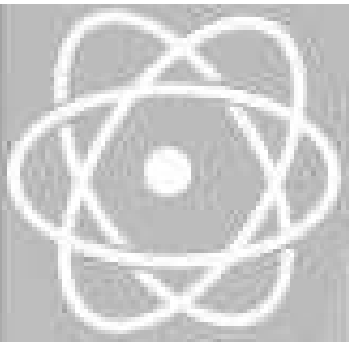


SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL7 No2
JUNE2023

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 7(2): 1-6 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

მომხმარებლის მდებარეობის განსაზღვრა 5G ქსელში - High-Band ის გამოყენებით

LOCATING USER IN 5G NETWORKS USING HIGH-BAND

გიორგი ახალაია, საქართველოს ტექნიკური უნივერსიტეტი
Giorgi Akhalaia, georgian technical university

აბსტრაქტი: ბოლო წლებია ციფრულ ტექნოლოგიებსა და სერვისებში განსაკუთრებული ყურადღება ექცევა მომხმარებლის პერსონალური და მაიდენტიფიცირებელი ინფორმაციის უსაფრთხოებას. ახალი ფუნქციონალის, სერვისის დანერგვამდე, უსაფრთხოების ტესტირების პროცესში მუდმივი განხილვის საგანია მომხმარებლის პრივატულობა. მობილური ტექნოლოგიების, ხელოვნური ინტელექტის, ავტომატიზაციის სისტემების განვითარებამ, აუცილებელი გახადა მობილური კომუნიკაციების ახალი სტანდარტების დანერგვა. 3 მთავარი პრინციპით (ულტრა-საიმედო/დაბალი დაყოვნება; გაუმჯობესებული მობილური ბროუდბენდი; მანქანების მასიური რაოდენობით მიერთება), 5G სტანდარტი ცდება მობილური კავშირგაბმულობის ეკოსისტემას და და ქმნის უფრო მასშტაბურ ქსელს. გაუმჯობესებული დაცვის მექანიზმების მიუხედავად, 5G ქსელში ისევ რჩება სისუსტეები, რომლიდანაც თავდამსხმელს შეუძლია გარკვეული კიბერ შეტევების განხორციელება. MITM ტიპის შეტევით შესაძლებელი ხდება მომხმარებლის მოწყობილობის მოსმენა. კვლევის მიზანია 5G ქსელში არსებული საფრთხეების შეფასება მომხმარებლის პერსონალური მონაცემების უსაფრთხოებასთან მიმართებაში. ყურადღება გამახვილებულია მომხმარებლის მდებარეობის დადგენასთან დაკავშირებული საფრთხეების შეფასებაზე, 5G ქსელში არსებული სისუსტის გამოყენებით მომხმარებლის მდებარეობის დადგენაზე და მისგან თავის დაცვის რეკომენდაციების შემუშავებაზე.

საკვანძო სიტყვები: *5G ქსელის უსაფრთხოება, უსაფრთხო კომუნიკაცია, ლოკაციასთან დაკავშირებული შეტევები, მომხმარებლის უსაფრთხოება*

ABSTRACT: In recent years, in digital technologies and services, special attention has been paid to the security of user's personal and personally identifiable information. Prior to the introduction of new functionality, the service, user privacy is a constant consideration during the security testing process. The development of mobile technologies, artificial intelligence, automation systems made it necessary to introduce new standards of mobile communications. With 3 key principles (ultra-reliability/low latency; improved mobile broadband; massive vehicle connectivity), the 5G standard will disrupt the mobile communications ecosystem and create a more scalable network. Despite the improved protection mechanisms, there are still weaknesses in the 5G network from which an attacker can carry out certain cyber attacks. A MITM type of attack makes it possible to eavesdrop on the user's device. The aim of the study is to assess the threats in the 5G network in relation to the security of the user's personal data. The focus is on assessing threats related to user location, using vulnerabilities in the 5G network to determine user location, and developing recommendations to protect against it.

KEYWORDS: *5G Network Security, Secure Communications; Location-Based Attacks, End-user privacy*

1. შესავალი

ტექნოლოგიურად განვითარებულმა და ძლიერი ეკონომიკის მქონე ქვეყნებმა ბოლო წლებში აქტიურად დანერგეს მეხუთე თაობის ქსელი. აშშ_სა და საქართველოს შორის 2021 წელს გაფორმდა მემორანდუმი. რომლის მიხედვითაც, ქვეყნებს მჭიდრო თანამშრომლობა ექნებათ და აშშ დაეხმარება საქართველოს როგორც 5G ქსელის დანერგვაში, ასევე მისი უსაფრთხოების უზრუნველყოფაში. მეხუთე თაობის ქსელის სამი KPIია:

- > 10Gb/s - (eMBB)
- > 1M/km²-(mMTC). ეს სიმჭიდროვე აღებულია IoT მოწყობილობებიდან გამომდინარე.
- < 1ms Latency - არაუმეტეს 1 მილიწამი დაყოვნება.(URLLC) [1]

ხოლო მეხუთე თაობის ქსელის სამუშაო სპექტრი, შემდეგნაირადაა დაგეგმილი:

1. **ქვედა არხი - (Low-band) -- < 1 GHz**
2. **შუა არხი - (Mid-band) -- 1 GHz – 6 GHz**
3. **მაღალი არხი - (High-band(mmWave)) – 6 GHz – 100 GHz**

High-Band - ძირითადად ამ სპექტრს მოიაზრებენ როცა 5G ქსელზეა საუბარი. ამ სპექტრის საშუალებით შესაძლებელი ხდება მინიმალური დაყოვნებით, პიკური სიჩქარის ათობით Gbps_მდე გაზრდა. ხშირად მოიხსენიებენ როგორც mmWave ტექნოლოგიად. ზემოთ ჩამოთვლილი სპექტრული დანაყოფებიდან, სწორედ High-band წარმოადგენს მთავარ რგოლს 5G ქსელის იმპლემენტაციაში.[2]

კვლევისას აქცენტი გაკეთებულია High-Band ის სიხშირეზე არსებული სისუსტის გამოყენებით შეტევის განხორციელებაზე და მომხმარებლის მდებარეობის დადგენაზე.

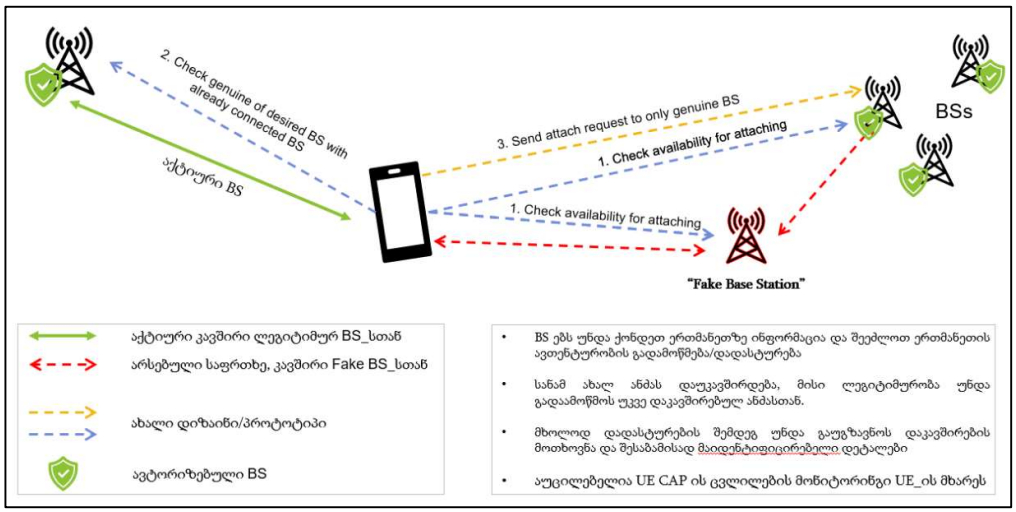
2. 5G_ს უსაფრთხოება

5G ქსელი თავისი არქიტექტურიდან, იდეიდან გამომდინარე კიდე უფრო კომპლექსურია. იქიდან გამომდინარე, რომ მეხუთე თაობის ქსელში ჩაირთვება სხვადასხვა მწარმოებლის, კატეგორიის, არქიტექტურისა და პროგრამული უზრუნველყოფის მქონე მოწყობილობა, რომლებიც განსხვავებულ ტექნოლოგიებს იყენებენ მათი ცალ-ცალკე არსებული სისუსტე, გადმოყვება სისტემაში და უკვე გახდება სისტემის შემადგენელი სისუსტე. ასევე ყურადსაღებია LBS(Location Based Service) ტიპის სერვისები, მომხმარებლის პერსონალური ინფორმაციაზე, მოწყობილობის სხვადასხვა სერვისის გამოყენებისას გაცემული პირადი ინფორმაცია საბოლოოდ დასაცავი აღმოჩნდება.

მართალია 4G_სგან განსხვავებით 5G ქსელი მომხმარებლის უსაფრთხოება შედარებით დახვეწილია, მაგრამ მაინც რჩება ინფორმაციის ნაწილი, რომელიც ე.წ. clear text_ად მიმოიცვლება ქსელში ბაზასთან დაკავშირებისას. რომელიც შემდეგ სხვა ინფორმაციის მოპარვისთვის შეიძლება გამოიყენოს თავდამსხმელმა. ეს აჩენს ე.წ. Fake Base Station Attack ის საფრთხეს. ამ დროს მესამე

პირი მომხმარებელს თავს აჩვენებს თითქოს ის არის რეალური cell tower, რის შედეგადაც მასთან დაკავშირებას ცდილობს. [5]

ამ ეტაპზე შემუშავებული დიზაინი, კვლევების თანახმად, მეხუთე თაობის ქსელი მოწყვლადია MITM ტიპის შეტევების მიმართ. რომელიც არის ერთ-ერთ ყველაზე ძლიერი შეტევა ქსელში. კვლევის შედეგად შევიმუშავეთ განახლებული, უსაფრთხო კონცეპტუალური დიზაინი, რომელიც მნიშვნელოვნად შეამცირებს ქსელში ე.წ. ცრუ ანძების ეფექტურობას.



ილუსტრაცია 1

ილუსტრაცია 1_ზე ნაჩვენებია განახლებული დიზაინის მიხედვით როგორ მოხდება მომხმარებლის მოწყობილობის ანძასთან დაერთება,

მოწყობილობის ლოკაციის განსაზღვრის 2 ძირითადი ტექნიკა, მეთოდი არსებობს: გლობალური სატელიტური სანავიგაციო სისტემა - GNSS ან A-GPS. GNSS გულისხმობს სატელიტების საშუალებით მოწყობილობის მდებარეობის დადგენას, A-GPS კი ოპერატორის ანძების გამოყენებით მომხმარებლის მოწყობილობის ლოკაციის გადათვლას/დაანგარიშებას. ორივე მეთოდს აქვს თავისი სუსტი მხარე და უპირატესობა: პირველის შემთხვევა (GNSS), მუშაობს ე.წ. ღია ცის პრინციპი, ანუ მოწყობილობას უნდა ქონდეს სატელიტების პირდაპირი ხედვა. მაგრამ ყველაზე დაბალ ცდომილებას იძლევა, ხოლო მეორე A-GPS, ოპერატორის მინიმუმ სამი ანძის მეშვეობით ითვლის თავის მდებარეობას. პირველ მეთოდთან შედარებით, ეს ნაკლებად ზუსტია, თუმცა, შეუძლია დახურულ სივრცეებშიც (შენობებში) განსაზღვროს მოწყობილობის კოორდინატები.

MITM ის შეტევის დროს, როდესაც ე.წ. “Fake Base Station“_ის ხდება, დიდია საფრთხე, რომ მოწყობილობის ლოკაცია არასწორად განისაზღვროს, რადგან თუ მიწოდებული მონაცემები არასწორია, შესაბამისად შედეგსაც არასწორს მივიღებთ. ეს კი დიდ საფრთხესა და პრობლემას უქმნის ე.წ. მდებარეობასთან დაკავშირებულ სერვისებს, მათ შორის გადაუდებელი სერვისებისთვის, როგორიცაა 911/112 საჭირო პროცესებს.

გამომდინარე იქიდან, რომ მოწყობილობა მუდმივად არ ითვლის თავის კოორდინატებს GPS გამოყენებით, პროგრამული უზრუნველყოფით ამ ტიპის ინფორმაციის მოპარვისას, მომხმარებელი ღებულობს გაფრთხილებას, რომ აპლიკაცია ცდილობს GPS მოდულის

გამოყენებას და მდებარეობის განსაზღვრას. უარყოფითი მხარეა ისიც, რომ თუ მოდული გამორთულია, ან მოწყობილობა შენობაშია, მაშინ არ იმუშავებს. ამ შემთხვევაში უფრო ეფექტურია, მომხმარებლის მოწყობილობიდან თუ A-GPS ის მონაცემებს წამოვიღებთ. დეტალური ინფორმაციის მიღება შეგვიძლია ანძების შესახებ, მათ შორის უნიკალური ID, სიგნალის სიძლიერე, კოორდინატები.

მოწყობილობამ რომ გამოიყენოს High-Band ანძები, ე.წ. mmWave, აუცილებელია რომ იმყოფებოდეს ანძასთანს ძალიან ახლოს, ე.წ. პირდაპირი ხედვით. გამომდინარე იქიდან, რომ ამ სიხშირეების ტალღებს ძალიან ამახინჯებს შენობები. შესაბამისად, ეს შეგვიძლია გამოვიყენოთ და 1 ანძითაც განვსაზღვროთ მოწყობილობის მდებარეობა. რაც დიდ საფრთხეს წარმოადგენს მომხმარებლის უსაფრთხოებისთვის.

კვლევისას გამოყენებული ინფრასტრუქტურა:

მოწყობილობა	**რაოდენობა**	**დანიშნულება**
Raspberry Pi (LTE და GPS მოდულებით)	30	10 - საბაზისო სადგური, 15 - ცრუ საბაზისო სადგური 5 - მომხმარებელი
GPS მოდულიანი მობილური მოწყობილობები	5	მომხმარებელი
Laptop (Kali OS)	2	ექსპერიმენტის მონიტორინგი და მართვა
შედეგები		
ალგორითმის ტიპი	**წარმ/ჩავარნა**	**კომენტარი**
GPS (GNSS კოორდინატების მოწყობილობიდან აღება)	წარმატებული	Success with noise if GPS module was enabled. User interaction was needed. As they were alerted by the system
A-GPS (ინფორმაციის მოწყობილობიდან წამოღება)	წარმატებული	10/10
MITM by Fake BS	წარმატებული	10/10
ანძების ინფორმაციის(სიხშირეების, აქტიური ანძების) წამოღება	წარმატებული	8/10

ცხრილი 2

კვლევისას დავაიდენტიფიცირეთ შეტევა, კერძოდ, შესაძლებელია მობილური ტელეფონის ანძასთან დაკავშირებისას გაგზავნილი, დაუშიფრავი „დაკავშირების მოთხოვნის“ გადამისამართება High-band ანძასთან. რომლის შემდეგაც ერთი ანძიცათ მოხერხდება მდებარეობის განსაზღვრა. ამისგან თავის დასაცავად შევიმუშავეთ ორი რეკომენდაცია:

- High-Band ანტენები არ უნდა ავრცელებდეს მაღალი სიზუსტის კოორდინატებს.
- მოწყობილობა არ უნდა უკავშირდებოდეს თავიდანვე high-band_ს. უნდა დაუკავშირდეთ ქვედა კატეგორიის ანძებს და მხოლოდ მათგან უნდა მოხდეს კავშირის გადამისამართება.

4. დასკვნა

მეხუთე თაობის ქსელის დანერგვა უპირობოდ მნიშვნელოვანია ქვეყნის ეკონომიკური განვითარებისთვის. მისი მასშტაბიდან გამომდინარე, აუცილებელია უსაფრთხოების მაღალ დონეზე უზრუნველყოფა. ბოლო პერიოდში განსკუთრებით ყურადღების ქვეშაა, მომხმარებლის პერსონალური ინფორმაცია. ნაშრომის ფარგლებში ჩატარებულმა კვლევებმა აჩვენა, რომ შესაძლებელია კიბერ შეტევით მეხუთე თაობის ქსელში მომხმარებლის მდებარეობის განსაზღვრა ერთი ანძითაც. შევიმუშავეთ ახალი, უსაფრთხო დიზაინი, რომლითაც შევამცირებთ MITM ის რისკს და ასევე ორი რეკომენდაცია, რომლითაც შეუძლებელს გავხდით ერთი ანძით ზუსტი მდებარეობის განსაზღვრას.

5. დადასტურება/აღიარება

კვლევა PHDF-21-088 განხორციელდა შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით

6. ბიბლიოგრაფია

1. Huawei Technologies CO,. LTD in “5G Network Architecture – A high Level Perspective”, 2016
2. S. Asad Hussain, S. Ahmed, M. Emran, “Positioning a Mobile Subscriber in a Cellular Network System based on Signal
    a. Strength”, IAENG International Journal of Computer Science, 34:2, IJCS_34_2_13,2007.
    b. https://www.researchgate.net/publication/26492533
3. Qualcomm Technologies inc. “What is 5G”, in online article. https://www.qualcomm.com/5g/what-is-5g
4. M. Hanif, “5G Phones Will Drain Your Battery Faster Than You Think”, in online journal, 2020.
    a. https://www.rumblerum.com/5g-phones-drain-battery-life/
5. Shaik, R.Borgaonkar, S. Park, J.P. Selfert. ” New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities” in WiSec ’19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, DOI: 10.1145/3317549, ISBN: 9781450367264, 2019.
6. Ultrasecurity, “Strom-Breaked” (Software Package), (Last access: 8.12.2021)
    a. https://github.com/ultrasecurity/Storm-Breaker
7. SK Telecom, in “5G architecture design and implementation guideline”, 2015.
8. Samsung in online report “Samsung Phone Battery Drains Quickly on 5G Service”
    a. https://www.samsung.com/us/support/troubleshooting/TSG01201462/
9. Purdy, “Why 5G Can Be More Secure Than 4G” in Forbes online journal, 2019.
    a. https://www.forbes.com/sites/forbestechcouncil/2019/09/23/why-5g-can-be-more-secure-than-4g/?sh=2ffcdf1657b2
10. Cell Phone Trilateration Algorithm, Online Journal “Computer Science”, 2019. (Last access: 10.12.2021)
    a. https://www.101computing.net/cell-phone-trilateration-algorithm/

11. Johhny, “How to find the Cell Id location with MCC, MNC, LAC and CellID (CID)”, 2015
    a. https://cellidfinder.com/articles/how-to-find-cellid-location-with-mcc-mnc-lac-i-cellid-cid
12. M. Iavich, G. Akhalaia, S.Gnatyuk. Method of Improving the Security of 5G Network Architecture Concept for Energy and Other Sectors of the Critical Infrastructure, In: Zaporozhets A. (eds) Systems, Decision and Control in Energy III. Studies in Systems, Decision and Control, vol 399. Springer, Cham. https://doi.org/10.1007/978-3-030-87675-3_14,
13. M. K. Maheshwari, M.Agiwal, N. Saxena, R. Abhishek. "Flexible Beamforming in 5G Wireless for Internet of Things”, in IETE Technical Review, 36:1, 3-16, DOI: 10.1080/02564602.2017.1381048, 2017. https://doi.org/10.1080/02564602.2017.1381048
14. M. Ivezic, L. Ivezic, “5G Security & Privacy Challenges” in 5G.Security Personal Blog, 2019.
    a. https://5g.security/cyber-kinetic/5g-security-privacy-challenges/
15. Yusof, R., Khairuddin, U., and Khalid, M., ‘A New Mutation Operation for Faster Convergence in Genetic Algorithm Feature Selection’,In International Journal of Innovative Computing, Information and Control, Vol. 18, No. 10, 2012, pp 7363-7380.
16. Ibrahim S. Shehu, Olumide S, Adewale, Muhammad B.”Vehicle Theft Alert and Location Identification Using GSM, GPS and Web Technologies”, in I.J. Information Technology and Computer Sciences, 2016, 7, 1-7.
        i. Published Online July 2016 in MECS (http://www.mecs-press.org/)
17. The EU Space Programme (Last Access: 10.12.2021)
    a. https://www.euspa.europa.eu/european-space/eu-space-programme
18. Hu Z, R. Odarchenko, S. Gnatyuk “Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior”, in I.J. Computer Network and Information Security, 2020, 6, 1-13
    a. Published Online December 2020 in MECS (http://www.mecs-press.org/)
19. M, Iavich, T. Kuchukhidze, S. Gnatyuk, “Novel Certification Method for Quantum Random Number Generators“, in I.J. Computer Network and Information Security, 2021, 3, 28-38
    a. Published Online June 2021 in MECS (http://www.mecs-press.org/)
20. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili// Novel Version of Merkle Cryptosystem// Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 4, 2017, p. 28-33
21. Giorgi Iashvili, Zhadyra Avkurova, Maksim Iavich, Madina Bauyrzhan, Avtandil Gagnidze, Sergiy Gnatyuk// Content-Based Machine Learning Approach for Hardware Vulnerabilities Identification System// International Conference on Computer Science, Engineering and Education Applications // Springer, Cham, No 23 2021, p. 117 - 126

Scientific and Practical Cyber Security Journal (SPCSJ) 7(2): 7-22 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, Wuhan, China, Department of Computer Science, Kaduna State University, Kaduna, Nigeria
Jinshuo liu, School of Cyberscience and Engineering, Wuhan University, Wuhan, China
Ezekia Gilliard, School of Cyberscience and Engineering, Wuhan University, Wuhan, China

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.

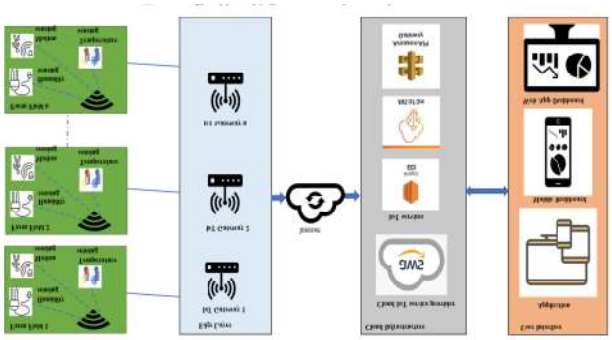


Fig. 1. Cloud-based IoT smart-agriculture application.

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.

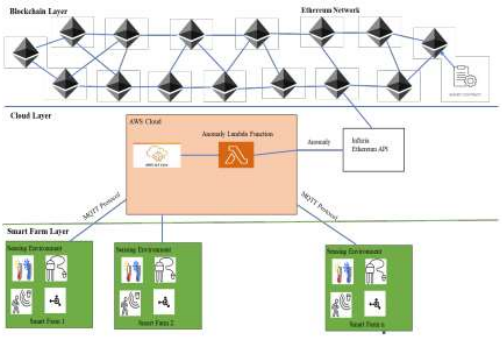


Fig. 2. Blockchain cloud-based smart-agriculture application.

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.

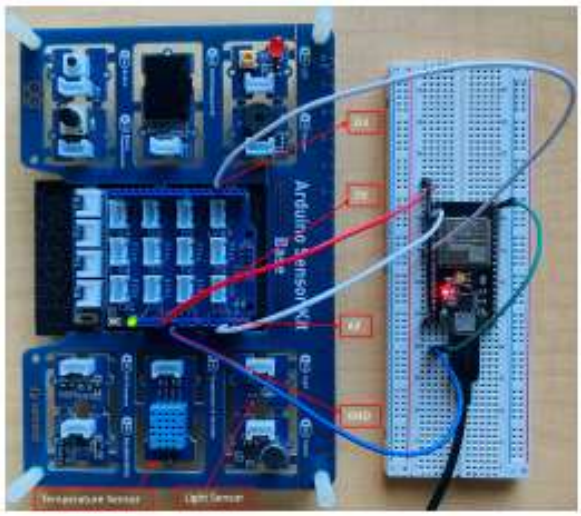


Fig. 3. Arduino sensor kit to sense the environment.

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.

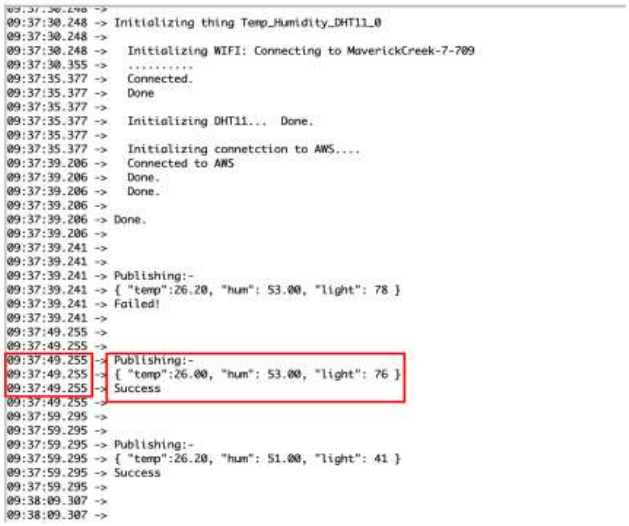


Fig. 4. Sensor devices connected to Wi-Fi and initializing connection to AWS Cloud.

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**.**

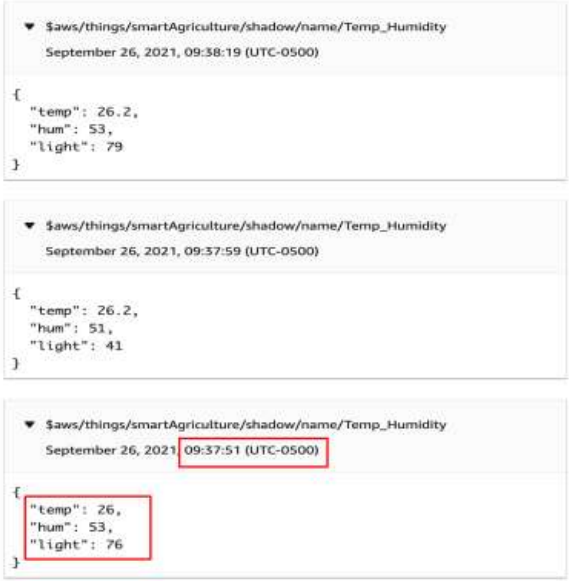


Figure 5. Sensor data real-time recording in AWS Cloud-IoT core service

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.

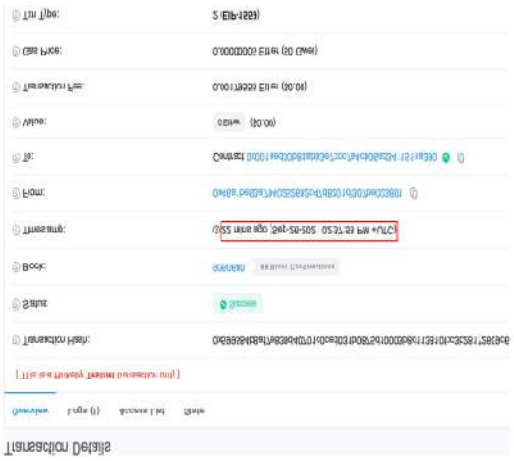


Figure 6. Ethereum smart-contract transaction details.

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.

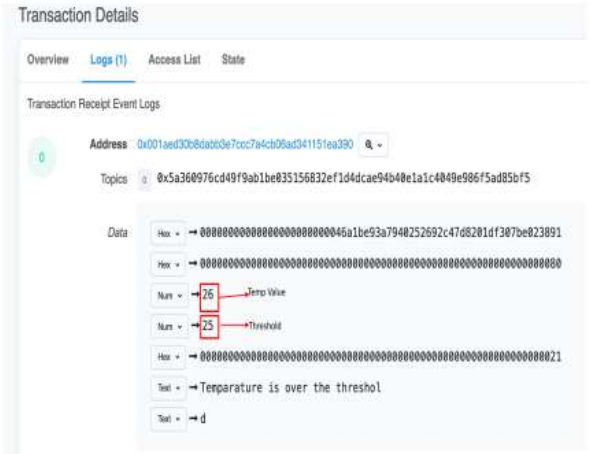


Figure 7. Ethereum smart-contract transaction storing the sensor data.

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.

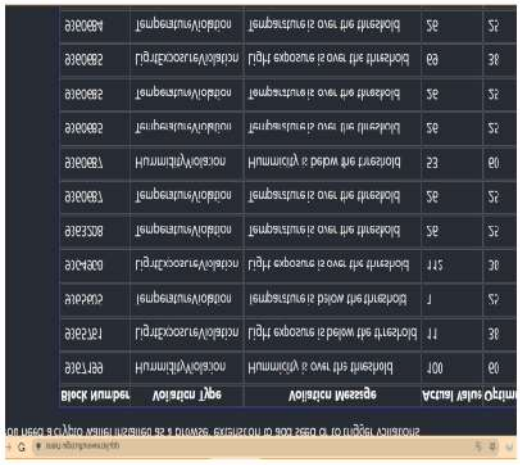


Fig. 8. Smart-contract web application frontend—alert notifications.

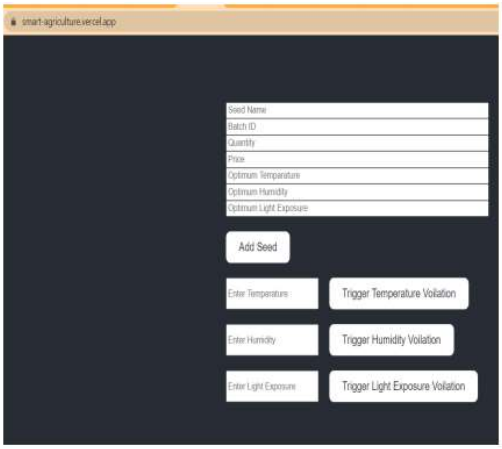


Fig. 9. Smart-contract web application—frontend GUI.

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]

Scientific and Practical Cyber Security Journal (SPCSJ) 7(2): 23-28 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

სარეკომენდაციო სისტემების გამოყენება კიბერუსაფრთხოების მიმართულებით

RECOMMENDER SYSTEMS USE IN CYBERSECURITY FIELD

Giorgi Iashvili – Caucasus University, Tbilisi, Georgia
Roman Odarchenko – National Aviation University, Kyiv, Ukraine
Sergii Gnatyuk - National Aviation University, Kyiv, Ukraine
Avtandil Gagnidze - East West University, Tbilisi, Georgia

აბსტრაქტი. ნაშრომი აღწერს ვებ-ზე დაფუძნებულ ინტეგრირებულ სისტემას, რომელიც აანალიზებს უსაფრთხოების პოტენციურ საკითხებს, რამაც შეიძლება გავლენა მოახდინოს გარკვეულ აპარატურაზე დაფუძნებულ სისტემაზე და, შესაბამისად, გვთავაზობს ოპტიმალურ გადაწყვეტილებებს. შემუშავებული სისტემა ტესტირება ხდება რეალურ სამყაროში ინდუსტრიული და კორპორატიული შემთხვევების გამოყენებით და შეფასების პროცესის შედეგი ადასტურებს, რომ მას შეუძლია მნიშვნელოვნად გააუმჯობესოს სისტემების კიბერუსაფრთხოების დონე, რომელიც ეკუთვნის სხვადასხვა ორგანიზაციებს. კვლევის შედეგად შეიქმნა ვებ-სისტემის პროტოტიპი, რომელიც აგროვებს ინფორმაციას თანამედროვე აპარატურასთან დაკავშირებული მოწყვლადობის შესახებ და აძლევს მომხმარებლებს შესაბამის რეკომენდაციებს კონკრეტული სიტუაციიდან გამომდინარე.

საკვანძო სიტყვები: *სარეკონებდაციო სისტემა, თადასხმის ანალიზი, მონაცეცმებთან მუშაობა;*

ABSTRACT. The paper describes an integrated web-based system that analyzes potential security issues that may affect a certain hardware-based system and therefore suggests optimal solutions. The developed system is tested using real-world industrial and corporate cases, and the result of the evaluation process confirms that it can significantly improve the level of cyber security of systems belonging to various organizations. As a result of the research, a prototype of a web system was created, which collects information about vulnerabilities related to modern hardware and provides users with appropriate recommendations based on a specific situation.

KEYWORDS: *recommender system, attacks analysis, work with data;*

შესავალი

კიბერუსაფრთხოების პრობლემატიკის გათვალისწინებით, გამოთვლითი სიჩქარე არის ერთ-ერთი მთავარი პრობლემა, რომელიც უნდა გადაიჭრას. პროცესორის არქიტექტურა

განსაზღვრავს მონაცემთა დამუშავების მახასიათებლებს და ზოგიერთ შემთხვევაში მთელი აპარატის შესაძლებლობებს. სხვადასხვა ფიზიკური არქიტექტურის გათვალისწინებით, პროცესორებს შეიძლება ჰქონდეთ გარკვეული შეზღუდვები, რამაც შეიძლება გამოიწვიოს შეუთავსებლობა ზოგიერთ დაკავშირებულ სისტემასთან, მათ შორის უსაფრთხოების შესაბამის მექანიზმებთან. გარდა ამისა, მნიშვნელოვანია აღინიშნოს, რომ ცენტრალური გადამამუშავებელი განყოფილების კარგად შემუშავებული არქიტექტურა საშუალებას აძლევს ახალი აპარატურის დანერგვას თანამედროვე სისტემებში, როგორიცაა მიკროარქიტექტურები და ენერგიის დაზოგვის ცენტრალური გადამამუშავებელი ერთეული. ეს გულისხმობს, რომ არსებული პროგრამული უზრუნველყოფა შეიძლება იმუშაოს ახალ აპარატურულ პლატფორმებზე. მაგრამ დღესდღეობით აპარატურაზე ორიენტირებული შეტევები საკმაოდ პოპულარულია. აპარატურაზე დაფუძნებული სისტემების დიდი ნაწილი დაუცველია თუნდაც მარტივი ფიზიკური შეტევებისა და გვერდითი არხის შეტევების მიმართ.

გვერდითი არხის შეტევების დროს, როდესაც შეყვანის სახით მიიღება შეტყობინება და გასაღები და გამოიყენება სტანდარტული კრიპტო ალგორითმი, ჩვენ მაინც შეგვიძლია მივიღოთ შიფრის გაჟონვა ტექნიკის პრობლემების გამო. სამუშაოს ამოცანა იყო არსებული აპარატურაზე ორიენტირებული შეტევების ანალიზი, ამ შეტევებით გამოწვეული მონაცემების გაჟონვის გამოთვლა და ტექნიკის შეთავაზება, რომელსაც შეუძლია შეამსუბუქოს ან აღმოფხვრა ეს გაჟონვა.

თანამედროვე მიდგომების განხილვა

კიბერუსაფრთხოებაში ცენტრალური პროცესორის გამოყენების საინტერესო მაგალითია Morpheus, რომელიც არის CPU-ის ახალი არქიტექტურა, რომელიც შეიქმნა მიჩიგანის უნივერსიტეტში 2019 წელს. Morpheus პროცესორის სპეციფიკური არქიტექტურის გათვალისწინებით, მას შეუძლია შეტევების დაბლოკვა მექანიზმის გამოყენებით, რომელიც მოიცავს დაშიფვრას და შემთხვევით გადაკეთებას საკუთარი კოდისა და მონაცემების გასაღების ბიტების წამში ოცჯერ. პრინციპში, ის უფრო სწრაფია, ვიდრე ყველაზე ეფექტური თანამედროვე ავტომატური ჰაკერების მექანიზმები და, ბუნებრივია, ბევრად უფრო სწრაფია, ვიდრე ნებისმიერ ადამიანს შეუძლია იმუშაოს. Morpheus არქიტექტურა შეიძლება გამოყენებულ იქნას სხვადასხვა პროგრამული და აპარატურის პლატფორმებისთვის, მათ შორის პორტატული და IoT მოწყობილობებისთვის. პროცესორის ეს არქიტექტურა ორიენტირებულია დეველოპერებზე და მომხმარებლებზე და დაფუძნებულია მონაცემების ბიტების რანდომიზაციაზე, რომლებიც ცნობილია როგორც განუსაზღვრელი სემანტიკა, რომელიც წარმოადგენს CPU არქიტექტურის სპეციალურ ნაწილებს, რომლებიც ეხება დაპროგრამებული აპლიკაციის კოდის ფორმატსა და შინაარსს. მორფეუსის არქიტექტურა ვერ აგვარებს კიბერუსაფრთხოების ყველა საკითხს, მაგრამ მისი არქიტექტურა ორიენტირებულია კონტროლის ნაკადის მთლიანობის შეტევებისგან დაცვაზე, როგორიცაა ბუფერული გადადინება.

დღევანდელი კიბერ სამყარო იცვლება ახალი ტენდენციებისა და მიმართულებების გავლენით. ამრიგად, კვლევისა და განვითარების ერთ-ერთი მნიშვნელოვანი მიმართულება წარმოდგენილია IoT ეკოსისტემით, რომელიც მნიშვნელოვნად განვითარდა ბოლო რამდენიმე წლის განმავლობაში. შესაბამისად, სმარტ მოწყობილობების მნიშვნელოვანი რაოდენობა გამოიყენება სხვადასხვა ინდუსტრიაში. ხშირ შემთხვევაში, ასეთი მოწყობილობები გამოიყენება ტექნიკური ან განმეორებითი ამოცანების შესასრულებლად, როგორიცაა მონაცემთა შეგროვება და ადეკვატური დახარისხება, ან შეტყობინებების გაგზავნა და მიღება. გარდა ამისა, არსებობს კომპლექსური ინდუსტრიული გარემო, რომელიც სარგებლობს IoT ქსელური ინფრასტრუქტურის საკმარისი სიმძლავრით და მრავალფეროვნებით, როგორიცაა თანამედროვე ავტომობილების ქარხნები, რომლებიც იყენებენ IoT-ზე დაფუძნებულ ჭკვიან სისტემებს მანქანების აწყობის პროცესში.

საინტერესოა აღინიშნოს, რომ მხოლოდ რამდენიმე წლის წინ, ინტეგრაციული კონცეფცია, როგორიცაა ჭკვიანი სახლი, აღიქმებოდა და მიდგომა მნიშვნელოვნად განსხვავებულად იქნა მიღებული, ვიდრე დღეს. ადრე ჭკვიანი მოწყობილობების კონცეფცია და იდეა უფრო ორიენტირებული იყო სხვადასხვა პროცესების ავტომატიზაციაზე. მიუხედავად ამისა, დღევანდელი IoT მოწყობილობები და მასთან დაკავშირებული ცნებები უფრო მეტად არის ორიენტირებული პრაქტიკული პრობლემების გადაჭრაზე უფრო ფართო მასშტაბით, როგორიცაა ბუნებრივი რესურსების გამოყენების შემცირების წვლილი.

IoT მოწყობილობების უსაფრთხოება. მთელ მსოფლიოში ჭკვიანი მოწყობილობების გამოყენების მნიშვნელოვანი ზრდის გათვალისწინებით, IoT-ზე დაფუძნებულ გამოთვლით გარემოზე მიმართული შეტევების რისკი მუდმივად იზრდება. IoT მოწყობილობებზე თავდასხმები დღეს ძალიან გავრცელებულია და ჭკვიანი მოწყობილობების ახალი მოდელებისა და მიდგომების შემუშავებით, თავდასხმები უფრო და უფრო ხშირი ხდება და, ასევე, უფრო მრავალმხრივი, იმის გათვალისწინებით, რომ მათ შეუძლიათ ადაპტირდნენ მიზნობრივი IoT მოწყობილობების სხვადასხვა პროგრამულ და აპარატურულ კონფიგურაციებთან. უმეტეს შემთხვევაში, ჭკვიან მოწყობილობებზე თავდასხმის მიზეზი არის მონაცემთა ცენტრების წვდომა, რომლებიც აკონტროლებენ მოწყობილობებს, რომლებიც ერთი ან მეტი ქსელის ნაწილია. სხვა გამოთვლითი სისტემების მსგავსად, IoT მოწყობილობები ასევე დაუცველია კიბერშეტევებისგან. შესაბამისი დაუცველობა შეიძლება დაიყოს სხვადასხვა კატეგორიად მათი განსხვავებული ბუნების მიხედვით. მაგალითად, ჩვეულებრივი შეჭრის ტექნიკა გულისხმობს ჰაკერის წვდომას ჭკვიან მოწყობილობაზე მოძველებული პროგრამული უზრუნველყოფის ან სპეციალური პროგრამული უზრუნველყოფის მიერ მართული აპარატურის შედეგად. ტექნიკის ხარვეზების აღმოჩენა და გამოსწორება ჩვეულებრივ ბევრად უფრო რთულია, ვიდრე პროგრამული ხარვეზები ან ხარვეზები. მნიშვნელოვანია თანამედროვე მოწყობილობებისთვის არსებული ტექნიკის უსაფრთხოების ზომების ყოვლისმომცველი ანალიზი. ახალი მიდგომები ამ მიმართულებით გაზრდის უსაფრთხოების არსებული საკითხების გაგებას და ხელს შეუწყობს ტექნიკის უსაფრთხოების მექანიზმების გაუმჯობესების მეთოდების შემუშავებას.

პოტენციური შეტევები IoT მოწყობილობებზე. დაკავშირებული ჭკვიანი მოწყობილობების ინფრასტრუქტურისა და მასთან დაკავშირებული სხვადასხვა ინდუსტრიების განვითარებამ ხელი შეუწყო სმარტ მოწყობილობების ინფრასტრუქტურაზე სხვადასხვა კიბერშეტევების სერიას, რომლებიც გამოიყენება სხვადასხვა ორგანიზაციაში. ბოლო რამდენიმე წლის განმავლობაში, ჰაკერებმა მოახდინეს დიდი რაოდენობით თავდასხმები IoT-ზე დაფუძნებულ ინფრასტრუქტურაზე მთელს მსოფლიოში. კვლევის ფარგლებში, რომელიც მოხსენებულია ამ ნაშრომში, ჩვენ გავაანალიზეთ ყველაზე გავრცელებული პოტენციური თავდასხმები IoT მოწყობილობებზე.

ინტერაქტიული ფორმა მოვლენების იდენტიფიცირებისთვის

სისტემა, რომელიც შემუშავებულია ჩვენი კვლევის ფარგლებში, აქვს შესაძლებლობა შეამოწმოს კონკრეტული კლასიკური, ინდუსტრიული, საოფისე ან IoT მოწყობილობების აპარატურა. წარმოდგენილი ამოცნობის სისტემა არის ვებ-აპლიკაცია, რომელიც ხელმისაწვდომია უფასოდ. შეფასების ნაგულისხმევი მეთოდი ეყრდნობა სანდო რესურსების სიის გამოყენებას, რომლებიც ინახება აპლიკაციის მონაცემთა ბაზაში. მონაცემთა ბაზა შედგება ინფორმაციისგან პოპულარული ონლაინ დაუცველობის აღმოჩენისა და მითითების პლატფორმებიდან, როგორიცაა AttackerKB , ExploitDB , CVE MITER და ეროვნული დაუცველობის მონაცემთა ბაზა.

სისტემა ეფუძნება ამ წყაროებიდან ყველაზე რელევანტურ ინფორმაციას. მონაცემთა ბაზაში შენახული მონაცემები ეხება შემდეგ კატეგორიებს: ახალი აპარატურაზე დაფუძნებული თავდასხმის ვექტორები, ახალი მოწყვლადობა არსებულ პროდუქტებში და უსაფრთხოების საკითხები Wireframes-ის მოძველებულ ვერსიებში. ამრიგად, შესაბამისი საძიებო მოთხოვნების გათვალისწინებით, სისტემა მომხმარებელს აწვდის ინფორმაციას აღნიშნულ პროდუქტში არსებული უსაფრთხოების საკითხების შესახებ, უსაფრთხოების დონის ამაღლების დეტალურ რეკომენდაციებთან ერთად.

ცნობილი დაუცველობისა და კიბერუსაფრთხოების მონაცემთა ბაზებიდან მოთხოვნებთან და ტენდენციებთან ერთად, სისტემა აგროვებს ინფორმაციას შიდა შემთხვევების შესახებ, სისტემის მომხმარებლების მიერ შესრულებული საძიებო მოთხოვნების საფუძველზე. სურათი 3 ასახავს რამდენიმე პოპულარულ საძიებო მოთხოვნას პლატფორმის ჩარჩოში და სისტემა ინახავს ადგილობრივ მონაცემთა ბაზაში. პლატფორმაზე მომხმარებლის ქცევის უკეთესი თვალყურის დევნებისთვის, მომხმარებლის შეყვანის ფორმა ხელმისაწვდომია მხოლოდ ავტორიზებული მომხმარებლებისთვის. თითოეულ მომხმარებელს აქვს პირადი პროფილი კონკრეტული სტატისტიკური მონაცემებით.

უპირველეს ყოვლისა, სისტემა ათავსებს ყველა ინფორმაციას აპარატურაზე დაფუძნებული პრობლემების შესახებ ზემოთ ნახსენები სანდო წყაროებიდან. შემდეგი ნაბიჯი არის შესაბამისი რეკომენდაციების გენერირება და შეგროვებული მონაცემების პრიორიტეტიზაცია. გათვალისწინებულია შემდეგი კრიტერიუმები: შესაბამისობა,

მითითების თარიღი, გავრცელება, ზოგადი ინფორმაცია და რისკის დონე. ყველა ეს პარამეტრი გამოიყენება კონკრეტული საკითხისთვის ყველაზე სასარგებლო და პრაქტიკული რეკომენდაციის შესაქმნელად. ჩვენ შევაგროვეთ მონაცემები, რომელიც ეფუძნება აპარატურულ თავდასხმებს შემდეგ კატეგორიებში: საოფისე აღჭურვილობა, სამრეწველო მოწყობილობები, IoT მოწყობილობები და კლასიკური მოწყობილობები, რომლებსაც იყენებენ საშუალო მომხმარებლები.

დასკვნა

მრავალი ბიზნესის ყოველდღიურ ოპერაციებში აპარატურაზე დაფუძნებული სისტემების მნიშვნელობის გათვალისწინებით, მოწყობილობის უსაფრთხოების მეთოდების გაძლიერება სისტემის შენარჩუნების სასიცოცხლო კომპონენტია. შედეგად, ჩვენ ვაპირებთ გავაძლიეროთ უსაფრთხოების საკითხების იდენტიფიკაციის სისტემის შესაძლებლობები ისეთი ვარიანტების მიწოდებით, რომლებიც მომხმარებლებს საშუალებას აძლევს აირჩიონ მომხმარებლის დონე. შედეგად, სისტემამ უნდა აირჩიოს შესაბამისი ტექნიკა აპარატურაზე დაფუძნებული სისტემის უსაფრთხოების არსებული პრობლემის გადასაჭრელად, მომხმარებლის განსაზღვრული უნარების დონის მიხედვით, გაზრდის ასეთი მეთოდის გამოყენებადობას კიბერუსაფრთხოების პრობლემების გადასაჭრელად ბიზნესის ფართო სპექტრში. გარდა ამისა, ალგორითმული ბირთვი დაემატება მანქანური სწავლების საჭირო ასპექტებს, რათა გააუმჯობესოს სისტემის მიერ გენერირებული ანგარიშების სარგებლიანობა, ისევე როგორც საბოლოო მომხმარებლების საერთო გამოცდილება.

შედეგად, კონკრეტული ანალიზის პროცედურები შეისწავლის მონაცემთა ბაზაში არსებულ მონაცემებს, ასევე ახლად შეყვანილი მონაცემების გათვალისწინებით, გააერთიანებს არსებულ მონაცემებს და საბოლოოდ დაამატებს საჭირო დამატებით მონაცემებს მონაცემთა ბაზაში. საბოლოო მომხმარებლის პოპულარულ ძიებებზე დაფუძნებული მონაცემთა ახალი წყაროების ინტეგრირებით, ეს ტექნიკა ეფექტურად გაზრდის რეკომენდაციების შესაბამისობას.

კვლევის მიზანი, რომელიც მოხსენებულია ამ ნაშრომში, იყო გაერკვია აპარატურაზე დაფუძნებული მოწყობილობებისა და მასთან დაკავშირებული პროგრამული სისტემების სუსტი მხარეები, რათა გაუმჯობესებულიყო უსაფრთხოების აუცილებელი მექანიზმები. ამ პროცესში მომხმარებლის ჩართვა უსაფრთხოების მექანიზმის დაკალიბრებას უფრო ეფექტურს ხდის. საბოლოო მომხმარებლის უკეთესი განათლება უსაფრთხოების პრობლემებთან დაკავშირებით ზრდის მათი გამოვლენისა და შესაბამისი გადაწყვეტილებების პოვნის ალბათობას. შემუშავებული პროგრამული სისტემა დაეხმარება საბოლოო მომხმარებლებს უკეთ გააცნობიერონ უსაფრთხოების პრობლემების წყარო და სტრუქტურა , რათა მოხდეს სათანადო ზომების მიღება. თავდასხმის სტრატეგიები მუდმივად იცვლება და სისტემა, რომელიც წარმოდგენილია, შეუძლია დაეხმაროს მომხმარებლებს ოპტიმალური შემარბილებელი სტრატეგიების მიღებაში. გარდა ამისა,

სისტემა შესაფერისია უფრო დიდი ორგანიზაციების აპარატურული ინფრასტრუქტურის უზრუნველსაყოფად, რათა მკაცრი კანონებიც კი, როგორიცაა მონაცემთა დაცვის ზოგადი ევროპული რეგულაცია, სრულად იყოს გათვალისწინებული და ეფექტურად დანერგილი პრაქტიკაში.

ნაშრომი შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის დაფინანსებით FR-22-14060 პროექტის ფარგლებში

გამოყენებული ლიტერატურა

1. Gagnidze, A., Iavich, M., & Iashvili, G. (2017). A Roman Version of the Merkle's Cryptosystem. Proceedings of the National Academy of Sciences of Georgia, 11(4), 28–33.
2. Deogirikar, J., & Vidhate, A. (2017). Security Breaches in IoT: A Study. In Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud (pp. 32-37). Coimbatore, India: IEEE.
3. Ronen, E., & Shamir, A. (2016). Extended Functional Attacks on IoT Devices: The Case of Smart Lights. In Proceedings of the European Symposium on Research in Computer Security (pp. 3-12). Zarrabrücken, Germany: IEEE.
4. Iashvili, G., Iavich, M., Gagnidze, A., & Gnatyuk, S. (2020). Increasing the Usability of the TLS Certificates Generation Process Using Safe Design, CEUR Workshop Proceedings, 2698, 35-41.
5. Lukova-Chuiko, N., Fesenko, A., Papirna, H., & Gnatyuk, S. (2021). Risk Management as a Method of Protection Against Cyber Threats, CEUR Workshop Proceedings, 2833, 103-113.
6. Iavich, M., Gnatyuk, S., Odarchenko, R., Bocu, R., & Simonov, S. (2021). The Novel System of Attacks Detection in 5G. In Lecture Notes in Networks and Systems (Vol. 226, pp. 580-591).

Scientific and Practical Cyber Security Journal (SPCSJ) 7(2): 29-33 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

მანქანური მეთოდების გამოყენება სარეკომენდაციო სისტემებში
USE OF MACHINE LEARNING IN RECOMMENDER SYSTEMS

Giorgi Iashvili – Caucasus University, Tbilisi, Georgia
Roman Odarchenko – National Aviation University, Kyiv, Ukraine
Sergii Gnatyuk - National Aviation University, Kyiv, Ukraine
Avtandil Gagnidze - East West University, Tbilisi, Georgia

აბსტრაქტი მანქანური სწავლება და ხელოვნური ინტელექტი დღეს სულ უფრო გავრცელებული ხდება. ისინი გამოიყენება სხვადასხვა სფეროში, მათ შორის ენერგეტიკის, სამედიცინო და ფინანსური სექტორების, სხვადასხვა ამოცანების შესასრულებლად და ძირითადი არჩევანის დასახმარებლად. სხვა გამოყენებასთან ერთად, მანქანათმცოდნეობა და ხელოვნური ინტელექტი გამოიყენება მძლავრი სარეკომენდაციო ძრავების შესაქმნელად, რათა მომხმარებელს მიაწოდოს შესაბამისი რეკომენდაციები სხვადასხვა მიმართულებით, როგორიცაა ფილმების რეკომენდაციები, მეგობრების წინადადებები სოციალურ ქსელებში და მრავალი სხვა. ამ ნაშრომის მიზანი არის აპარატურაზე დაფუძნებული სისტემების და მასთან დაკავშირებული მექანიზმების მოწყვლადობის იდენტიფიცირება და გაგება, უსაფრთხოების შესაბამისი ზომების გასაუმჯობესებლად. ნაშრომის მიზანია განახლებული ამოცნობის სისტემის მოდელის შემუშავება, რათა გამოავლინოს აპარატურაზე დაფუძნებული ხარვეზები და მიაწოდოს მომხმარებლებს საჭირო რეკომენდაციები.

საკვანძო სიტყვები: *მანქანური სწავლება, კონტენტზე დაფუძნებული, დაუცველობის იდენტიფიკაცია;*

ABSTRACT Machine learning and artificial intelligence are becoming increasingly common today. They are used in a variety of fields, including the energy, medical and financial sectors, to perform a variety of tasks and assist with key choices. Among other applications, machine learning and artificial intelligence are used to build powerful recommendation engines to provide users with relevant recommendations in a variety of areas, such as movie recommendations, friend suggestions on social networks, and much more. The objective of this paper is to identify and understand the vulnerabilities of hardware-based systems and related mechanisms in order to improve appropriate security measures. The aim of this paper is to develop an updated detection system model to detect hardware-based faults and provide users with necessary recommendations.

KEYWORDS: *machine learning, content-based, vulnerability identification;*

შესავალი:

მანქანური სწავლება და ხელოვნური ინტელექტი დღეს სულ უფრო გავრცელებული ხდება. ისინი გამოიყენება სხვადასხვა სფეროებში, მათ შორის ენერგეტიკის, სამედიცინო და ფინანსური სექტორებში, სხვადასხვა ამოცანების შესასრულებლად. სხვა გამოყენებასთან ერთად, მანქანური სწავლება და ხელოვნური ინტელექტი გამოიყენება მძლავრი სარეკომენდაციო სისტემების შესაქმნელად, რათა მომხმარებელს მიაწოდოს შესაბამისი რეკომენდაციები სხვადასხვა მიმართულებით, როგორიცაა ფილმების რეკომენდაციები, მეგობრების წინადადებები სოციალურ ქსელებში და მრავალი სხვა. კომპიუტერულ მეცნიერებაში არსებობს მრავალი გზა და მექანიზმი, რომლებიც იყენებენ კომპიუტერის ცენტრალურ პროცესორს (CPU). CPU-ს არქიტექტურა ასევე გადამწყვეტია კიბერუსაფრთხოების პროცესის შესრულების თვალსაზრისით. შედეგად, დღევანდელი პოპულარული ავტომატიზაციისა და

დაშიფვრის პროცედურები ეყრდნობა პროცესორის სიმძლავრეს კიბერუსაფრთხოების სხვადასხვა საკითხთან დაკავშირებით.

ეფექტური კიბერუსაფრთხოების მექანიზმების შემუშავება და დანერგვა არსებითად ეყრდნობა სათანადო ალგორითმული ბირთვების განხილვას. ამიტომ, უსაფრთხოების ალგორითმების შემუშავების მიზნით, რომლებიც უფრო ეფექტური და გამოსაყენებელია, განიხილება სხვადასხვა მიდგომები. ამრიგად, ავტომატიზაციის მექანიზმების ეფექტურობისა და უსაფრთხოების გაუმჯობესება შეიძლება განხორციელდეს მანქანის ცენტრალური დამუშავების ერთეულის ერთდროულად მუშაობისას სისტემის ზოგიერთ ასპექტზე შესაბამის პროგრამულ კომპონენტებთან ერთად. ამრიგად, CPU-ს ეფექტური გამოყენება შესაბამისი კიბერუსაფრთხოების მექანიზმების ოპტიმიზაციის მიზნით, გულისხმობს რამდენიმე ფაქტორის გათვალისწინებას.

ეს უფრო ფართო სამეცნიერო სფერო გულისხმობს რამდენიმე კვლევის თემის განხილვას, როგორიცაა ცენტრალური დამუშავების განყოფილების ფიზიკური განხორციელება, მონაცემთა ეფექტური გამოთვლა და მონაცემთა გადაცემის მეთოდები პროგრამულ კომპონენტებთან ან საბოლოო მომხმარებელთან კომუნიკაციის დროს. ნაშრომი სტრუქტურირებულია შემდეგი სექციების მიხედვით: მეორე განყოფილებაში განხილულია უსაფრთხოების მექანიზმი, რომელიც ჩამოყალიბებულია ცენტრალური პროცესორის დონეზე. გარდა ამისა, წარმოდგენილია თანამედროვე თავდასხმების ძირითადი ელემენტები, რომლებიც მიზნად ისახავს ცენტრალური პროცესორის სიმძლავრის გამოყენებას. გარდა ამისა, წარმოდგენილია უსაფრთხოების შესაბამისი მექანიზმი, რომელიც ეხება IoT-ის საზღვრებს, რის შემდეგ წარმოდგენილია აპარატურაზე დაფუძნებული დაუცველობის ამოცნობის ახალი სისტემა და შეფასებულია მისი პრაქტიკული შესრულება.

დღევანდელი მექნიზმების განხილვა

უსაფრთხოების თანამედროვე მექანიზმების განვითარების მიუხედავად, კიბერშეტევები სხვადასხვა სისტემაზე თითქმის ყოველდღე ხდება. თავდამსხმელები ცდილობენ გამოიყენონ ყოველთვის უფრო რთული და კრეატიული მეთოდები თავიანთი მიზნების მისაღწევად. შესაბამისად, დაუყოვნებლივ უნდა აღინიშნოს, რომ თანამედროვე პროგრამული უზრუნველყოფის და ტექნიკის დაცვის სქემების შემუშავებასთან ერთად იქმნება ახალი თავდასხმის ვექტორები, რომ ცნობილი ორგანიზაციებიც კი ხდებიან ჰაკერების სამიზნე. დღესდღეობით არსებობს უამრავი აპარატურაზე ორიენტირებული შეტევა სხვადასხვა კატეგორიაში. ამრიგად, ყველაზე გავრცელებული შეტევები, რომლებიც ძირითადად ეხება ცენტრალურ პროცესორს, არის DoS შეტევები და CPU-ს გვერდითი არხის შეტევები.

DoS შეტევები - DoS შეტევების კლასი აჯგუფებს უსაფრთხოების საფრთხეებს, რაც თითქმის შეუძლებელს ხდის ცენტრალური პროცესორის სწორ მუშაობას. ამრიგად, DoS შეტევა გულისხმობს, რომ გამოყენებულია ხელმისაწვდომი გადამამუშავებელი რესურსების მნიშვნელოვანი რაოდენობა, ისე, რომ ცენტრალური დამუშავების ერთეულის მოქმედება მნიშვნელოვნად მცირდება. თავდამსხმელს შეუძლია აიძულოს CPU მთლიანად შეწყვიტოს მუშაობა მთელი DoS შეტევების დროს. ასეთი მკვეთრი ეფექტი მიიღწევა პროცესორის რესურსების მეშვეობით, როგორიცაა რეგისტრების, ფუნქციური და ლოგიკური ერთეულების აქტიურ მდგომარეობაში შენახვით. შესაბამისად, ცენტრალური პროცესორის განყოფილება დაკავებულია და ვერ ასრულებს დამატებით დავალებებს. ზოგიერთ შემთხვევაში, ასეთი შეტევა ხელს უწყობს სტრუქტურის ხარვეზებს, რომლებიც ეხება ცენტრალური პროცესორის განყოფილების არქიტექტურას. ამრიგად, ასეთი შეტევები ხორციელდება გარე მოწყობილობების ენერგიის გამოყენებით.

IoT მოწყობილობები წარმოადგენს განხილული თავდასხმების პროგნოზირებულ სამიზნეს. კლასიკური DoS შეტევების გათვალისწინებით, ჰაკერები აკონტროლებენ სხვადასხვა მოწყობილობას, მათ შორის IoT პარამეტრებს. თავდამსხმელები ქმნიან ლოგიკურ სტრუქტურებს დაზარალებული IoT მოწყობილობებიდან, რომლებსაც ბოტნეტებს უწოდებენ და ისინი უგზავნიან უამრავ მავნე მოთხოვნას მსხვერპლს, რითაც ეფექტურად ქმნიან DoS შეტევას. ადგილობრივი ცენტრალური დამუშავების

ერთეულების შემთხვევაში, თავდამსხმელებს ასევე შეუძლიათ გამოიყენონ სპეციალური მავნე პროგრამები, რომლებიც აიძულებენ CPU-ს არქიტექტურულ დაუცველობას ჰაკერისთვის.

CPU-ს გვერდითი არხის შეტევები - კლასიკური გვერდითი არხის შეტევები ეფუძნება კრიპტოგრაფიული მექანიზმების დარღვევას და ინფორმაციის მიღებას დაშიფვრის სისტემის ფიზიკური იმპლემენტაციისგან. გვერდითი არხის შეტევები იყენებს კრიპტოგრაფიული მექანიზმების გაჟონულ ინფორმაციას, როგორიცაა დროის ინფორმაცია, ელექტრომაგნიტური გაჟონვა ან ენერგიის მოხმარება. ჩვეულებრივი გვერდითი არხის შეტევის ტიპიური მაგალითია დაშიფვრის გასაღების მოპარვის უნარი, რაც შეიძლება მიღწეული იყოს ჰაკერის მიერ სამიზნე მოწყობილობის ენერგიის მოხმარებაზე თვალთვალის გზით. გვერდითი არხის შეტევებმა ასევე შეიძლება ჰაკერებს მისცეს საშუალება დააკვირდნენ კომპიუტერის ეკრანის ელექტრომაგნიტურ ველს ან განახორციელონ აკუსტიკური შეტევა სამიზნე მოწყობილობის კლავიატურის ხმის ჩასაწერად, რათა მიიღონ შესაბამისი ფრაზები.

ცენტრალური დამუშავების ერთეულზე ორიენტირებული გვერდითი არხის შეტევები, როგორიცაა საზღვრების შემოწმების შემოვლითი, შეუძლია გამოიყენოს CPU ქეში, როგორც გვერდითი არხი. ეს შეტევა შეიძლება განხორციელდეს Intel-ზე, IBM-ზე და ARM-ის ზოგიერთ ცენტრალურ დამუშავების ერთეულზე. ასეთი თავდასხმის დროს ჰაკერები იღებენ მონაცემებს პროცესორის ქეში მეხსიერებიდან. შესაბამისად, თავდამსხმელს შეუძლია მიიღოს წვდომა კრიტიკულ მონაცემებზე იმით, რომ ერთ პროცესს საშუალებას აძლევს ამოიღოს ინფორმაცია სისტემაში აქტიური სხვა პროცესის მეხსიერებიდან. გარდა ამისა, ცენტრალური დამუშავების ერთეულზე ორიენტირებული გვერდითი არხის შეტევა იყენებს თანამედროვე Intel პროცესორების Rogue Data Cache Load (RDCL) დაუცველობას. ეს დაუცველობა საშუალებას აძლევს თავდამსხმელს აიძულოს მომხმარებლის პროცესები წაიკითხოს ბირთვის დაცული მეხსიერება, რითაც ეფექტურად გადალახოს უსაფრთხოების საზღვრები [1].

ცენტრალური დამუშავების ერთეულზე ორიენტირებული გვერდითი არხის შეტევა არის ZombieLoad Attack, რომელიც ძირითადად მიზნად ისახავს Intel-ის მიერ გამოშვებულ პროცესორების უახლეს ვერსიებს. შეტევა ეყრდნობა მიკროარქიტექტურული მონაცემების შერჩევის დაუცველობას, რომლებიც გამოიყენებოდა ინტელის პროცესორების წინასწარი თაობების წინასწარი შეტევებისთვის. ZombieLoad თავდასხმის დროს თავდამსხმელი იღებს წვდომას და კითხულობს სენსიტიურ ინფორმაციას, რომელიც ინახება ცენტრალურ დამუშავების განყოფილებაში.

დაუცველობა ეფუძნება პროცესორის მიერ შემოთავაზებულ ფუნქციას, რომელიც ცდილობს სისტემის მიერ გაცემული მომავალი ბრძანებების პროგნოზირებას და ამ მეთოდს ეწოდება სპეკულაციური შესრულება. ეს ფუნქცია საშუალებას აძლევს ცენტრალური დამუშავების ერთეულს უფრო სწრაფად იმუშაოს , მაგრამ ასევე შეუძლია თავდამსხმელებს საშუალება მისცეს ჩაჭრას მგრძნობიარე მონაცემები, როგორიცაა მომხმარებლის ინფორმაცია და პაროლები. შესაბამისად, Intel-მა გამოუშვა პატჩები, რომლებიც აგვარებენ მოწყვლადობას, მაგრამ ისინი ასევე აღიარებენ, რომ შესაბამისი შემარბილებელი ღონისძიებები სრულად ვერ აღკვეთს მგრძნობიარე მონაცემების გაჟონვას CPU-ზე ორიენტირებული გვერდითი არხის შეტევების დროს, როგორიცაა ZombieLoad Attack-ის ახალი ვერსია .

ფიზიკური თავდასხმების განხილვა

ფიზიკური შეტევები - ჰაკერისთვის მთავარი მიზანი წარმატებული შეტევის მიღწევაა, მაგრამ შეტევის შესაბამისი მეთოდები შეიძლება განსხვავდებოდეს. ფიზიკურ შეტევებს IoT მოწყობილობებზე ესაჭიროებათ უშუალო კონტაქტი მიზანთან. უმეტეს შემთხვევაში, ასეთი თავდასხმების შედეგი არის აპარატურის გატეხვა სხვადასხვა ფიზიკური ფაქტორების გამო. გარდა ამისა, ზოგიერთი IoT მოწყობილობა განთავსებულია შენობების გარეთ და ძალიან მგრძნობიარეა ფიზიკური შეტევების მიმართ.

სადაზვერვო შეტევები – IoT მოწყობილობებზე ასეთი თავდასხმის დროს ჰაკერები არ ახორციელებენ ავტორიზებულ მანიპულაციებს სისტემასთან ან ქსელთან მიმართებაში. ამრიგად, სადაზვერვო შეტევები შეიძლება შედგებოდეს პორტის სკანირებით, პაკეტების ამოცნობით და ქსელის ტრაფიკის ანალიზით.

Distributed Denial-of-Service (DDoS) თავდასხმები – თავდასხმის ყველაზე პოპულარული სახეობა, რომელიც ჩვეულებრივ ხორციელდება უკვე ინფიცირებული მოწყობილობების (ბოტნეტის) გამოყენებით და ორიენტირებულია ერთ კონკრეტულ სამიზნეზე. ასეთი თავდასხმების მიზანია სერვისის ან მოწყობილობის მიუწვდომელი გახადოს დიდი რაოდენობით არალეგიტიმური მოთხოვნების გაგზავნით, რაც ქმნის მავნე ტრაფიკის ნაკადს მიზნობრივი სისტემებისთვის.

წვდომის შეტევები – ამ კატეგორიის თავდასხმის გათვალისწინებით, ჰაკერი იძენს არაავტორიზებულ წვდომას გარკვეულ ქსელებსა თუ მოწყობილობებზე. წვდომის შეტევები შეიძლება განხორციელდეს ორი განსხვავებული გზით: სისტემაზე ფიზიკური წვდომით ან დისტანციურად. ცხადია, მეორე მეთოდი ნაკლებად სარისკოა თავდამსხმელისთვის, შესაბამისად, უფრო ხშირად გამოიყენება ვიდრე პირველი.

თავდასხმები კონფიდენციალურობაზე - კონფიდენციალურობის დაცვა IoT-ის კონტექსტში ძალიან რთულია ინფორმაციის დიდი მოცულობის გამო, რომელიც ადვილად ხელმისაწვდომია დისტანციური წვდომის არხებით. ამრიგად, კონფიდენციალურობაზე პოპულარული თავდასხმები წარმოდგენილია მონაცემთა მოპოვებით და კიბერ ჯაშუშობით.

ექსპერიმენტები

არსებული პრობლემების გათვალისწინებით, რომლებიც დაკავშირებულია აპარატურულ ინფრასტრუქტურასთან, განსაკუთრებით დიდ ორგანიზაციებში, ძალზე მნიშვნელოვანია იმ მოწყობილობებზე თავდასხმების პრევენციის გზების პოვნა, რომლებიც უმეტეს შემთხვევაში კონფიდენციალურ ინფორმაციას ინახავს და გადასცემს. აპარატურაზე ორიენტირებული შეტევების განხორციელების შესაძლებლობა თუნდაც დისტანციურად აყენებს დიდი რაოდენობით სისტემებს რისკის ქვეშ. ბუნებრივია დავასკვნათ, რომ აპარატურა არის ძალიან მნიშვნელოვანი კვლევის მიმართულება კიბერუსაფრთხოების სფეროში, რომელსაც დიდი ყურადღება სჭირდება როგორც საბოლოო მომხმარებლების, ასევე მწარმოებლების მხრიდან. გარდა ამისა, აუცილებელია იმ პროცესების ეფექტური და ზუსტი მენეჯმენტის უზრუნველყოფა, რომლებიც მხარდაჭერილია სპეციალიზებული აპარატურით, როგორიცაა IoT-ზე დაფუძნებული სისტემები, რომლებიც აკონტროლებენ სამრეწველო მანქანებს ან ახორციელებენ მაღაზიების მენეჯმენტს. ამრიგად, რთული პროცესია უსაფრთხოების სტანდარტული მექანიზმის შექმნა, რომელიც გამოიყენება ნებისმიერი თანამედროვე აპარატურაზე ორიენტირებული სისტემისთვის. მწარმოებლები, რომლებიც იყენებენ არსებულ სტანდარტებს მიკრო სქემების და ტექნიკის ნაწილების შესაქმნელად, რომლებიც ძირითადად იმართება სპეციალური პროგრამული კომპონენტებით. პროგრამული უზრუნველყოფა შეიძლება შეიქმნას კონკრეტული სისტემის ან სისტემების ჯგუფისთვის.

დასკვნა

დღეისთვის არსებული სარეკომენდაციო მექანიზმები შესაძლებელია მოერგოს კიბერუსაფრთხოების მიმართულებას და იქნეს გამოყენებული სხვადასხვა ტიპის თავდასხმების ვექტორების იდენტიფიცირებისთვის და შემდგომი პრევენციისთვის.

საჭიროა მეტი მუშაობა ჩატარდეს ამ მიმართულებით. ერთ-ერთი რეალური ვარიანტი ამ სფეროს განვიტარებისა არის ახალი, კიბერუსაფრთხოების სფეროზე მორგებული სისტემის შემუშავება, რომელიც იქნება გამოყენებადი სხვადასხვა კიბერ თავდასხმების ან / და სხვა ინციდენტებზე რეაგირების თანამედროვე მეთოდი.

ნაშრომი შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის დაფინანსებით FR-22-14060 პროექტის ფარგლებში

გამოყენებული ლიტერატურა

1. Taehyun, K., & Youngjoo, S. (2019). Reinforcing Meltdown Attack with the Use of Return Stack Buffer. IEEE Access, 2019, 186065–186077. DOI: 10.1109/ACCESS.2019.29
2. Schwarz, M., Lipp, M., Moghimi, D., et al. (2019). ZombieLoad: Cross-Privilege-Boundary Data Sampling. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (pp. 753–768). London, UK.
3. Clavier, C., Coron, JS., & Dabbous, N. (2000). Differential Power Analysis with Countermeasures against Techniques. In CHES Proceedings (pp. 252–263). Worcester, MA.
4. Schaumont, P., & Tiri, K. (2007). Masking and dual-rail logic don't add up. In Proceedings of Cryptographic Hardware and Embedded Systems (pp. 95–106). Vienna, Austria.
5. Abomhara, M., & Køien, G. M. (2015). Cybersecurity and Internet of Things: Challenges, Risks, Protection, and Safety Measures. Journal of Cybersecurity and Mobility, 4(1), 65-68.
6. Iavich, M., Gnatyuk, S., Odarchenko, R., Bocu, R., Simonov, S. (2021). The Novel System of Attacks Detection in 5G. In: Barolli, L., Woungang, I., Enokido, T. (eds) Advanced Information Networking and Applications. AINA 2021. Lecture Notes in Networks and Systems, vol 226. Springer, Cham. https://doi.org/10.1007/978-3-030-75075-6_47
7. Iavich, M., Iashvili, G., Gnatyuk, S., Tolbatov, A., Mirtskhulava, L. (2021). Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. In: Lopata, A., Gudonienė, D., Butkienė, R. (eds) Information and Software Technologies. ICIST 2021. Communications in Computer and Information Science, vol 1486. Springer, Cham. https://doi.org/10.1007/978-3-030-88304-1_15

Scientific and Practical Cyber Security Journal (SPCSJ) 7(2): 34-44 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

MALICIOUS ANDROID APPS DETECTION USING MACHINE LEARNING

Bilal Ahmad Kamal, Adeela Muhammad Askari, Salman Tariq
Air University Islamabad Pakistan

ABSTRACT: The use of smartphones has wisely evolved in the 20th century. Many people all over the world can connect to their smartphones in a variety of ways. Some invaders are leveraging the power of the rapidly growing smartphone usage to Developing rogue Android applications to steal handsets' sensitive data To address these grave issues, a malicious program that is both effective and efficient is required. Numerous malware detection programs have historically been built, but some of them are not able to identify recently developed malware programs or programs contaminated with different Trojan horses, worms, and spyware. The software for detecting fraudulent programs can be enhanced especially thanks to ML algorithms.

The system uses ML classification algorithms like Support Vector Machine (SVM) to improve the malware application detection in the proposed system. The proposed ML classification and fusion algorithms will improve performance metrics like the accuracy of malware application exposure and decrease the complexity of the detection process. The suggested approach integrates detecting software with a training application that users can install on Android cellphones to flag hazardous activities when they are accessible.

KEYWORDS: *support vector machine, ML, Android Apps, malicious*

1. INTRODUCTION

Smartphone usage has been gradually increasing in recent years, along with the growth of Android app users. Given the rise in Android app users, hackers are developing malicious Android apps as a tool to steal sensitive data and commit identity theft/fraud on mobile wallets and banks. Tools and software for detecting malicious applications are widely accessible. However, to deal with and handle increasingly sophisticated harmful apps developed by intruders or hackers, malicious application detection systems must be effective and efficient.

In this project, we created a strategy for detecting anomalous Android apps using machine learning methods.

We must first generate a dataset of previously infected applications as a training set. Then, using the Supervised Learning method, we must compare the training dataset with the trained information to forecast the malware Android apps up to 95.2% of the time.

1.1 Machine Learning

Machine learning is a study that involves feeding data and knowledge in the form of observations and in-person interactions into computers so they can learn better over time and autonomously. The goal of machine learning is demonstrated by the

aforementioned sentence. The main thought behind machine learning is to give computers knowledge through data so they can interact and observe the outside world. Machine learning is a subset of machine intelligence. It will let the computer learn and prepare itself to carry out numerous tasks much like a person. In machine learning, there are so many different types of algorithms that can be distinguished based on how they learn or by similarities in their design or functionality. The following variables are present in all possible combinations of machine learning algorithms. This is also the fundamental idea to comprehend the field. The variables that aid in comprehending machine learning principles are representation, evaluation, and optimization. To help a computer learn, representation is a collection of classifiers or machine language. Finding a scoring function is done through the process of evaluation. The final search optimization technique is frequently referred to as the classifier with the greatest score. According to the aforementioned metrics, the primary goal of algorithms is to generalize beyond the training samples themselves in order to obtain high-quality analysis data that has never been used. Although there are numerous distinct and various ways to train a machine, from employing

We must choose the best learning algorithm that may improve performance and provide us with the correct accuracy of the clustering to decision tree, two layers of ANN (Artificial Neural Network).

outcome. Because of their computing capability, reading machines are frequently helpful to humans. where computing forces can quickly spot trends and even highlight the key

features in a massive data set that humans would have otherwise overlooked. Humans frequently utilize machine learning to enhance their problem-solving skills, and many systems employ it to develop educated advisors on a range of issues.

1.2 Mobile Malware

Mobile malware is malicious software that targets mobile devices, especially wireless smartphones and Personal Digital Assistants (PDA). With the rise in popularity and complexity of PDA networks and wireless mobile devices, it has become more challenging to maintain protection and security from electronic attacks like viruses, worms, and other malware. Malicious software, commonly referred to as malware, is intended to attack a mobile device, such as a smartphone or tablet, in order to harm or interrupt it. The majority of mobile malware is made to compromise smartphones, allow criminal users to remotely manage them, and steal the user's personal data that is kept on the device.

All of our contact information as well as many other entries on our smartphone could be accessed by or deleted by mobile viruses. It could send an infected SMS to each and every phone in your contact list.

call directory and grow on your side over the network. Fraudulent phone bills, obtaining unsuitable content, and losing highly essential data that is saved on the smartphone are the top three issues that worry mobile consumers. Mobile devices have historically been utilised primarily for the programs that are built into them, or more recently, for malware that has been put into smartphones. As the demand for apps grows, hackers today insert several malwares inside applications. Once the programme is downloaded and installed on a smartphone, the malware runs and fixes itself to the device and may transfer a lot of personal data about the user without their knowledge or consent. Malware in applications has grown to be one of the biggest issues facing people today.

2. APPROACHES RELATED TO MALWARE DETECTION

The earlier research studies examine malware detection in smartphone harmful Android applications. The many methods for detecting malware are covered in this section.

A simple yet effective method for malware detection that specifies the Android APIs sub-set as classification functions was proposed by Jaemin Jung et al. in "Detecting Malicious Android Apps using API's Popularity and Relationships" [1]. The number of APIs utilised in an app is its feature because it depends on the use of a number of Android APIs to achieve its main goal. Their methodology creates two rating Android API lists: one for safe APIs and one for dangerous APIs. The most often used APIs by good applications are included in the benign API list, whereas the most frequently used APIs are included in the harmful API list. If the number of inverse values based on benign apps is more than the amount based on hazardous devices, they conclude that the device being offered is fine and determine whether the gadget is benign or harmful by comparing the two numbers. They will then presume that the presented system is malevolent. For the detection of Android malware, the suggested technique obtains an accuracy of 87.35 percent to 89.93 percent. However, it has a low detection accuracy and cannot quickly detect freshly developed malware. Android Malware Detection Using Parallel Machine Learning Classifiers, Suleiman et al., [2]. Droid Fusion can be used with both ensemble learners and traditional method students. They recommend using algorithms based on four rankings to combine the learners. The methods are utilized to provide a finished, better classification model for Android malware detection. A fusion classifier strategy that frequently focuses on multilevel architecture, the results of a Droid Fusion performance comparison with layered generalization. This is utilized to enhance the algorithm as well as to employ an ensemble of the algorithm and random forest learning.

It is challenging to identify which harmful or recently updated software is present. Their algorithms are becoming more complicated. "Pin droid: A revolutionary Android malware detection system employing ensemble learning approaches," Idrees et al., [3]

They employed features like permissions and tries to enhance performance categorization and train machine learning models. They started their tests on a variety of device samples by contrasting the results of different algorithms like decision tables, decision trees, and random forests. The decision table, MLP, and decision tree classifiers were then combined using two different approaches. The algorithm is improved using this application, and efficiency is also improved using ensemble learning algorithms like the random forest algorithm. It is challenging to determine whether a programmer is recently updated or maliciously produced. This is not being used in a real-time environment. "Feature Selection and ensemble of classifiers for Android malware detection," Coronado et al., [4]. For the committee, they proposed and investigated a hybrid classifier strategy based on random forest and random group classifiers. In their method, a task that creates a model Meta ensemble incorporates random forest. For efficiency, learning methods like random forest algorithms are used. less training data sets were used. This is not carried out in real-time settings. Malicious programs that have just been updated or created are difficult to identify. "Machine learning helped Android malware classification," Milosevic et al., [5]. The tested classification fusion methodology based on Android permissions and source code-based analysis with static method is mentioned in the study. They employed classifiers like JRip, JRandom Forests, and linear regression. However, the experiments only employed a small sample of data.

The JRip method is applied to classification fusion in order to better both the algorithm itself and ensemble learning algorithms like random forests. This system does not operate in authentic. With a machine learning approach like SVM and L2 linear classifiers, Lindorfer et al., [6] "MARVIN: Efficient and comprehensive mobile app classification through static and dynamic analysis." This research examines a thorough and effective classification of mobile applications. The system rates the likelihood of malicious activity in a scale from 0 to 10 for various untested Android applications. Despite employing an efficient algorithm, they were unable to produce an exact result.

3. CURRENT MALWARE IDENTIFICATION APPROACHES

Many Android malware detection technologies have historically been created, but some of these solutions are not able to identify newly created malicious applications or malware applications that have been infected with different Trojan, worms, spyware, etc. The detection of several harmful applications among the millions of Android applications is still a difficult process when done the old-fashioned method. Additionally, in the current system, non-machine learning techniques for identifying

malicious applications based on their traits, traits, and behaviours have been created, although the accuracy of diagnosis is still low.

3.1 Issues in the Current System

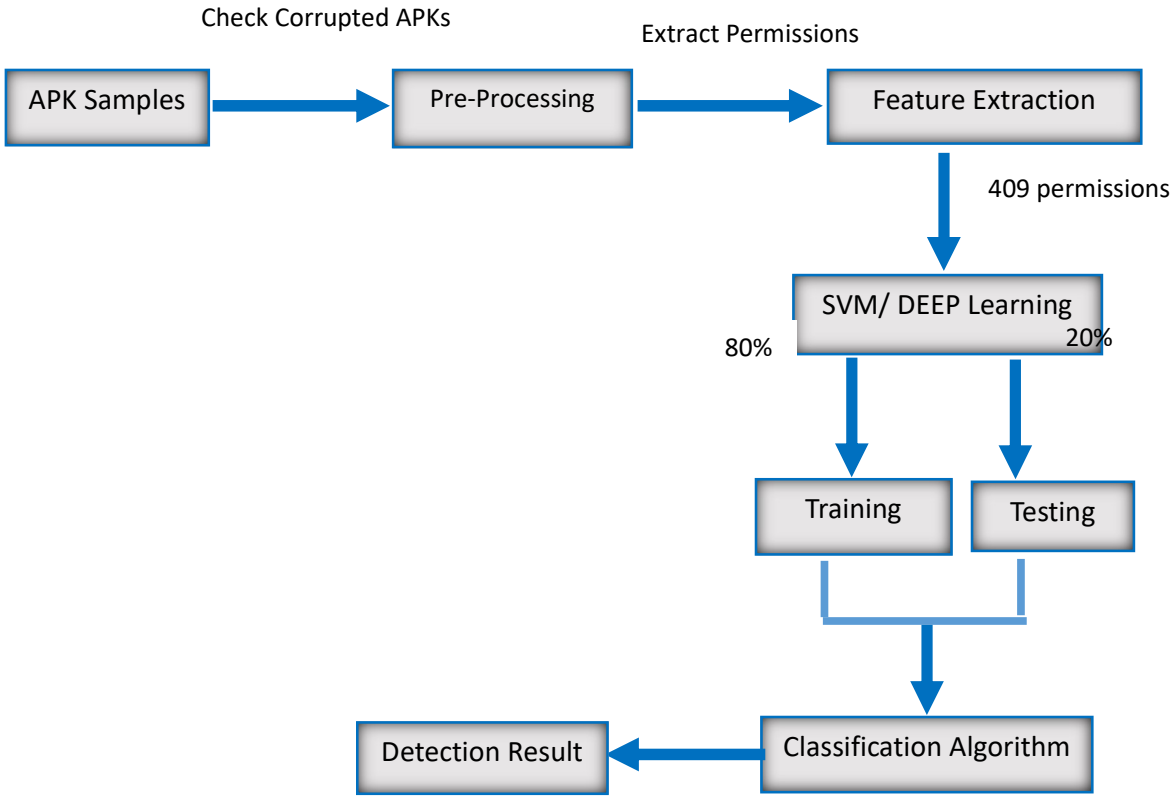
The detection of several harmful applications among the millions of Android applications is still a difficult process when done the old-fashioned method. This demonstrates that the technique for Android malware detection [12] using popular ML algorithms like random forest, K-means, does not accurately detect any other new malware. However, only detection was unable to show us how detection functions in a real-time setting. As we all know, the real-time view is crucial for giving us an authentic perspective of the software that has developed over the course of detection with the provided datasets, but when it comes to a real-time mobile device, it should be able to gather the datasets and identify malicious applications on its own.

4. MACHINE LEARNING CLASSIFIERS FOR MALWARE APP DETECTION

Classification techniques, the Support Vector Machine (SVM) system, is used in the proposed system to improve malware detection. The suggested ML classification and fusion techniques will effectively enhance the detection of malware applications and will improve performance metrics like the accuracy of revealing the malware applications and reducing detection time complexity. The suggested approach integrates the detection software into a trained application that can be installed on an Android smartphone and can identify dangerous applications in a smartphone user's accessibility from the beginning. The benefits of the suggested system include its reliability, ease of identifying newly updated or created malicious Android applications, effective and efficient detection, an increase in accuracy for exposing Android malware applications from 95% to 99%, and a decrease in time complexity for detection. Additionally, the system covers more program privileges so that we may find malware even in unexpected places. The original view of the software's method of machine learning is provided via real-time application.

Implementation Diagram

At first stage, we provided apk samples to check corrupted apks and comes pre-processing to Extract Permissions. After extracting Permissions, we began to find 409 permissions whereas SVM/DEEP learning is used. After that Training and Testing was performed. Then it goes with Classification Algorithm and Detection results as drawn below.



SVM System.

It depicts the data classification and fusion system procedure. Fusion of classifications occurs in this module. To improve prediction accuracy, two or more classification algorithms are combined in a process called classification fusion. Most frequently, very accurate classified data are used. Due to the fact that we are utilizing algorithms—SVM. Therefore, by using this approach, we are enhancing the accuracy of the detection of malware from 95% to 99%, which can efficiently and effectively detect the malware in an application. The SVM method is a method in that fusion, where here each classified result from the algorithm is taken and by means of the SVM () the classification algorithm with high accuracy and consistency is voted and a further percentage of accuracy is drawn. In many existing works they have considered

ranking method whereas in our case we are considering the SVM method. By means of this SVM the detection of malware in real time is also increased.

Malware Detection

The malware detection module procedure is depicted in, the real-time view is crucial for giving us a fresh perspective on the software that has learnbeened through dataset-based detection, but when it comes to a real-time mobile device, it should be able to gather the datasets and identify harmful applications on its own. Therefore, in our suggested method, we are integrating the detection software into a training application to install into an Android smartphone and identify the malicious application in an original view for the accessibility of the end users. The apps display the malicious and innocent scores for the app; if the malicious score is higher than the innocent score, "POTENTIAL THREAT" is displayed; otherwise, "SAFE" is displayed. Here, the malevolent score is determined by averaging Type 1 permissions, while the innocence score is determined by averaging Type 0 privileges.

Performance Analysis

Performance Evaluation

The efficiency of several categorization modules is shown in the aforementioned. These modules are improved and studied to produce effective results by comparing with the current and suggested techniques in the detecting attacks, such as:

Malicious App Identification Efficiency

Malware detection speed allows for quick and accurate identification of malware applications. With the suggested algorithms, such as SVM, detection is accomplished successfully and efficiently. For quick and accurate malware app detection, it covers additional app permissions.

Effectiveness of Malicious App Screening

Malicious detection accuracy demonstrates how each everything change's accuracy affects our ability to recognize malware apps. Methods based on machine learning are more trustworthy. The data fusion concept also improves the accuracy of revealing the infected application.

Malicious Software Detector Period

The length of time it took for an application to identify a smartphone's malware app is provided by the malware detection time. There is less time complexity for detection. The classification fusion technique improves app detection performance and speeds up the process.

5. EXPERIMENTAL EVALUATION

The suggested solution integrates the detection software into a training program by installing it into an Android smartphone using the Android Studio IDE and detecting the malicious application in a first-person perspective of the end user accessibility in smartphones. The malicious score and innocence score of the app are displayed in a safe real-time application, which displays "SAFE" if the malicious score is lower than the innocent score and "POTENTIAL THREAT" if the malicious score is higher than the innocence score. In this case, the malevolent score is determined by averaging Type 1 permissions, while the innocence score is determined by averaging Type 0 rights. By computing the entire permission score, it will also display the app's overall goodness %. The application is now prepared to find any malware that may be installed on smartphones.

Android Malicious Application Detection SVM, Version

The number of Malware Apps Found Compared to the Number of Mobile Apps Figure above compares the quantity of legitimate mobile apps to the quantity of malware-identified apps. It also demonstrates how SVM, improves the accuracy of malware program identification. The SVM has the highest accuracy in the Neural Network. The analysis shows clearly that the number of malware apps identified has been in increasing numbers with the SVM algorithm.

		Actual	
		Positive	Negative
Predicted	Positive	1480	8
	Negative	7	860

Figure. No. of Malware APPs identified Vs No. of Mobile Apps

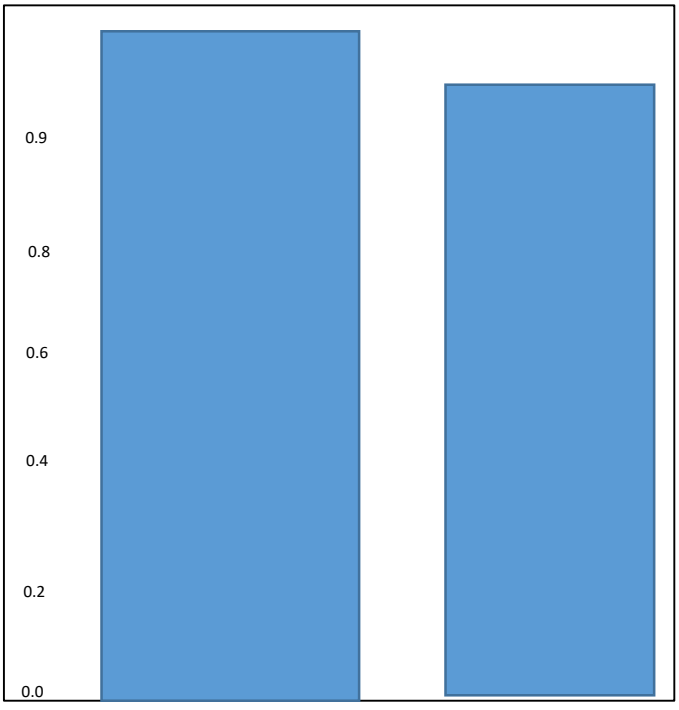
Data Accuracy (%) vs. Number of Malware Apps Identified

The amount of malware programs found about data accuracy is shown above. This graph displays the SVM algorithm's data accuracy for identifying all malicious apps. The Positive is regarded to be the data accuracy in percentage and the Negative is considered to be the number of malware applications found for all three methods, giving us an accurate result for detecting the proper amount of malware apps with high type 1 permissions.

Data Accuracy

The accuracy above displays the performance of each classification technique, including, SVM.

Figure. Data Accuracy



CONCLUSION AND FUTURE WORK

One of a user's primary sources of income is now a smartphone. A person's complete details and data sources are now available on his or her smartphone for everyday use as smartphone usage grows. In that situation, an outside intruder could learn a lot about a user just installing the malicious application in the smartphone, making smartphone security one of the day's biggest issues of the day. As for as Future work is concerned, we can increase Neural Network accuracy from 92% which would be a great addition.

BIBLIOGRAPHY

1. Vinod, P., Zemmari, A., & Conti, M. (2019). A machine learning based approach to detect malicious Android apps using discriminant system calls. Future Generation Computer Systems, 94, 333-350.
2. Xiao, J. X., Lu, Z. C., & Xu, Q. H. (2018, December). A new Android malicious application detection method using feature importance score. In Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence (pp. 145-150).
3. Kambar, M. E. Z. N., Esmaeilzadeh, A., Kim, Y., & Taghva, K. (2022, January). A survey on mobile malware detection methods using machine learning. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0215-0221). IEEE.
4. Arslan, R. S. (2021). AndroAnalyzer: Android malicious software detection based on deep learning. PeerJ Computer Science, 7, e533.
5. Jiang, X., Mao, B., Guan, J., & Huang, X. (2020). Android malware detection using fine-grained features. Scientific Programming, 2020.
6. de la Puerta, J. G., Pastor-López, I., Porto, I., Sanz, B., & Bringas, P. G. (2021). Detecting malicious Android applications based on the network packets generated. Neurocomputing, 456, 629-636.
7. Mohamed, S. E., Ashaf, M., Ehab, A., Shereef, O., Metwaie, H., & Amer, E. (2021, May). Detecting Malicious Android Applications Based On API calls and Permissions Using Machine learning Algorithms. In 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (pp. 1-6). IEEE.
8. Jung, J., Lim, K., Kim, B., Cho, S. J., Han, S., & Suh, K. (2019, June). Detecting malicious Android apps using the popularity and relations of APIs. In 2019 IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering (AIKE) (pp. 309-312). IEEE.
9. Razgallah, A., Khoury, R., Hallé, S., & Khanmohammadi, K. (2021). A survey of malware detection in Android apps: Recommendations and perspectives for future research. Computer Science Review, 39, 100358.
10. OS, J. N. (2021). Detection of malicious Android applications using Ontology-based intelligent model in mobile cloud environment. Journal of Information Security and Applications, 58, 102751.

11. Liu, L., Ren, W., Xie, F., Yi, S., Yi, J., & Jia, P. (2021). Learning-Based Detection for Malicious Android Application Using Code Vectorization. Security and Communication Networks, 2021.

12. Sharma, T., & Rattan, D. (2021). Malicious application detection in Android—a systematic literature review. Computer Science Review, 40, 100373.

13. Song, Y., Geng, Y., Wang, J., Gao, S., & Shi, W. (2021). Permission Sensitivity-Based Malicious Application Detection for Android. Security and Communication Networks, 2021.

14. Chen, X. R., Shi, S. S., Xie, C. L., Yang, Z., Guo, Y. J., Fang, Y., & Wen, W. P. (2021, February). SUIP: An Android malware detection method based on data flow features. In Journal of Physics: Conference Series (Vol. 1812, No. 1, p. 012010). IOP Publishing.

15. Sembera, V., Paquet-Clouston, M., Garcia, S., & Erquiaga, M. J. UNCOVERING AUTOMATIC OBFUSCATION-AS-A-SERVICE FOR MALICIOUS ANDROID APPLICATIONS.