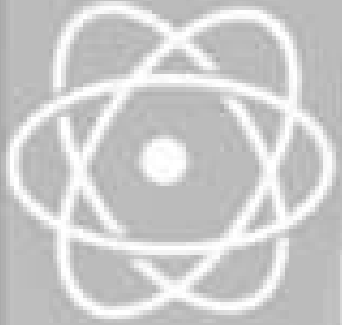

SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

Vol 7 No 1
March 2023

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 7(1): 1-10 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INFORMATION-MILITARY SECURITY IS A COMPONENT OF STATE SECURITY

Volodymyr Khoroshko, National Aviation University, Doctor in Technical Sciences, Professor
Ruslan Hryshchuk, National Aviation University, Doctor of Engineering Science, Full Professor
Nikolay Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor
Mariia Kapustian, Khmelnytskyi National University Computer Engineering and Information Systems Department, PhD in Engineering Science, Assistant professor

ABSTRACT: In modern conditions, the nature of the information-military struggle has changed significantly - it is increasingly taking on the characteristics of a hybrid war. The emphasis of the military struggle is shifting towards the practical implementation of information technologies. At the same time, informational and psychological operations, actions and actions are gaining more and more importance in achieving political and military goals. In the article, using the example of Ukraine, the issue of the distribution of sources of information and military danger according to their origin and internal nature was considered, specific manifestations of information and military danger for the country from the side of the aggressor state were given, general reasons for ensuring the national security of the country were given, and principles were formulated that have be laid in the basis of the activity of this system. The proposed functional scheme for ensuring the information and military security of the country. General recommendations on confrontation in the information war have been formed.

KEYWORDS*: national security, information warfare, information warfare, the concept of security, ensuring the security of the state.*

Introduction

The existence and development of modern states is closely intertwined with geopolitical and geostrategic conditions and largely depends on international relations. At the same time, even more importance is given to ensuring national security - the state of protection of the vital interests of the individual, society and the state from internal and external threats [1].

Among the many factors affecting the formation of the foreign and domestic policy of states, the determining role belongs to national interests. Being realized at all levels of social life, the needs of the country's population in the preservation and multiplication of national values and national wealth, in economic prosperity and political stability of society, national interests are reflected in the formulation and achievement of national goals. Thus, national interests and actions related to their satisfaction are connected. In international relations, not only such actions, but also their prerequisites or intentions regarding their implementation are objects of close attention, careful study and comprehensive assessment. This is particularly typical for Europe.

The experience of Ukraine clearly shows that true state independence exists only under the condition of reliable provision of national security.

The priority national interests of Ukraine, the conditions and ways of their reliable protection from existing and potential threats are defined in the national security strategy of Ukraine [1,2,3].

Ensuring state sovereignty, territorial integrity and inviolability of borders plays a pivotal role for the national interests of Ukraine. It is ensuring the security of Ukraine as an important component of its national security as a whole that is the main task.

It should be noted that in addition to military security, the country's security includes information security, which is both a component of military security and an independent part of state security. [4].

The transformation of Ukraine into an independent subject of geopolitics and international relations made the country face the problems of finding its place and reliable movement guidelines in the ambiguous military and political situation that has developed in the world and in the European region as a result of the collapse of the USSR, changes in the geostrategic interests and political orientations of most states of Central and Eastern Europe. Under these conditions, as well as as a result of fundamental democratic transformations in the state and society of Ukraine, security, both military and informational, is a matter of foreign and domestic policy, economy, legislative and regulatory framework of the state, etc.

Fundamental socio-political changes that took place in Central and Eastern Europe at the end of the 20th century led to the formation of a new structure of geopolitical space in this part of the continent. International relations at all levels - global, regional and bilateral have acquired fundamentally new qualities. At the same time, a complex and multidimensional foreign policy situation has developed around Ukraine.

The formation of the new geopolitical environment of Ukraine is influenced by two opposite trends: disintegration and integration.

The disintegration process resulted in the disintegration of several states in the region (USSR, Yugoslavia, Czechoslovakia). Moreover, this process spread to the internal disintegration of parts of these states (Georgia, Moldova, Russia, etc.).

A dangerous feature of disintegration processes is their tendency to take the form of an armed conflict. Only the disintegration of Czechoslovakia had a civilized form, other countries that ended their existence could not avoid the outbreak of armed violence, and the war in Yugoslavia became a clear example of what destructive forms disintegration can take even in a fairly civilized and generally developed country. The search for an effective solution to the problem of halting or civilizing the disintegration processes is of utmost importance, because the continuation of these processes can restore powerful anti-democratic forces that are capable of creating new autocratic supranational structures.

As for integration processes, they have two rather clearly defined spheres of action. First of all, it is Western Europe, which actually turned into a single geopolitical space through the European Union.

The second sphere consists of some countries of Eastern Europe and Central Asia, which are part of the interstate association of the former republics of the USSR - the Commonwealth of Independent States (CIS).

Each of these spheres differs in the degree of internal integration, the nature of internal contradictions, economic potential, and the level of socio-political stability. Western European integration has the best parameters and is a model for other regions of the continent. Rather contradictory processes are taking place in the CIS - from the almost complete unification of Belarus and Russia to a certain distancing of the states of Central Asia.

Against such a general geopolitical backdrop, Ukraine has been developing as a sovereign European state for 30 years. Taking into consideration the world experience, it can be argued that this development will be successful only under the conditions of reliable provision of national, including military and information security. At the same time, the security of Ukraine is an integral part of international security both at the global and regional levels.

Main part

It should be noted that during the thirty-year period of its independence, Ukraine, as a subject of international security and cooperation, has done a lot to assert a positive role in the field of European and regional security [5]:

- clearly defined the main principles of its foreign policy, focused on maintaining peace and stability in Europe;
- strengthened its authority as a member of many universal international organizations, in the founding of which it participated, actively cooperates with other states in peacekeeping activities under the auspices of the UN;
- became a fully-pledged member of the OSCE and the Council of Europe, established fruitful cooperation with the European Union;
- signed and ratified the agreement on its nuclear disarmament, joined the Treaty on the Non-Proliferation of Nuclear Weapons, etc.

This is far from complete list, as well as Ukraine's considered and moderate policy regarding manifestations of instability and conflicts in the immediate geopolitical environment (Russia's military aggression against Moldova, Georgia and Ukraine) contribute to Ukraine's international authority and strengthening of trust in it on the part of the world community.

However, the modern world remains controversial, and the most important thing for most states is informational and military danger.

In any case, the danger of the state has its own sources - existing or potential contradictions, for the solution of which military force can be applied. These contradictions can be external or internal. The basis for the emergence of these contradictions is the incompatible interests of individual states or social groups of the population in the sphere of political, economic, religious, national-ethnic and other relations, and their development is a consequence of the persistent actions of the opposing party (in this case, Russia) in the direction of achieving its goal (satisfaction of one's interests), despite the disagreement and resistance of the other party [6,7].

From the viewpoint of Ukraine, the sources of informational and military danger can be divided into three groups according to their origin and internal nature [4,6]:

The first group is sources of external (primarily from Russia) informational and military danger. This group includes the aspects as follow:

- existence of territorial claims to Ukraine;
- interest in changing the external and internal political course of Ukraine to one's advantage;
- interest in weakening the political, economic, and military role of Ukraine in the region, on the continent, and in the world in the interests of its dominance;
- a positive attitude and support for the actions of separatist forces in Ukraine and for the exacerbation of inter-ethnic and inter-confessional conflicts in Ukraine on the part of Russia;
- Russia's interest in establishing control over strategic objects and communications of Ukraine;
- the presence of significant military groups of Russia near the borders of Ukraine.

The second group consists of the sources that are formed by objective external factors and conditions that operate and exist in the neighboring states (primarily in Russia and Belarus), but have direct signs of both military danger and informational danger of Ukraine [3,6, 8] :

- steady growth of expenses for informational and military aggression;
- availability of powerful informational and military potential;
- unsettled legal issues of interstate relations with Ukraine.

The third group includes sources of internal origin, which in one way or another affect the level of informational and military danger for Ukraine [9,10]:

- unsatisfactory state of Ukraine's economy;
- unsatisfactory financing of Ukraine's own defense needs from the state budget;
- certain manifestations of socio-political instability in society.

The initial, initiating role is played by the factors of the first group, as they determine Russia's aggressive intentions and actions towards Ukraine. The factors of the second and third groups create certain prerequisites for the realization of their military danger for Ukraine.

Therefore, it is obvious that the sources of informational and military danger for Ukraine should be considered only as a whole, since there is a close relationship between them.

Specific manifestations of informational and military danger for Ukraine from the aggressor state can be as follow [4,6,11]:

- conducting hostile propaganda against Ukraine, inciting international conflicts, supporting separatist movements;
- interference in the internal affairs of Ukraine;
- submission of territorial claims to Ukraine;
- direct preparation for war against Ukraine, and the seizure of Crimea and war in Donbas, as well as actions aimed at undermining its sovereignty, violation of territorial integrity, etc.

The system of providing information and military security is an important subsystem of the general system of providing national security of Ukraine.

The functioning of the information and military security system of Ukraine is related to both external and internal spheres of state activity. The external aspect consists in the stabilization of the military-political situation in the region and the world at a reduced level of informational-military danger for Ukraine. The internal sphere covers issues related to the solution of socio-economic problems and maintaining the state's defense capability at an appropriate level.

It should be noted that the state and political security of the country consists of the aspects as follow [1,2,10,11]:

- the protection of the country's constitution, state and political system from attempts to liquidate or change them by force;
- ensuring the sovereignty and territorial integrity of the state, the inviolability of its borders, protection of internal and external interests;
- the protection of constitutional rights, freedoms and legitimate interests of citizens of the state and their associations.

For Ukraine, the main sphere of state and political security is the creation of domestic, regional, and global conditions for peaceful existence, the work of the Ukrainian people, and the sustainable democratic development of society. This includes, in particular, the end of the war in Donbas and the liberation of Crimea, active opposition to military threats, the exclusion of political isolation of Ukraine and the dictates of other states. Depending on the implementation mechanisms, state and political security can be divided into political and military.

Social-economic, national-cultural, informational, ecological and other types of national security also have military aspects.

Economic security is the foundation of Ukraine's national security. It is under the conditions of sustainable economic security that all our tasks of ensuring national security can be solved, that is, the creation of the necessary conditions for the stability of the development of the economic, socio-political, informational, ecological, demographic, scientific and intellectual foundations of society. On the other hand, real economic security exists only under conditions of reliable protection of Ukraine's national interests from any forceful pressure and encroachments from the use of military force. Therefore, among the main prerequisites of Ukraine's national security, its informational and military security should be considered alongside economic security, and under certain circumstances, informational and military security may take priority.

Three basic concepts should be used to ensure the information and military security of Ukraine as a nuclear-free state.

First, it is the concept of a military-political partnership based on a developed economy, a stable social sphere, and a well-founded information-military policy.

Secondly, it is the concept of defensive deterrence, according to which, within the limits of defensive sufficiency, a military organization of the state is created, which is capable of resisting a military conflict and causing unacceptable damage to the aggressor.

Thirdly, it is the concept of repelling aggression, which is based on the mobilization of all forces, means and resources of the country to oppose the aggressor.

The activities of all components of the information and military security system of Ukraine are concentrated on these three directions.

Taking into account the general reasons for ensuring the national security of Ukraine, it is possible to formulate the principles that should be the basis of the activity of this system [1,2,3]:

- the rule of law;
- the priority of contractual means in the resolution of interstate conflicts with the sufficiency of national defense;
- not harming the security of other states;
- adequacy of countering real threats;
- counteracting influences on individual units of the information system of the state;
- prevention of destruction or damage of state resources;
- countering the impact on the personnel of information and telecommunication systems with the use of software tools for keeping information in the subconscious or deterioration of human health;
- the balance of the interests of man, society and the state, their mutual responsibility in the field of ensuring information and military security;
- adequacy of measures against terrorist actions of the opposing party;
- openness to democratic civil control (except for cases in which there is a caveat in the legislation).

Taking into account the abovementioned, the functional scheme of ensuring the information and military security of Ukraine in its general form is shown in Fig. 1.

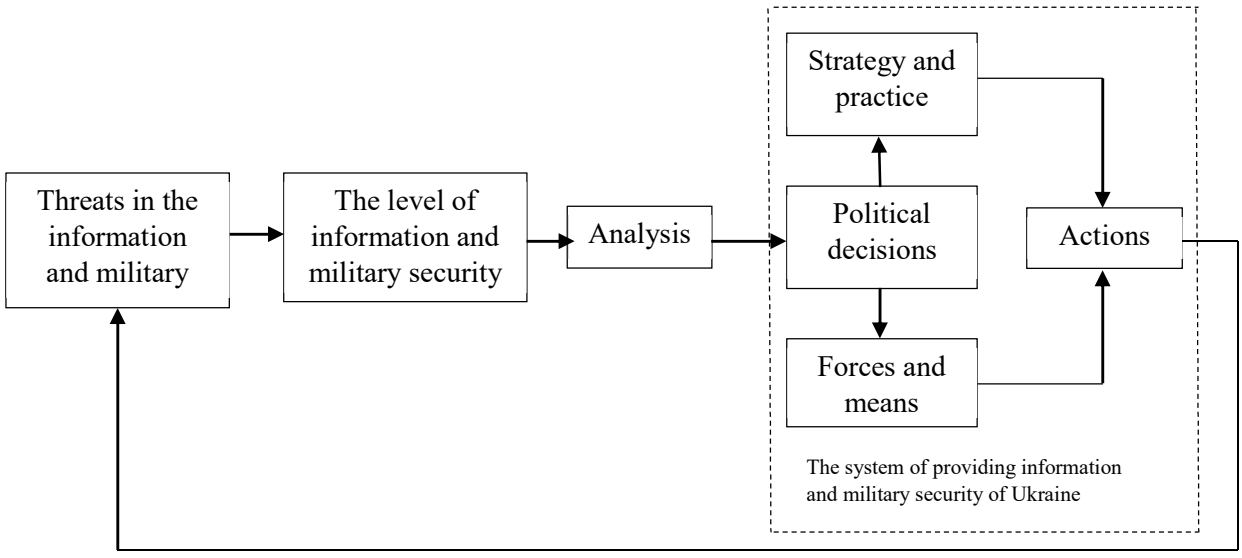

Fig. 1 Functional diagram of information and military security of Ukraine

The main content of providing information and military security is [4,6,12]
In peacetime:

- assessment and forecasting of the level of military security and military threats;
- implementation of effective and adequate measures aimed at preventing military conflicts in the foreign political sphere and within the state;
- preparation of the Armed Forces and other military formations to perform defense tasks and planning their use;
- protection of the state border, airspace, underwater environment and maritime economic zone of Ukraine;
- countering the implementation of destructive ideological influence on people, society and the state, manipulation of public opinion in order to create political tension and a state close to chaos;
- countering the formation of a negative image of Ukraine in the international arena and the destabilization of political relations between parties, associations and movements with the aim of inciting conflicts, stimulating mistrust, exacerbating enmity and the struggle for power;
- prevention of provocation of social, political, national, ethnic and religious clashes, creation or strengthening of oppositional and separatist groups and movements;
- a particularly necessary countermeasure against undermining the morale of the population and, as a result, the reduction of defense capability and combat potential;
- military and patriotic education of citizens of Ukraine;
- development of the defense-industrial complex, ensuring the mobilization readiness of the economy, state authorities, and the population to fulfill the tasks of territorial and civil defense;
- development of international military cooperation, active participation in peacekeeping activities under the auspices of international security organizations.

During the period of repelling armed aggression, the content of the actions consists of two separate directions, where the first is military opposition to the aggressor, and the second is informational opposition.

Military countermeasures include: [4,13,14,15]

- timely introduction of martial law or state of emergency in Ukraine or in some of its territories, implementation of full or partial deployment of the Armed Forces, bringing them and other military formations to readiness for the performance of tasks to repel armed aggression;
- transfer of the national economy, transport and communications enterprises to work under martial law;
- deployment in accordance with wartime requirements of the system of strategic management of the Armed Forces and other military formations, systems of operational, rear, technical and medical support, forces and means of territorial and civil defense;
- concentration of efforts of state authorities and military administration bodies, public organizations and citizens on the fulfillment of state defense tasks;
- repelling an armed attack, striking the aggressor's troops and the most important object with the aim of forcing him to refuse further hostilities;
- full use of the capabilities of international security organizations to stop military aggression, localize it and prevent it from turning into a full-scale war.

With regard to the information confrontation with the aggressor (in this case, Russia), Ukraine has already gained much of experience.

In the course of countering the aggressive actions of the enemy, general recommendations were formed regarding confrontation in the information war with Russia, namely: [4,9,16,17,18,19]:

- strengthening state control over the information space of Ukraine;
- coordinating the information impact on vulnerable elements of the aggressor's information system in a quicker manner;
- developing methods and means of countering the aggressor's information actions to reduce the sphere of his influence;
- applying a complex approach when forming an information war strategy, that is, to combine purely informational methods of influence with military, political, economic, etc.

It should be noted that information and psychological operations (IPO) in the southeast of Ukraine should be carried out in three directions:

- the first - the zone of operations of the joint forces (for the formation of opinions about the legality of the decisions and plans of the military and political leadership of Ukraine);
- the second - the internal territory of Ukraine (to demonstrate the confidence of the actions of the Ukrainian leadership and to form views among the population in support of the decisions of the military and political leadership of Ukraine);
- the third - foreign countries, in particular Russia (to create informational conditions for a positive perception of Ukraine's politics).

According to the first direction, IPO objects (especially in the Anti-Terrorist Operation Zone) are: [4,12]

- the population living in the Anti-Terrorist Operation Zone;
- a special composition of the forces involved in conducting the Anti-Terrorist Operation;
- illegal armed formations and personnel of the armed forces of the Russian Federation, which are in the Anti-Terrorist Operation Zone.

It should be taken into account that the population living in the Anti-Terrorist Operation Zone is subjected to double information physiological influence (IPI) - both from terrorists and Russia, and from Ukraine. Therefore, during IPO, the entire range of types, methods, methods and techniques of IPO are used, relying on the wide use of psychogenic factors.

The IPI objects in the second direction (internal territory of Ukraine) are as follow [17,18]:

- population of Ukraine;
- temporarily displaced persons;

The IPI should target the population of Ukraine in order to:

- support the patriotic mood in society;
- support and approve military operations against illegal armed formations and Russian mercenaries;
- clarify the need for various measures to limit and strengthen control;
- condemn and criticize the actions of illegal armed groups and Russians in relation to Ukraine;
- do counter-propaganda, namely the implementation of measures to counter attempts to manipulate public consciousness, in particular by spreading unreliable, incomplete or biased information about the social-political and socio-economic situation in the state, primarily in the Donetsk and Luhansk regions.

Special attention should be paid to temporarily displaced persons. IPI for this population category should be carried out by adapting them to new living conditions, namely:

- provision of housing (temporary or permanent);
- provision of various social benefits;

- involvement in social work.

IPI for the main composition of the forces, which is preparing to participate in the Joint Forces Operation, should be carried out in the directions of moral and psychological support of combat operations. At the same time, the main attention should be paid to psychological readiness to participate in combat operations.

At the level of the world community, it is necessary to ensure Ukraine's support for the preservation of territorial integrity, the implementation of all agreements regarding the peaceful settlement of the military confrontation by all participants in the conflict, including Russia, and in the event of an escalation of the situation on the part of illegal military formations, to ensure the legitimization of hostilities.

IPI on the population and military personnel of foreign states should be carried out in the following directions [17]:

- clarification of the goals of foreign policy and actions to establish peace in the southeast of Ukraine;
- to inform the world community, influential foreign political, governmental, business and cultural circles, as well as foreign mass media about actions to establish peace in the southeast of Ukraine;
- discrediting the military and political leadership of the Russian Federation.

In addition, it is recommended to work to support anti-war and anti-government sentiments in Russia.

For the effective implementation of the information policy in the south-eastern region of Ukraine and, above all, in the area where the EO is conducted, there is an urgent need to create appropriate IPO centers directly in the sectors of its implementation. This makes it possible to respond promptly to changes in the situation in the relevant sector, taking into account the mentality, views and lifestyle of the local population, the characteristics of industry, agriculture, the activities of authorities and local self-government in each sector, and the composition of the military formations of the opposing parties.

In our opinion, the main tasks of these centers should be as follow:

- reconnaissance and implementation of information-analytical activities to identify real and potential objects of action to determine ways and methods of their neutralization;
- operational study, evaluation and forecasting of the development of the social and political situation in the areas of responsibility;
- organization and implementation of IPIO on selected objects of influence in cooperation with information agencies, TV and radio companies, publishing houses, editorial offices, cultural and educational centers, as well as legal entities and individuals (legally or under cover);
- counter-propaganda;
- production and distribution of campaign materials;
- introduction of special programs for interception, creation of information and computer viruses into the computer networks of the enemy in order to reduce the efficiency of the functioning of the enemy's control and communication system;
- radio-electronic suppression of the enemy's radio-electronic means that can be used to carry out IPI and use the laws of radio-electronic protection of their troops;
- coordination with the IPO tasks of the regional media centers of the Armed Forces of Ukraine on the dissemination of information to the objects of influence;
- supporting the activities of local executive bodies and local self-government, creating a positive attitude among the local population towards the actions of their troops;

- promoting the development of the resistance movement and partisan movement in the temporarily occupied territory.

Conclusion

It should be noted that in modern conditions, the nature of the information-military struggle has changed significantly: it is increasingly taking on the characteristics of a hybrid war. The emphasis of the military struggle is shifting towards the practical implementation of information technologies. At the same time, informational and psychological operations, actions and actions are gaining more and more importance in achieving political and military goals.

It should also be noted that this article was prepared in November 2021. However, on February 24, 2022, Russia's war against Ukraine began. Therefore, it one should state that some conclusions and provisions of the article have been confirmed in life.

Bibliography

1. National security strategy of Ukraine. Approved by Decree of the President of Ukraine No. 392 of 09/14/2020.

2. Constitution of Ukraine

3. Selivanov V.M. Concept of national security of Ukraine. Kind. 2nd / V.M. Selivanov K: 2015. – 28 p.

4. Pirtschalava L.G. Information confrontation in modern conditions / L.G. Pirtskhalava, V.A. Khoroshko, Yu.E. Khokhlacheva, M.E. Shelest - K: CP "Comprint", 2019. - 226 p.

5. Kulinich M.A. Ukraine in the new geopolitical space: problems of regional and subregional security / M.A. Kulinich // Science and Defense, No. 1, 2015. – pp. 8 – 19.

6. Shkidchenko V.P. Elements of the theory of military security / V.P. Shkidchenko, V.D. Kohno - K: BF "Myrotvorets", 2001. - 194 p.

7. Manachynskyi O.Ya. Modern military and political relations of Ukraine with neighboring states. Kind. 2nd / O.Ya Manachynskyi - K: NISD, 2016. - 102 p.

8. Pyrumov V.S. Two sides of parity and defense adequacy / V.S. Pyrumov // Military thought, No. 2, 2015. - pp. 25 - 34.

9. V. Khoroshko. The concept of using informational influences and countermeasures against informational weapons / V. Khoroshko, Yu. Khokhlacheva, M. Prokofiev // Legal, regulatory and metrological support of the information protection system in Ukraine, Issue 1(31), 2016. - p .9 -23 .

10. Manoilo A.V. Technologies of non-violent resolution of modern conflicts / Ed. Prof. A.N. Petrenko / A.V. Manoilo - M: Hotline - Telecom, 2008. - 392 p.

11. Information security doctrine of Ukraine. Decree of the President of Ukraine No. 47/2017 dated February 25, 2017.

12. Chuev Yu.A. Forecasting in military affairs. Ed. 3rd supplement / Yu.A. Chuev, Yu.V. Mykhailov – M: Voenizdat, 2014. – 392 p.

13. Lobov V.N. Ways of realizing the concept of sufficiency for defense (strategy) / V.N. Lobov // Military thought, No. 2, 2002. - p. 18 - 27.

14. Nikolaev Yu.A. Defense adequacy: criteria and evaluation methods / Yu.A. Nikolaev // Military thought, No. 4-5, 1992. - pp. 35 - 45.

15. Tuchkov Y.N. Unification of group troops and forms of their use in armed conflicts and local wars/ Y.N. Tuchkov // Military thought, No. 2, 2007. - pp. 45 - 51.

16. Biloborodov O.O. Technologies of informational and psychological warfare and informational and psychological weapons / O.O. Biloborodov, A.S. Dovgopoly //Armament and military equipment, No. 4 (24), 2019. - p. 93 - 97.

17. Pevtsov G.V. Informational and psychological operations of the Russian Federation in Ukraine: models of influence and countermeasures / G.V. Pevtsov, S.V. Zalkin, S.O. Sidchenko, K.I.Khudarkovskii // Science and Defense, No. 2, 2015. – pp. 28 – 32.

18. Chepkov I.V. Organization of resistance to "hybrid war" in modern conditions: technical aspect / I.V. Chepkov, S.V. Lapytskyi, A.Yu. Hupalo, M.M. Chepura // Armaments and military equipment, No. 1(13), 2017. – p. 3 – 8.

19. Nenashev S.M. Informational - technological and informational - psychological security of users of social networks / S.M. Nenashev // Questions of cyber security, No. 5(18), 2016. - p. 65-71.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(1): 11-15 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INFORMATION SECURITY: AN EFFECTIVE TOOL FOR SUSTAINABLE NIGERIAN NATIONAL SECURITY AND DEVELOPMENT

Aliyu Ahmed Abubakar, Department of Computer Science, Kaduna State University, Kaduna, Nigeria1 School of Cyberscience and Engineering, Wuhan University, Wuhan, China Corresponding Adamu Umaru Shamsuddeen, Department of Computer Science, Kaduna State University, Kaduna, Nigeria1 School of Cyberscience and Engineering, Wuhan University,

ABSTRACT: Information security is the exercise of protecting information by means of mitigating information threats and risks by averting or decreasing the probability of inappropriate or unauthorized access to data, or the unlawful usage, exposure, disruption, erasure, corruption, alteration, assessment, recording, or devaluation of information.It similarly encompasses actions planned to decrease the adversarial effects of such incidents. Information security's prime goal is the protection of the integrity, confidentiality, and availability of data for efficient policyimplementation, and without obstructing the productivity and development of the organization. An effective information security strategy would be the best measure to adopt to tackle the insecurity challenges faced by Nigeria which as well obstructs its potential to drive sustainable national security and development. This studydefines those effective information security measures and strategies to be adopted as a tool to attain the desiredsaid information security goal. This paper concludes that these measures and strategies will be effective for sustainable Nigerian national security and development. Nevertheless, this study provides recommendations thatwill enhance sustainable Nigerian national development by adopting these information security measures.

KEYWORDS: *Information Security, Cyber Security, National Security, National Development, Information Security Strategy*

1. INTRODUCTION

The global security environment is constantly changing with an evolving landscape of threats (Świątkowska, 2017). Various countries are suffering from one security challenge to another ranging from war, terrorism, cyber terrorism and theft, arm banditry, kidnapping for ransom, blackmail, coup, civil unrest, etc. This makes information security and assurance more in need than ever as a countermeasure to most of the security challenges. Countries that are victims of such security concerns need a more sophisticated information security strategy for sustainable national development. Africa specifically is occupied with such security concerns led by countries such as Mali, CAR, Libya, and Sudan with Nigeria as the nerve centre due to dreaded insurgents such as Boko Haram and the Islamic States West Africa Province (ISWAP). The problem here according to Paul (2022) is that most African militaries are ineffective because most African countries lack a strong sense of national identity. An important and critical threat among the Eko (2022) five threats to national security is cybersecurity. Others are hostile governments, terrorism, proliferation, and national disaster & diseases.

Since the Iraqi war, the Saudi Arabian government has embarked on a course of political, economic, and social reform that reflects a growing understanding by the royal family members, technocrats, and businessmen that Saudi Arabia must reform and diversify its economy and create vast numbers of new jobs for its growing population which has yielded results (Anthony, 2005). On June 10, 2021, the Standing Committee of China's National People's Congress passed the Data Security Law (DSL), which took effect on September 1, 2021. The major drive of the DSL is to regulate data activities, safeguard data security, promote data development and usage, protect individuals and entities' legitimate rights and interests, and safeguard state sovereignty, state security, and development interests (Latham & Watkins, 2021). The DSL, together with the Network Security

Law and the proposed Personal Information Protection Law, formed an increasingly comprehensive legal framework for information and data security in the People's Republic of China (PRC). As the protection of ICT infrastructure is in Switzerland's national interest, the Swiss Federal Council commissioned the national strategy for the protection of Switzerland against cyber risks pursuing the early identification of threats and dangers in the cyber field, improvement of the resilience of critical infrastructure and effective reduction of cyber risks, especially cybercrime and cyber sabotage (National strategy for the protection of Switzerland against cyber risks, 2012). The formation of a joint task force for cyber security and the building of a National Cyber Command Center that will be the go-to centre for cyber security in Nigeria, facilitate the integration for all cyber intelligence in all governmental parastatals and other institutions in Nigeria and also collaboration among stakeholders is a recommended measure in reforming information security in Nigeria (Tope, 2016).

2. RELATED CONCEPT

2.1 Nigerian National Security

National security also called national defence is the security and defence of a sovereign nation including its citizens, economy, and institutions which is observed as the obligation of the government. National Security as documented by President Obasanjo's regime in 2002 is the aggregation of the security interest of all individuals, communities, ethnic groups, political entities and institutions in the territory of Nigeria (Saleh & Émile, 2018). Components of national security such as military security, socio-political security, information security, energy security, food security, environmental security, health security, education system security, etc. must be utterly collaborated and improved to achieve sustainable national development (Rasim, Yadigar, Rasim, & Aliguliyev, 2021).

The approach of the Nigerian government towards national security remains unsatisfactory according to Chinecherem & PaulIregbenu (2015) hence, conducted research examining the security challenges facing the Nigerian government and their implications for national stability. Among the recommendations of the research is the provision of better information security measures. Sahel security at the Tony Blair Institute, USA, has reported that there are five (5) security challenges bedevilling Nigeria. They are; Jihadism, Farmers-Herders clashes, Banditry and Kidnapping, Separatist agitation, and Oil militants (Aliyu, 2021). According to United Nations, by the end of 2020, conflict with Boko Haram alone has led to the death of about 350,000 people and forced millions out of their homes while another splinter group called the ISWAP has emerged in recent years (Aliyu). ISWAP has allied and surpassed Boko Haram with strong resistance to the Nigerian military and this has become a distinct threat to Nigeria's national security.

The Nigerian national security strategy (2019) has defined some key security concerns of the nation for which policies and strategies to implement them have been articulated depending on other national strategic policies such as the National Counter Terrorism Strategy, Cybersecurity Policy and Strategy, the National Defence Policy and the Economic Recovery and Growth Plan. Conversely, the security situation has persisted.

2.2 Information Security

Statistically, all over the world and since 2006, there has been a form of cybercrime committed daily (Yakubu, 2017). Nigerian cyber criminals are daily formulating different methods of committing this form of crime and the existing methods of trailing these criminals are no longer suitable to deal with their new tricks. Tope (2016) has conducted research he called Cyberharam: Can Nigeria Prepare For The Next Generation Of Terrorists where he explained that in confronting the challenges posed by cyber threats, one major deliberation is to identify our critical infrastructure and evaluate the risks to these systems so as to identify threats and vulnerabilities. Examples of the said critical infrastructure include those supporting our financial and telecommunication

systems, and systems hosting classified national security information amongst others. At the conclusion of the assessment, a long-term roadmap that will guide investments in securing our infrastructure should be set.

Another area of concern is cloud security as many governments today host their data on the cloud. A number of security threats associated with cloud data services, not only cover traditional security threats, e.g., network eavesdropping, illegal invasion, and denial of service attacks, but also includes specific cloud computing threats, e.g., side-channel attacks, virtualization vulnerabilities, and abuse of cloud services have been a serious area of concern in terms of information security (Ahmed, 2020).

2.3 National Development

National development is the capability of a country to raise the standard of living of its citizens. It can be accomplished by providing individuals with basic livelihood requirements such as security, food, health, and education, and also supplying them with employment. The Nigerian national development plan is a bridge for the country's long-term plan currently being developed, that is, National Development Plan 2021-2025 Olanrewaju (2021) and Nigeria Agenda 2050 with vision to make Nigeria a country that has unlocked its potential in all sectors of the economy for a sustainable, holistic, and inclusive national development (Ariyo-Dare, 2020).

3. INFORMATION SECURITY STRATEGY

Developing an effective information security strategy and taking steps to ensure compliance is a critical step to avert and mitigate security breaches. To make the security strategy justly effective, one needs to update it in response to changes in Nigeria. New threats, conclusions drawn from previous breaches, and other changes to the information security posture should be observed (Orion, 2019). Also make the information security policy practical and enforceable

with an exception system in place to accommodate requirements and urgencies that arise from different parts of Nigeria. It’s also vital to differentiate between Information Security and Cyber Security strategies and policies. The National Institute of Standards and Technology (2022) defines information security as the "protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability." The institute defines cyber security as the "ability to defend or protect the use of cyberspace from cyber-attacks." Notably, the difference is in the scope.

4. CONCLUSION AND RECOMMENDATIONS

The Nigerian government needs an effective information security strategy as the best measure to deploy so as to tackle the insecurity challenges faced by the country which as well obstructs its potential to drive sustainable national security and development. There are many advantages of enhancing information security such as having a secure national identity database, nurturing good governance, improving the physical security of citizens, encouraging economic development, fostering confidence among citizens established on the security and transparency it provides, and eventually reinforcing democracy (Sixtus, 2021). Therefore, the recommendations of this study which revolve around the three basic principles of information security; confidentiality, integrity, and availability can be stated as follow:

1. The Nigerian Government should increase it efforts towards the enhancement of capturing and registering citizens and foreigners through the National Identity Management Commission (NIMC); NIMC should enhance its collaboration with databased government parastatals and private organizations

such as INEC for voters cards, Banks for BVN, the Nigerian police, military, customs, immigration service for international passport, federal road safety corps for vehicle registration and drivers licence, all telecom companies for sim cards, all basic, secondary and tertiary institutions, examination bodies such as NECO, JAMB, WAEC NBAIS, and NAPTEP to construct a mega data pool using the National Identification Number (NIN) as the Nigerian social security number. NIN registration is still faulty due to internal challenges such as lack of power, tribalism, religion, illiteracy, scammers, and lacks of clear benefits definition attached (Sixtus, 2021).

2. Another recommendation is the full adoption of the Global Position System (GPS) and Closed-Circuit Television (CCTV) for tracing known and unknown armed bandits,

Kidnappers, and other terrorist organizations across the country. It is also recommended to sensitize and monitor social media and messaging applications such as Facebook, Twitter, and Whatsapp.

3. The Nigerian government should boost the Information and Communication Technology (ICT) sector as It is believed that ICT has the potential to help Nigerians develop various skills including entrepreneurial skills, research and academic skills, economic and management skills, political skills, etc., which have become a potent force in transforming social, economic and political life globally (Emmanuel, Eneh, Isaac, Arinze, & Ahmed, 2021).
4. Building a go-to information security centre that will collaborate with all security and intelligence agencies with other related and relevant government parastatals.

REFERENCES:

1) Ahmed, A. A. (2020). Improving Cloud Data Security by hybridization of ZeroKnowledge Proof and Time-Based One-Time Password. *KASU JOURNAL OF MATHEMATICAL SCIENCES*, 116-126.
2) Aliyu, T. (2021, July 19). *Nigeria's security crises-five different threats*. Retrieved from BBC News website: www.bbc.com
3) Anthony, H. C. (2005). *National Security in Saudi Arabia: Threats, Responses, and Challenges.* Riyadh: https://www.csis.org/analysis/national-security-saudi-arabia.
4) Ariyo-Dare, A. (2020, July 13). *Agenda 2050: A new thinking with citizen participation and inclusion*. Retrieved from Vanguard Website: https://www.vanguardngr.com/2020/07/agenda-2050-a- new-thinking-with-citizen-participation-and-inclusion/
5) Chinecherem, U., & PaulIregbenu, P. (2015). *Security Challenges and Implications to National Stability.* Anambra : Project: Child Labour and Its Determinants in Informal Sector of Onitsha.
6) Eko, O. (2022, 03 10). *five threats to national security and how the government protects its citizens .* Retrieved from Safetymanagement.eku.edu: Safetymanagement.eku.edu
7) Emmanuel, I. T., Eneh, A. H., Isaac, S., Arinze, U. C., & Ahmed, A. A. (2021). ICTs - An Efficient Tools for Entrepreneurs Amongst the Nigerian Youths. *Proceedings of the 27th SMART-iSTEAMS- IEEE, MINTT Conference Academic City University College* (pp. 267-272). Accra, Ghana: www.isteams.net/ghana2021.
8) Latham & Watkins. (2021, July 21). *China's New Data Security Law: What to Know.* Retrieved from LW website: https://www.lw.com/thoughtLeadership/china-new-data-security-law-what-to- know
9) *National strategy for the protection of Switzerland against cyber risks.* (2012, June 19). Retrieved from Enisa Website: https://www.enisa.europa.eu/topics/national-cyber-security-
10) strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf

11) NSS. (2019). *National Security Strategy.* Abuja: https://ctc.gov.ng/wp-content/uploads/2020/03/ONSA-UPDATED.pdf.
12) Olanrewaju, O. (2021, December 21). *As Nigeria Unveils National Development Plan 2021-2025, these are Twenty Key Points to Note*. Retrieved March 11, 2022, from Dataphyte Website: https://www.dataphyte.com/latest-reports/economy/as-nigeria-unveils-national- development-plan-2021-2025-these-are-twenty-key-points-to-note/#:~:text=The%20National%20Development%20Plan%20targets,persons%20and%2020 25%2074.01%20persons.
13) Orion, C. (2019, May 30). *The 8 Elements of an Information Security Policy*. Retrieved from Exabeam Website: https://www.exabeam.com/information-security/information-security-policy/
14) Paul, C. (2022, 03 10). *Security Threats Facing Africa and its Capacity to respond.* Retrieved from cco.ndu.edu: cco.ndu.edu
15) Rasim, M. A., Yadigar, N. I., Rasim, S. M., & Aliguliyev, R. M. (2021). Information Security as a National Security Component. *Information Secuirty Journal: A Global Perspective*, 1.
16) Saleh, B., & Émile, O. (2018). NATIONAL SECURITY STRATEGY DEVELOPMENT: CASE STUDY NIGERIA. *Africa Center for Strategic Studies*.
17) SIXTUS, E. (2021, October). *Issues in national identity in the 21st century*. Retrieved from The Cable Website: https://www.thecable.ng/issues-in-national-identity-in-the-21st-century
18) Świątkowska, J. (2017). Cybersecurity Statecraft in Europe: A Case Study of Poland. *Georgetown Journal of International Affairs*, 84-94.
19) The National Institute of Standards and Technology. (2022, March 11). *COMPUTER SECURITY RESOURCE CENTER*. Retrieved from CSRC Website: https://csrc.nist.gov/glossary/term/cybersecurity
20) Tope, A. (2016). 'Cyberharam': Can Nigeria Prepare For The Next Generation Of Terrorists? *Deloitte Nigeria*. Retrieved March 11, 2022, from https://www.mondaq.com/nigeria/terrorism- homeland-security-defence/533396/cyberharam39-can-nigeria-prepare-for-the-next- generation-of-terrorists
21) Yakubu, A. M. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research inComputer Science and Software Engineering*, 315.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(1): 16-19 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

THE ANALYSIS OF CYBERSECURITY PROBLEMS IN FINANCIAL SERVICES SECTOR

Oksana Kovalchuk, Sokhumi State University
Diana Popova, Georgian Technical University

ABSTRACT: The concentration of money, bank-centricity of the financial market, a vast range of online services, and a significant customer base make banks and other financial institutions an alluring target for cybercriminals, leading to a sophisticated form of fraud. This intellectualized form of fraud reduces trust in financial institutions, decreases resources in the economy, and negatively impacts the country's financial and economic security, along with its image as a trustworthy financial partner in integration processes. The international regulatory community recognizes the importance of finding solutions to combat cybercrime and safeguard the rights of consumers of financial services, and they prioritize these issues as critical scientific challenges.
The financial services sector is a prime target for cyber-attacks and is heavily regulated across the globe. Financial services organizations face a constant barrage of intrusion attempts and other attacks, and they often struggle to transition from a reactive to a proactive cybersecurity posture. Achieving this goal is complicated by the ever-increasing number of attack avenues that arise due to the use of new technologies as part of digital innovation initiatives. Along with this complexity, there is a growing need to comply with regulations regarding the use of financial and personal data.
Analyzing cyber threats and addressing issues related to financial organizations' activities is an extremely relevant topic. This article aims to examine the primary cyber problems faced by the financial sector while also providing recommendations for financial institutions to help mitigate these challenges.

KEYWORDS*: cybersecurity problems, financial sector, regulations, cyber threats*

1. OVERVIEW OF THE PROBLEM

Good progress in overall digitization of finance has been made over the recent years. Indeed, the World Bank reports that between 2014 and 2017 the number of adults using digital payments increased from 41 to 52% (11% increase) [1] and the share of adults with an account has grown from 62 to 69% (7% increase) [2]. This translates into half a billion new users connected to the digital financial infrastructure – as well as half a billion new targets for cyber attackers. Yet, just as cyber-attacks were not invented yesterday, so financial institutions are aware of potential risks. After all, cybersecurity risk is but one form of operational risk that 'needs to be part of general risk management procedures, of general crisis management, and general business continuity planning'. However, until recently, rules relating to cyber-resilience rarely took the form of dedicated cybersecurity instruments and instead were generally included into other regulations (e.g on data protection) – and, for this reason, often remained rudimentary. Over the past several years, the cybersecurity regulatory landscape has undergone substantial changes. New laws and regulatory instruments focusing exclusively on cyber resilience have been adopted in a number of jurisdictions, including Hong Kong, the USA and Singapore. Cybersecurity has also become the focus of international rules and recommendations adopted by numerous organisations, including the BCBS, CPMI, FSB, G7, IAIS, IMF, IOSCO, OECD and the World Bank Group. Nonetheless, the apparently high interest in possible international harmonization of cybersecurity regulatory regimes has not yet translated into hard international law.
Bank-centricity of the financial market, high concentration of money, variety of online services, and significant client base - all this makes banks and financial institutions attractive to cybercriminals and leads to the "intellectualization" of fraud. This reduces trust in financial institutions, reduces the number of resources in the economy, and negatively affects the financial and economic security of the country and its image as a reliable financial partner in integration processes. Solutions to the problems of combating cybercrime and protecting the rights of consumers of financial services are recognized by

international regulators and priority scientific problems at the world level by the expert community [3-4].

The financial services sector is a particularly important target for cyber-attacks and is heavily regulated by jurisdictions around the world. Faced with constant intrusion attempts and other attacks, financial services organizations often struggle to transition from a reactive to a proactive cybersecurity posture. Achieving this goal is complicated by the ever-increasing number of attack avenues as a result of the use of new technologies introduced as part of digital innovation initiatives. In addition to this complexity, there is the need to comply with a growing number of regulations regarding the use of financial and personal data.

Protecting highly sensitive data is a top priority for both business and compliance. But sacrificing network performance for security is unacceptable, as consumers and businesses, from online and mobile banking to high-frequency trading, increasingly need real-time access to every offer. At the same time, to remain competitive in a multi-player industry, organizations must control costs and optimize operational efficiency.

In addition to malware, most businesses have had to deal with the rapid shift to remote work in recent years. The changes took place in an extremely short period of time, so companies did not have enough time to ensure safe conditions for remote work. Many organizations still work remotely, and remote work remains one of the challenges for financial cybersecurity.

According to an IBM report, one of the top three causes of data breaches is human error, which accounted for 23% of breaches. Employee mistakes can take many forms — they can become victims of phishing, social engineering attacks, or other types of malware [5-7].

In recent years, losses from financial fraud have increased dramatically. This has negative consequences for clients of financial and economic agents, who become the main object of fraud and lose funds. Fraud also causes significant damage to banks, which is manifested in the loss of customers, the need to reimburse stolen funds, increased funds for the modernization of the cyber security service, and the strengthening of protective measures.

The most common are:

1) Fraud with bank cards, as the most simple, accessible, and mass payment method, which makes it possible to forge cards, devices that read information, and steal data from cards;

2) Internet fraud, where the Internet, which is a platform for bank customers through which online payments are made, is used by fraudsters as a tool to steal customers' personal financial data;

3) Social engineering, when a fraudster on behalf of the bank learns all his information from the client and steals funds from his account. In the arsenal of fraudsters, there are quite a few methods of fraud involving psychological tools, computer programs, various technical devices, databases with customer information, etc.

In general, the financial sphere faces a large scale of threats every day, therefore it is very important to analyze these threats, as well as to develop recommendations, first of all, for employees of the financial sphere.

2. REASONS FOR INCREASING CYBER THREATS

The daily activities of financial institutions are closely related to the use of modern computer technologies and are completely dependent on the reliable and uninterrupted operation of electronic computing systems. World experience shows the unconditional vulnerability of any company given the fact that cybercrimes have no national borders, so hackers have the opportunity to equally threaten information systems anywhere in the world.

Cyber threat - existing and potentially possible phenomena and factors that pose a danger to the interests of people, society, and the state due to violations of the availability, completeness, integrity, reliability, and authenticity of the regime of access to information that circulates in critical objects of the national information infrastructure.

The fundamental causes of cyber threats are:

- lack of necessary legislation and uniform safety standards;
– insufficient funding from the financial organizations themselves;

- lack of corporate culture in the field of cyber security within the financial institution.

3. THE MAIN PROBLEMS OF CYBER SECURITY IN THE FIELS OF FINANCIAL SERCISES

We analyzed and highlighted the main cybersecurity issues in the financial services industry. In this section, we will look at the most basic problems and those that tend to increase:

1) Tracking

The attack surface is constantly growing, complicating the process of protecting against threats. The proliferation of Internet of Things (IoT) devices, the adoption of multi-cloud solutions for business services, and the use of mobile devices by customers and employees lead to a rapid increase in the number of attack vectors. As a result, financial services companies are being forced to deploy more and more specialized defenses to close the gaps created by the growing number of such attack avenues. The resulting security silos negatively impact traceability, increasing operational inefficiencies and increasing risk.

2) Operational efficiency

The lack of integration between different security elements and the fragmentation of the architecture increase operational inefficiencies. In the absence of integration, many work processes must be managed manually. In addition to delaying threat detection, prevention, and response, architectural storage creates redundancy, increases operational costs, and creates potential gaps in an organization's cybersecurity system.

3) Flexibility

As financial services organizations increasingly use cloud-based applications and infrastructure, the security architecture must be flexible enough to ensure the high speed, security, and interoperability of public, private, and hybrid cloud services while simultaneously protecting traditional on-premises services.

4) Compliance reporting

Financial services are one of the most demanding industries in the world, and all financial data, personal and corporate, is stored online—from the campus to the data center, the edge, and the cloud. Organizations must demonstrate compliance with several norms and standards. They should not involve employees performing strategic tasks to manually prepare audit reports.

5) Cost reduction

Financial organizations are constantly under pressure to limit and reduce the costs of maintaining their IT environment. In connection with the limitation of budgets for cyber security, it is necessary to use a strategic approach to the distribution of financial and human resources. Given the fact that money and staff time is limited, a strategy that limits the margin of risk and trade-offs is required.

These problems are exacerbated by the lack of personnel in the field of cyber security, which leads to the complexity and cost of the process of finding certain specialists, and also calls into question the possibility of finding them.

4. CONCLUTIONS AND RECOMMENDATIONS

Given the recent trends, financial institutions are obliged to invest significantly in the modernization of the cyber protection system by purchasing or creating modern fraud detection and prevention systems, which in the end may also prove to be ineffective. Therefore, to fight against cyber-attacks, the financial sector must take a consistent and systematic approach.

1) First, a clear regulation of the actions of personnel regarding access to data is necessary, which will allow avoid the facts of their access to the personal information of clients and, accordingly, its theft.

   Financial cyber security will reduce the chances of becoming a victim of phishing. To reduce the chances of infection, institutions should ensure that employees are informed about the basic rules of Internet security. It is important that employees know how to recognize phishing or

social engineering attempts. In addition, it is a good idea to provide staff with advice on safe remote work. Using even these measures will help organizations avoid financial and reputational losses.

2) Second, implement strategies that include fraud awareness training, public outreach through mass media and the Internet, fraud risk assessment, and continuous monitoring.

3) Thirdly, to improve the software and information support of the automated banking system, taking into account intelligent processing algorithms, which will allow identifying the fraudster and the victim at the stage of fraud, to prevent the implementation of such an operation, and to identify the criminal.
Criminals breach the financial cyber security of companies due to the lack of reliable IT solutions. Although financial institutions remain profitable targets for cybercriminals, there are a sufficient number of modern solutions and tools that allow timely detection of suspicious processes on the network and immediate response to incidents.

4) Another common mistake is that organizations overestimate their own cybersecurity. Even though a company may use quality solutions, not regularly updating the operating system and all software can compromise the security of the entire network.

In order to build strong enough defenses, companies need to take a balanced approach that combines employee training and the use of powerful security technology solutions.
While employee training is an important aspect of improving an organization's financial cybersecurity, the primary protection against threats is provided by the security solutions implemented in the corporate network and compliance with international standards.

5. RESOURCES:

1. Trend Report "Financial Cyber Threats Q1 2017". Electronic resource: http://www.level3.com//media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regionalbanks.pdf
2. IT threat evolution Q3 2017. Statistics. Electronic resource: https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/
3. Ryan C. Hybrid Risk: The truth behind first party fraud / Chris Ryan // The official site of the company "Experian". – 2015. – Electronic resource: http://www.experian.com/blogs/insights/2015/10/hybrid-risk-the-truth-behind-first-party-fraud/.
4. Third Party Fraud // Open Risk Manual. – 2017. – Electronic resource: https://www.openriskmanual.org/wiki/Third_Party_Fraud
5. IBM Annual reports 2019-2022. – Electronic resource: https://www.ibm.com/annualreport
6. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, AndriyFesenko, Security methods against modern cyber-attack vectors in countries of Europe, Scientific and practical cyber security journal, 2019
7. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, AndriyFesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019

Scientific and Practical Cyber Security Journal (SPCSJ) 7(1): 20-30 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

რადიოლოგია კლინიკის მართვის ციფრულ სისტემებში

ლაშა შარვაძე, საქართველოს ტექნიკური უნივერსიტეტი

RADIOLOGY IN DIGITAL CLINIC MANAGEMENT SYSTEMS

Lasha Sharvadze, Georgian Technical University

აბსტრაქტი:სტატიაში აღწერილია ავტორების კვლევები კლინიკის მართვის ერთიანი ციფრული სისტემის შექმნის მიმართულებით. კვლევის მიზანია, შეიქმნას კლინიკის მართვის ისეთი ერთიანი სისტემა, რომელიც იქნება მარტივი, ერთი ფანჯრის პრინციპით, სრულად გააერთიანებს კლინიკის მართვის ყველა სისტემას ერთ გარემოში და მოახდენს მათ სრულ გაციფრულებას. პროცესების სხვადასხვა მიმართულებით გაშლის გამო, არსებულ კლინიკის მართვის სისტემებს არ აქვთ გაერთიანებული ერთ ელექტრონულ სივრცეში ყველა დაკავშირებული სტრუქტურები, პროცესები, მონაცემები და სისტემები.

სისტემას გააჩნია web ინტერფეისი და მორგებულია სხვადასხვა მობილურ მოწყობილობებზე. სისტემაში გათვალისწინებულია უსაფრთხოების ფუნქციები, ისეთები როგორც პაროლის პოლიტიკები და მომხმარებლის როლების მართვა. სისტემა მუშაობს უსაფრთხო ქსელურ გარემოში.

ჩატარებულია ექსპერიმენტები სატესტო გარემოში და ნაჩვენებია, რომ ახალი სისტემა ზრდის სამედიცინო სერვისების მიღების ეფექტურობას და ამცირებს მომსახურეობის დროს.

საკვანძო სიტყვები: *კიბერუსაფრთხოება, რადიოლოგია, მედიცინა*

ABSTRACT: The paper describes the authors' research in the direction of creating a unified digital system of clinic management. The aim of the study is to create a unified system of clinic management, which will be simple, with a single window principle, will fully integrate all clinic management systems in one environment and will fully digitize them. Due to the spread of processes in different directions, the existing clinic management systems do not have all related structures, processes, data and systems integrated in one electronic space.

The system has a web interface and is adapted to various mobile devices. The system provides security features such as password policies and user role management. The system operates in a secure network environment.

Experiments have been conducted in a test environment and it has been shown that the new system increases the efficiency of receiving medical services and reduces service time.

KEYWORDS: *cybersecurity, medicine, software implementation, radiology*

შესავალი

PACS (Picture Archiving and Communication Systems/ სურათების არქივაციის და კომუნიკაციის სისტემები), არის სისტემა, რომელიც გამოიყენება სერვერების, კომპიუტერების და სამედიცინო მოწყობილობების დასაკავშირებლად და ემსახურება სამედიცინო რადიოლოგიური სურათების შენახვას, მოძიებას, გამოყენებას და მართვას. PACS სისტემები მუშაობს განსხვავებულ ფორმატის სურათებთან. PACS სისტემებში ციფრული გამოსახულების და კომუნიკაციების ფორმატის, ყველაზე გავრცელებული ფორმატია (DICOM) [1-4].

PACS (სურათების არქივისა და კომუნიკაციის სისტემა) არის სამედიცინო გამოსახულებების ტექნოლოგია, რომელიც ძირითადად გამოიყენება ჯანდაცვის ორგანიზაციებში, ელექტრონული სურათების და კლინიკურად მნიშვნელოვანი ინფორმაციის უსაფრთხოდ შესანახად და გამოსაყენებლად სამედიცინო პერსონალის მიერ. PACS-ის გამოყენება გამორიცხავს სენსიტიური სამედიცინო ინფორმაციის, სურათების და ჩანაწერების ხელით ფაილის შენახვას, მოძიებას და გაგზავნას. ამის ნაცვლად, სამედიცინო დოკუმენტაცია და სურათები შეიძლება უსაფრთხოდ განთავსდეს კლინიკის სერვერებზე და დაშიფრული არხებით განხორციელდეს წვდომა/გამოყენება მსოფლიოს ნებისმიერი ადგილიდან სხვადასხვა საკომუნიკაციო მოწყობილობების გამოყენებით (კომპიუტერი, პლანშეტი, მობილური ტელეფონი და აშ).

სამედიცინო გამოსახულების შენახვის ტექნოლოგიები, როგორიცაა PACS, სულ უფრო მნიშვნელოვანი და აუცილებელი ხდება, რადგან ციფრული სამედიცინო სურათების მოცულობა იზრდება ჯანდაცვის ინდუსტრიაში და ამ სურათების მონაცემთა ანალიტიკა უფრო გავრცელებული ხდება.

რადიოლოგების მხრიდან ესეთი სისტემების გამოყენებამ დაგვანახა მისი უპირატესობა, საჭიროება, აუცილებლობა და ამ სისტემის ქვეშ გაერთიანდა სხვადასხვა სამედიცინო მიმართულებები, რომლებიც იყენებენ ვიზუალიზირებულ მონაცემებს, როგორიცაა კომპიუტერული ტომოგრაფია, მაგნიტურ რეზონანსული ტომოგრაფია, რენტგენი, ულტრაბგერითი დიაგნოსტიკა, რადიონუკლიდური დიაგნოსტიკა, ბირთვული მედიცინა, კარდიოლოგია, პათოლოგია, რადიაციული ონკოლოგია, დერმატოლოგია, ენდოსკოპია, ბრონქოსკოპია, გინეკოლოგია, პალსტიკური ქირურგია.

სამედიცინო გამოსახულებები გადაღებულია და გამოიყენება კლინიკური ანალიზისთვის, დიაგნოსტიკისთვის და მკურნალობისთვის, როგორც პაციენტის მოვლის გეგმის ნაწილი. შეგროვებული ინფორმაცია შეიძლება გამოყენებულ იქნას ნებისმიერი ანატომიური და ფიზიოლოგიური პათოლოგიის იდენტიფიცირებისთვის, მკურნალობის პროგრესის გამოსათვლელად და პაციენტების სურათების მონაცემთა ბაზის შესანახად.

PACS სისტემები შედგება ოთხი ძირითადი კომპონენტისგან:

1. გამოსახულების დამუშავების მოწყობილობები;
2. უსაფრთხო ქსელური გარემო პაციენტის სურათების და მონაცემების გაცვლისთვის;
3. სამუშაო სადგური, კომპიუტერი ან მობილური მოწყობილობა სურათების სანახავად, დამუშავებისა და ინტერპრეტაციისთვის;
4. ელექტრონული არქივი სურათების და შესაბამისი დოკუმენტაციის შესანახად და შემდეგ გამოსაყენებლად.

PACS გამოსახულების საინფორმაციო სისტემებმა, შეცვალა ბეჭდური მასალების და მატარებლების შენახვისა და მართვის აუცილებლობა, თაროებსა და ოთახებში. ამის ნაცვლად, სამედიცინო გამოსახულებები, სამედიცინო ჩანაწერები და სხვა კლინიკური მონაცემები შეიძლება უსაფრთხოდ შეინახოს ციფრულად შენობაში ან ღრუბელში (Cloud).

პროვაიდერები ხშირად იყენებენ ჰიბრიდულ ღრუბლოვან სისტემას, რომელშიც პირველადი სურათები ინახება შენობაში და სარეზერვო ასლები ინახება ღრუბელში. შენახვის არქიტექტურის და უსაფრთხოების დამატებითი ტიპები შეიძლება იყოს კონფიგურირებული და მიმაგრებული PACS სერვერზე, როგორიცაა უშუალოდ მიმაგრებული საცავი (DAS), ქსელთან მიმაგრებული საცავი (NAS) ან შენახვის არეალის ქსელის (SAN) მეშვეობით, რომელთაგან თითოეული მათგანი უზრუნველყოფს განახლების, დაკავშირების, გაუმჯობესების და დამატებითი უსაფრთხოების შესაძლებლობას.

წარმოიდგინეთ, რომ თქვენ მიიღეთ ტრამვა და გჭირდებათ საავადმყოფოში მისვლა. კლინიკაში მისვლისას გაივლით რეგისტრაცის პერსონალური მონეცემების გამოკითხვით და ეს ინფო შეიყვანებას საავადმყოფოს საინფორმაციო სისტემაში. მოკლე პერიოდის ლოდინის შემდეგ ხვდებით ექიმთან კონსულტაციაზე. ექიმი გაგსინჯავთ და დაგინიშნავთ რიგ გამოკვლევებს თქვენი მდგომარეობის შესაფასებლად, რენტგენის და სისხლის ანალიზების. ესენი ინფორმაცია ასევე შედის HIS (Hospital Information System)-ში. ეს ინფორმაცია ეხლა საჭიროა სხვა სამედიცინო პერსონალთვის, მათ კომპიუტერულ სისტემაში, რათა გააგრძელოს თქვენი დაავადების დიაგნოსტირების და მკურნალობის პროცესი. კლინიკის მართვის სისტემებში კლინიკური, ლაბორატორიული და რადიოლოგიური მოწყობილობების კომუნიკაციის ენაა HL7 (Health Level 7) პროტოკოლი [5,6].

HL7 არის სტანდარტების ნაკრები საავადმყოფოს საინფორმაციო სისტემებს შორის კლინიკური და ადმინისტრაციული მონაცემების გასაცვლელად. ის ჰგავს ენას, რომელიც აღწერს თქვენ და თქვენს

სამედიცინო ინფორმაციას საავადმყოფოს ყველა საინფორმაციო სისტემაში და ყველაზე მნიშვნელოვანი ის არის, რომ ყველა სისტემა ერთსა და იმავე ენაზე საუბრობს. ასე რომ, როდესაც HL7 შეტყობინება მიიღება სხვა კომპიუტერული სისტემაში, ის შესაძლებელია დამუშავდეს და გამოყენებული იქნას სამედიცინო პერსონალის მიერ.

HL7 შეტყობინება აგებულია შემდეგნაირად:

MSH|^~\&|HL7Soup|HIS|HL7Soup|HIS|201407271408||ADT^A04|1817457|D|2.5.1|EVN|A04|AL
PID||0493575^^^2^ID1|454721||DOE^JOHN^^^^|DOE^JOHN^^^^|19480203|M||B|254E238ST^^Howick^OH^3252^USA|| (216)631-4359|||M|AGN|400003403~1129086|999-|
NK1||CONROY^MARI^^^^|SPO||(216)731-4359||EC||||||||||||||||||||||||
PV1||O|O/R||||277^ALLEN^BONNIE^J^^^|||||||||| ||2688684|||||||||||||||||||||201407271408|||||002376853

დიახ, ვეთანხმები, თუ აქამდე არ გინახავთ HL7 შეტყობინება, ეს საკმაოდ საშინელია. მაშინაც კი, თუ თქვენ მუდმივად მუშაობთ ამ გზავნილთან, ეს არ არის ყველაზე მარტივი წასაკითხი მესიჯი. ის შექმნილია მანქანების გასაგებად და არა ადამიანებისთვის.

PACS სისტემებში სამუშაო პროცესი შემდეგნაირია:

პაციენტი რეგისტრირდება სისტემაში პერსონალური მონაცემებით, ჩასატარებელი კვლევაზე, კონკრეტულ ექიმთან. შემდეგ ექიმი/ასისტენტი ახდენს პაციენტის კვლევის დაწყებას. კვლევის მიმდინარეობისას ახდენს პაციენტის და გადაღების პროცესის მონიტორინგს პროგრამაში და საჭიროების შემთხვევაში კვლევას (კვლევები შედგება პროგრამებისგან) ამატებს დამატებით პროგრამებს ან უშვებს თავიდან კონკრეტულ პროგრამებს. კვლევის დასრულების შემდეგ ექიმი ახდენს თითოეული სამედიცინო ვიზუალის დეტალურ დათვალიერებას. ორგანოების და გადახრების ზომის, სტრუქტურის დადგენას. საყურადღებო და კლინიკურად მნიშვნელოვანი უბნების მონიშვნა/გაზომვას. გამოსაკვლევი ორგანოების ანატომიის დადგენას. ამის შემდეგ იგი ახდენს დასკვნის დაწერას პროგრამაში და კვლევის საბოლოო დასრულებას. თუ სისტემა დაკავშირებულია CD დისკების ჩამწერ პრინტერთან და სამედიცინო ფირების პრინტერთან, სისტემა ავტომატურად აგზავნის კვლევას გარე მატარებელზე (CD Disk) ჩასაწერად და ფირის დასაბეჭდად.

არსებული პრობლემები

PACS სისტემები წარმოდგენილია, როგორც ცაკლე მდგომი პროგრამული უზრუნველყოფა და არა კლინიკის მართვის ერთაინი სისტემის ნაწილი. ამის გამო რთულდება პაციენტის ერთერთ ყველაზე საჭირო ინფოზე წვდომა, რადგან ექიმებს უწევთ რამოდენიმე პროგრამაში მუშაობა და რთულია ერთიან ჭრილში სურათის დანახვა. ასევე რთულია სხვა დაკავშირებულ სისტემებში ამ ინფოს მოხვედრა და რეპორტინგი.

ამის მოსაგვარებლად PACS სისტემების მწარმოებლები გვთავაზობენ არსებული კლინიკის მართვის სისტემებთან ინტეგრაციას, თუმცა ყველა გავრცელებული ინტეგრაცია არის არასრული და ინტეგრაციის შემდეგ პაციენტის DICOM მონაცემების სანახავად პროგრამას მაინც გადაყავს PACS სისტემაში (ინტეგრირებულია მონაცემების ლინკი და არა თვითონ მონაცემი) და სამედიცინო ჩანაწერების შესაძლებლობაც ძალიან მშრალია. ასევე ვერ იძლევა სრულ რეპორტინს და სამედიცინო ისტორიას. ძირითადად ინტეგრირდება პაციენტის პერსონალური მონაცემები და ჩასატარებელი კვლევა, ხოლო თვითონ ვიზუალის მდებარეობის ლინკი.

სამედიცინო ვიზუალიზაცია არის ერთ ერთი ყველაზე საჭირო და ხშირ შემთხვევაში ერთადერთი ინფორმაცია პაციენტის დაავადებების დიაგნოსტირების და მკურნალობის დაგეგმვა/მიმდინარეობის პროცესისთვის. ამ ინფორმაციას იყენებს თითქმის ყველა მიმართულების ექიმი, ქირურგი და სხვა სამედიცინო პერსონალი.

ბაზრის კვლევა

გავარჩიეთ და შევისწავლეთ მსხვილი მომწოდებლების PACS სისტემები. ყველა სისტემა მორგებულია ექიმი რადიოლოგების და დიაგნოსტების სამუშაო პროცესზე და სხვა კლინიცისტებისთვის რთულად წვდომადია და კლინიკის მართვის ერთიან სისტემასთან ინტეგრაციის შემდეგაც კი ვერ იძლევა სრულ ერთიან სურათს ერთ ფანჯარაში.

საქართველოს მაშტაბით შევისწავლეთ კლინიკებში არსებული მდგომარება სამედიცინო სურათების შესახვის სისტემების მიმართულებით და შედეგები სამწუხაროდ ძალიან ცუდია. შევისწავლეთ 50 მსხვილი კლინიკა და აღმოჩნდა, რომ მხოლოდ 7 კლინიკას აქვს სამედიცინო ვიზუალიზაციის სურათების და მონამცემების შენახვის სრულყოფილი სისტემები (PACS). სხვა დანარჩენ შემთხვევაში ერთჯერადად ხდება მონაცმების ელექტრონულ მატარებელზე (CD Disk, USB, ფირი) ჩაწერა და პაციენტისთვის გადაცემა. თუ დაზიანდება ან დაიკარგება ელექტრონული მატარებელი, კვლევის შედეგებიც დაკარგულია. ასევე რთულად გამოსაყენებელია პაციენტის სამედიცინო ისტორიის ერთიან ჭრილში გამოსაყენებლად ექიმების ან სხვა სამედიცინო პერსინალის მიერ. ესეთი ტიპის ინფორმაცია

ასევე ვერ ხვდება კლინიკის მართვის ელექტრონული სისტემების რეპორტებში და ამახინჯებს სტატისტიკურ მონაცემებს.

კლინიკების რაოდენობა	აქვს PACS სისტემა	არ აქვს PACS სისტემა
50	7	43

PACS სისტემები საკმაოდ ძვირადღირებული მოსავლელია. რადგან სამედიცინო გამოსახულებების ზომა ხშირ შემთხვევაში არის საკმაოდ დიდი და ის შეიძლება რამოდენიმე გიგაბაიტიც იყოს. სტაბილურად მუშაობისთვის მას სჭირდება მძლავრი პროცესორები, ბევრი ოპერატიურლი მეხსიერება, კიდევ უფრო ბევრი HDD, კარგად დაცული და სწრაფი ქსელური გარემო. სერვერული და ქსელური ინფრასტრუქტურა უნმიშვნელოვანია ესეთი სისტემების სწორი და სწრაფი ფუნქციონირებისთვის. ხშირ შემთხვევებში ყველა სამედიცინო მოწყობილობა და PACS სერვერი არის შემოსაზღვრულ ქსელში, რომ არ მოხდეს სხვა დამატებითი ტრაფიკებით ქსელის გადატვირთვა, მონაცმების დაკარგვა და სისტემის შენელება.

სამედეცინო პერსონალი	რაოდენობა	აუცილებლობა	User Friendly	Not User Friendly
ექიმი რადიოლოგი	40	40	37	3
ქირურგი	50	50	5	45
კლინიცისტი	50	50	17	33
უმცროსი სამედიცინო პერსონალი რადიოლოგია	40	40	24	6
სხვა უმცროსი სამედიცინო პერსონალი	30	30	5	25

ჩვენმა კვლევებმა აჩვენა, რომ საქართველოს გარდა სხვა ქვეყნებშიც კლინიკების მცირე ნაწილს თუ აქვს დანერგილი PACS სისტემები, რადგან მათი მოვლა საკმაოდ ძვირია. ყველაზე მეტად ეს სისტემები განვითარებულია და ბევრ კლინიკაშია დანერგილი ამერიკაში, გერმანიაში და თურქეთში. ამ ქვეყნებში აქტიურად მიმდინარეობს PACS სისტემების განვითარება და ოპტიმიზაცია. ერთერთი ყველაზე დიდი გამოწვევა ამ მიმართულებით არის კვლევების ზომა. მიუხედავად იმისა რომ DICOM ფორმატი

ითვალისწინებს ვიზუალის ფაილის ზომის კომპრესიას და ზომის შემცირებას იმის გათვალისწინებით, რომ არ მოხდეს ხარისხის გაუარესება, კვლევის ზომები მაინც საკმაოდ დიდია. მისი დიდი ზომებიდან გამომდინარე რთული და ძვირია მათი მოვლა.

განხორციელდა კვლევა რადიოლოგებთან, კლინიცისტებთან, ქირურგებთან და სხვა სამედიცინო პერსონალთან ვინც საჭიროებს PACS სისტემაში პაციენტების მონაცემებზე წვდომას, პაციენტის მკურნალობის ან დაავადებების დიაგნოსტირებისთვის. კვლევა ითვალისწინებდა PACS სისტემის აუცილებლობას მათ სამუშაო პროცესში და პროგრამასთან მუსაობის სიმარტივეს. ყველა გამოკითხულმა დააფიქსირა ესეთი სისტემის საჭიროების აუცილებლობა მათ სამუშაო პროცესში. იმ სამედიცინო პერსონალმა (ექიმი რადიოლოგები და რადიოლოგიის უმცროსი სამედიცინო პერსონალი), რომელიც უშუალოდ მუშობს სამედიცინო ვუზაულიზაციის მიმართულებით უმეტესობამ აღნიშნა, რომ პროგრამა საკმაოდ User Friendly და მარტივია. ხოლო სხვა დანარჩენმა უმრავლესობამ დააფიქსირა, რომ პროგრამში მუშაობა არც ისე მარტივია.

შეთავაზებული მეთოდოლოგია

ამ კვლევების საფუძველზე დავადგინეთ, რომ საჭიროა ისეთი PACS სისტემის შექმნა, რომელიც მარტივად დაკავშირდება კლინიკის მართვის სისტემასთან და მოახდენს მონაცემების სრულ გაცვლას და სამედიცინო ვიზუალები პაციენტის სამედიცინო ისტორიაში გადმოვა სრულად და მარტივად სამართავად. უნდა მოხდეს კლინიკის მართვის ერთიან სისტემაში HL7 პროტოკოლების და DICOM-ის წამკითხველის ინტეგრირება, რომ სისტემას შეეძლოს ესეთი ტიპის მესიჯების დამუშავება დამოუკიდებლადაც და გააჩნდეს ამ მონაცემების საკუთარი მონაცემთა სრული ბაზა. ამ მეთოდით ყველა სამედიცინო პერსონალს ექნება სამედიცინო ვიზუალებზე წვდომა თავიანთ ერთიან სისტემაში, როგორც პაციენტის სამედიცინო ისტორიის ნაწილი და მარტივად შესაბამის ქრონოლოგიაში სანახავი და გამოსაყენებელი.

ჩვენი მიზანია შევქმნათ ისეთი სამედიცინო გამოსახულებების მოდული, რომელიც გამოსახულებიდან წაიკითხავს ყველა საჭირო ინფორმაციას, როგორიცაა მაგალითად: გამოკვლეული ორგანო, უბანი, გადახრა, ზომები და ა.შ. ისეთი ინფო რომელიც არის სურათის ფორმატის, შემდეგ სისტემა ავტომატურად მოახვედრებს ამ ინფოს პაციენტის სამედიცინო ისტორიაში, შესაბამის ადგილას.

ჩვენი მიზანია შევქმნათ PACS სისტემა, აღნიშნული მოდელის მიხედვით, რომელიც იქნება მაქსიმალურად იაფი და ხელმისაწვდომი ჯანდაცვის სექტორისთვის. მის რეალურ გარემოში

რეალიზებაზე და დანერგვაზე მუშაობა დავიწყეთ და პირველ შედეგებს უახლოეს მომავალში ველოდებით.

PACS სისტემის სწორი ინტეგრირება კლინიკის მართვის ერთიან სისტემაში ასევე შექმნის მედიცინის მიმართულებით ხელოვნური ინტელექტის გამოყენების მეტ შესაძლებლობას. რადიოლოგიის მომავალში ფართოდ იქნება ჩართული ხელოვნური ინტელექტი, რომელიც დაეხმარება რადიოლოგს თითოეული პიქსელის დეტალურ გაანალიზებაში და ნორმიდან გადახრების იდენთიფიცირებაში.

უნდა ავღნიშნოთ, რომ ხელოვნური ინტელექტისთვის სწორი მონაცემთა ბაზის შექმნა არის შესაძლებელი კლინიცისტებთან და სხვა დაკავშირებული სამედიცინო პერსონალითან ერთად მუშაობით, რომლებიც უნდა ჩაერთონ მანქანური სწავლების პროცესში.

ხელოვნური ინტელექტის ინსტრუმენტი კარგად უნდა იყოს გაწვრთნილი. უნდა არსებობდეს სათადარიგო კონტროლის და ტესტირების მექანიზმი. მკაცრი ხარისხის კონტროლის უზრუნველსაყოფად.

ხელოვნური ინტელექტის ინსტრუმენტები რთული საკონტროლებელია და ამიტომ უნდა ხორციელდებოდეს პროცესების ავტორიზაციების გზით. მკაცრი ხარისხის კონტროლის განხორციელება გააძლიერებს კლინიკური და ანალიტიკური დამუშავებული მონაცემების სანდოობის ხარისხს და მოგვცემს მისი განვითარების შესაძლებლობას.

ხელვნური ინტელექტი დაეხმარება სამედიცინო პერსონალს სამდიცინო გადაწყვეტილებების მიღებაში. პაციენტის კონკრეტული შემთხვევისთვის მკურნალობის საუკეთესო და უახლესი მეთოდების მოძიება, თანაც, მისთვის შესაბამისი მზრუნველობის გაწევა, ექიმებისგან ძალიან დიდ რესურსს მოითხოვს. ხელოვნურ ინტელექტზე დაფუძნებული ტექნოლოგიების გამოყენებით, ჯანდაცვის პროფესიონალებს უახლეს ბიოსამედიცინო მონაცემებსა და ჯანდაცვის ელექტრონულ ჩანაწერებში შესაბამისი ინფორმაციის მოპოვების პროცესი უმარტივდებათ. ზოგიერთ ინსტრუმენტს აქვს ბუნებრივი ენის დამუშავების უნარი, რაც ექიმებს საშუალებას აძლევს კითხვები დასვან ისე, როგორც მათ სამედიცინო კოლეგას დაუსვამდნენ. შედეგად კი, სწრაფი და სანდო პასუხები მიიღონ.

დიაგნოსტირების მიმართულებით აღსანიშნია ხელოვნური ინტელექტის სამედიცინო გამოსახულებების გაანალიზების პროცესში გამოყენებაც. ტიპურ კლინიკურ კვლევაში შეიძლება დაგროვდეს მონაცემთა

ათასობით გამოსახულება, რომელთა სათითაოდ შესწავლაა აუცილებელი. ხელვნური ინტელექტი აადვილებს მათ გაშიფვრას და გარკვეული პატერნების გამოვლენას. ამის გარდა, ამგვარი ტექნოლოგიები სამედიცინო სფეროში ყოველდღიურ პროცესებშიც გამოიყენება, კომპიუტერული ან მაგნიტურ-რეზონანსული ტომოგრაფიის შედეგების გაანალიზებისა და დიაგნოზის დასმისას.

ხელოვნური ჩატბოტების საშუალებით, მომხმარებლებს შეუძლიათ ჯანმრთელობასთან დაკავშირებულ სხვადასხვა თემაზე, როგორიცაა გადახდის პროცესები, ავადმყოფობასა და სიმპტომებზე, შესაბამისი პასუხები მიიღონ. ჯანმრთელობის ვირტუალური ასისტენტები კი პასუხისმგებელნი არიან ისეთ საკითხებზე, როგორებიცაა პაციენტის სამედიცინო ინფორმაციის მართვა, სენსიტიური მონაცემების დაფარვა, ექიმებთან შეხვედრების დაგეგმვა, მათთვის შეხსენებების გაგზავნა და ა.შ.

ექსპერიმენტები

ექსპერიმენტები ჩატარდა სატესტო გარემოში. ჯერ დავთვალეთ არსებულ დეცენტრალიზირებულ გარემოში ექიმის, რომელსაც ჭირდება გამოსახულების კვლევის შედეგების ნახვა, მიერ პაციენტის სამედიცინო გამოსახულების მოძიების და შემდეგ ხელით მეორე სისტემაში პაციენტის სამედიცინო ისტორიაში ამ მონაცემების გადმოტანის და პაციენტის ისტორიის ერთიან ჭრილი გაანალიზების დრო, გამოიკვეთა, რომ ამ პროცესს დაჭირდა 30-45 წუთი, ხოლო შემდეგ ჩვენი მეთოდის მიხედვით სიმულირებული სატესტო გამოსახულების მონაცემები ავტომატურად გადავიტანეთ პაციენტის ერთიან ისტორიაში.

ექსპერიმენტის საფუძველზე გამოვლინდა, რომ ეს დრო შემცირდა უკეთეს შემთხვევაში 6 ჯერ. რადგან პროცესები იყო გაფანტული სხვადასხვა პროგრამებში და შესაბამისად საჭირო იყო ყველა სისტემაში პაციენტის სათითაოდ ნახვა, გაანალიზება.

დასკვნა

საჭიროებები, რომელიც მთელი კვლევის მანძილზე იკვეთება არის ის, რომ ყველა კლინიკის მართვის ცუფრული სისტემა უნდა გაერთიანდეს ერთ დიდი კლინიკის მართვის სრულ სისტემად და მასში უნდა გაერთიანდეს მედიცინის ძირითადი მიმართულებები და მონაცემები შესაბამისი ქრონოლოგიით და თანმიმდევრობით.

ამ პროცესში ძალიან მნიშვნელოვანია სისტემის მიერ მოპოვებული, შეგროვებული ინფორმაცია პაციეტნის მკურნალობის ირგვლივ უნდა დალაგდეს ქრონოლოგიურად, იყოს ადაპტირებული

სხვადასხვა სამართავ, თუ პერიფერიულ მოწყობილობებთან. სისტემა უნდა იძლეოდეს ზუსტ, თანმიმდევრულ და მარტივ რეპორტინგს ყველა მიმართულებით.

ესეთი ტიპის სისტემის შექმნა და ისეთ მარტივ გადასატან ტექნიკასთან ადაპტირებამ, როგორიცაა პლანშეტი და მობილური ტელეფონი, საგრძნობლად ამარტივებს და ასწრაფებს პაციენტების მონიტორინგის და მკურნალობის პროცესი.

პაციენტის სამედიცინო სურათების შენახვამ, ისტორიის შექმნამ და მარტვიდან წვდომამ, შეიძლება დააჩქაროს და გააუმჯობესოს დაავადებების დიაგნოსტირება, შეამციროს მკურნალობის დრო, მინიმუმამდე დაიყვანოს შეცდომების ალბათობა და თავიდან აგვაცილოს ზედმეტი გამოკვლევების ჩატარება. ციფრული სისტემები ასევე აუმჯობესებს პაციენტის პერსონალური მონაცემების უსაფრთხოებას და ამცირებს სამედიცინო სერვისების მიღების დროს.

პაციენტის სამედიცინო ისტორიის სრულყოფა გვაძლევს შესაძლებლობას, რომ შევქმნათ მედიცინაში ხელოვნური ინტელექტის ფართოდ გამოყენების პლათფორმა.

სწორად სტრუქტურირებული ელექტრონული მონაცემების ერთობლიობამ და გამოთვლების ელექტრონულად წარმოებამ გააუმჯობესა მკურნალობის ხარისხი, ინფორმაციის სანდოობა, მკვეთრად აასწრაფა დიაგნოსზის დასმის და მკურნალობის სქემის დადგენის დრო. ექიმებს მიეცათ შესაძლებლობა მარტივად ერთ ფანჯარაში დააკვირდნენ პაციენტის მდგონარეობას და გაეცნონ პაციენტის ყველა საჭირო მონაცემებს და შედეგებს.

აღნიშნული სისტემის განახლება, დახვეწა, გაუმჯობესება განხორციელდა რამოდენიმეჯერ და კვლავ აქტიურად მიმდინარეობს კვლევა და სიახლეების დანერგვა.

სისტემა მუდმივ რეჟიმში ვითარდება და ფართოვდება. სამედიცინო პერსონალთან ინტენსიურად მიმდინარეობს ამ პროექტის კვლევა, განვითარება და ოპტიმიზაცია. ამ ეტაპისთვის ზემოთხსენებული სისტემის განახლება/ოპტიმიზაცია მოხდა რამოდენიმეჯერ და კვლავ ვაგრძელებთ კვლევას, სიახეების დანერგვას და სისტემის გაფართოებას პროცესების და მონაცემების გაციფრულების მიმართულებით.

გამოყენებული ლიტერატურა

1. Iavich, M., Sharvadze, L. (2023). The Model of the Novel One Windows Secure Clinic Management Systems. In: Hu, Z., Wang, Y., He, M. (eds) Advances in Intelligent Systems, Computer Science and Digital Economics IV. CSDEIS 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 158. Springer, Cham. https://doi.org/10.1007/978-3-031-24475-9_29
2. Smith, G. (2006). Introduction to RIS and PACS. In: Dreyer, K.J., Thrall, J.H., Hirschorn, D.S., Mehta, A. (eds) PACS. Springer, New York, NY. https://doi.org/10.1007/0-387-31070-3_2
3. Bick, U., Lenzen, H. PACS: the silent revolution. Eur Radiol 9, 1152–1160 (1999). https://doi.org/10.1007/s003300050811
4. Siegel, E.L., Reiner, B. Work Flow Redesign: The Key to Success When Using PACS . J Digit Imaging 16, 164–168 (2003). https://doi.org/10.1007/s10278-002-6006-9
5. Lee, H.W., Ramayah, T. & Zakaria, N. External Factors in Hospital Information System (HIS) Adoption Model: A Case on Malaysia. J Med Syst 36, 2129–2140 (2012). https://doi.org/10.1007/s10916-011-9675-4
6. Ahmadian, L., Khajouei, R., Nejad, S.S. et al. Prioritizing Barriers to Successful Implementation of Hospital Information Systems. J Med Syst 38, 151 (2014). https://doi.org/10.1007/s10916-014-0151-9
7. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili, SOME ASPECTS OF POST-QUANTUM CRYPTOSYSTEMS, Eurasian Journal of Business and Management, 5(1), 2017, 16-20 DOI: 10.15604/ejbm.2017.05.01.002.
8. Iavich, M., Gnatyuk, S., Fesenko, G.: Cyber security European standards in business. Scientific and Practical Cyber Security Journal. J. 3, 36–39 (2019).

Scientific and Practical Cyber Security Journal (SPCSJ) 7(1): 31-37 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ორწერტილოვანი დაშიფვრის საჭიროება ფინანსურ ტრანზაქციებში

დიანა პოპოვა, სამეცნიერო კიბერ უსაფრთხოების ასოციაცია
ოქსანა კოვალჩუკ, სახუმის უნივერსიტეტი

THE NEED OF POINT-TO-POINT ENCRYPTION IN FINANCIAL TRANSACTIONS

Diana Popova, Scientific Cyber Security Association

Oksana Kovalchuk Sokhumi State University

აბსტრაქტი: დღეს, როგორც არასდროს, მომხმარებლებს სურთ ისარგებლონ სწრაფი და უსაფრთხო გადახდის საშუალებებით. ამავდროულად, ბიზნესმა უნდა დაიცვას მომხმარებლის მონაცემები. მაგრამ მუდმივად ცვალებადმა მოთხოვნამ და გადახდის ტექნოლოგიამ გაზარდა ბიზნესის ოპერაციული და ტექნიკური სირთულე.

ფედერალური ფინანსური ინსტიტუტების ექსპერტიზის საბჭოს მიერ გამოქვეყნებული IT Examination Handbook-ს სახელმძღვანელოს მიხედვით, ფინანსურმა ინსტიტუტებმა ინფორმაციის შენახვისა და ტრანზიტის დროს მგრძნობიარე ინფორმაციის გამჟღავნების ან ცვლილების რისკის შესამცირებლად უნდა გამოიყენონ დაშიფვრა.

ორწერტილოვანი დაშიფვრა (P2PE) იცავს ბარათის მფლობელთა მონაცემებს, უადვილებს ორგანიზაციებს გადახდის მონაცემების უსაფრთხოდ შენახვას და ეხმარება მათ PCI SSC (Payment Card Inductry Security Standards Council) შესაბამისობის მოთხოვნების და უსაფრთხოების უახლესი სტანდარტების დაცვაში, რაც ამცირებს თაღლითობის რისკს.

P2PE სტანდარტების გამოყენება ცალკეული კომპანიების პასუხისმგებლობაა, რომლებიც სთავაზობენ პროდუქტებსა და სერვისებს ამ სტანდარტების გამოყენებით, და არა თავად PCI SSC მმართველი საბჭოსი. გადახდის სისტემების მოთხოვნების დამსახურებით PCI SSC სტანდარტები ხორციელდება უამრავ ორგანიზაციაში, მაგრამ ისინი არ არის გათვალისწინებული სახელმწიფო დონეზე, როგორც სავალდებულო. რიგი ფაქტორების გაანალიზების შემდეგ შეგვიძლია ვთქვათ, თარლითობის რისკის მინიმუმამდე დასაწევად, საჭიროა მიღებული სტანდარტები გავხადოთ სავალდებულო ყველა ორგანიზაციისთვის. სტატიაში ასევე მოცემულია რეკომენდაციები მომხმარებლისათვის თაღლითური სქემის თავიდან ასარიდებლად.

საკვანძო სიტყვები: *დაშიფვრა, მონაცემები, უსაფრთხოება, ფინანსური*

ABSTRACT: Today, more than ever, consumers need fast and secure payment options. At the same time, businesses must protect customer data. But ever-changing demand and payment technology have increased the operational and technical complexity of business.

According to the IT Examination Handbook published by the Federal Financial Institutions Examination Board, financial institutions must use encryption in storage and transit to reduce the risk of exposure or alteration of sensitive information.

Point-to-point encryption (P2PE) protects cardholder data, makes it easier for organizations to secure payment data, and helps them meet PCI SSC (Payment Card Industry Security Standards Council) compliance requirements and the latest security standards, reducing the risk of fraud.

The use of P2PE standards is the responsibility of the individual companies that offer products and services using those standards, not the PCI SSC Governing Board itself. Thanks to the requirements of payment systems, PCI SSC standards are implemented in many organizations, but they are not considered mandatory at the state level. After analyzing a number of factors, we can say that in order to minimize the risk of fraud, we need to make the accepted standards mandatory for all organizations. The article also provides recommendations for consumers to avoid fraudulent schemes.

KEYWORDS: *encryption, data, security, financial*

შესავალი

დღეისათვის რადიკალური ცვლილებები ხდება ფინანსური ტექნოლოგიების სფეროში, რაც გავლენას ახდენს სექტორის მთელ ინფრასტრუქტურაზე და ასოცირდება ავტომატიზაციის, ღიაობისა და მომხმარებელზე ფოკუსირების დონის მატებასთან. ხელოვნური ინტელექტის ტექნოლოგიების განვითარება, დიდ მონაცემთა დამუშავება, ახალი ანალიტიკური ინსტრუმენტები და ღრუბლოვანი სერვისები ხელს უწყობს მომხმარებლის მომსახურების ხარისხის ახალ დონეზე გადასვლას. პრაქტიკულად შესაძლებელია ნებისმიერი ფინანსური ტრანზაქცის განხორციელება მობილური მოწყობილობის გამოყენებით, რომელიც უზრუნველყოფს პირადი ფინანსური მენეჯმენტის, ბიომეტრიული გადახდების, სოციალური გადახდების და ა.შ. შესაძლებლობებს.

ონლაინ პლატფორმების ფარგლებში პროდუქტების გაცვლაზე ან ალტერნატიული ვალუტების გამოყენებაზე აგებული ტრანზაქციების რაოდენობა აქტიურად იზრდება; ფართო გავრცელება ჰპოვა სრულიად ახალი ტიპის ფინანსურმა ტრანზაქციებმა მოწყობილობებს შორის, რომელსაც არ ესაჭიროება ადამიანის ჩარევა. იზრდება კიბერუსაფრთხოების, პერსონალური მონაცემების დაცვის, ტრანზაქციების განხორციელებისას პირის საინფორმაციო სივრცეში იდენტიფიცირების პრობლემების მნიშვნელობა.

ფინანსური მონაცემების დაშიფვრა

გრემის-ლიჩის-ბლაილის კანონი (GLBA) კონკრეტულად მოითხოვს, რომ ინსტიტუციებმა, რომლებიც აწარმოებენ ბიზნესს აშშ-ში, დააწესონ შესაბამისი სტანდარტები მომხმარებელთა არა-საჯარო პერსონალური ინფორმაციის უსაფრთხოებისა და კონფიდენციალურობის დასაცავად [1].

მიზნები არის შემდეგი:

- მომხმარებლის ჩანაწერებისა და ინფორმაციის უსაფრთხოების და კონფიდენციალურობის უზრუნველყოფა.

- ასეთი ჩანაწერების უსაფრთხოებასა და მთლიანობაზე მოსალოდნელი საფრთხეებისგან დაცვა.
- დაცვა ინფორმაციაზე არაავტორიზებული წვდომისგან, რამაც შეიძლება გამოიწვიოს მნიშვნელოვანი ზიანი ან დისკომფორტი ნებისმიერი კლიენტისთვის.

გარდა ამისა, ფედერალური ფინანსური ინსტიტუტების ექსპერტიზის საბჭო (FFIEC), რომელიც „უფლებამოსილია განსაზღვროს ერთიანი პრინციპები, სტანდარტები და ანგარიშგების ფორმები ფინანსური ინსტიტუტების ზედამხედველობის ერთგვაროვნების ხელშეწყობის მიზნით“, დასძენს:

„ფინანსურმა ინსტიტუტებმა მგრძნობიარე ინფორმაციის გამჟღავნების ან შეცვლის რისკის შესამცირებლად უნდა გამოიყენონ დაშიფვრა ინფორმაციის შენახვისა და ტრანზიტის დროს“.

FFIEC-სა და GLBA-ს თანახმად ბანკებმა და ფინანსურმა ინსტიტუტებმა უნდა დაშიფრონ:

- ნებისმიერი სენსიტიური ინფორმაცია, რომელსაც ინდივიდი გასცემს ფინანსური პროდუქტის ან სერვისის მისაღებად (როგორიცაა სახელი, მისამართი, შემოსავალი, სოციალური დაცვის ნომერი ან სხვა ინფორმაცია განაცხადის შესახებ);
- ნებისმიერი ინფორმაცია, რომელსაც ისინი იღებენ ინდივიდის შესახებ ტრანზაქციისგან, რომელიც მოიცავს ფინანსურ პროდუქტებს ან მომსახურებას (მაგალითად, ის ფაქტი, რომ ფიზიკური პირი არის ფინანსური ორგანიზაციის მომხმარებელი, ანგარიშის ნომრები, გადახდის ისტორია, სესხის ან დეპოზიტის ნაშთები და საკრედიტო ან სადებეტო ბარათით შესყიდვები);
- ნებისმიერი ინფორმაცია, რომელსაც ისინი იღებენ ფიზიკური პირის შესახებ ფინანსური პროდუქტის ან მომსახურების მიწოდებასთან დაკავშირებით (მაგალითად, ინფორმაცია სასამართლოს ჩანაწერებიდან ან მომხმარებლის ანგარიშიდან).

გასაღების გენერირება და მართვა

დაშიფვრა ხშირად განიხილება პირადი მონაცემების დაცვის ურთულეს ნაწილად. პირველი ნაბიჯი, რომლის გადადგმაც ბანკებს და ფინანსურ სერვისებს შეუძლიათ, არის დაშიფვრის დანერგვა ინდუსტრიაში გამოცდილი და მიღებული ალგორითმების საფუძველზე, გასაღების საიმედო სიგრძესთან ერთად [2,3].

დაშიფვრა - სპეციფიკური მოთხოვნაა, რადგან დაშიფვრისა და გაშიფვრის ოპერაციები უნდა განხორციელდეს ადგილობრივად, არა დისტანციური სერვისით, რადგან გასაღებებიც და მონაცემებიც უნდა დარჩეს მონაცემთა მფლობელის უფლებამოსილებაში თუ რა თქმა უნდა კონფიდენციალურობის მიღწევა დგას დღის წესრიგში. ამის პრაქტიკაში მისაღწევად, ორგანიზაციები სავარაუდოდ განიხილავენ ფსევდონიმიზაციის ტექნიკის გამოყენების გაზრდას.

დაშიფვრა ისეთივე უსაფრთხოა, როგორც თქვენი დაშიფვრის გასაღები. გასაღებების მართვის გადაწყვეტის არსებითი ფუნქციები მოიცავს დაშიფვრის გასაღებების

განცალკევებით შენახვას იმ მონაცემებისგან, რომლებსაც ისინი იცავენ, ასევე დაშიფვრის გასაღებების მართვას მთელი სასიცოცხლო ციკლის განმავლობაში, მათ შორის:

• გასაღებების გენერირება სხვადასხვა კრიპტოგრაფიული სისტემებისთვის და სხვადასხვა აპლიკაციებისთვის;

• საჯარო გასაღებების გენერირება და მიღება;

• გასაღებების განაწილება შესაბამის მომხმარებლებს შორის, გაქტიურების ინსტრუქციის ჩათვლით;

• გასაღებების შენახვა, მათ შორის, ავტორიზებული მომხმარებლების გასაღებებზე წვდომის წესები;

• გასაღებების შეცვლა ან განახლება, მათ შორის წესები, როდის და როგორ უნდა შეიცვალოს გასაღებები;

• კომპრომეტირებული გასაღებების ადრესაცია;

• დაარქივება, უკუკავშირი და გასაღებების ამოღების ან დეაქტივაციის მითითებები;

• დაკარგული ან დაზიანებული გასაღებების აღდგენა, როგორც ბიზნესის უწყვეტობის მენეჯმენტის ფარგლებში;

• გასაღებების მართვასთან დაკავშირებული ძირითადი აქტივობების აუდიტი;

• განსაზღვრული აქტივაციისა და დეაქტივაციის თარიღების დაწესება და გასაღებების გამოყენების პერიოდის შეზღუდვა.

დაშიფვრის განხორციელება

FFIEC უზრუნველყოფს GLBA-ს ხელმძღვანელობასა და ზედამხედველობას ბანკებისა და ფინანსური ორგანიზაციებისთვის. ისინი აქვეყნებენ IT Examination Handbook-ს, რომელიც გამოსცემს მითითებებს IT უსაფრთხოების კონტროლისთვის, რომელიც შეიძლება ან უნდა იქნას გამოყენებული პერსონალური ინფორმაციის დასაცავად GLBA-ს ფარგლებში [4,5]. სახელმძღვანელოს მიხედვით, ფინანსურმა ინსტიტუტებმა უნდა გამოიყენონ დაშიფვრა ინფორმაციის შენახვისა და ტრანზიტის დროს მგრძნობიარე ინფორმაციის გამჟღავნების ან ცვლილების რისკის შესამცირებლად. დაშიფვრის განხორციელება უნდა შეიცავდეს:

- საკმარის დაშიფვრის სიძლიერეს ინფორმაციის გამჟღავნებისგან დასაცავად მანამ, სანამ გამჟღავნება არ წარმოადგენს მატერიალურ რისკს;
- გასაღების მართვის ეფექტურ პრაქტიკას;
- მაღალ საიმედოობას.

ორწერტილოვანი დაშიფვრა (P2PE)

P2PE არის ტექნოლოგიური სტანდარტი, რომელიც შემუშავებულია ელექტრონული ფინანსური ტრანზაქციების უსაფრთხოების დასაცავად.

იგი შექმნილია გადახდების დამმუშავებელი მსხვილი კომპანიების კონსორციუმის მიერ.

ახალი ტექნოლოგიების გაჩენისთანავე P2PE სტანდარტები განაგრძობს განვითარებას.

P2PE სტანდარტების შესაბამისად, ტრანზაქციის მონაცემები სრულად არის დაშიფრული იმ მომენტიდან, როდესაც კლიენტი შეიყვანს თავის მონაცემებს ამ ინფორმაციის გადახდის პროცესორზე გადაცემის მომენტამდე. მიღებისთანავე, გადახდის პროცესორი ახდენს მონაცემების გაშიფვრას და ამტკიცებს ან უარყოფს ტრანზაქციას.

რადგან მთელი პროცესის განმავლობაში ტრანზაქციის მონაცემები სრულად არის დაშიფრული, ის არის დაცული არაავტორიზებული მესამე პირის მიერ მოპოვებისა და ბოროტად გამოყენებისგან. იმ შემთხვევაშიც კი, თუ ჰაკერი კონკრეტულ ტრანზაქციას ხელში ჩაიგდებს, მიღებული ინფორმაცია გაუგებარი იქნება, რადგან ის მაინც დაშიფრულია. ინფორმაციის გაშიფვრისთვის მომხმარებელს უნდა ჰქონდეს დაშიფვრის გასაღები, რომელიც ხელმისაწვდომია მხოლოდ ავტორიზებული მხარისთვის.

ცალკეულ კომპანიებს შეუძლიათ თავისუფლად განავითარონ ახალი პროდუქტები და სერვისები, რომლებიც ურთიერთქმედებენ ელექტრონული გადახდების ეკოსისტემასთან. თუმცა, იმისათვის, რომ ამ კომპანიებმა მიაღწიონ P2PE შესაბამისობას, მათ უნდა აჩვენონ, რომ მათი ახალი შეთავაზება აკმაყოფილებს ან აღემატება P2PE სტანდარტებს. პრაქტიკაში, ეს ნიშნავს, რომ მათ უნდა უზრუნველყონ ყველა ტრანზაქციის ინფორმაციის სრულად დაშიფვრა და შეთავაზებაში ჩართული ნებისმიერი აპარატურის უსაფრთხოდ მართვა. ასევე პროცესში გამოყენებული ნებისმიერი კრიპტოგრაფიული გასაღები უნდა იყოს უსაფრთხოდ გენერირებული, გადაცემული და შენახული.

PCI SSC უსაფრთხოების სტანდარტების საბჭო ატარებს რეგულარულ ღონისძიებებს და ხელს უწყობს ინფორმაციის გაცვლას ამ სტანდარტების ცვლილებებთან დაკავშირებით ფინანსური ტრანზაქციების ინდუსტრიაში ჩართული ორგანიზაციების დასახმარებლად. ისტორიულად, ეს მმართველი ორგანო დაარსდა მსხვილი გადახდის ბრენდების მიერ, მათ შორის American Express (AXP), Discover Financial Services (DFS), MasterCard (MA) და Visa (V). ამასთან, P2PE სტანდარტების გამოყენება ცალკეული კომპანიების პასუხისმგებლობაა, რომლებიც სთავაზობენ პროდუქტებსა და სერვისებს ამ სტანდარტების გამოყენებით, და არა თავად მმართველი საბჭოსი.

დასკვნა

PCI SSC სტანდარტები არ არის გათვალისწინებული სახელმწიფო დონეზე, როგორც სავალდებულო, უფრო ზუსტად რომ ვთქვათ, მხოლოდ აშშ-ის ზოგიერთმა შტატმა მიიღო ისინი საკანონმდებლო დონეზე. მაგრამ, გადახდის სისტემების მოთხოვნების წყალობით,

ისინი ხორციელდება უამრავ ორგანიზაციაში. Cisco-ს 2011 წელს აშშ-ს შესაბამისობის კვლევამ დაადგინა შემდეგი:

- საცალო ვაჭრობა სრული სერიოზულობით მოეკიდა PCI DSS სტანდარტის დანერგვას და რეალიზებას. (Payment Card Industry Data Security Standard ერთ-ერთი ძირითადი სტანდარტია).
- გამოკითხულთა 85% თვლის, რომ მათ ორგანიზაციებს ამჟამად შეუძლიათ წარმატებით გაიარონ PCI DSS აუდიტი.
- სამთავრობო ორგანიზაციების 85%-მა წარმატებით გაიარა PCI DSS აუდიტი პირველივე ცდიდან. ყველაზე ცუდად ეს აუდიტი გავლილი აქვთ სამედიცინო ორგანიზაციებს (72%).
- გამოკითხული აღმასრულებელი დირექტორიებისა და საბჭოს წევრების 67% ამბობს, რომ PCI DSS ძალიან მნიშვნელოვანი ინიციატივაა.

ჩემი აზრით, გასათვალისწინებელია ის, რომ თაღლითობის რისკის შესამცირებლად საჭიროა მიღებული სტანდარტები გავხადოთ სავალდებულო ყველა ორგანიზაციისთვის, სასურველია, რომ ეს მოხდეს სახელმწიფოს დონეზე.

რეკომენდაციები

ამჟამად, გადახდის ინდუსტრიაში ყველაზე დიდი საფრთხე არის სოციალური ინჟინერიის თაღლითობა. აქედან გამომდინარე, მნიშვნელოვანია საბანკო სერვისების მომხმარებლებში ტექნოლოგიური წიგნიერების განვითარება.

ციფრული ჰიგიენის ზომები რომლებიც რეკომენდირებულია გადახდის სისტემების მომხმარებლისთვის:

- ნუ შეინახავთ გადახდის მონაცემებს საეჭვო სერვისებზე, შეადარეთ რისკები და გადახდის მონაცემების შეყვანის აუცილებლობა რესურსებზე, რომლებიც არ უჭერენ მხარს 3D Secure სტანდარტს (PCI Three-Domain Secure Core Security Standard» (3DS), ის არის PCI SSC სტანდარტული პაკეტის ნაწილი და მოითხოვს მხარდაჭერას არა მხოლოდ გადახდის სისტემისა და ფინანსური ორგანიზაციის, არამედ თავად სავაჭრო კომპანიის);
- არ შეინახოთ კოდი ბარათის უკანა მხარეს განთავსებული (CVV კოდი) და არავის გაუმზილოთ შემდეგი კოდები: CVV კოდი, SMS კოდი, Push შეტყობინებები, ბარათის PIN კოდი;
- მოერიდეთ თაღლითობებს: იყავით ფხიზლად, ნუ ენდობით სატელეფონო ზარებს. არ გაამჟღავნოთ თქვენი პირადი მონაცემები: სრული სახელი, დაბადების ადგილი და წელი, პასპორტის მონაცემები.
- დააწესეთ ბარათის ლიმიტები წარმატებული თაღლითობის შემთხვევაში დიდი თანხების დაკარგვის თავიდან ასაცილებლად.

ბიბლიოგრაფია:

1. H. DeYoung, D. Garg, L. Jia, D. Kaynar and A. Datta, "Experiences in the logical specification of the hipaa and glba privacy laws", Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society ser. WPES '10, pp. 73-82, 2010.
2. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili, SOME ASPECTS OF POST-QUANTUM CRYPTOSYSTEMS, Eurasian Journal of Business and Management, 5(1), 2017, 16-20 DOI: 10.15604/ejbm.2017.05.01.002
3. Iavich, M., Gnatyuk, S., Fesenko, G.: Cyber security European standards in business. Scientific and Practical Cyber Security Journal. J. 3, 36–39 (2019)
4. H. Qin, Z. Li, P. Hu, Y. Zhang and Y. Dai, "Research on Point-To-Point Encryption Method of Power System Communication Data Based on Block Chain Technology," 2019 12th International Conference on Intelligent Computation Technology and Automation (ICICTA), Xiangtan, China, 2019, pp. 328-332, doi: 10.1109/ICICTA49267.2019.00076.
5. S. Jahan, M. S. Rahman and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," 2017 International Conference on Networking, Systems and Security (NSysS), Dhaka, Bangladesh, 2017, pp. 39-44, doi: 10.1109/NSysS.2017.7885799.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(1): 38-53 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

BLOCKCHAIN-BASED POISONING ATTACK PREVENTION IN SMART FARMING

Aliyu Ahmed Abubakar, School of Cyberscience and Engineering, Wuhan University
Department of Computer Science, Kaduna State University
Jinshuo liu, School of Cyberscience and Engineering, Wuhan University
Ezekia Gilliard, School of Cyberscience and Engineering, Wuhan University

ABSTRACT: Rapid progress and advancement in the Internet of Things (IoT) significantly affect how businesses are conducted in this 21st century. Smart Farming, also Intelligent Farming as a component of the IoT, allows agribusiness to generate high-yield income, ease of doing business, and with a favorable professional environment. Smart farming combines agribusiness competency recognition, data progression, and information collected from equipment with statistical analysis to highlight facts from the acquired information, allowing farmers to make wise decisions for greater harvest benefits. However, incorporating such cutting-edge technology necessitates the acquisition of more sophisticated safety and security majors. Thus, system safety testing may be the most important safety consideration to implement. This paper presents a blockchain-based smart farm security framework that effectively screens device status and sensor irregularities and alleviates security threats. In addition, a blockchain-based smart-contract application was developed to securely store security anomaly data and proactively moderate comparative assaults on other farms in the community. The study used the security-monitoring framework for smart farms, ESP32, AWS cloud, and the smart contract on the Ethereum Rinkeby. The performance evaluation of the proposed system revealed that our framework could identify and prevent security anomalies in real time while giving updates on the situation.

KEYWORDS: *Blockchain, Poisoning Attacks, Internet of Things, Smart Farming, Signature*

1. INTRODUCTION

As the population of the world increases, the need and significance of farming also grow, and farmers aimed at developing crops to deliver nourishment all over the world. The economies of most nations depend heavily on their execution within the rural division [1]. Moving forward, agricultural segment bureaus in many countries try to reinforce their country's economy, especially through agriculture. The advancement of science and technology which includes the IoT has changed how farming is practiced and has moved forward the operational capabilities of the farming sector [2]. Integrating the IoT in farm development is called smart or intelligent farming which is fast becoming the new normal as robots and smart things exhibition all over the world is anticipated to reach $15.93 billion by 2028, creating a compound annual advancement rate of 20.31% from 2021 to 2028 [3]. The rural areas are the target for competitors to conduct cyber assaults as the integration of advanced agric. frameworks are coming up in those locations. Take as an example, a meat management company, JBS, within the food transport division got a ransomware outbreak which ended the operations of 13 meat industrial facilities. The company had to pay about $11 million to keep functioning [4]. Thus, we can agree that safety is seen as a major issue in sectors such as the agric. where the progression of rural safety measures is critically needed.

In this manner, security is seen as a major issue in the smart farming domain, and the progression of rural security arrangements is critically needed.

The existing security arrangements proposed in smart cultivating and farming generally cover food-supply-chain administration and the checking of different exercises utilizing cloud innovations, ML- and AI-based data-analytic procedures, and verification and authorization arrangements for compelled IoT gadgets [12]. Cloud-based observing smart

Farming arrangements can still have security results, on the off chance that the secured code strategies are not considered amid the advancement and IoT security best hones are not taken after. To bolster the past articulation, truly IoT gadgets uncovered on the Web have been compromised and utilized as a weapon to perform large-scale denial-of-service assaults or other noxious exercises such as controlling the sensor values to information presentation [14].

In this manner, the existing cloud-based arrangements or gateway-based security arrangements for checking smart farming applications are not adequate for giving full promised security. Decentralized applications and capacity have security points of interest compared to conventional applications and capacity in terms of secured occasions capacity, traceability, permanence, and made strides security and security. Blockchain innovation is known to be utilized for decentralized application advancement. Separated from blockchain-based advanced money, smart-contract-based applications are well known and utilized for numerous applications, counting advanced personalities, budgetary security, secured capacity, and supply chain administration [16]. Analysts investigated blockchain innovation openings in settling IoT security and protection issues [17], counting smart farming security. A few of the blockchain applications in smart farming are food-production supply-chain administration, and secured exchange capacity [8,18]. Blockchain empowers keeping track of the arrangement of occasions to preserve straightforwardness and, within the conclusion, farmers are reasonably treated and pick up benefits. Considering the blockchain innovation focal points in shrewd farming, we were propelled to utilize blockchain innovation for executing shrewd farming-security-monitoring.

The current security observing arrangements in smart Farming either center on cloud-based choices or blockchain innovation [10]. Besides, as talked about prior, most of the cloud- or blockchain-based arrangements address supply-chain issues. The points of interest of cloud and blockchain innovation can be considered to propose ideal security arrangements in savvy farming. Generally, to overcome the restrictions of the existing cloud-based arrangements [10] and make strides in security utilizing blockchain applications, we utilized a cloud and blockchain solution to always handle the detecting information within the cloud and store irregularities in blockchain exchanges. Moreover, none of the existing arrangements gave an end-to-end arrangement utilizing cloud and blockchain execution for smart Farming and assessing the organized idleness execution. In this manner, we executed an end-to-end arrangement utilizing an Arduino sensor pack with a Wi-Fi module, AWS cloud, and Ethereum smart contract arrange for testing real-time applications and assessed their execution in terms of security, ease of use, and execution arrangement.

This study is therefore focused on assessing block-chain poisoning attack prevention in smart farming using signature. The objectives include;

- Assessment of various data poisoning attacks faced by smart farming in the agricultural sector
- Assessing cloud solutions in smart Agriculture.
- Assessing Blockchain solutions in Smart Farming.

Significantly, this investigation is balanced to be of extraordinary significance to the agriculturists, the government, and the information assurance specialists. The ponder set out to translate different information-harming assaults that have been experienced by smart cultivating proprietors within the world. It'll uncover different ways that information-harming assaults can be deflected through the application of different planned and executed systems within the security server of the savvy cultivate. It'll also bring to the spotlight the security and security challenges that have ruined the total working of smart cultivating within the agribusiness industry. Due to the results of information harming upon nourishment generation, this will give a conceivable arrangement that will advantage the government, shrewd cultivating specialists, and cyber-security specialists on different strategies of savvy cultivate assaults and ways to turn away the information harming separately.

The gaps this consider will fill incorporate:

- Recognized potential cybersecurity concerns in shrewd cultivating and displayed scenario-specific cyberattacks categorized into supply chains such as information, systems, and other common assaults.

- Presents a comprehensive evaluation of current cybersecurity inquiries and countermeasures utilizing blockchain in shrewd farming.
- Verbalize open security and security challenges over spaces such as next-generation organized security, trusted supply chains and compliance, antagonistic machine learning, and AI, get to control, and believe and data sharing.

2. LITERATURE REVIEW

Agribusinesses and farmers are turning to a run of shrewd cultivating strategies that utilize IoT gadgets to extend efficiency. The different sensor associations utilized on the cultivate and their communication over the Web can be hacked. This has driven an increment in cyber assaults pointed at the agrarian industry, counting information breaches, refusal of benefit assaults, site changes, and more. As of late, [8] has shed light on security and protection issues in savvy agri-ecosystems. They displayed a layered engineering and distinguished potential cybersecurity issues in smart farming. In expansion, their investigation moreover presents particular cyber assault scenarios categorized into information, arrange supply chain, and other common assaults. A prevalent assault called "The Night Mythical Serpent" is an illustration that permits assailants to take expansive sums of data from numerous petrochemical companies. Another case was the harm to a German steel plant, where aggressors utilized online phishing to pick up and get to the factory's workplaces, systems, and generation frameworks.

The exponential development in the number of internet-connected gadgets has made genuine security issues within the rural division, as agriculturists cannot endure the plausibility of misfortune and damage to their crops. Surname. Surname. Subsequently, guaranteeing the differences of sensors within the smart cultivate biological system is a critical errand of present-day farming. Maria and partners. [9] Their report highlights the importance of accuracy farming (Dad) and related cybersecurity dangers and potential vulnerabilities. This report highlights security, smartness, and accessibility models for data security in agribusiness. It distinguishes different advances included in shrewd Farming, such as on-farm gear, checking and inaccessible detecting strategies, and machine learning. It too briefly portrays significant bunches such as farmers, herders, and businesses that back or depend on farming.

Moreover, security issues that can emerge from the utilization of IoT sensors in agribusiness have been well distinguished [10]. Information and data security alludes to the assurance of information by diverting or lessening the plausibility of unseemly or unauthorized get to or illicit utilize of information, intrusion, revelation, cancellation, and assessment. , debasement, distorting records, or distorting data. and to ensure information and data by lessening chance. [11]. Aggressors can perform diverse sorts of assaults. B. Mass dissent of benefit (DoS) assaults using various IoT sensors sent in smart ranches. Manos et. al, [12] in their ponder affirmed the 2016 Mirai botnet as an illustration, misusing an expansive number of associated shrewd domestic gadgets to dispatch different DoS attacks. down. As of late, an analyst from a security company called Sucuri [13] found that a DoS botnet can make 50,000 HTTP requests per moment. Numerous websites have been hit by DDoS assaults. Comparable conditions exist in shrewd agroecosystems, so comparable assaults can happen. Such assaults not as it disturbed the typical operation of distinctive modules within the same bunch, but can too be utilized to disturb true blue arrange administrations in other domains.

The creators of [35] actualized a shrewd contract based on soil- and climate-condition observing measurements in shrewd agribusiness. In any case, nitty gritty smart-contract usage is not given. In addition, the real-time tests detecting the rural conditions and testing the proposed smart-contract-based metric checking are not performed. Ref. [36] examined Ethereum blockchain-based smart-agriculture supply-chain information arrangements. The creators observed the farming sensor information utilizing Ethereum. Be that as it may, the arrangement did not specify information capacity utilization within the cloud. Ref. [37] performed a confirmation of concept for executing the Ethereum blockchain arrangement to store Farming sensor points of interest. Be that as it may, the execution of the executed arrangement isn't decided in their work. Practical test tests by setting the sensor gadgets are moreover not performed. Caro et al. [38] proposed AgriBlockIoT, a blockchain-based arrangement for Farming nourishment supply-chain administration. The Ethereum and hyper record blockchain-based execution is performed to store the Agribusiness IoT device's information.

The creators appeared that the Hyperledger inactivity is much lower than the Ethereum arrange inactivity. In any case, the end-to-end execution of the Farming blockchain, counting empowering the sensors to send information in real-time, is lost. Moreover, the message network's idleness to overhaul the exchanges within the blockchain is higher. We address those issues and executed a more reasonable blockchain-based arrangement to send the sensor alarm information as an exchange in the blockchain. The creators of [39] outlined a smart-contract-based IoT device-to-device and device-to-gateway verification component in savvy farming. The piece is shaped by the edge server conveyed within the IoT environment. The blockchain hubs within the cloud perform the agreement component and include the squares to the blockchain. A crossover blockchain hyper ledger– sawtooth stage reenacts the author's proposed method. Although blockchain and cloud technologies are included within the author's work, the center of their work is on the plan of IoT gadget confirmation components. On the other hand, we centered on checking smart farming natural conditions utilizing cloud and blockchain innovations. We actualized an end-to-end generation-level Ethereum smart-contract arrangement.

2.1 CLOUD SOLUTION IN SMART FARMING

Cloud-computing integration with smart Farming is required to perform IoT detecting information capacity and analytics, counting big-data applications. Analysts proposed arrangements to address the issues in IoT-based savvy Farming utilizing cloud computing. Nurzaman et al. [2] proposed a fog-computing-based network architecture for savvy cultivating and Farming to screen ranches and control agribusiness operations. The creators presented a cross-layer-based channel get-to and steering arrangement to optimize the organized communication associated with smart-farming endpoints. This progressed the arranged inactivity of the IoT cultivating gadgets associated with the cloud. In any case, the paper did not talk about the security and security angles of IoT-based shrewd agribusiness. Chen et al. [27] displayed an IoT platform to develop turmeric outside for precision agriculture. The author's application empowers agriculturists to control turmeric cultivation with GUI, moving forward the quality and efficiency of the turmeric while keeping up the arranged inactivity that roughly matches real-time communication. However, this work is specific to smart-agriculture turmeric-cultivation application execution.

[28] proposed an intelligent security framework to screen gadgets within the farming field. The creators actualized the framework on Rasberry Pi 2. The framework can communicate information remotely and send SMS alarms to a farther client. Be that as it may, the work did not consider blockchain innovation to make savvy contracts and safely store the information when observing the gadgets in Farming. Li *et al*. [11] talked about the confinements of utilizing big-data arrangements in IoT-based savvy farming. The creators utilize the K-means calculation to perform the agribusiness information analytics and highlighted that information is deficient to apply big-data arrangements. Anandarup *et al.* [29] proposed a strategy for recognizing connection disappointments between neighborhood hubs and ace hubs and recognizing nearby hubs from organized parcels. The MLP facilitated in farther hubs is utilized to test the recognizable proof of the hubs. Generally, the writing shows that cloud arrangements advantage the agribusiness industry by remotely observing and making strides in efficiency in agriculture. However, the cloud-based arrangements are inclined to information exposures and may lead to security breaches on the cloud benefit provider if security controls are not legitimately actualized.

2.2 BLOCKCHAIN SOLUTIONS IN IOT AGRICULTURE

Blockchain innovation has points of interest such as secure capacity, namelessness, and straightforwardness. The client's personality and private key will not be uncovered in the open, even though the user's open key and exchange data can be seen within the open blockchain. A few analysts investigated the utilization of blockchain innovation in IoT applications [19,30–32]. Ferrang et al. [33] portrayed blockchain conventions in IoT and displayed danger models to blockchain conventions in IoT. The IoT application spaces for blockchain are talked about, and the state of the art of blockchain advances within the Web of Things are examined, emphasizing security and protection. The inquiry about challenges and future headings for utilizing blockchain in IoT are talked about. Ref. [8] examined the security and security issues in green IoT-based agriculture. The application of blockchain innovation in protecting protection in green IoT-based agribusiness is examined. Anusha et al. [31] performed a writing survey of the information-security investigation advance in blockchain-based smart-agriculture applications. Oscar et al. [32] performed a nitty gritty consideration of utilizing blockchain in savvy

farming. The creators highlighted that security and security issues are one of the most concerns of shrewd agribusiness. The state-of-the-art survey on utilizing the blockchain in Farming [32] portrayed that most of the works centered on understanding the nourishment or agribusiness supply-chain issue, and secure information capacity, further checking, and computerization are the slightest centered on regions in blockchain-enabled shrewd agribusiness. To entirety up, the earlier blockchain innovation in IoT agriculture review articles demonstrate that blockchain arrangements can make strides in the security and protection of savvy agribusiness. In any case, challenges such as information capacity in blockchain and tall organize association rates in country regions to perform agreement movement still have to be addressed within the agribusiness application setting. Saikat [12] proposed a blockchain-based IoT design for the nourishment supply chain. RFID sensors captured the distinguishing proof ID from the item bundle from different stakeholders within the nourishment supply chain and were included in the blockchain to preserve astuteness. Any partner can confirm the open blockchain information concerning the products' status. Mubariz et al. [34] presented blockchain-based cloud hubs to confirm the benefit given by the edge servers for benefit verification to IoT devices. The proof-of-specialist (POA) instrument is considered for keeping up the agreement among blockchain cloud hubs. IoT gadgets grant the rating to the edge servers based on the edge-server benefit given and utilized for deciding the benefit confirmation. Mohamed et al. [19] investigated blockchain innovation to actualize security arrangements and their execution. The creators highlighted that expansive throughput and capacity are the specialized challenges in executing security arrangements. Generally, blockchain arrangements have been utilized within the literature to address a few issues in savvy farming.

2.3 SMART FARMING, SENSING TECHNOLOGY, AND SECURITY ATTACKS

A normal cloud-enabled IoT-savvy Farming is shown in Figure 1. The cloud-based design is comprised of the IoT gadget associated with the ranches and rural arrive to screen different physical conditions such as fertilizer utilization, appropriate seed spilling, climate state, nourishment developing quality, and capacity environment conditions. Different sensors such as temperature, mugginess, and weight are utilized to screen the cultivating condition. The IoT gadgets are associated with the common portal to pass the state data to the third-party cloud seller, who gives the item administrations. The door can be a nonexclusive or committed switch outlined for the savvy cultivate. The cloud supplier can be any essential benefit supplier such as AWS, Google Cloud, Microsoft Sky blue, or a self-managed cloud. The portal is associated with the cloud assets to prepare the IoT gadget demands.

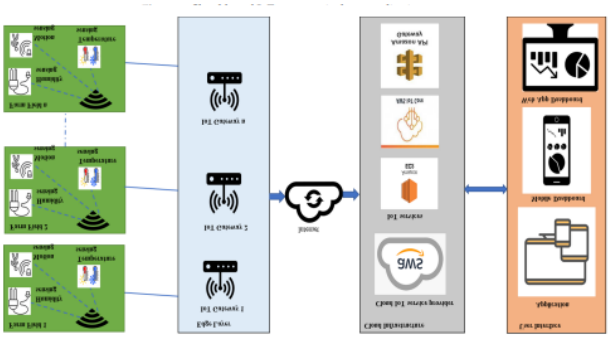

Fig. 1. Cloud-based IoT smart-agriculture application.

The various IoT sensors and their applications in smart agriculture include;

Temperature sensor: The sensor detects temperature changes within the application. The water temperature, the surrounding air temperature, and plant temperature monitoring capabilities improve the effectiveness of agriculture duties.

Humidity sensor: The humidity sensor measures the humidity changes in the agricultural land environment. The humidity sensor helps measure the soil moisture and water consumption rate, tracking waterfall trends for future irrigation requirements estimation. The normal humidity ranges are 0%RH–100%RH.

Light sensor: The light sensors in agriculture monitor the light in the agricultural greenhouse, cloud shadow, and the required light to grow the plants.

Accelerometer sensor: Accelerometer sensors in agriculture help to maintain the agriculture or farming equipment. The movement and vibration changes in the equipment are monitored to detect the equipment replacement needs.

pH sensor: The pH sensors in agriculture improve the productivity of crops. The pH sensor detects unwanted chemicals in the soil and soil nutrient deficiencies. Soil-pH fluctuation monitoring can help farmers to take precautions and effectively grow plants.

GPS sensors: An animal herd or any objects in the agricultural location can be monitored using a GPS sensor. Remote monitoring and location tracking helps to achieve precise agriculture. **Pressure sensor**: A pressure sensor in agriculture may be used to monitor pipes and tanks. The pressure sensor improves water management, irrigation management, and precision farming. **Infrared sensor**: Infrared sensor integrated with drones monitors the crop and measures the plant's strength. The plants can be adjusted and optimized for the agriculture resources to manage agriculture activities effectively

2.4 DATA POISONING ATTACKS IN AGRICULTURE

The attack surface of IoT in smart agriculture opens up a new range of cyberattacks and several security defenses that can be integrated into IoT devices due to memory and processing limitations. As a result, we may need to rely on security detection and protection mechanisms at the port or network level. This work will address the following attacks using IoT state and anomaly data monitoring solutions.

Denial of Service (DoS): The adversary can send malicious network traffic to the victim farmer's network to shut down services, including detection devices and routers connected to the network. This can disrupt operations as these devices are used for food supply chain applications. The attack can also originate from many different source IP addresses, making it difficult to detect and block attack traffic. DoS attack scenarios in IoT include resource consumption of IoT devices, congestion of IoT devices and gateways, or flooding of ports with traffic.

Physical security attack: Intruders into agricultural fields and farm facilities to destroy property or with other evil purposes like theft, arson, etc. Camera sensors installed on the farm premises will send data to monitor and alert the farm owner when physical attacks occur in smart agriculture. Enemies can also access the farm to install or compromise the farm network.

Data manipulation attack detected: Malicious manipulation of IoT sensor data before it reaches its destination is another type of attack seen in IoT. An adversary can perform a man-in-the-middle attack to read data passing through the communication channel and embed malicious data to carry out attacks. Zero-day vulnerabilities in IoT devices can also be exploited to compromise sensors and spoof sensor data to mask malicious activity. There are different ways to access the network and manipulate data unless we have good security controls that cover protocols from the data link layer to the application layers.

3. MATERIALS AND METHOD

The proposed approach improves the security and monitoring of smart farming by incorporating technologies into multiple layers of smart agriculture architecture. The Ethereum blockchain is used in another layer to run smart contracts

and trigger events when anomalies are identified during smart farming security monitoring. Figure 2 illustrates the layered architecture of the proposed method. The smart farm layer contains different sensor devices on the farm premises for different purposes. A smart farming community is formed with IoT sensor devices installed on every farmland. These sensors continuously generate events like device health, device data, etc. Generated events are transmitted to the cloud using an edge gateway or a router connected to the sensor. The cloud layer consists of components that continuously listen to sensor events and process event data to retrieve the desired information. MQTT is the typical protocol for end-to-end packet data transmission. We have defined a lambda function in the AWS cloud to parse data from the AWS IoT core component and extract the required data from sensor devices connected to the farms. Whenever the lambda function logic defines a security alert observed from the sensor generation data, the lambda function executes an infura-API POST request to update the Ethereum blockchain. The updated transaction may include abnormal values of sensor data, device status, etc. Infura runs Ethereum nodes and provides an API to update transactions from user accounts if they have an account with them. Updated blockchain transactions will be updated on all nodes in the Ethereum network. Although the user layer is not shown in Figure 2, the GUI can read transactions from the Ethereum node using an API call and display the details in the GUI when the user wants to see smart farming alerts.

The description of the main components used in the proposed approach is discussed in the following paragraph.

AWS IoT core: Several IoT sensing devices exist in the smart-farming environment. An IoT message-processing infrastructure is needed to support the IoT message protocols such as MQTT and accommodates the network bandwidth to collect messages from numerous IoT devices. We selected AWS IoT core service to perform the smart agriculture IoT data processing. The AWS IoT core offers low latency and high throughput performance, and these characteristics support the building of real-time production-level IoT monitoring systems.

AWS Lambda: The collected IoT data should be processed and given as input data to the Ethereum blockchain. Therefore, AWS Lambda runs the code in the backend and stores the smart-farming information in the Blockchain. AWS Lambda is a serverless computing service to run code virtually without provisioning the server infrastructure.

Infura API: The study did not rely on deploying the Ethereum full node to create and run the farming smart contracts. Infura is an Ethereum API service to run smart contracts in Ethereum nodes and performs Ethereum-based transactions. We leverage the Infura API calls to interact with Ethereum nodes once we collect and process the farming sensor data.

Ethereum: The study implemented the Ethereum-based smart contract to store the farming sensor data and check the farming environment conditions. The Ethereum first version works on the proof-of-stake (POS) consensus mechanism to approve and add the transactions to the Ethereum blockchain. A Web3 frontend application is implemented to review and alert the farmers when security events are detected.

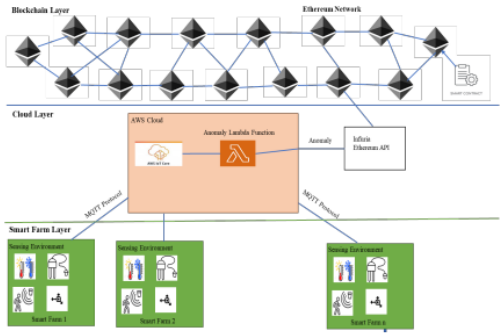

Fig. 2. Blockchain cloud-based smart-agriculture application.

ADVANTAGES OF OUR PROPOSED METHODOLOGY

This research solution inherits the benefits of secure data storage using blockchain. Only certified farmers with access to smart farming records are included. Cloud-based data storage carries the security risk of data breaches due to access control misconfiguration. Blockchain enables secure storage of records with no maintenance costs for storage. Our solutions are cloud-scalable and provide solutions for a variety of security use cases in smart agriculture. Blockchain transaction alert data immutability can be used as evidence in litigation, can be used to ensure the security of insurance claims, and data corruption-free security investigation data to protect farmers' farm assets and property. For example, natural disasters can severely affect agricultural land. Evidence of when, what, where, and how it can be captured as blockchain transaction data and used for insurance claims. A farm cannot deny ownership of a transaction once it has been added to the blockchain. This property can be used to identify malicious farmer activity and maintain transparency. Some of the use cases for the proposed smart farming approach are discussed below. **Sensor status**: Sensors constantly monitor farmland and farm physical conditions and transmit these data to farmers or crop owners to effectively manage their farms for higher yields, lower losses, and increased productivity. need to do it. Sensors/actuators must work continuously to receive regular updates. Sensors are attacked with passive and active attacks. Therefore, monitoring the health of these device sensors is essential and continuously monitored. A mobile application needs to notify the farmer when the health status of the device is turned off. Farmers can then find the root cause and fix the problem.

Abnormal sensor data: You can flag anomalies in sensor data to draw attention and look for anomalies. Set thresholds to trigger alarms and monitor smart farming applications. For example, temperatures in agricultural warehouses are constantly monitored to keep goods safe. A temperature sensor is installed in the storage tank to monitor the temperature of the storage tank. A blockchain-based monitoring solution alerts storage unit owners when temperatures exceed threshold temperatures. Similarly, an image sensor installed near the storage unit is used to identify moving objects. Image processing techniques were applied to detect unauthorized access to the storage unit. Cloud resources integrated into the solution can process images and generate output.

Community Farming Blockchain: The crop productivity or quality impact on any single farm may gradually affect other farms in the community or nearby farms in the surrounding area. The effect can be due to the infection of bugs, severe weather disturbing the crop's life cycle, or more. Communication of this information to the community farmers may save their crops from infection and stop the infection from spreading. Therefore, the blockchain-based community can use this as a farm blockchain for sharing the latest updates among the farmers and keep connected to be aware of what is happening on the surrounding people's farms for awareness. For instance, a burglar with unauthorized farmland storage access can be reported to the farmers around the premises using the proposed blockchain-based application. The number of applications is numerous using the smart-farm community blockchain.

4. IMPLEMENTATION OF THE PROPOSED BLOCK-CHAIN DEFENSE

To evaluate the proposed method for smart agricultural security monitoring using blockchain and cloud technology, we implemented a prototype using the Arduino Sensor with Wi-Fi capability to mimic various sensors deployed in farmland, AWS cloud components to process sensor data, Ethereum blockchain to store monitoring alerts and other important information using the smart contract and develop a web interface to view alerts for users.

Test setup: The following hardware/software components such as the Arduino sensor, EP8266 Wi-Fi module, AWS IoT core component, AWS lambda function, infura Ethereum API account, and Web Javascript were used to perform the experiment. The Arduino module with Wi-Fi is connected to the home Wi-Fi router to communicate with the cloud. Our security monitoring application can be developed as a third-party security monitoring product or tool to secure smart agricultural IoT devices. The Arduino Sensor Kit contains a potentiometer, light sensor, sound sensor, air pressure sensor, temperature sensor, and accelerometer to monitor and capture environmental, physical, and other conditions. different conditions. The circuit board is used to connect these sensors to the communication device. Wi-Fi module H. The WLAN module also acts as a peripheral gateway for all the detection devices mentioned in the test setup. The Arduino C language

code is written to connect a Wi-Fi module to a home router and communicate externally with its remote AWS IoT node to update events. His SSID and password key details for his home Wi-Fi router are provided with the Arduino to connect to the internet. AWS IoT core services are built on top of the AWS cloud with some common configuration settings. AWS IoT Core runs on the free RTOS operating system to process data from IoT devices and exchange data via the MQTT protocol. AWS IOT Core can expose sensor device data and store it in cloud storage like S3. AWS Lambda functions are written in the JavaScript programming language and continuously poll the AWS core for sensor event data.

The observing rationale is executed within the AWS lambda work to distinguish the sensor status and sensor information irregularities. The infrua API calls were too performed utilizing the AWS lambda work to upgrade the sensor observing data for changeless capacity within the blockchain. The infura account is required to produce the API key and build up an association with the Ethereum organization. Hence, the alarm data is upgraded to the blockchain and put away within the exchange. To execute the end-to-end application, the infura API calls are utilized to recover the caution exchange from the Ethereum blockchain. The rancher may download the portable application or web app to screen the cultivate alarms remotely. Figure 3 shows the Arduino microcontroller utilized to control and interface to the IoT-detecting gadgets. The temperature sensor and mugginess and light sensor are associated with the microcontroller, and the microcontroller underpins a Wi-Fi association to communicate with cloud administrations. The sensors can be considered agribusiness application conclusion gadgets. As appeared in Figure 3, the temperature and light sensor positive terminals such as A3, and D3 are associated with the microcontroller PINS. The negative terminals are grounded to avoid short-circuiting issues. The microcontroller is control provided with 5V, which is appeared in Figure 3 with a ruddy wire association.

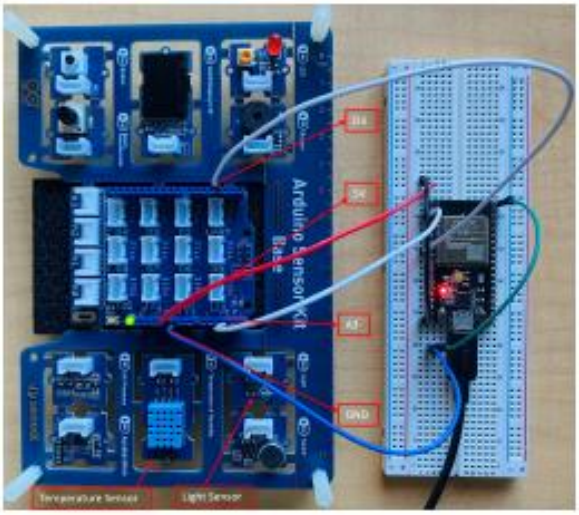

Fig. 3. Arduino sensor kit to sense the environment.

As appeared in Figure 4, the detecting device's status will be checked utilizing the desktop application. The Arduino controller is associated with the tablet using wired communication. The sensor measures real-time movement such as temperature and light within the cultivating. We introduced the Arduino computer program application on the portable workstation machine to run the C code on the Arduino pack. The code comprises the WIFI association qualifications; AWS IoT Center association necessities such as Client ID, and AWS Have URL; and the MQTT point title and the programming rationale to study the sensor information as an MQTT subject and publish the MQTT point within the AWS IoT cloud utilizing the arrange association. The code is dumped on the Arduino microcontroller to run the application and post the information in AWS IoT Cloud. Figure 4 shows the print explanations demonstrating the Arduino pack associated with the author's domestic WIFI organization "maverick creek-7-709" and starting an association with the AWS Cloud. Once it is associated with the AWS, the sensor information is distributed as an MQTT subject with values temperature: 26, light: 26, and mugginess 51. The data publish-success message can moreover be seen in Figure 4.

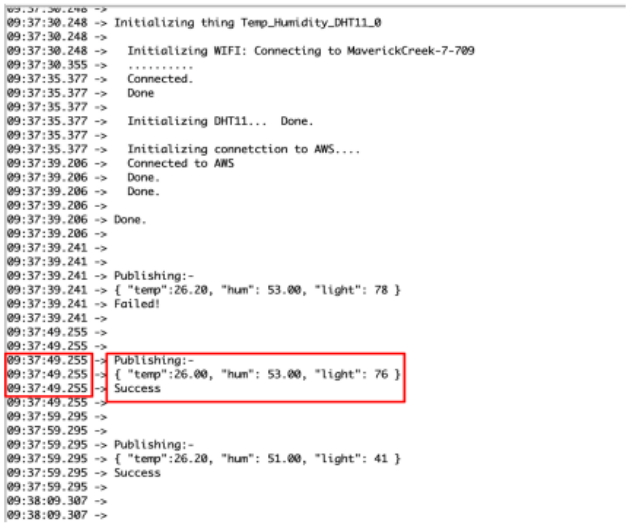

Fig. 4. Sensor devices connected to Wi-Fi and initializing connection to AWS Cloud.

The MQTT publishes messages and can also log in to the AWS IoT Core. Figure 5 displays the published IoT sensor data in the AWS Cloud. As seen in Figures 4 and 5, the data publication time in the IoT core cloud is 2 s. The highlighted red boxes in Figure 5 indicate the timestamp and sensing temperature, humidity, and light values in the Arduino kit environment**.**

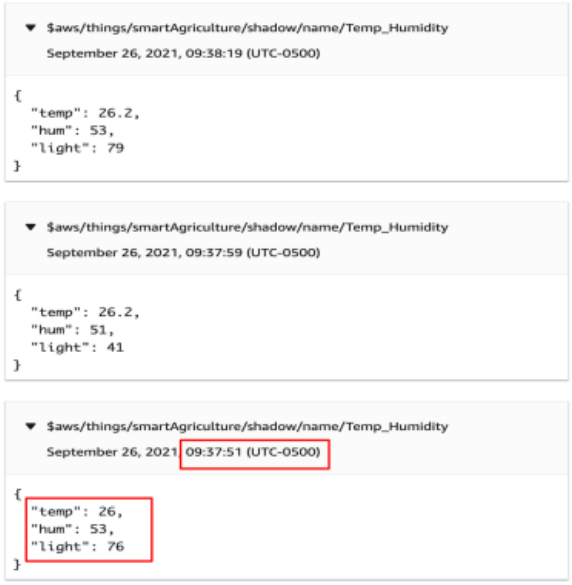

Figure 5. Sensor data real-time recording in AWS Cloud-IoT core service

The AWS lambda work composed in JavaScript peruses the AWS IoT Center distributed information and compares the sensor limit values for irregularity discovery. The code may trigger a sensor gadget wellbeing alarm on the off chance that the information isn't gotten for a particular time interim. To connect with the Ethereum blockchain, the Infura API qualifications are put away as factors, and the AWS lambda work reads the credentials to put through with Infura to keep up Ethereum's primary hub. The meta mask application is utilized for the program wallet and to be associated with the

Ethereum blockchain. The wallet subtle elements are moreover given within the AWS lambda work to perform the exchanges in Ethereum. The smart-contract code is written using robustness programming dialect and sends the caution-activated information as an exchange within the Ethereum blockchain. Figure 6 appears that Ethereum exchanges subtle elements when the temperature-threshold-exceeded alarm is seen within the AWS IoT core. The exchanges incorporate the piece number, from and to address, exchange expense, gas cost, and timestamp. Based on the timestamps watched within the end-to-end blockchain- and cloud-based execution, we decided that the time to overhaul the agriculturist when the agribusiness environment inconsistency cautions trigger is 9 s. The Ethereum exchange completion time is 7 s. Be that as it may, we utilized the Rinkeby testing arrange to test the Ethereum arrange, and the general caution notice organizes idleness will not be the same within the Ethereum generation organize. In general, we prove that organize idleness is negligible when performing farming security observing utilizing blockchain and cloud administrations and alarming the farmers.

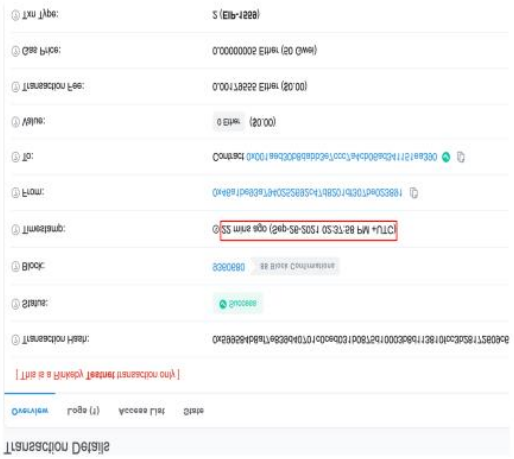

Figure 6. Ethereum smart-contract transaction details.

Figure 7 indicates the data field format in the Ethereum transaction. The sensor threshold value, current value, and alert message are stored in the data transaction. This data will not be tampered with and will be stored securely in the blockchain. The boxes highlighted in red clearly show that the temperature value of 25 does not exceed the threshold value of 26.

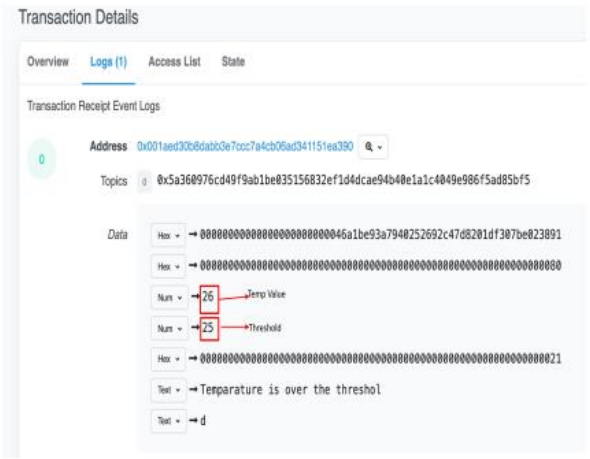

Figure 7. Ethereum smart-contract transaction storing the sensor data.

The experimental transaction performed on the rinkeby network can be seen publicly for reader understanding. Figure 8 displays the list of transactions stored in the Ethereum test network. The from and to address, transaction hash value, and block ID can be seen for each transaction.

We have developed a front-end web application to receive farm safety alerts such as device status and anomaly alerts. The UI app displays an alert message as an Ethereum transaction. Figure 9 shows a warning message with details about sensor data and policy violations. For example, block number 9363208 in Figure 9 notifies farmers of temperature changes in the monitoring environment. When the temperature exceeded the threshold value, a policy violation message was displayed on the UI test web application. We used the vertical web platform to develop our test web application. Users may also want to update transactions using the user interface application. For example, users should store sensor anomaly data for future reference. We have integrated this functionality into the front-end web application to update the breach detection data conditions in the blockchain. Figure 10 shows the front-end web application with interactive options for updating transactions in the Ethereum test net. This feature helps farmers or web application users control the blockchain platform used to monitor farm safety. To add a new transaction using the web interface, the user must log in to their wallet and fill in the transaction details. The temperature, humidity, and light sensor values and their optimal values are entered and these are sent using the web application. The infura API is connected to the blockchain node and adds a new transaction when the config sensor data policy is violated. Other users can view the transaction data after the transaction is updated in the blockchain.

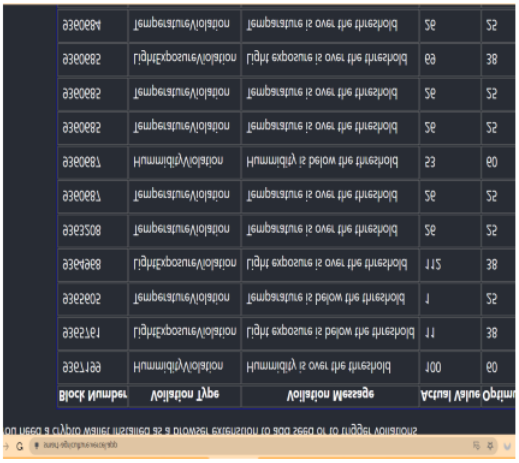

Fig. 8. Smart-contract web application frontend—alert notifications.

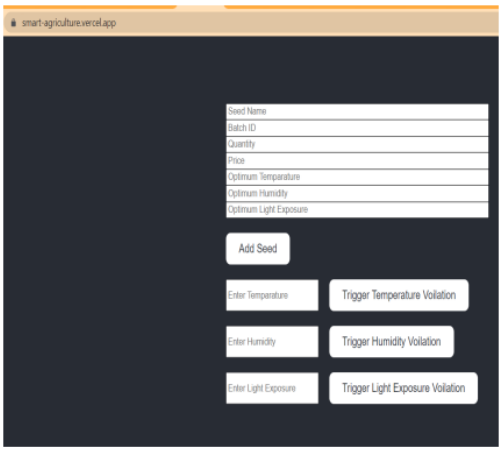

Fig. 9. Smart-contract web application—frontend GUI.

Our blockchain solution can be used on the farming community blockchain platform. As shown in Figure 10, a farmer can update the real-time agriculture environment condition to fellow farmers so that fellow farmers do not have to visit the farming location and can effectively make decisions from home to perform daily agriculture and farming operations. Although we only used three sensors to test our prototype, our solution can be easily tweaked to support processing multi-sensor data, and our implementation is used for various IoT applications.

PERFORMANCE EVALUATION MONITORING SYSTEM PERFORMANCE

The end-to-end framework execution has to be assessed to assess the solution's adequacy. The organized idleness and throughput are the pointers seen within the writing as performance components for blockchain-based applications. The time is taken to get the sensor alarm when a peculiarity of the arranged inactivity may be a few seconds. The organized throughput was not tried utilizing our usage due to the infura API free-access restriction. Execution comparison with existing works:

Our arrangement execution is compared with the existing works utilizing blockchain in shrewd contracts. Even though none of the existing works actualized the end-to-end arrangements with AWS cloud and smart contracts, we included the closely related smart-contract execution for smart farming. Table 3 delineates the message organize idleness in comparison of our work with existing works. The creators [38] actualized Ethereum-based smart contracts to overhaul the IoT detecting information to the blockchain and assessed the arranged idleness of issuing an exchange within the blockchain. The creators detailed an ad up to arrange inactivity of 16.55 s. This work is closely related to our work in terms of including the IoT sensor information in the blockchain. Our arrangement performed much superior to the work [38] since we utilized real-time usage applications, counting IoT centers and smart contracts using Infura API. The extra idleness in [38] can moreover be caused by the blockchain hub running in the virtual machine. The work [27] performed reenactments to test the IoT devices sending upgrades to the blockchain and evaluated the arrange idleness. They considered 4G as a communication medium to show the communication connection and gotten less than 0.2 s idleness. We utilized the domestic WiFi to perform the tests and got the matchable execution with [27]. The creators [34] moreover utilized Ethereum to construct the farming savvy contract. The creators detailed that it took 272 s to total one exchange. The tall organize idleness may be caused by the utilization of the genuine Ethereum organize. Our arrangement detailed a add up to arrange inactivity of 0.11 s, which is real-time caution announcing. We moreover decided the cruel time to distinguish (MTTD) when the 95% certainty interim is utilized. The MTTD is detailed as 0.115 with an edge of mistake of 0.00919 and a standard deviation of 0.016. occurs within the sensor environment straightforwardly demonstrates the arranged inactivity. Our test comes about on Rinkeby appears that the network inactivity may be a few seconds. The organized throughput was not tried utilizing our usage due to the infura API free-access restriction.

EXECUTION AND COMPARISON WITH EXISTING WORKS

Our arrangement execution is compared with the existing works using blockchain in shrewd contracts. Even though none of the existing works implemented the end-to-end arrangements with AWS cloud and smart contracts, we included the closely related smart-contract execution for savvy agribusiness. Table 3 delineates the message arrange inactivity comparison of our work with existing works. The creators [38] actualized Ethereum-based smart contracts to overhaul the IoT detecting information to the blockchain and assessed the arranged inactivity of issuing an exchange within the blockchain. The creators detailed an ad up to arrange inactivity of 16.55 s. This work is closely related to our work in terms of including the IoT sensor information in the blockchain. Our arrangement performed much way better than the work [38] since we utilized real-time usage applications, counting IoT centers, and smart contracts utilizing Infura API. The extra inactivity in [38] can too be caused by the blockchain hub running within the virtual machine. The work [27] performed recreations to test the IoT gadgets sending upgrades to the blockchain and assessed the organized inactivity. They considered 4G as a communication medium to show the communication connection and gotten less than 0.2 s idleness. We utilized the domestic WiFi to perform the tests and got the matchable execution with [27]. The creators [34] moreover utilized Ethereum to construct the farming smart contract. The creators detailed that it took 272 s to total one transaction. The tall organize

idleness may be caused by the utilization of the genuine Ethereum organize. Our arrangement detailed a add up to arrange inactivity of 0.11 s, which is real-time alarm announcing. We too decided the cruel time to distinguish (MTTD) when the 95% certainty interim is utilized. The MTTD is detailed as 0.115 with an edge of mistake of 0.00919 and a standard deviation of 0.016.

5. DISCUSSION, LIMITATION, AND FUTURE WORK

We actualized a real-time situation agribusiness security-monitoring framework, which screens the sensor device's well-being status and sensor peculiarities to perform accurate agribusiness and profitable cultivating. Be that as it may, we did not send the sensors to the agriculture field to capture the farmland environment conditions. We imagine that the network inactivity will be unimportant, considering the wide spread of the web in provincial regions. Our arrangement can indeed screen the rural conditions in rural areas as long as an online association is accessible. We did not actualize the IoT gateway in our work. We utilized the domestic switch as an IoT portal and associated the IoT sensor devices with the arrange using domestic WiFi. This is often one of the restrictions of our work. Implementing an IoT organize with an IoT portal and different detecting gadgets to imitate the reasonable smart-agriculture environment is one of the expansions of our work. The current execution as it were works on the Ethereum proof-of-work (POW) agreement mechanism blockchain. One future work will be implementing the current arrangement within the Ethereum 2.0 arrangement, which is backed by the proof-of-stake (POS) agreement

There are various IoT applications to screen the IoT environment, counting agribusiness applications, savvy homes, smart well-being, smart transportation applications, etc. In this manner, we imagine our model will too be utilized to execute the observing arrangements in other areas. The arranged traffic can be collected from a smart-agriculture edge gateway and stored the arranged events data within the cloud. Organized occasions can be utilized to apply machine-learning and deep-learning techniques and recognize the anomaly network activity in a smart-agriculture arrangement. One future work will be executing ML- and DL-based network-security observing arrangements in savvy agribusiness and utilizing blockchain to store the arrange inconsistency occasions as transactions. The generation Ethereum blockchain gas cost is tall. Subsequently, blockchain advances such as Cardano and Solano-based blockchain implementation are considered to plan more network-latency applications and decrease the end user/farmer exchange fetched in shrewd farming. 9. Conclusions In this article, we proposed a cloud- and blockchain-based security observing framework for smart-agriculture IoT applications. The end-to-end application model was executed utilizing an Arduino sensor pack, AWS cloud components, web application GUI, and the Ethereum blockchain smart contract to caution the farmers of security anomalies and sensor-device status. The prototype was able to alarm the farmers in real-time, permit inaccessible observation of the cultivated and farming environment, and empower the cultivating community to communicate using blockchain. The execution assessment in terms of organized idleness is appeared to be ostensible with our model and it may be expressed that the delay can indeed be diminished with the execution of high-performance exchange blockchain technologies such as Cardano. We talked about the limitations and future openings to progress the security of shrewd farming.

CONFLICT-OF-INTEREST DISCLOSURE: This research declares no conflict of interest.

FUNDING: Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University.

REFERENCES

1. Dutta, S. Top 25 Agricultural Producing Countries in the World. 2020. Available online: https://www.yahoo.com/video/top-20 -agricultural-producing-countries-151350776.html?guccounter=1 (accessed on 15 July 2022).
2. Ahmed, N.; De, D.; Hussain, I. Internet of Things (IoT) for smart precision agriculture and farming in rural areas. IEEE Internet Things J. 2018, 5, 4890–4899. [CrossRef]
3. Steve, C. Cyber Threats Are a Real Threat to Modern Agriculture's Expanding Digital Infrastructure | AgWeb. 2022. Available online: https://www.agweb.com/news/business/technology/cyber-threats-are-real-threat-modern-agricultures-expandingdigital (accessed on 13 August 2022).
4. Nicole, S. JBS Paid $11 Million to Hackers after Ransomware Attack—CBS News. 2020. Available online: https://www.cbsnews. com/news/jobs-ransom-11-million/ (accessed on 13 August 2022).
5. Badran, A.I.; Kashmoola, M.Y. Smart Agriculture Using Internet of Things: A Survey. In Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC-SDSP, Cyberspace, 28–30 June 2020; p. 10
6. Baskar, C.; Balasubramaniyan, C.; Manivannan, D. Establishment of lightweight cryptography for resource constraint environment using FPGA. Procedia Comput. Sci. 2016, 78, 165–171. [CrossRef]
7. Brewster, C.; Roussaki, I.; Kalatzis, N.; Doolin, K.; Ellis, K. IoT in agriculture: Designing a Europe-wide large-scale pilot. IEEE Commun. Mag. 2017, 55, 26–33. [CrossRef]
8. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. IEEE Access 2020, 8, 32031–32053. [CrossRef]
9. Friha, O.; Ferrag, M.A.; Shu, L.; Maglaras, L.A.; Wang, X. Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies. IEEE CAA J. Autom. Sin. 2021, 8, 718–752. [CrossRef]
10. Mekala, M.S.; Viswanathan, P. A Survey: Smart agriculture IoT with cloud computing. In Proceedings of the 2017 international conference on microelectronic devices, circuits, and systems (ICMDCS), Vellore, India, 10–12 August 2017; pp. 1–7.
11. Li, C.; Niu, B. Design of smart agriculture based on big data and Internet of things. Int. J. Distrib. Sens. Netw. 2020, 16, 1550147720917065. [CrossRef]
12. Mondal, S.; Wijewardena, K.P.; Karuppuswami, S.; Kriti, N.; Kumar, D.; Chahal, P. Blockchain inspired RFID-based information architecture for the food supply chain. IEEE Internet Things J. 2019, 6, 5803–5813. [CrossRef]
13. Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. A privacy-preserving communication protocol for IoT applications in smart homes. IEEE Internet Things J. 2017, 4, 1844–1852. [CrossRef]
14. Chaganti, R.; Gupta, D.; Vemprala, N. Intelligent network layer for cyber-physical systems security. Int. J. Smart Security. Technol. (IJSST) 2021, 8, 42–58. [CrossRef]
15. Chaganti, R.; Ravi, V.; Pham, T.D. Deep Learning based Cross Architecture Internet of Things malware Detection and Classification. Comput. Secure. 2022, 120, 102779. [CrossRef]
16. Geroni, D. Top 12 Smart Contract Use Cases—101 Blockchains. 2021. Available online: https://101blockchains.com/smartcontract-use-cases/ (accessed on 16 July 2022)
17. . Chaganti, R.; Bhushan, B.; Ravi, V. The role of Blockchain in DDoS attacks mitigation: Techniques, open challenges, and future directions. arXiv 2022, arXiv:2202.03617.
18. Li, X.; Wang, D.; Li, M. Convenience analysis of sustainable E-agriculture based on blockchain technology. J. Clean. Prod. 2020, 271, 122503. [CrossRef]
19. Torky, M.; Hassanein, A.E. Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. Comput. Electron. Agric. 2020, 178, 105476. [CrossRef]
20. Sinha, B.B.; Dhanalakshmi, R. Recent advancements and challenges of the Internet of Things in smart agriculture: A survey. Future Gener. Comput. Syst. 2022, 126, 169–184. [CrossRef]
21. Hassan, S.I.; Alam, M.M.; Illahi, U.; Al Ghamdi, M.A.; Almotiri, S.H.; Su'ud, M.M. A systematic review on monitoring and advanced control strategies in smart agriculture. IEEE Access 2021, 9, 32517–32548. [CrossRef]
22. Talavera, J.M.; Tobón, L.E.; Gómez, J.A.; Culman, M.A.; Aranda, J.M.; Parra, D.T.; Quiroz, L.A.; Hoyos, A.; Garrett, L.E. Review of IoT applications in agro-industrial and environmental fields. Comput. Electron. Agric. 2017, 142, 283–297. [CrossRef]
23. Farooq, M.S.; Riaz, S.; Abid, A.; Abid, K.; Naeem, M.A. A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. IEEE Access 2019, 7, 156237–156271. [CrossRef]

24. Elijah, O.; Rahman, T.A.; Orikumhi, I.; Leow, C.Y.; Hindia, M.N. An overview of the Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet Things J. 2018, 5, 3758–3773. [CrossRef]

25. Hari Ram, V.V.; Vishal, H.; Dhanalakshmi, S.; Vidya, P.M. Regulation of water in agriculture field using Internet Of Things. In Proceedings of the 2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR), Chennai, India, 10–12 July 2015; pp. 112–115.

26. Postolache, O.; Pereira, M.; Girão, P. Sensor network for environment monitoring: Water quality case study. In Proceedings of the 4th Symposium on Environmental Instrumentation and Measurements 2013, Lecce, Italy, 3–4 June 2013; pp. 30–34.

27. Chen, W.L.; Lin, Y.B.; Lin, Y.W.; Chen, R.; Liao, J.K.; Ng, F.L.; Chan, Y.Y.; Liu, Y.C.; Wang, C.C.; Chiu, C.H.; et al. AgriTalk: IoT for precision soil farming of turmeric cultivation. IEEE Internet Things J. 2019, 6, 5209–5223. [CrossRef]

28. Baranwal, T.; Nitika; Pateriya, P.K. Development of IoT-based smart security and monitoring devices for agriculture. In Proceedings of the 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence), Noida, India, 14–15 January 2016; pp. 597–602.

29. Mukherjee, A.; Misra, S.; Raghuwanshi, N.S.; Mitra, S. Blind entity identification for agricultural IoT deployments. IEEE Internet Things J. 2018, 6, 3156–3163. [CrossRef]

30. Yadav, V.S.; Singh, A. A systematic literature review of blockchain technology in agriculture. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Toronto, ON, Canada, 23–25 October 2019; pp. 973–981.

31. Vangala, A.; Das, A.K.; Kumar, N.; Alazab, M. Smart secure sensing for IoT-based agriculture: Blockchain perspective. IEEE Sens. J. 2020, 21, 17591–17607. [CrossRef]

32. Bermeo-Almeida, O.; Cardenas-Rodriguez, M.; Samaniego-Cobo, T.; Ferruzola-Gómez, E.; Cabezas-Cabezas, R.; Bazán-Vera, W. Blockchain in agriculture: A systematic literature review. In Proceedings of the International Conference on Technologies and Innovation, Guayaquil, Ecuador, 6–9 November 2018; pp. 44–56.

33. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J. 2018, 6, 2188–2204. [CrossRef]

34. Rehman, M.; Javaid, N.; Awais, M.; Imran, M.; Naseer, N. Cloud-based secure service providing for IoTs using blockchain. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–7.

35. Voutos, Y.; Drakopoulos, G.; Mylonas, P. Smart agriculture: An open field for smart contracts. In Proceedings of the 2019 4th SouthEast Europe Design Automation, Computer Engineering, Computer Networks, and Social Media Conference (SEEDA-CECNSM), Piraeus, Greece, 20-22 September 2019; pp. 1–6.

36. Pranto, T.H.; Noman, A.A.; Mahmud, A.; Haque, A.B. Blockchain and smart contract for IoT enabled smart agriculture. PeerJ Comput. Sci. 2021, 7, e407. [CrossRef]

37. Shyamala Devi, M.; Suguna, R.; Joshi, A.S.; Bagate, R.A. Design of IoT blockchain-based smart agriculture for enlightening safety and security. In Proceedings of the International Conference on Emerging Technologies in Computer Engineering, Jaipur, India, 1–2 February 2019; pp. 7–19.

38. Caro, M.P.; Ali, M.S.; Vecchio, M.; Giaffreda, R. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), Tuscany, Italy, 8–9 May 2018; pp. 1–4.

39. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart contract-based blockchain-envisioned authentication scheme for smart farming. IEEE Internet Things J. 2021, 8, 10792–10806. [CrossRef]