UDK 004.738.5:007
DOI 10.7251/ZRSNG2101013C

Multi-factor Authentication for the Internet of Things

Aleksandar Sandro Cvetković [1*], Vesna Radojčić [1], Saša Adamović [1]
[1] Faculty of Computing and Informatics, Sinergija University, Bijeljina, Bosnia and Herzegovina
[*]ascvetkovic@sinergija.edu.ba

Abstract – The Internet of Things (IoT) is integrated and applied in various domains such as Smart Home, Healthcare, Industrial IoT (IIoT), and others. IoT allows physical objects to be able to create, receive and exchange huge amounts of data at any time. The goal of such applications is to automate physical objects that will be able to function without human intervention or with minimal intervention depending on the purpose of the application. Because all domains involved involve the use of sensitive data and that data is usually transmitted over insecure channels, security and privacy issues arise due to potential cyber-attacks. This paper presents various IoT security techniques as well as the main security goals and characteristics. Three types of authentication schemes, one-factor, two-factor, and three-factor are then explained. Since authentication is one of the most important security goals, a special focus is on two-factor authentication schemes.

Keywords – Authentication, Internet of Things, WSN, IoT security, Cybersecurity, Authentication schemes.

Introduction

Throughout history, the industrial revolution has always been linked to technological development. Digitalization in a production led to the fourth industrial revolution which introduced major changes in technology for production systems. This entails the use of the Internet, Cyber-Physical Systems (CPS), the Internet of Things (IoT), Smart Factories, and new information technologies to integrate products, machines, and production systems. CPS are systems that transfer the physical activities of objects to virtual systems. CPS are crucial for production because they allow all levels of production such as products, machines, and factories to be interconnected. The IoT enables mutual communication of all objects in production. A set of physical objects that are interconnected that are connected to the Internet daily can be defined as the Internet of Things. Smart Factories serve to enable rapid fulfillment of customer requirements and adaptation to required changes during production [1]. With the advent of the fourth industrial revolution, new problems appear such as cyber-attacks, problems with storage, and loss of large amounts of data.

I. IoT Security Techniques

Devices that have a wide application such as desktops and smartphones already have certain built-in security features, however, IoT devices used today lack these security features. A well-defined IoT security framework and standard are not yet available. Since there are a huge number of different devices, it is very difficult to create a universal one [2]. Currently, the following Internet of Things security techniques stand out the most:

- Blockchain
- Fog Computing
- Machine Learning
- Edge Computing

Blockchain

The blockchain and IoT combination improves transparency, visibility, and the level of user trust. IoT provides real-time data while blockchain provides the key to the security of that data. All entries in the blockchain are chronological and time-stamped, and each entry is linked to the previous entry using cryptographic hash keys. Blockchain uses replicated log files.

Fog Computing

The difference between IoT and cloud computing is that IoT provides users with a large number of smart devices and applications, while cloud computing provides great solutions for storing and managing data that can be accessed from anywhere. The combination of IoT and cloud computing enables data processing, storing, managing, and securing more efficiently. Because IoT generates huge amounts of data, the benefits that cloud computing provides are not enough to solve all the problems that come with IoT. This is why fog computing has emerged that builds on the shortcomings of cloud computing. Fog computing has the task of handling data generated locally by the IoT for better management. There are two frameworks, the Fog-Device framework which provides various services to users without the involvement of a cloud server, and the Fog-Cloud-Device framework which makes simpler decisions on the fog layer while making more complex decisions on the cloud. Fog-Cloud-Device improves security, prevents data thefts, and minimizes data stored on the cloud. Only selected and important data is sent to the cloud. Within the fog architecture, data is collected through fog devices which can be routers, switches, or any devices that have computing, storage, and network connection.

Machine Learning

Machine learning is also used for IoT security in addition to all other applications it has. It provides a promising solution to protect IoT devices from cyber attacks using a different approach compared to traditional protection methods. Machine learning uses and trains algorithms to detect anomalies in IoT

devices or to detect undesirable activities within an IoT system to prevent data loss or other problems.

Edge Computing

Edge computing is an upgrade of cloud computing as well as fog. Cloud, fog and edge seem similar but work on different layers of IoT applications. The main difference is in the location where intelligence and power computation are performed. Edge computing uses a small edge server that is set up between the user and the cloud or fog. Certain activities are performed on the edge server instead of on the cloud. Edge computing architecture consists of edge devices, cloud servers, and fog nodes. Devices can create networks with each other and collaborate with the goal of computing data. This can prevent a lot of data from reaching the cloud or fog nodes. This approach can also enhance the security of IoT applications.

II. IoT Security Goals

Authenticated Key Agreement

To deal with security and privacy issues in the IoT, it is crucial to design a secure and efficient authentication scheme. To achieve data transfer, the user and the sensing device must exchange a session key, which is why there must be mutual authentication between them.

Entity authentication

Identities must be valid so that the attacker cannot impersonate someone else.

Data confidentiality

The opponent will not be able to read the information collected by sensing devices.

User Anonymity

The anonymity of the user guarantees that the attacker will not be able to access user information via messages that are transmitted. An attacker will also not be able to connect two different sessions with the same user [3].

For the user authentication scheme for WSNs to be satisfactory, it needs to meet certain characteristics:

- mutual authentication between user and gateway node,
- mutual authentication between gateway node and sensor node,
- mutual authentication between the user and sensor node,
- secure and user-friendly password change facility,
- user anonymity,
- reparability,
- session key establishment,
- secure and user-friendly smart card,
- gateway node secret key/parameter is secure,
- user-friendly registration phase [4].

III. Authentication Schemes

There are currently three types of authentication schemes:

- One-Factor Authentication Schemes
- Two-Factor Authentication Schemes
- Three-Factor Authentication Schemes

One-Factor Authentication Scheme

It uses only one parameter for authentication, knowledge factor such as password or inherence factor such as biometric. This is the traditional way to design authentication schemes. Although one-factor authentication schemes have less communication and computation cost, they are not able to support most security features. Because the password is not secure, biometrics is most used. The one-factor authentication scheme is the least researched type.

Two-Factor Authentication Schemes

It uses any of two parameters of the password (knowledge factor), biometric (inherence factor), and smart card (possession factor) for authentication. Two-factor authentication is the most researched type.

Three-Factor Authentication Schemes

All three-factor authentication schemes in WSN are a combination of password (knowledge), smart card (physical possession), and biometric (inherence factor). The three-factor authentication scheme is the second most researched type [5].

IV. Authentication Schemes Solutions

In [6], the authors analyzed one two-factor authentication scheme for WSNs and identified three new attacks, gateway node impersonation attack, gateway node bypassing attack, and privileged-insider attack. A new scheme has been introduced that prevents these attacks and reduces the computational cost and the direct storage cost on the smart card and the gateway node. The authors also stated that their scheme cannot provide user privacy which means that an attacker can track a user who is his target through his authentication session.

In [7], the authors state that the way to design efficient remote user authentication schemes for real-time data access directly from sensor nodes in Hierarchical Wireless Sensor Networks (HWSN) remains a very challenging problem. Two two-factor authentication schemes for HWSN without the inclusion of public-key techniques were analyzed. The schemes were considered safe, but the authors found various security flaws. The authors point out that the techniques of using the public key are necessary to prevent the violation of the anonymity of users under the assumption of unauthorized use of smart cards.

The authors in [8] propose an enhanced two-factor user authentication scheme with unlinkability. In addition, the proposed scheme further reduces calculation costs. The scheme provides more security features, such as the vulnerability attack

of a weak stolen smart card, user anonymity, and unlinkability. The authors point out that their proposed solution provides a secure authentication system that offers balanced features in terms of security and performance.

In [9], the authors point out the shortcomings of an authentication scheme and find that it is not resistant to de-synchronization attack, the off-line guessing attack, and the user forgery attack. They also state that the scheme they analyzed is sensitive to offline password guessing attacks and user impersonation attacks without user anonymity. As a solution, the authors present a new improved authentication scheme with proof that it is secure with the formal security model.

In [10], the authors propose a novel two-factor authentication scheme to provide security in Wireless Medical Sensor Networks (WMSNs) for Personalized Healthcare Systems (PHS). The authors point out that there is mutual authentication with both participants and that it protects data transmitted in dangerous wireless circumstances from various attackers. The protocol achieves security requirements with low time and communication cost which is suitable for data transmission for PHS. Also, the authors using the Proverif tool showed that their scheme withstands various sorts of attacks.

The authors of [11] analyzed several remote user authentication schemes developed specifically for healthcare monitoring on WMSN and concluded that none of them is completely secure. They presented their remote user authentication scheme for healthcare monitoring based on smart card and password, two-factor. The authors used BAN logic to confirm that their presented scheme provides session key agreement and mutual authentication securely. By simulating using the AVISPA tool, the authors confirm that the presented scheme is resistant to replay and man-in-the-middle attacks. Also, the performance evaluation concluded that the scheme includes a large number of security features as well as efficient computation cost and communication cost.

The authors [12] presented a new two-factor authentication key exchange protocol for WSN in IoT applications with the aim of contributing to IoT security. The protocol is based on Elliptic Curve Cryptography (ECC) and allows the exchange of information between users with sensor nodes after a secure link is established. The authors state that the protocol is resistant to various known attacks. They also point out that the protocol has good performance for computation and communication costs and therefore has certain advantages compared to ECC schemes of the same type.

In [13], the authors proposed a protocol for anonymous authentication and key exchange for WSNs. They pointed out that the protocol has strong anonymity of the user where no one but the user knows his true identity. As a disadvantage of this protocol, the authors point out the higher consumption of computer resources due to the use of asymmetric cryptographic mechanisms to achieve strong anonymity. The protocol is suitable for applications that require strong anonymity and high security in WSNs.

CONCLUSION

IoT has a complex architecture consisting of a variety of heterogeneous devices. Due to this architecture, IoT represents a great challenge in the field of security because it is necessary to solve the problem of scalability, transparency, and reliability. IoT security is not only related to software but also to hardware, which means that the number of possible attacks is much higher. In this paper, we focus mostly on WSN and IoT security threats, as well as certain countermeasures to prevent and mitigate IoT attacks. Although some solutions have already been proposed, there is no single solution to defend WSNs and IoT against cyber attacks. Therefore, countermeasures represent potential solutions for the safety of certain characteristics of WSNs, especially IoT. Since it all depends on the needs of IoT devices, future research should focus on optimizing the resources that IoT devices will use as well as designing lightweight security protocols and cryptographic algorithms that are tailored to the specific needs of IoT devices.

REFERENCES

[1] E. Kamber and G. I. S. Bolatan, "INDUSTRY 4.0 CONCEPT AND APPLICATIONS ON DIFFERENT SECTORS," *Journal of Global Strategic Management,* vol. 14, no. 1, pp. 31-44, 2020, doi: https://doi.org/10.20460/JGSM.2020.284.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access,* vol. 7, pp. 82721-82743, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2924045.

[3] R. Vinoth, L. J. Deborah, P. Vijayakumar and N. Kumar, "Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT," *IEEE Internet of Things Journal,* vol. 8, no. 5, pp. 3801-3811, 2021, doi: https://doi.org/10.1109/JIOT.2020.3024703.

[4] S. Kumari, M. K. Khan and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks,* vol. 27, pp. 159-194, 2015, doi: https://doi.org/10.1016/j.adhoc.2014.11.018.

[5] D. Singh, B. Kumar, S. Singh and S. Chand, "Evaluating Authentication Schemes for Real-Time Data in Wireless Sensor Network," *Wireless Personal Communications,* vol. 114, p. 629–655, 2020, doi: https://doi.org/10.1007/s11277-020-07385-0.

[6] D.-Z. Sun, J.-X. Li, Z.-Y. Feng, Z.-F. Cao and G.-Q. Xu, "ON the security and improvement of a two-factor user authentication scheme in wireless sensor networks," *Personal and Ubiquitous Computing,* vol. 17, no. 5, p. 895–905, 2013, doi: https://doi.org/10.1007/s00779-012-0540-3.

[7] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Networks,* vol. 20, pp. 1-15, 2014, doi: https://doi.org/10.1016/j.adhoc.2014.03.003.

[8] Q. Jiang, J. Ma, X. Lu and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-to-Peer Networking and Applications,* vol. 8, no. 6, p. 1070–1081, 2015, doi: https://doi.org/10.1007/s12083-014-0285-z.

[9] F. Wu, L. Xu, S. Kumari and X. Li, "A new and secure authentication scheme for wireless sensor networks with formal proof," *Peer-to-Peer Networking and Applications,* vol. 10, no. 1, p. 16–30, 2017, doi: https://doi.org/10.1007/s12083-015-0404-5.

[10] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Generation Computer Systems,* vol. 82, pp. 727-737, 2018, doi: https://doi.org/10.1016/j.future.2017.08.042.

[11] P. Chandrakar, "A Secure Remote User Authentication Protocol for Healthcare Monitoring Using Wireless Medical Sensor Networks," in *Research Anthology on Telemedicine Efficacy, Adoption, and Impact on Healthcare Delivery*, 2021, doi: https://doi.org/10.4018/978-1-7998-8052-3.ch029, pp. 549-572.

[12] M. Qi and J. Chen, "Secure authenticated key exchange for WSNs in IoT applications," *The Journal of Supercomputing,* vol. 77, pp. 1-14, 2021, doi: https://doi.org/10.1007/s11227-021-03836-y.

[13] K. Zhang, K. Xu and F. Wei, "A Provably Secure Anonymous Authenticated Key Exchange Protocol Based on ECC for Wireless Sensor Networks," *Wireless Communications and Mobile Computing,* vol. 2018, 2018, doi: https://doi.org/10.1155/2018/2484268.