SECURITY ANALYSIS THREATS, ATTACKS, MITIGATIONS AND ITS IMPACT ON THE INTERNET OF THINGS (IOT)

Alireza Nik Aein Koupaei,
Moscow Institute of Physics and Technology -MIPT (State University), Moscow region, Dolgoprudny, Russia;
Asia Pacific University (APU), Kuala Lumpur, Malaysia; Staffordshire University (SU), United Kingdom;
University of Applied Science and Technology (UAST), Isfahan, Iran,
anikaeinkoupaei@phystech.edu

Alexey N. Nazarov,
Federal Research Center Computer Science and Control of Russian Academy of Sciences, Moscow, Russia,
a.nazarov06@bk.ru

DOI: 10.36724/2664-066X-2020-6-4-36-41

ABSTRACT

In the past, only mobiles and computers were connected to the internet but in the new era with the advent of new technologies other things like security cameras, microwaves, cars and industrial equipment's are now connected to internet. Internet of things (IoT), there are over several billion electronic equipment de- vices already on the internet, and within a decade these number is expected to scale above 20 billion devices. Smartphones and computers have various software security solutions to defend and protect them from most of threats and attacks, although there are indiscernible security solutions to take care of the rest of the IoT [1]. Lately, as a strong example, several thousands of security cameras were breached to proceed DOS and DDOS attacks that caused the Twitter down. Solutions in the IoT are not exclusively software but the entire physical environment of hardware, World Wide Web (WWW), Software, Cloud and mobile interfaces involved. The IoT ecosystem services are young and not very fully developed yet for these reasons there are main primarily concerns fact around IoT adoption due to security threats/attacks. IoT Top Security Concerns: Secure constrained devices, Secure communication, Keeping IoT hardware updated, Distributed Denial of Service (DDoS), Authorize and authenticate devices, Ensure data privacy and integrity. This research reviews the achievements of mitigation IoT security challenges and the key viewpoint is for authors to clearly dene adversary goals, assumptions and dependencies.

KEYWORDS: *Internet of Things (IoT), Cybersecurity threats and attacks, DDoS, Authorize and authenticate devices, Secure constrained devices, Ensure data privacy and integrity.*

INTRODUCTION

Internet of Things (IoT) is a comprehensive and detailed framework for the information society. Various applications and programs are using in IoT which affect smart devices installed in different environments specifically in workfellow optimization, health and energy deficiency [2]. The formatter will need to create these components, incorporating the applicable criteria that follow. These equipment's consist of integrating sensors and devices, limited processing power and energy recourses that are connected to the internet with different internet protocols and computational components. These restrictions rule communication technologies that require provide efficient performance under different conditions, limited energy overheads and reliance larger address space. A certain number of communication technologies have moved out to facilitate and help these requirements.

These contain as part of a whole Wireless Sensor Networks (WSN) [3], Radio Frequency Identification (RFID) [4], Bluetooth and IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)[5], Zig Bee [6], and have shaped M2M communication as well as dedicated communication technologies for emerging paradigms such as Light Fidelity (LiFi), IoT and Internet of Vehicles (IoV). Unlikely, the majority of these equipment's and applications are not addressed to handle the security and privacy attacks, such a reason brings up security and privacy challenges in the IoT networks such as confidentiality, authentication, data integrity, access control, secrecy, etc. [7]. On every day, the IoT devices are targeted by attackers and intruders. An appraisal discloses that 70 per of the IoT devices are very easy to attack. Therefore, an efficient mechanism is extremely needed to secure the devices connected to the internet against hackers and intruders [8].

Nevertheless, the lack of IoT network architecture also attracted attackers to use this network of dozen devices for penetrating malicious content such as the Active content, Scareware and recent IoT Botnets [9,10]. Furthermore, recent study by Howard [11] has addressed and predicted IoT based attacks to the all enterprise vulnerabilities highlighting the need for preferable mitigation methods. Due to security enhancements not interactively devices in almost every aspect of our life, the threats constituted due to their inadequate and incomplete security are unique with unsecured devices exposing the software programs to the serious security and privacy threats. For example, if the attacker having considerable skill to penetrate vehicular ad-hoc networks (VANETs), the data could be at risk. As long as the attacker is inside the network car's data can spoof with a connection to outside data sources and steal the owner's personal data including the credit card information [12].

Due to the emerging threats, the need to respond to security challenges for the IoT system is very important. There are numbers of effort to address different dimensions of security for IoT such as secure applications [11] [12], privacy of information [13], and authentication [14]. However, the challenges in the embedding security into applications is divided into the 3 different categories: firstly, a user-centered threat model which is an analysis of what tasks the user is trying to achieve, and the concepts which user has to work with, before beginning the design of a traditional threat model. Secondly, inferring security action form (user intention) injecting effective human-computer-interaction (HCI) design toward the security-related components of applications is implied security real – to conclude what essential changes in security state are implicated by the user's actions. The last, reflecting security state back to the user - provide the user visibility into their security state, and in that context, make it possible to provide interface principle that control and change that state without requiring them to understand arbitrary security technology science [15]. Intrusion detection systems (IDS) are normally used as monitors network or systems for preventing malicious activity or policy violations. During the past decade, IDS for the IoT system according to a various number of IDS purposed methods such as [16-18]. Diverse research dimensions focus on broadcast authentication in resource-constrained devices for different applications for concurrency, network management, and software updates [19-22].

In the secure constrained devices, the attackers proved that resource-constrained has limited storage capabilities and computational analysis are defenseless because they have not been purposefully designed to have successful security measures. Keeping protect IoT devices might be sophisticated for the IoT scientist designer and developer because it needs an experiment with embedded system security. Providing encryption and authentication in the chip and firmware has its own complexity which is challenging for the companies without appropriate experiment in cryptography with new threats and technologies. Five of the key challenges in securing these resource-constrained devices are detailed as:

a. Limited CPU and Memory,

b. b. Vulnerable Networking Options,

c. c. High Performance, Lightweight Cryptography,

d. d. Strong Passwords Are Not Enough,

e. Enabling Secure Updates.

According to the [23] a new authentication approach based on the state-of-the-art protocol TESLA, that helps to decrease the delay of forged packets in the buffer of the receiver, by efficiently computing the key disclosure delay. In addition, TESLA addressed to prevent the DDoS Attack by integrating the LEAP and LEAP++ protocols.

Blockchain technologies are able to enable decentralized and reliable features for IoT. However, existing blockchain based solutions to make adequate preparation for data integrity verification for semi-trusted data storages (e.g. cloud providers) cannot qualify as time determinism required by Cyber-Physical Systems (CPS). Additionally, they cannot handle resource-constrained IoT devices as well. According to the [24] architecture can take benefit of blockchain features to make sure data integrity verification of data produced by IoT devices both in the area of CPS.

I. Corporate and Personal Data

Today, the most common threats to corporate information security are crime as a service, the risks associated with the Internet of things and the work of companies with suppliers.

The use of the crime-as-service model by non-professional hackers is becoming increasingly widespread.

Cybercrime today has become available for almost every novice hacker because of the penetration of inexpensive criminal services from mature hacker communities to the darknet market. This in turn significantly increases the number of cyber-attacks in the world and creates new threats for corporations. Potential risks include the use of the Internet of things in various companies. IoT devices today, as a rule, are characterized by weak protection, which opens up additional opportunities for their attack. According to Kaspersky Lab, in 2017 the number of malicious programs that attack the Internet of things devices has more than doubled. In addition, companies using the Internet of Things cannot always track which of the data collected by smart devices is transmitted to external organizations.

Supply chains threaten companies to lose control over valuable and confidential information that they pass on to their suppliers. Such organizations are faced with all three types of threats: risks of breach of confidentiality, integrity and availability of information. Meanwhile, almost every one of us faces information security threats in every-day life. For individuals, significant risks are represented by malware (viruses, worms, Trojans, ransomware), phishing (gaining access to user logins and passwords) and identity theft (using someone else's personal data to enrich). In this case, the attackers of social networks and applications, passport data and data of users' credit cards become the subject of hunt for intruders.

Particularly relevant now is also the issue of selling personal data of customers of large companies to third parties. One of the most notorious cases of illegal use of a large amount of personal data is the scandal involving the consulting company Cambridge Analytica and the social networking site Facebook, which broke out in March 2018. According to journalists, the British company used data from about 50 million Facebook users to influence the course of elections in different countries of the world.

II. ADVENCED DATA PROTECTION TECHNOLOGIES

A. Cryptography

Security experts are paying special attention today to cryptographic encryption of information. Cryptographic encryption methods are divided into symmetric and asymmetric[12]. In the first case, the same key is used to encrypt and decrypt data. In the second case, two different keys are used: one for encryption, the other for decryption. In this case, the choice of a decision depends on the goals that the specialist has set himself. Data encryption using cryptography remains protected by itself, and access to encrypted information may not be limited to any other technology.

Today far from all developed countries can afford really strong means of cryptographic protection. Only individual states, including Russia, possess the necessary knowledge and tools for this. An example of cryptographic data protection methods is a digital (electronic) signature. When developing it, algorithms of hash functions can be used - this is the third type of crypto algorithms, except for the other two, which were discussed above. The digital signature allows you to authenticate electronic documents and has all the main advantages of a regular handwritten signature.

B. EDS

To date, not all e-signatures are used (therefore, for example, the possibility of identifying a mobile phone number as an identity is being discussed - this is expected to be a more affordable option. - Rusbase note), however, numerous enthusiasts among private individuals and companies. In addition, an electronic digital signature is an indispensable element when carrying out certain operations in Russia, such as filing financial statements, participating in procurement, maintaining legally relevant document flow and filing arbitration claims in courts.

C. Quantum Cryptography

One of the most promising data protection technologies today analysts call quantum cryptography. This technology allows you to provide almost absolute protection of encrypted data from hacking.

The basis of the quantum network is the principle of quantum key distribution. The key is generated and transmitted through photons brought into the quantum state. You cannot copy such a key. When trying to break in, the photons that transmit information, according to the laws of physics, change their state, introducing errors in the transmitted data. In this case, you can only pick up and send a new key - until the transmission reaches an acceptable level of errors.

Quantum cryptography is not yet used in practice, but the technology is already close to this. IBM, GAP-Optique, Mitsubishi, Toshiba, the National Laboratory in Los Alamos, California Institute of Technology, as well as the QinetiQ holding, supported by the British Department of Defense, are conducting active research in this area today.

D. Blockchain

The development of information security technologies is also closely related to the blockchain and smart contract capabilities. When researchers realized that not only data from cryptocurrency transactions but also various meta-data could be entered into the register, the blockchain began to actively expand to the area of information security. This technology can guarantee not only the safety, but also the immutability and authenticity of the data, and also makes it almost impossible to deceive identification systems. Today, experts call the blockchain one of the most secure, transparent and unchanging information storage systems.

The possibilities of using distributed registry technology for credit card verification are already being studied at Mastercard. The payment company says that the integration of the new solution into POS terminals will reliably protect transactions and save users from having to carry payment cards with them.

E. Tokenization

One of the most reliable ways to protect payment information is tokenization technology. Its essence lies in the substitution of real confidential data with other values, or tokens. As a result, trading companies may no longer need to store user billing information, and attackers who will have access to information on the cards of companies 'clients will not be able to use it.

Tokenization is especially actively used in e-commerce. At present, the technology is supported by the VISA and MasterCard payment systems, however, with the development of contactless payments and financial technologies, the use of tokenization may spread to the entire trading market in the near future.

F. Moving Target Protection Technology

The protection technology of a moving target can also make a significant contribution to cybersecurity in the future. Now this technology is only being tested and is not widely used in practice.

The new protection system was first introduced in 2016 by scientists from the University of Pennsylvania. Using the technology of protecting a moving target, developers intend to solve one of the main problems of data protection - to deprive the authors of cyber-attacks of access to the code that is used for encryption. Experts say that having one fact of encryption today is not enough. To protect data, you need to continuously change the system, and then the attacker will not be able to obtain relevant information about its state, which can be used

at the next moment in time. As a result, it will be extremely difficult to plan an attack.

G. Biometric Authentication

Among the promising areas of information security, experts also include biometric authentication technologies that allow users to be authenticated by measuring the physiological parameters and characteristics of a person and his behavior.

Voice biometrics and face recognition technologies are developing the fastest in this segment. These solutions are already actively used in the field of forensic science and social control and are gradually becoming a standard feature in smartphones. However, analysts believe that the future of biometrics is due to the use of \closed data", such as heart pulse, drawing of intraocular vessels, the shape of earlobes, and more. In addition, biometric data can be protected by implanted under the skin chips, tablet computers, as well as DNA testing and analysis of human neural connections.

H. Artificial Inteligence

New opportunities for information security professionals open artificial intelligence. Machine learning technologies are already helping to protect corporate data in the Gmail mail service. In June 2017, Google introduced a new system for detecting Phishing attacks for companies using machine learning technologies that send instant warnings about clicking on suspicious links, sending messages about sending an unwanted response to recipients outside the domain and offering built-in protection against new threats.

Artificial intelligence is actively applied by Kaspersky Lab to protect data. Technology Machine Learning for Anomaly Detection, presented by the company in January 2018, allows you to prevent cyber-attacks aimed at sensors and controllers installed in industrial facilities. The new solution analyzes all changes in production processes and informs enterprises about potential attacks.

III. Forinet Framework For Prtotection Against Advanced Threats

One of the greatest solutions for protection against modern threats, the so-called Fortinet ATP (Advanced Threat Protection) Framework, which is positioned as a complete modular solution for cybersecurity. Below is an overview of the solution for automated identification, prevention, suppression of malware and the protection of the entire ecosystem.

Advanced malware can cause huge damage to organizations, from data theft through compromised individuals to the termination of important operations. The attacks of cyber criminals are complex, constantly evolving developments aimed at creating new and cunning methods of penetration and attack.

Partly due to the ever-increasing frequency of public attacks, most organizations have realized the need to improve the IT security infrastructure. According to ESG research, 37

Organizations must evaluate both the ability to identify threats to their IT infrastructure and their ability to counter them. Most of the advanced malware is hidden or zero-day software. Hidden threats are built to penetrate the system undetected, sometimes stored in the system in an inactive state for a certain period of time. Zero-day threats are attacks that exploit previously unknown vulnerabilities of a network, operating system, or application, making it difficult to control them.

Traditionally, security has been implemented on the basis of a perimeter firewall in conjunction with endpoint scanners (workstations). Perimeter firewalls blocked simple types of attacks, preventing unauthorized access to internal systems at the time when antivirus on endpoints scanned user devices according to the signatures of previously known or suspected malware. Firewalls of the new generation and endpoint protection software increase the depth of inspection both at the perimeter and at the end device, but they still rely on the search for already known attacks. They are simply not designed to detect the latest, previously unknown attacks. Too often, organizations are not aware of such threats until the moment of significant damage.

A. Fortinet Framework For Preventing Advanced Threat

Fortinet has developed its own protection framework for advanced threats to provide comprehensive visibility of all activities on the network using existing and new methods using a modular approach to integrating its security products for the network, applications, endpoints and cloud services.

The Advanced Threat Protection Framework includes:

1) FortiGate is a next-generation firewall that provides in-depth inspection of packets and the definition of network security and threat protection applications.

2) FortiWeb - Web Application Firewall is designed to protect applications available from the Internet. Two-way protection against advanced threats including denial of service, SQL injection, XSS, buffer overfllow, cookie poisoning and a large number of other attacks.

3) FortiMail - a security gateway for mail, protects email users from incoming threats using anti-spam, anti-phishing, and malware prevention techniques. Outgoing mail protection includes information leakage prevention (DLP), identification-based encryption (IBE), and message archiving.

4) FortiClient - protection for Windows, Mac, IOS, and Android endpoints, including, but not limited to, malware protection, application control, web filter, vulnerability management, two-factor authentication, and remote access.

5) FortiSandbox - centralized analysis and detection of potential threats using code emulation and execution of this code in a virtual protected environment. Checks activity in addition to attributes to determine unwanted behavior. Dynamically takes steps to respond to incidents and update security.

6) FortiGuard - Fortinet researchers use information from global sources to research threats and attacks, and also

maintain a cloud-based knowledge base about the study of threats and how to prevent them.

FortiGate, FortiWeb and FortiMail are the most common solutions, presented in both hardware and software form, in conjunction with the FortiClient application that is used on end devices that meet the needs of organizations of all sizes. Each product ATP Framework can act as a separate solution or can be combined with other products for enhanced protection due to compatibility. In a fully integrated Framework, protection against network threats and endpoints send potentially dangerous data to FortiSandbox for analysis, which in turn returns instructions for handling data to these products, as well as to FortiGuard's laboratory for distribution to Fortinet products.
Fortinet describes the three phases of its products to ensure coordinated protection: prevention, detection and mitigation.

- Prevention - prevent attacks from many known and highly suspicious threats.
- Detection - identify previously unknown threats and spread information about the threat for an accelerated response.
- Mitigation - research and analyze new data; create a signature and turn the unknown into the known for prevention in the future.

B) Revealing
Fortinet's main approach to identifying advanced threats is to identify unknown threats and redirect them to FortiSandbox to reveal the behavior, tactics, techniques, and procedures used in cyber-attacks. FortiSandbox uses virtual machines as tools for assessing potential threats from executable files, compressed files (zip files), application data such as Adobe Flash, Adobe PDF, and JavaScript, etc. However, the execution of each suspicious file on a virtual machine can be resource intensive and take some time. This can limit the total number of suspicious files that can be evaluated, with a significant impact on performance.
Fortinet uses many different techniques to increase efficiency. Prior to sand-boxing, suspicious files can be pre-filtered, including screening by the antivirus engine, requests to the FortiGuard cloud service, OS-independent simulation, which is possible thanks to the Compact-Net patented recognition language (CPRL). CPRL is a system for deep code inspection and pattern recognition, which allows you to significantly expand the capabilities of protection methods against advanced threats (APT) and recognition of advanced circumvention techniques (AET) that are possible with traditional signature-based analysis.

CONCLUSION

Any corporate infrastructure computing device, from smartphones and tablets to laptops, desktops, and application services, is subject to security breaches. Attacks affect organizations of any size indiscriminately, the consequences can be devastating for operations, company reputation and bank accounts. Costs arising from successful attacks can include not only the resumption of operations and the resolution of security problems but also legal liability and regulatory fines.

The Fortinet framework for protection against advanced threats is easy to understand and manage. Fortinet's modular approach with stand-alone products that can be combined to implement prevention, detection, and mitigation can improve detection and protection against advanced attacks in comparison with individual security systems from other manufacturers. Integration of Fortinet products into an entire ecosystem is quite simple in terms of configuration, thanks to an intuitive interface and many publicly available documentations. After configuration, the analysis of unknown files, no matter how they got into the ecosystem, occurs automatically. The FortiSandbox graphical user interface provides intuitive access to understandable and clear information. FortiSandbox makes understanding current security levels clear and easy to understand.

The Fortinet solution offers the functionality, features, and connectivity that solve the entire spectrum of an organization's security requirements, giving security teams the ability to detect, prevent, and mitigate threats. The ability to work as standalone products or unite into a full framework provides the flexibility to integrate into almost any system. Companies that are looking for more flexible, effective solutions to improve security will be satisfied with the Fortinet Framework for protection against advanced threats.

REFERENCES

[1] S. Naik and V. Maral. 2017. "Cyber security | IoT," *2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, Bangalore, 2017, pp. 764-767. doi:10.1109/RTEICT.

[2] Pacheco J., Hariri S. 2016. IoT security framework for smart cyber infrastructures. *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*. https://doi.org/10.1109/FAS-W.2016.58.

[3] Z. C. L. V. Sheng Z, Mahapatra C. 2015. Recent advances in industrial wireless sensor networks toward efficient management in IoT, *IEEE Access*, vol. 3, pp. 622-37.

[4] C. S. Chen, M. 2017. RFID Technologies for Internet of Things. Springer Cham.

[5] J. Hui and P. Thubert. 2011. Compression format for ipv6 datagrams over ieee 802.15.4-based networks," IETF, Tech. Rep.

[6] C. V. C. S. G. A. H. Y. Baronti P, Pillai P. 2007. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and zigbee standards," *Computer Communications*, vol. 30, p. 16551695.

[7] M. M. Hossain, M. Fotouhi, and R. Hasan. 2015. Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), *2015 IEEE World Congress on. IEEE*, 2015, pp. 21-28.

[8] Ragupathy, Somasundaram Thirugnanam, Mythili. 2017. IoT in Health-care: Breaching Security Issues.

[9] M Antonakakis, T April, Akamai, M Bailey, M Bernhard, A Arbor, E Bursztein, J Cochran, Cloud are, Z Durumeric and J. Alex Halderman, L Invernizzi, M Kallitsis, D Kumar, C Lever, Z Ma and Joshua Mason, D Menscher, C Seaman, Akamai, N Sullivan, K Thomas, Yi Zhou. 2016. "Un- derstanding the Mirai Botnet", 26th USENIX Security Symposium ,Vancouver, BC, Canada ISBN 978-1-931971-40-9

[10] K. Townsend. 2018. Financial services ddos attacks tied to reaper botnet," in available at: https://www.securityweek.com/ nancial-servicesddos-attacks-tied-reaper-botnet.

[11] Howard Solomon. 2018. Top 10 IoT vulnerabilities," in https://www.itworldcanada.com/article/top-10-iot-vulnerabilities-of-2018/413433.

[12] A. N. Nazarov and A. N. A. Koupaei. 2019. "An Architecture Model for Active Cyber Attacks on Intelligence Info-communication Systems:Application Based on Advance System Encryption (AES-512) Using Pre-Encrypted Search Table and Pseudo-Random Functions(PRFs)," *2019 International Conference on Engineering and Telecommunication (EnT),* Dolgoprudny, Russia, 2019, pp. 1- 10.1109/EnT47717.2019.9030541.

[13] Mahmoud Ammar, Giovanni Russello, Bruno Crispo,, 2018. Internet of Things: A survey on the security of IoT frameworks, Jour- nal of Information Security and Applications. Vol. 38. P. 8-27, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2017.11.002. (http://www.sciencedirect.com/science/article/pii/S2214212617302934)

[14] A. N. Nazarov and A. Nik Aein Koupaei. 2019. "Models of Risk of Attack of university Infocommunication System," *2019 Systems of Signals Generating and Processing in the Field of on Board Communications,* Moscow, Russia, pp. 1-8, doi: 10.1109/SOSG.2019.8706780.

[15] Angen, Gaute, Hallstensen, Christo er, nekkenes, Einar. 2018. A frame-work for estimating information security risk assessment method completeness," *International Journal of Information Security,* vol. 17, no 6, p681-699.

[16] D. X. Z. Xuanxia Yao, Xiaoguang Han,, 2013. A lightweight multicast authentication mechanism for small scale iot applications," IEEE Sensors, vol. 13, pp. 3693-3701.

[17] Rebecca E. Grinter and D. K. Smetters., 2018. "Three Challenges for Em-bedding Security into Applications", Palo Alto Research Center (PARC) 3333 Coyote Hill Road Palo Alto, CA 94304 USA.

[18] H. Haddad Pajouh, R. Javidan, R. Khayami, D. Ali, and K. Choo. 2016. A two-layer dimension reduction and two-tier classi cation model for anomaly-based intrusion detection in iot backbone networks," *in IEEE Transactions on Emerging Topics in Computing.*

[19] Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou, Abdelmad-jid Bouabdallah. 2013. "A Systemic Approach for IoT Security." *IEEE. DCOSS*, 2013, Boston, United States, pp. 351-355.

[20] A. N. Nazarov, A. N. A. Koupaei, A. Dhoot, A. Azlan and S. M. R. Siadat. 2020. "Mathematical Modelling of Infrastructure as a Service," *2020 Systems of Signals Generating and Processing in the Field of on Board Communications,* Moscow, Russia, pp. 1-6, doi: 10.1109/IEEECONF48371.2020.9078629.

[21] M. K. Khan, S.-K. Kim, and K. Alghathbar. 2011. Cryptanalysis and security enhancement of a more efficient secure dynamic id-based remote user authentication scheme," *Computer Communications*, vol. 34, no. 3, pp. 305-309.

[22] A. Nazarov, A. Sychev, A. N. A. Koupaei, S. K. Ojha and H. Rai. 2019. "Statistical compaction of a monitoring cloud cluster resource when processing streaming services," *2019 International Conference on Engineering and Telecommunication (EnT),* Dolgoprudny, Russia, pp. 1-5, doi: 10.1109/EnT47717.2019.9030598.

[23] Liu and P. Ning. 2004. Multilevel tesla: Broadcast authentication for distributed sensor networks," *ACM Transactions on Embedded Computing Systems (TECS),* vol. 3, no. 4, pp. 800-836.

[24] W. Ben Jaballah, M. Mosbah, and H. Youssef. 2013. Performance evaluation of key disclosure delay-based schemes in wireless sensor networks," *in Pervasive Computing and Communications Workshops (PERCOM Workshops), International Conference on Pervasive Computing and Communications Workshops, PERCOM*. IEEE, 2013, pp. 566-571.

[25] B. Mbarek, A. Meddeb, W. B. Jaballah and M. Mosbah. 2015. A secure authentication mechanism for resource constrained devices, *IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA),* Marrakech, pp. 1-7. Doi: 10.1109/AICCSA.2015.7507270.

[26] Achado, Caciano. 2018. IoT Data Integrity Verication for Cyber-Physical Systems Using Blockchain. 10.1109/ISORC.2018.00019.17.