information explosion" was the name given to the process of global development of information technologies and rapid growth of users. This process was further accelerated by the existence of the pandemic, during which the use of the Internet and Internet technologies at both the household and professional levels reached an unprecedented limit. Unfortunately, the positive process of rapid development of the Internet and Internet technologies is accompanied by certain risks, which threaten the unity and security of the global Internet network, its stability and stable development. When we talk about the unity, security and stability of the global Internet network, we must mention the Internet Governance Forum convened by the Secretary General of the United Nations, whose work involves all interested parties - public and private sectors, civil society and representatives of academic circles. It is the best platform where the exchange of ideas, discussion and sharing of experiences about the processes taking place in the Internet space takes place among the interested parties at the global, national and regional levels.

KEYWORDS: Internet, Internet Technology, Internet Fragmentation, Cyberspace, Cybersecurity, Cybercrime, Internet Protocols, Conflicts, Internet Governance Forum, Tunis Agenda

[1] https://www.intgovforum.org/en/about#about-us

1. შესავალი

2005 წელს გაერთიანებული ერების ორგანიზაციის მიერ მიღებულ იქნა საინფორმაციო საზოგადოებისთვის ტუნისის დღის წესრიგის მიღება[2], რაც წინ უსწრებდა ინტერნეტ მმართველობის ფორუმის მოწვევას. ეს მოიცავდა ტერმინის ინტერნეტის მმართველობის განმარტებასა და იმის აღიარებას, რომ ინტერნეტის მართვის პროცესი მოიცავს დაინტერესებულ მხარეთა ჩართულობას სხვადასხვა როლებში. კერძოდ, საინფორმაციო საზოგადოებისთვის ტუნისის დღის წესრიგში ვკითხულობთ, რომ „ინტერნეტის მმართველობა არის მთავრობების, კერძო სექტორისა და სამოქალაქო საზოგადოების მიერ თავიანთი როლების შემუშავება და გამოყენება საერთო პრინციპების, ნორმების, წესების, გადაწყვეტილების მიღების პროცედურებისა და პროგრამების, რომლებიც აყალიბებენ ინტერნეტის ევოლუციას და გამოყენებას“ (Tunis Agenda for the Information Society) [1].

აქვე უნდა აღინიშნოს, რომ ტუნისის დღის წესრიგის 72 - ე პარაგრაფი ადგენს ინტერნეტ მმართველობის ფორუმის მანდატს[3], სადაც ვკითხულობთ, რომ:

- **a)** ინტერნეტის მართვის ძირითად ელემენტებთან დაკავშირებული საჯარო პოლიტიკის საკითხების განხილვა, რათა ხელი შეუწყოს ინტერნეტის მდგრადობას, გამძლეობას, უსაფრთხოებას, სტაბილურობას და განვითარებას;
- **b)** ხელი შეუწყოს დისკუსიას იმ ორგანოებს შორის, რაც ეხება ინტერნეტთან დაკავშირებით სხვადასხვა საერთაშორისო თუ საჯარო პოლიტიკას და განიხილავს ისეთ საკითხებს, რომლებიც არ განეკუთვნება არცერთ არსებულ ორგანოს სფეროს;
- **c)** მათ დაქვემდებარებაში მყოფ საკითხებზე შესაბამის სამთავრობათაშორისო ორგანიზაციებთან და სხვა ინსტიტუტებთან ურთიერთობა;
- **d)** ინფორმაციისა და საუკეთესო პრაქტიკის გაცვლის ხელშეწყობა და ამ კუთხით აკადემიური, სამეცნიერო და ტექნიკური საზოგადოებების ექსპერტიზის სრულად გამოყენება;
- **e)** ურჩიეთ ყველა დაინტერესებულ მხარეს განვითარებად სამყაროში ინტერნეტის ხელმისაწვდომობისა და მისი დაჩქარების გზებისა და საშუალებების შეთავაზებაში;
- **f)** გააძლიეროს დაინტერესებული მხარეების ჩართულობა ინტერნეტის მართვის არსებულ და/ან მომავალ მექანიზმებში, განსაკუთრებით განვითარებადი ქვეყნებიდან;
- **g)** აღმოაჩინოს წამოჭრილი საკითხები, მიაწოდოს ისინი შესაბამის ორგანოებსა და ფართო საზოგადოებას. საჭიროების შემთხვევაში, რეკომენდაციების გაცემა;
- **h)** წვლილის შეტანა განვითარებად ქვეყნებში ინტერნეტის მართვის შესაძლებლობების განვითარებაში, ცოდნისა და ექსპერტიზის ადგილობრივი წყაროების სრულად გამოყენებით;
- **i)** ინტერნეტის მართვის პროცესებში WSIS[4] პრინციპების ხელშეწყობა და შეფასება;
- **j)** კრიტიკულ ინტერნეტ რესურსებთან დაკავშირებული საკითხების განხილვა;
- **k)** დახმარება ინტერნეტის ბოროტად გამოყენების შედეგად წარმოქმნილი საკითხების გადაწყვეტაში, რაც განსაკუთრებით აწუხებს ყოველდღიურ მომხმარებლებს;
- **l)** საქმიანობის ღიაობა.

[2] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[3] https://www.iisd.org/system/files/publications/igf_mandate_review.pdf
[4] World Summit on the Internet Society

ფაქტიურად, გაერთიანებული ერების ორგანიზაციის ასამბლეა აღიარებს ფორუმის მნიშვნელობას ინტერნეტის მდგრადობის, გამძლეობის, უსაფრთხოების, სტაბილურობისა და განვითარების ხელშეწყობაში.

სწორედ ინტერნეტ და ინტერნეტ ტექნოლოგიების სულ უფრო აქტიურმა გამოყენებამ კიდევ უფრო გაზარდა მისი მნიშვნელობა და მასზე დამოკიდებულება. გარდა ამისა, ინტერნეტი და ზოგადად, კიბერსივრცე დადგა ახალი საფრთხის წინაშე, რაც უკავშირდება ცალკეული ავტოკრატული ხელისუფლებების მხრიდან მასზე ტოტალური კონტროლის დაწესებას, გლობალურად არსებულ ეთნოკონფლიქტებსა და საომარ მოქმედებებს, გაზრდილ კიბერდანაშაულებებს. ყოველივე ეს კი არღვევს ინტერნეტის ერთიანობასა და მდგრადობას, საფრთხეს უქმნის მის სტაბილურ და უსაფრთხო განვითარების პროცესს. მოცემული პროცესი ასევე ეწინააღმდეგება გაერთიანებული ერების ორგანიზაციის ასამბლეის მიერ თავის დროზე მიღებულ ტუნისის დღის წესრიგს [2].

ბოლო წლებში სულ უფრო ხშირად გამოითქმის შეშფოთება იმის თაობაზე, რომ ინტერნეტს ემუქრება დაშლის საფრთხე ერთმანეთთან სუსტად დაკავშირებულ ცალკეულ ფრაგმენტებად. მთელი რიგი შემაშფოთებელი ტენდენციები, რაც უკავშირდება ტექნოლოგიურ განვითარებას, სახელმწიფოების ინტერნეტ პოლიტიკასა და კომერციულ სამიანობას, ასევე არსებულ საერთაშორისო ვითარებას, ვრცელდება ინტერნეტ ქსელში, მის ცალკეულ ფენებში, რაც გავლენას ახდენს პროცესზე რასაც უწოდეს ინტერნეტ ფრაგმენტაცია. თუმცა უნდა აღინიშნოს, რომ ჯერ კიდევ არ არსებობს ფართო გაგება იმისა თუ რა არის და რა არ არის „ფრაგმენტაცია“, ან რა რისკებს უქმნის ის ინტერნეტის, იგივე კიბერსივრცის ერთიანობას, სტაბილურობასა და უსაფრთხოებას.

აქ ჩნდება კითხვა რა არის „ინტერნეტ ფრაგმენტაცია“ და როგორ შეიძლება ეს ტერმინი თუ ქმედება განისაზღვროს?

ინტერნეტ ფრაგმენტაცია, იგივე Splinternet, ეს არის ინტერნეტის საწინააღმდეგო, მისი საპირისპირო. Splinternet არის იდეა, რომლის მიხედვით ღია, უსაფრთხო და სტაბილური გლობალურად ერთიანი ინტერნეტი, რომლითაც ჩვენ ვსარგებლობთ, იყოფა ცალკეულ ერთმანეთისგან იზოლირებულ ქსელებად, რომლებიც კონტროლდება სახელმწიფოებისა და კორპორაციების მიერ. გარდა ამისა, „ინტერნეტ ფრაგმენტაციის“ მსგავს განსაზღვრებას, ბოლო დროს განვითარებული გლობალური მოვლენების გათვალისწინებით, შეიძლება დავუმატოთ ასევე საომარი მოქმედებები და ეთნოკონფლიქტები, რომლებიც უკვე ფიზიკურად აზიანებს კიბერსივრცის ერთიანობას [3].

2. ინტერნეტის ფრაგმენტაციის ფორმები

განსაზღვრებიდან გამომდინარე, არსებობს ინტერნეტ ფრაგმენტაციის ყველასთვის ნაცნობი სამი ფორმა:

1. **ტექნიკური ფრაგმენტაცია** - ეს არის საბაზისო ინფრასტრუქტურის პირობები, რომლებიც აფერხებენ სისტემების სრულყოფილ და თანხვედრილ ურთიერთობას, მონაცემთა პაკეტების გაცვლასა და ინტერნეტის ნორმალურ ფუნქციონირებას;
2. **სახელმწიფო ფრაგმენტაცია** - ცალკეული ქვეყნების მთავრობების ინტერნეტ პოლიტიკა და ქმედებები, რომლებიც ზღუდავს ან ხელს უშლის ინტერნეტის გარკვეულ გამოყენებას საინფორმაციო რესურსების შესაქმნელად, მათი გავრცელების ან წვდომისათვის;
3. **კომერციული ფრაგმენტაცია** - ბიზნეს პრაქტიკა, რომელიც ზღუდავს ან ხელს უშლის ინტერნეტის გარკვეულ გამოყენებას საინფორმაციო რესურსების ინფორმაციის რესურსების შესაქმნელად, მათი გავრცელების ან წვდომისათვის.

აქვე, ინტერნეტ ფრაგმენტაციის მეოთხე ტიპად შეიძლება დავამატოთ - **საერთაშორისო, გლობალური თუ რეგიონალური ინტერნეტ ფრაგმენტაცია,** რომელიც მივიღეთ ამა თუ იმ მთავრობების როგორც შიდა, ისე საგარეო ინტერნეტ პოლიტიკების, საომარი მოქმედებებისა და ზოგადად, გლობალურად თუ რეგიონალურად არსებული არამდგრადი ვითარების შედეგად, რაც ზიანს აყენებს ინტერნეტის ერთიანობას, უსაფრთხოებასა და სტაბილურობას [4-5].

სანამ თითოეული ფორმის განხილვას დავიწყებთ აუცილებელია ასევე აღინიშნოს ის გარემოება, რომ ინტერნეტ ფრაგმენტაციის თითოეული ტიპი შეიძლება ძალზედ განსხვავდებოდეს მთელი რიგი განზომილებების მიხედვით. ამ შემთხვევაში გამოვყოთ ოთხი ძირითადი მახასიათებელი, კერძოდ:

1) **წარმოშობა** - ანუ არსებობს თუ არა ფრაგმენტაციის ესა თუ ის ფორმა და რა პოტენციური საფრთხის შემცველია ფრაგმენტაციის კონკრეტული ფორმა;
2) **მიზანმიმართულობა** - ფრაგმენტაცია ეს არის მიზანმიმართული მოქმედების შედეგი თუ გაუთვალისწინებელი, სპონტანური შედეგი;
3) **გავლენა** - არის ფრაგმენტაცია ღრმა, სტრუქტურული და კონფიგურაციული, თუ ეს უფრო არის ზედაპირული, ვიწრო და შეზღუდული პროცესების ერთობლიობა;
4) **ხასიათი** - ზოგადად, არის თუ არა ფრაგმენტაცია დადებითი, უარყოფითი ან ნეიტრალური.

3. პრობლემური კატეგორიები

ინტერნეტ ფრაგმენტაციის თითოეულ ფორმის განხილვისას განიხილება სხვადასხვა სახის პრობლემური კატეგორიები და მათგან გამომდინარე ფრაგმენტაციის სახეობები, კერძოდ [6]:

1. ტექნიკური ფრაგმენტაციის დროს განიხილება ოთხი პრობლემური კატეგორია - ინტერნეტ მისამართები, ინტერნეტ დაერთებები, ინტერნეტის დასახელება და მისი უსაფრთხოება. მოცემული კატეგორიების ფარგლებში იდენტიფიცირებულია სხვადასხვა ხარისხისა და მნიშვნელობის ფრაგმენტაციის შემდეგი 12 სახეობა:
   - ქსელური მისამართების ტრანსლაცია (Network Address Translation);
   - IPv6 - ს შეუთავსებლობა და ორმაგი დასტის მოთხოვნა (IPv6 შეუთავსებლობა და ორმაგი წყობის მოთხოვნა);
   - კორუფციის მარშრუტირება;
   - Firewall-ის დაცვა;
   - ვირტუალური კერძო ქსელის იზოლაცია და დაბლოკვა;
   - TOR “onion space” და “dark web”;
   - ინტერნაციონალიზებული დომენური სახელების (IDN) ტექნიკური შეცდომები;
   - ახალი ზოგადი ტოპ დონის დომენების ბლოკირება;
   - პერსონალური სახელების სერვერები და დანაწევრებული ჰორიზონტის DNS;
   - სეგმენტირებული Wi-Fi სერვისები სასტუმროებში, რესტორნებში და ა.შ.;
   - ალტერნატიული DNS წყაროების შესაძლებლობა;
   - სერტიფიცირების ორგანოების მიერ ყალბი სერთიფიკატების წარმოება.
2. სახელმწიფო ფრაგმენტაციის შემთხვევაში განიხილება შემდეგი ექვსი კატეგორია:
   - შინაარსი და ცენზურა;
   - ელექტრონული კომერცია და ვაჭრობა;
   - ეროვნული უსაფრთხოება;

- კონფიდენციალურობა და მონაცემთა დაცვა;
- მონაცემთა ლოკალიზაცია;
- ფრაგმენტაცია, როგორც ყოვლისმომცველი ეროვნული სტრატეგია.

მოცემული კატეგორიების ფარგლებში იდენტიფიცირებულია სხვადასხვა ხარისხის ფრაგმენტაციის შემდეგი 10 სახეობა:

- იმ ვებსაიტების, სოციალური ქსელების ან სხვა რესურსების გაფილტვრა და დაბლოკვა, რომლებიც არასასურველ კონტენტს გვთავაზობენ;
- იმ საინფორმაციო რესურსებზე თავდასხმები, რომლებიც არასასურველ კონტენტს გვთავაზობენ;
- ციფრული პროტექციონიზმი ელექტრონული კომერციის ძირითადი პლატფორმებისა და ინსტრუმენტების გამოყენებაზე ბლოკავს მომხმარებლების წვდომას;
- საერთაშორისო ურთიერთკავშირის ცენტრალიზაცია;
- თავდასხმები ეროვნულ ქსელებსა და ძირითად აქტივებზე;
- ადგილობრივი მონაცემთა დამუშავების ან/და შენახვის მოთხოვნები;
- მონაცემთა ნაკადის შესანარჩუნებლად, ტერიტორიის ფარგლებში არქიტექტურული ან მარშრუტის ცვლილებები;
- გარკვეული კატეგორიის მონაცემების ტრანსსასაზღვრო გადაადგილების აკრძალვები;
- „ეროვნული ინტერნეტ სეგმენტების“ ან „კიბერსუვერენიტეტის“ შექმნის სტრატეგიები;
- საერთაშორისო ჩარჩოები, რომლებიც შემზღუდავი პრაქტიკის ლეგიტიმაციას ისახავს მიზნად.

3. კომერციული ფრაგმენტაცია განიხილავს ხუთ კატეგორიას. კერძოდ, ესენია - თანასწორობა და სტანდარტიზაცია; ქსელის ნეიტრალიტეტი; ე.წ. “walled gardens”; გეო-ლოკალიზაცია და გეობლოკირება; ინფრასტრუქტურასთან დაკავშირებული ინტელექტუალური საკუთრების დაცვა [7]. მოცემულ შემთხვევაში იდენტიფიცირებულია სხვადასხვა ხარისხის ფრაგმენტაციის შემდეგი 6 სახეობა:

- პოტენციური ცვლილებები ურთიერთკავშირის ხელშეკრულებებში;
- პოტენციური საკუთრების ტექნიკური სტანდარტები, რომლებიც IoT-ში თავსებადობას აფერხებენ;
- ქსელის ნეიტრალიტეტიდან ბლოკირება, ჩახშობა ან სხვა დისკრიმინაციული გადახრები;
- ე.წ. “Walled gardens”
- კონტენტის გეობლოკირება;
- დასახელებისა და ნუმერაციის პოტენციური გამოყენება ინტელექტუალური საკუთრების დაცვის მიზნით შინაარსის დასაბლოკად.

ინტერნეტ ფრაგმენტაციის თითოეული ფორმის განხილვისას გვაქვს სხვადასხვა სახის პრობლემური კატეგორიები და მათგან გამომდინარე ფრაგმენტაციის სახეობები, თუმცა ფართოდ განიხილება ასევე ინტერნეტ ფრაგმენტაციის სწორედ ის მეოთხე სავარაუდო ფორმა, რაც უკავშირდება ეროვნულ თუ გლობალურ უსაფრთხოებას და, რომელიც აჩვენებს ცალკეული მთავრობების მიერ გატარებული შიდა და საგარეო ინტერნეტ პოლიტიკების გავლენის შედეგს თავად ინტერნეტის, იგივე კიბერსივრცის ერთიანობაზე, მდგრადობაზე, უსაფრთხოებასა და სტაბილურობაზე.

როცა ვსაუბრობთ ინტერნეტ ფრაგმენტაციის მეოთხე სავარაუდო ფორმაზე, აუცილებლად უნდა ვახსენოთ ის ქვეყნები, რომელთა ხელისუფლებები ზღუდავენ ინტერნეტის მიწოდების პროცესს, ახდენენ კონტროლს ინტერნეტში კონტენტის გავრცელებას, ცდილობენ შექმნან თავიანთი

ეროვნული ინტერნეტ ქსელი, ონლაინ პლატფორმები და სოციალური ქსელები თავიანთი მოქალაქეებისთვის, შეზღუდონ საერთაშორისო სოციალური ქსელები, რითაც საშუალება ეძლევათ ადვილად მოახდინონ კონტროლი ინტერნეტ სივრცეზე, და რითაც ხელს უწყობენ გლობალური ინტერნეტ სივრცის ფარგმენტაციის პროცესს. ასეთ ქვეყნებს მიეკუთვნება ისეთი დიდი ქვეყნები, როგორებიც არის ირანი, რუსეთი და ჩინეთი. თითოეული მათგანი თავიანთი კიბერსივრცის შეტევებისგან თავდაცვის მომიზეზებით ცდილობენ მაქსიმალურად შეამცირონ წვდომა უცხოეთიდან მათ ინტერნეტ სივრცეზე და ქვეყნის შიგნით შექმნან ისეთი სახის ინსტრუმენტები, რაც ხელს შეუწყობს კონტროლსა და მათთვის არასასურველი კონტენტის გავრცელების პროცესს, მოახდინონ მაქსიმალური დაბლოკვა.

4. დასკვნა

ბოლოში დასკვნის სახით შეიძლება ითქვას, რომ დროა სახელმწიფოებმა გააძლიერონ თავიანთი ძალისხმევა მიმართული ინტერნეტის როგორც გლობალური საზოგადოებრივი კეთილდღეობის, ინტერნეტის ერთიანობის, უსაფრთხოებისა და სტაბილურობის შესანარჩუნებლად. გლობალურ ციფრულ ხელშეკრულებაზე მუშაობის ფარგლებში, რომელიც შეთანხმებული უნდა იყოს 2024 წლის სექტემბერში, გრძელდება გლობალური და ინკლუზიური პროცესი ციფრული სივრცის ერთიანი პრინციპების შემუშავების კუთხით. ეს არის შესაძლებლობა, რომლის მიხედვით მოხდება გლობალური ინტერნეტის აღიარება როგორც საერთო პრობლემების გადაწყვეტის მნიშვნელოვანი ისნტრუმენტი. ზოგადად უნდა აღინიშნოს, რომ ინტერნეტის ფრაგმენტაციის პროცესის შეჩერება რთული ამოცანაა, მაგრამ ეს შესაძლებელია სახელმწიფოთა შორისი მაღალი დონის შეხვედრებით, ფოკუსირებული დიალოგებითა და ძალისხმევით იმ ძირითად ფრაგმენტულ ფაქტორებზე, როგორიცაა კიბერჯაშუშობა, ინტერნეტის ინფრასტრუქტურაზე კონტროლის დაწესების მცდელობა და ინტერნეტისა და ინტერნეტ ტექნოლოგიების გამოყენებაზე როგორც იარაღი ქვეყნებისა და ადამიანთა წინააღმდეგ.

გამოყენებული ლიტერატურა

1. სვანაძე ვ. „კიბერუსაფრთხოების ახალი გამოწვევები და საქართველო“, 2022;
2. Carnap Kai Von, “Fragmentation the Internet-Beyond and Within the Great Firewall”, MERICS-Mercator Institute for Chinese Studies, 2023;
3. Christopher Meinel, „Russia’s War Against Ukraine is Catalyzing Internet Fragmentation“, Council on Foreign Relations, 2023;
4. Kamaitis Konstantions, “Internet Fragmentation: Why It Matters for Europe” , 2023;
5. Stokel-Wallker Chris, “Russia Inches Toward Its Splinternet”, 2022;
6. Sullivan Andrew, “Misguided Policies the World over are slowly killing the Open Internet”, Internet society, 2023;
7. Drake J. drake, Cerf Vinton G. ,Kleinwachter Wolfgang , “Internet Fragmentation: An Overwiev” , 2016.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 111 – 116 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

რუსული კიბერაქტორების მოკლე დახასიათება უკრაინაში სრულმასშტაბიანი შეჭრის წინ

ანდრო გოცირიძე[1]

[1]ბიზნესისა და ტექნოლოგიების უნივერსიტეტის პროფესორი

აბსტრაქტი. ზღვარი სახელმწიფო და არასახელმწიფო კიბერაქტორებს შორის რუსეთში წაშლილია. ეს აქტორები ინტენსიურად თანამშრომლობენ ერთმანეთთან, მოქმედებენ კოორდინირებულად, ხშირად იყენებენ კრიმინალური ჯგუფების საფარს და ახორციელებენ რუსეთის სახელმწიფო ინტერესებს, რაც საფრთხეს უქმნის საქართველოს და მთელ დასავლურ საზოგადოებას. სტატიაში დახასიათებულია ჩვენთვის ცნობილი კიბერ ჯგუფები, რომლებიც პირდაპირ ან ირიბად არიან დაკავშირებული რუსულ სახელმწიფო სისტემასთან. აღწერილია მათი პასუხისმგებლობის ზონები, მოტივაცია, შეტევის მეთოდები უკრაინაში სრულმასშტაბიანი შეჭრის წინ. აღნიშნულის ცოდნა დაგვეხმარება საქართველოში ეფექტური კიბერთავდაცვის მოდელების ჩამოყალიბებაში.

საკვანძო სიტყვები: კიბერ მსახიობები, თავდასხმის მეთოდები, კიბერთავდაცვა, კიბერ ომი

ABSTRACT. Distinguishing between state and non-state actors within Russia is often difficult, especially when these actors actively collaborate, cooperate, and condone criminal activity that pose a threat to the security of Georgia and the entire western society. This article covers principal cyber groups, directly or indirectly connected to the Russian special services or state institutions, their responsibilities, motivation, and attack methods before a full-scale invasion of Ukraine. This knowledge will help us build efficient cyber defense models established in Georgian defense institutions.

KEYWORDS: cyber actors, attack methods, cyber defense, cyber war

1. შესავალი

შემტევი კიბერპოტენციალის თვალსაზრისით, რუსეთი ერთ- ერთ მოწინავე პოზიციას იკავებს მსოფლიოში. საქართველოსთან 2008 წლის ომის, არაბული გაზაფხულისა და 2011 წელს რუსული ოპოზიციის მიერ სოციალური ქსელებით ორგანიზებული მასშტაბური გამოსვლების შედეგების ანალიზზე დაყრდნობით, კრემლმა განახორციელა ორგანიზაციულ-დოქტრინალური ცვლილებები და გააქტიურა კიბერსივრცის კონტროლი.

რუსული კიბერაქტორების ჩამონათვალი მოიცავს როგორც სახელმწიფო უწყებებს, რომელთაგან მნიშვნელოვანი წილი სპეცსამსახურებზე მოდის, (Galeotti 2016) ასევე კრემლთან აფილირებულ კერძო დაჯგუფებებს, კიბერკრიმინალურ ორგანიზაციებს, ჰაქტივისტებს თუ „პატრიოტ ჰაკერთა“ ჯგუფებს. უნდა აღინიშნოს, რომ კერძო სტრუქტურების დიდ ნაწილს კრემლთან დაახლოებული ოლიგარქები აფინანსებენ და მართავენ.

თანამედროვე რუსული სპეცსამსახურებისთვის დამახასიათებელია უკიდურესი პოლიტიზირება, წაშლილი ზღვარი პარტიასა და სახელმწიფოს შორის, მმართველი რეჟიმის უსაფრთხოებაზე ზრუნვა, უწყებათაშორისი კონკურენცია კრემლის კეთილგანწყობისა და შესაბამისად რესურსების მოსაპოვებლად, ასევე პოლიტიკურ იარაღად მათი გამოყენება.

უსაფრთხოების ფედერალური სამსახური (ФСБ, Федеральная Служба Безопасности) საბჭოთა კავშირის სახელმწიფო უშიშროების კომიტეტის მემკვიდრე და რუსეთის უძლიერესი სპეცსამსახურია. მიუხედავად მკაფიო კონტრდაზვერვითი ფუნქციისა, უწყება ხშირად საზღვარგარეთ, განსაკუთრებით კი ე.წ. „პოსტსაბჭოთა სივრცეში“ ახორციელებს ოპერაციებს, რადგან რუსეთი ამ რეგიონს საკუთარ გავლენის სფეროდ მოიაზრებს და მის დასავლურ ინტეგრაციას კონტრდაზვერვით საფრთხედ აღიქვამს. **ФСБ**, საზედამხედველო უწყებებთან და პროფილურ სამინისტროსთან ერთად, მნიშვნელოვან როლს თამაშობს რუსეთის საინფორმაციო სფეროს უსაფრთხოების დაცვაში. მაგალითად, იგი, ინტერნეტ-პროვაიდერების მონიტორინგის ფარგლებში, უფლებამოსილია აწარმოოს სატელეფონო მოსმენები და ინტერნეტის ტრაფიკის კონტროლი. თუმცა, მისთვის არც შემტევი კიბეროპერაციებია უცხო: სწორედ ФСБ-ს უკავშირდება ცნობილი მაღალტექნოლოგიური ჰაკერული ჯგუფი Turla (Snake, Uroburos, Venomous Bear). იგი ერთ ერთი უძველესი ჰაკერული ჯგუფია, რომლის კვალიც აღმოჩენილ იქნა ჯერ კიდევ 2008 წელს აშშ-ის სამხედრო ქსელებსა თუ ირანელი ჰაკერების სერვერების კომპრომეტაციაში მათი შემდგომი გამოყენების მიზნით.

სამხედრო დაზვერვის მთავარი სამმართველო - ГРУ ან ГУ (Главное Разведывательное Управление, Главное Управление Генерального Штаба Вооружённых Сил РФ) წარმოადგენს საგარეო დაზვერვის განმახორციელებელ უწყებას. კიბეროპერაციების ადრეულ ეტაპზე, მაგალითად 2007-2008 წლებში ესტონეთისა და საქართველოს წინააღმდეგ განხორციელებულ კიბერშეტევებში ГРУ-ს შედარებით მეორეხარისხოვანი როლი ჰქონდა, თუმცა მოგვიანებით, ეს უწყება გადაიქცა შემტევი კიბეროპერაციების ფლაგმანად. დასავლური სპეცსამსახურები სწორედ მას მიაწერენ მნიშვნელოვან გახმაურებულ კიბერშეტევებს საინფორმაციო-ტექნიკური თუ საინფორმაციო-ფსიქოლოგიური ეფექტით, რომლებიც ფართოდ არის აღწერილი სხვადასხვა წყაროს მიერ. მიუხედავად სპეცსამსახურისთვის დამახასიათებელი მკაცრი კონსპირაციისა, ცნობილია კიბეროპერაციების განმახორციელებელი ГРУ-ს რამდენიმე დანაყოფი:

- **85-ე სპეციალური უზრუნველყოფის ცენტრი** (ს/ნ 26165[1]) - ნომინალურად პასუხისმგებელია რადიოელექტრონულ დაზვერვასა და კრიპტოგრაფიაზე თუმცა სწორედ მას უკავშირდება ბოლო დრომდე APT28-ის (Fancy Bear, Pawn Storm, Sofacy, Strontium) სახელით ცნობილი აქტივობები. იგი წარმოადგენს ერთ ერთ ყველაზე აქტიურ, მაღალტექნოლოგიურ, მეტად დესტრუქციულ კიბერაქტორს და პასუხისმგებელია საჰაერო სივრცეზე, თავდაცვის და ენერგეტიკის სფეროებსა თუ სახელმწიფო და მედიასექტორზე განხორციელებულ კიბერთავდასხმებზე. თავდასხმების არეალი ფართოა და მოიცავს აშშ-ს, დასავლეთ ევროპას, ირანს, იაპონიას, საქართველოს, მალაიზიასა და სამხრეთ კორეას. APT28 ცნობილია თავდაცვის სექტორსა და სხვა სამხედრო მიზნებზე განხორციელებული კიბერშპიონაჟის გახმაურებული ფაქტებით. (FireEye 2014) ცნობილ შეტევებს მიეკუთვნება 2014 წ. უკრაინის და 2016 წ. აშშ-ის საპრეზიდენტო, 2015 წ. ბუნდესთაგის საარჩევნო სისტემებზე თავდასხმა, ფრანგულ ტელემაუწყებელ TV5Monde -ზე

[1] ს/ნ - სამხედრო ნაწილი. საბჭოთა დროიდან შეორჩენილი საიდუმლო სარეჟიმო ობიექტების აღრიცხვის მიღებული ფორმა.

კიბერშეტევა კიბერხალიფატის საფარქვეშ და 2018 წელს ფხენიანის ზამთრის ოლიმპიურ თამაშებზე თავდასხმა. ცნობილია კარგად ორგანიზებული ფიშინგ-შეტევებით.

- **სპეციალური ტექნოლოგიების მთავარი ცენტრის** (ს/ნ 74455) ძირითადი აქტივობები კომპიუტერულ ტექნოლოგიებზე დაფუძნებულ ოპერაციების უკავშირდება. მისი ქოლგის ქვეშ მოქმედებს ჰაკერული ჯგუფი **Sandworm** (Telebots, Voodoo Bear, Iron Viking), რომელიც გამოირჩევა განსაკუთრებით მაღალტექნოლოგიური და დესტრუქციული კიბერშეტევებით. იგი წარმოადგენს ტექნიკურ ეფექტზე ორიენტირებულ აქტორს და პასუხისმგებელია აშშ-ის 2016 წლის საპრეზიდენტო არჩევნებში ჩარევის ტექნიკურ მხარეზე, NotPetya-სა[2] და უკრაინის ენერგეტიკული სექტორის წინააღმდეგ 2015-2016 წლებში გამოყენებული KillDisk და Industroyer შექმნა-გავრცელებაზე. Sandworm-ის ანგარიშზეა ასევე 2018 წელს ფხენიანის ზამთრის ოლიმპიურ თამაშებზე განხორციელებული კიბერშეტევა.
- **72-ე სპეციალური ღონისძიებების ცენტრი (ს/ნ 54777)** წარმოადგენს ГРУ-ს ფსიქოლოგიური ომის ბირთვს, მინიმუმ 2014 წლიდან წარმართავს კიბერშეტევებს საინფორმაციო ოპერაციების განსახორციელებლად. აღნიშნული დანაყოფი მჭიდროდ თანამშრომლობს შეფარების უწყებებთან და პროქსი-ორგანიზაციებთან.
- სამხედრო დაზვერვის მთავარი სამმართველოს კიბეროპერაციების კიდევ ერთი ინსტრუმენტია დაჯგუფება **„კიბერბერკუტი“ (Киберберкут)**, რომელიც თითქოსდა ჰაქტივისტური მოტივით ახორციელებს რუსული სამხედრო ოპერაციებისა და სტრატეგიული ამოცანების მხარდაჭერას როგორც ტექნიკურ, ისე ფსიქოლოგიურ ეფექტზე გათვლილი კიბერშეტევებით. კიბერბერკუტი 2014 წლიდან აქტიურადაა ჩართული კიბერშპიონაჟის აქტებსა თუ DDoS -ს შეტევებში ნატოსა და უკრაინის, ასევე - გერმანიის სამთავრობო საიტების წინააღმდეგ. ფოკუსირება ხდება ჰაკერული გზით მოპოვებული დოკუმენტაციის ონლაინ გამოქვეყნებაზე, რაც ძირითადად ემსახურება მთავრობების დისკრედიტაციას, არჩევითი ორგანოებისადმი ნდობის შემცირებას, მოწინააღმდეგის დემორალიზებას, დაშინებას.

საგარეო დაზვერვის სამსახური (CBP) აწარმოებს სტრატეგიულ სადაზვერვო ოპერაციებს, მათ შორის კიბერსივრცეშიც. სამხედრო დაზვერვის მთავარი სამმართველოსგან განსხვავებით, რომლის ამოცანასაც კიბერშპიონაჟთან ერთად, საბოტაჟი და საინფორმაციო ოპერაციებიც შეადგენს, საგარეო დაზვერვის სამსახური ძირითადად კონცენტრირებულია კიბერშპიონაჟის ტრადიციულ მიზნებზე პოლიტიკურ დაზვერვასა და საიდუმლო ინფორმაციის მოპოვებაზე. CBP-თან არის დაკავშირებული ცნობილი APT29 (Cozy Bear/The Dukes)-ის აქტივობები. ეს მაღალტექნოლოგიური ჯგუფი კიბერშეტევებისთვის იყენებს ძვირ და კომპლექსურ ინფრასტრუქტურას. ახლო წარსულში CBP -მა განახორციელა წარმატებული კიბერშეტევები თეთრ სახლზე, სახელმწიფო დეპარტამენტსა და აშშ-ის გაერთიანებულ შტაბებზე. გარდა აღნიშნულისა, დაჯგუფების სამიზნეებს წარმოადგენს თავდაცვისა და ენერგეტიკის სექტორი,

[2] რუსეთის სამხედრო დაზვერვის მთავარი სამმართველოს კიბერდაჯგუფება Sandworm -ის მიერ 2017 წელს განხორციელებული მაღალტექნოლოგიური შეტევა რომელმაც გაანადგურა მონაცემები უკრაინის საბანკო და ენერგეტიკული სექტორის, სახელმწიფო უწყებებისა და აეროპორტების სერვერებზე. მოგვიანებით, მალვეარი გავრცელდა ევროპაშიც და მილიარდობით ზარალი მიაყენა ლოგისტიკურ კომპანიებს, ფარმაცევტულ სექტორს და სახელმწიფო უწყებებს.

საფინანსო და სადაზღვევო სფერო, ფარმაცევტული სფერო, ინდუსტრიულ-ტექნოლოგიური კვლევები, მედია და ანალიტიკური ცენტრები. აღწერილია თავდასხმები დასავლეთ ევროპის, ჩინეთის, ბრაზილიის, მექსიკის, იაპონიის, თურქეთის და სხვა სახელმწიფოების ქსელებზე. ცნობილია Spear-Phishing ტექნიკის მიზანმიმართული ფიშინგ-შეტევებით.

ГРУ-სთან ერთად CBP-ის კიბერდანაყოფები არიან პასუხისმგებელი 2016 წლის აშშ-ის საპრეზიდენტო არჩევნებში ჩარევაზე. ამ უკანასკნელს უკავშირდება ასევე აშშ-ის, გაერთიანებული სამეფოსა და კანადის COVID -ვაქცინაციის ცენტრებზე თავდასხმები და კიბერშპიონაჟის ბოლო წლების უმსხვილესი კამპანია 2020 წელს აშშ-ის სამთავრობო ქსელების, უსაფრთხოების სექტორის და კრიტიკული ინფრასტრუქტურის წინააღმდეგ, რომელიც „SolarWinds hack“-ის სახელითაა ცნობილი.

საინფრომაციო კონფრონტაცია[3] და მისი თანმხლები კიბეროპერაციები რუსეთის სახელისუფლებო ვერტიკალში სპეცსასმსახურების პასუხისმგებლობის ზონად ითვლება. აშშ-ის ეროვნული დაზვერვის დირექტორის ინფორმაციით, ეს სამსახურები აქტიურად ავითარებენ კრიტიკული ინფრასტრუქტურის ICS-ზე (**Industrial Control Systems - ICS**)[4] დისტანციური წვდომის საშუალებებს: ჯერ კიდევ 2015 წლის მონაცემებით, უცნობმა რუსმა აქტორებმა წარმატებულად განახორციელეს რამდენიმე ICS მწარმოებლის პროგრამის კომპრომეტაცია, ლეგალური პროგრამული უზრუნველყოფის განახლებებში **მავნე პროგრამული კოდის** ჩანერგვა და ამ გზით მომხმარებლის სისტემასთან პირდაპირი წვდომის დამყარება. მოგვიანებით, „SolarWinds" კიბერშეტევამ დაადასტურა რუსული სპეცსამსახურების ეს შესაძლებლობა, როდესაც ათასობით კომპანია თუ სახელმწიფო უწყება დაინფიცირდა პროგრამული განახლებების ლეგალური სერვერიდან გადმოწერილი რუსული მალვეარის შედეგად.

რუსეთის შეიარაღებული ძალების პასუხისმგებლობის სფეროა რადიოელექტრონული ბრძოლის საშუალებები და კიბეროპერაციების მათთან მომიჯნავე ველი. 2014 წელს რუსეთის თავდაცვის მინისტრმა ს. შოიგუმ დააანონსა კიბერსარდლობის შექმნა, თუმცა მოგვიანებით, 2017 წლის თებერვალში გაცხადდა საინფორმაციო ოპერაციების ჯარების შექმნის შესახებ, რომელიც პასუხისმგებელია, როგორც ტექნიკური ეფექტის მქონე კიბეროპერაციების წარმოებაზე, ისე საბრძოლო მოქმედებებისას პროპაგანდის გავრცელებასა და საინფორმაციო კონფრონტაციის სხვა ელემენტებზე.

---

[3] **საინფრომაციო კონფრონტაცია** - დაპირისპირება საინფორამციო სფეროში, რომელიც მოიცავს კომპლექსურ დესტრუქციულ ზემოქმედებას მოწინააღმდეგე მხარის ინფორმაციაზე, საინფორმაციო სისტემებსა და ინფრასტრუქტურაზე, ამავდროულად საკუთარი ინფორამციის, საინფორმაციო სისტემებისა და ინფრასტრუქტურის დაცვის გათვალისწინებით. ინფორამაციული კონფრონტაციის საბოლოო მიზანს ინფორმაციული უპირატესობის მოპოვება წარმოადგენს.

[4] **ICS (Industrial control system)** - კოლექტიური ტერმინი, რომელიც გამოიყენება კონტროლის სისტემებისა და მათთან დაკავშირებული ინსტრუმენტების აღსაწერად და აერთიანებს ინდუსტრიული პროცესების ავტომატიზაციისა და ოპერირებისათვის გამოყენებულ მოწყობილობებს, სისტემებს, ქსელებს და კონტროლის მექანიზმებს. დღეისათვის ფართოდ გამოიყენება კრიტიკული ინფრასტრუქტურის თითქმის ყველა მიმართულებაზე, როგორიცაა ინდუსტრია, ტრანსპორტი, ენერგეტიკა, ჰიდრომეურნეობა და სხვა, რის გამოც წარმოადგენს დესტრუქციული კიბეროპერაციების სამიზნეს. ICS-ს გავრცელებულ სახეობას წარმოადგენს ე.წ. **SCADA (Supervisory Control and Data Acquisition) და DCS (Distributed Control Systems) სისტემები.**

რუსეთის თავდაცვის სამინისტროს კიბერდანაყოფები მონაწილეობენ შემტევი კიბეროპერაციების, საინფორმაციო-ფსიქოლოგიური ეფექტის მქონე კიბერღონისძიებებისა და მოწინააღმდეგის მართვისა და კონტროლის სისტემებში მავნებელი პროგრამული უზრუნველყოფის ჩანერგვაში. რუსეთის მაღალი რანგის სამხედრო პირებზე დაყრდნობით, საინფორმაციო ოპერაციების ჯარებმა 2016 წლის სექტემბერში პირველად მიიღეს მონაწილეობა სამეთაურო-საშტაბო სწავლებაში „Кавказ-2016“.

საინფორმაციო კონფრონტაციის პროცესში დომინირებისათვის რუსეთი გარდა სახელმწიფო აქტორებისა, აქტიურად იყენებს კიბერკრიმინალის შესაძლებლობებს, რაც მას საშუალებას აძლევს დაუსჯელად და იაფად დააზიანოს მოწინააღმდეგე ქვეყნის კრიტიკული ინფრასტრუქტურა. ლიეტუვას და საქართველოს წინააღმდეგ 2008 წელს განხორციელებულ კიბერშეტევებში მნიშვნელოვანი როლი შეასრულა ძლიერი ტექნიკური შესაძლებლობების მქონე კიბერკრიმინალურმა ორგანიზაციამ RBN (Russian Business Network), რომელმაც ინტენსიური თავდასხმა განახორციელა ქართულ ქსელებზე.

2020 წელს აშშ- ის ერთ-ერთ უმსხვილეს ნავთობსადენზე განხორციელებული “Ransomware”[5] კიბერშეტევის შედეგად, კომპანია Colonial Pipeline- მა ნავთობსადენის მუშაობა დროებით შეაჩერა. ჰაკერებმა მილსადენის კომპიუტერულ სისტემაში შეაღწიეს და ხელში თითქმის 100 GB-ის მოცულობის მონაცემები ჩაიგდეს, ხოლო დაშიფრული მონაცემების გასახსნელად კომპანიისგან გამოსასყიდად რამდენიმე მილიონი დოლარის ღირებულების ბიტკოინები მიიღეს. თავდამსხმელი, DarkSide რუსეთში ბაზირებული კიბერკრიმინალური დაჯგუფებაა, რომელმაც 2019 წლიდან დასავლეთის ქვეყნებს უკვე მილიარდობით ზარალი მიაყენა. აშშ-ის მთავრობა იძულებული გახდა საგანგებო მდგომარეობა გამოეცხადებინა. მილსადენის გაჩერებამ საწვავის ფასის ზრდა გამოიწვია. რამდენიმედღიანი შეფერხების შედეგად, საწვავის ფასმა 2014 წლის ოქტომბრის შემდეგ ყველაზე მაღალ ნიშნულს მიაღწია.

ოდნავ მოგვიანებით, იმავე წლის ივნისის დასაწყისში განხორციელებულმა მორიგმა „Ransomware“ შეტევამ ხორცპროდუქტების უმსხვილეს მწარმოებელზე „JBS”-ზე აშშ-ის, კანადისა და ავსტრალიის ოპერაციებში მნიშვნელოვანი შეფერხება და ხორცპროდუქტებზე ფასების ზრდა გამოიწვია. შეტევის უკან რუსული კიბერკრიმინალური დაჯგუფება „REvil“ იდგა. „REvil“, იგივე Sodinokibi ცნობილი კიბერკრიმინალური ჯგუფია. იგი მინიმუმ 2019 წლიდანაა აქტიური და მისი წევრები რუსეთისა და პოსტსაბჭოთა ქვეყნების მოქალაქეები არიან.

გართულებული ატრიბუციის გამო, რუსული სადაზვერვო სამსახურები აარსებენ კონსპირაციის მაღალი დონის მქონე ჰაქტივისტურ ჯგუფებს ან მოქმედებენ უკვე არსებულთა საფარქვეშ. ჰაქტივისტური კიბერშეტევები წარმოადგენდა ერთ-ერთ ელემენტს რუსეთის მთავრობის მიერ მხარდაჭერილ კიბერშეტევებში 2007 წელს ესტონეთის, 2008 წელს კი

[5] „Ransomware“კიბერშეტევის ფორმაა, რომლის დროსაც კრიმინალები, არასანქცირებული წვდომის შედეგად მათ მიერვე დაშიფრული ან ბლოკირებული ინფორმაციის გასახსნელად გამოსასყიდს ითხოვენ. ამ ტიპის შეტევის გამოყენება, როგორც ფინანსურად მოტივირებული კიბერკრიმინალის, ასევე სახელმწიფოთა მიერ მხარდაჭერილი შეტევებისას დრამატულად გაიზარდა, რაც აშშ-ის უსაფრთხოების სამსახურების მზარდ შეშფოთებას იწვევს. ანონიმურობის და ქსელის დაცულობის მაღალი ხარისხის გამო, კიბერკრიმინალი გადახდის საშუალებად ხშირად კრიპტოვალუტას იყენებს. ატრიბუციის გარდა, გართულებულია ბიტკოინის ტრანზაქციის შეჩერება, მისი ამოღება, წართმევა ან უკან დაბრუნება.

საქართველოს წინააღმდეგ, ასევე მუდმივად იყო გამოყენებული რუსეთ-უკრაინის კონფლიქტში მეიდანზე განვითარებული პროცესებისას თუ ყირიმის ანექსიისას.
რუსეთი კიბერშეტევებს ე.წ. false flag ოპერაციებითაც ახორციელებს. პარტნიორი სპეცსამსახურების დადასტურებული მონაცემებით, სწორედ რუსეთი იდგა "ისლამურ სახელმწიფოსთან" ასოცირებული კიბერხალიფატის ("Cyber Chaliphate") მიერ ჰაქტივიზმის საფარვეშ საფრანგეთის სატელევიზიო არხ TV5 Monde-ზე 2015 წლის აპრილში განხორციელებული თავდასხმის უკან. შეტევა კარგად იყო ორგანიზებული და დაიწყო არხის თანამშრომლებისათვის ფიშინგ-წერილების დაგზავნის კამპანიით, რამაც კიბერკრიმინალებს შესაძლებლობა მისცა 3 თვის შემდგომ მოეპოვებინათ კონტროლი ათამდე საინფორმაციო არხსა და მათ სოციალურ მედიაარხებზე, გაევრცელებინათ ჯიჰადისტური პროპაგანდა და გამოექვეყნებინათ სირიაში დისლოცირებული ფრანგი სამხედროების პერსონალური მონაცემები.

3. დასკვნა

საინფორმაციო კონფრონტაციის მიზნების მისაღწევად რუსეთი ფართოდ იყენებს ანაზღაურებად კომენტატორთა არმიას - ე. წ. ტროლებს. ტროლები წარმოადგენენ შედარებით ღია, თუმცა მაინც გართულებული ატრიბუციის ინსტრუმენტს ანტირუსული ინფორმაციის დისკრედიტაციისა და პროკრემლისტური განწყობების ჩამოსაყალიბებლად. კონკრეტული ტროლი ხშირად მართავს მრავალრიცხოვან ონლაინპროფაილსა და ბლოგს. რუსული ტროლინგის მიზანი ყოველთვის რუსული თვალსაზრისის სისწორეში აუდიენციის დარწმუნება კი არ არის, არამედ, მათ მისიას წარმოადგენს სოციალური მედიის წალეკვა ყალბი კონტენტით, ეჭვის, შიშის, არასტაბილურობის განცდის შექმნა და ინტერნეტის დემოკრატიულ სივრცედ გამოყენების ხელისშეშლა.

ბიბლიოგრაფია:

1. Janne Hakala, Jazlyn Melnychuk. Russia's strategy in Cyberspace. e NATO StratCom COE. Riga, June 2021. ISBN: 978-9934-564-90-1
2. Joint Cybersecurity Advisory co-authored by authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. April 20. 2020.
3. Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. www.dia.mil/military-power-publications
4. UK Foreign and Commonwealth Office Report "UK exposes Russian involvement in SolarWinds cyber compromise" 2021
5. Hearing: Worldwide Cyber Threats (Open). Testimony of The Honorable James Clapper, Director of National Intelligence. September 10, 2015. https://docs.house.gov/meetings/IG/IG00/20150910/103797/HHRG-114-IG00-Wstate-ClapperJ-20150910.PDF
6. Nakashima E. and Timberg C. Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce, The Washington Post, 14 December 2020
7. Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of Russia's full-scale cyberwar against Ukraine. 2023