Available online at: https://proceeding.researchsynergypress.com/index.php/ihsatec
Proceeding on The International Halal Science and Technology Conference (IHSATEC)
ISSN 2828-1500 (Online) | 2828-1985 (Print)
Volume 1 Number 1 (2021): 29-35

Improving the security of the organization from the shadow IoT using Blow-fish encryption algorithm

Mr. M. Senthilkumar[1], Dr. B.S. Murugan[2]

[1]Research Scholar. Kalasalingam University
[2]Associate Professor. Kalasalingam University

Abstract

Smart cities, traffic congestion, waste management, structural health, security, emergency services, logistics, retail, industrial control, and health care are just a few of the applications that the Internet of Things (IoT) can help with. The Internet of Things (IoT) is a mega-technology that can connect to anything, anybody, at any time, place, platform, and network. It has a significant impact on the entire blockchain of enterprises, smart objects, and devices, systems, and services provided by heterogeneous network connection (HNC) and is being developed as a smart pervasive framework for smart devices. Because IoT devices link to complicated equipment, interact with hostile surroundings and are deployed on a variety of unregulated platforms, they confront several security risks and challenges. Because the Internet of Things (IoT) has the capacity to integrate any sort of network or sophisticated system, it may be vulnerable to vulnerabilities inherent in the separate systems that make up the integrated network. The purpose of this research paper is to investigate the security issues that individual systems responsible for IoT interconnection face, as well as their impact on the overall IoT system.

Keywords: *IoT, Shadow IOT, Congestion, HNC*

INTRODUCTION

Physical items can share data, coordinate operations, adapt swiftly to environmental changes and effectively utilize their resources thanks to the Internet of Things. Smart homes, smart cities, healthcare, agriculture, and environmental monitoring are all examples of IoT environments that have become more prevalent in recent years. The Internet of Things (Ashton, 2009) consists of many dispersed sensor nodes and actuators that can gather important information from the environment for individual users via wireless media. The data is forwarded to a gateway node with high-performance computing resources that can be trusted. According to IDC, by 2025, there will be over 41 billion linked IoT devices, generating 79.4 zettabytes (ZB) of data. This can have two effects: an increased likelihood of getting shadow or rogue IoT devices added to the network and an increase in the number of IoT devices added to the network. Second, there will be a massive data influx that will put data security concerns to the test. The inherent restricted computing capabilities of IoT devices, weak network protocols, vulnerable environment, and users' willingness to utilize default device credentials make them more vulnerable to security threats.

Corresponding author
Mr. M. Senthilkumar
rmsenthik@gmail.com
DOI: https://doi.org/10.31098/ihsatec.v14i1.483

Because data is transmitted through an insecure and fragile medium, it's critical to keep it safe from dangers like unauthorized access, manipulation, and unlawful eavesdropping. While impersonating legitimate users, malicious attackers attempt to enter, edit, and delete data in order to obtain sensitive data. The majority of these vulnerabilities might be addressed by using IoT-specific authentication methods. Mutual authentication (Moon et al., 2016) is a critical component in ensuring the integrity of both the device and the application. A number of secure IoT mutual authentication and key exchange techniques have been developed, with differing levels of security. Confidentiality, data integrity, availability, and other security requirements should be given via a dependable and efficient authentication mechanism that can withstand various security threats while consuming minimal communication and processing resources on the IoT node.

Artificial intelligence is also being used by researchers to develop IoT-based applications for efficient energy management and distribution, smart homes, and health care, among other things. These metaheuristic approaches, which have increased in popularity among optimization scholars, are effective in the vast majority of real-world situations. To optimize IoT-driven applications and network optimization, several researchers have used metaheuristic and heuristic algorithms that mimic biological and other physical phenomena. They use tried-and-true genetic processes to build frameworks for search algorithms that require the least amount of problem knowledge.

The traditional cryptographic technique cannot be implemented on resource-constrained nodes in order to provide an effective authentication system. As a result, we plan to use elliptical curve cryptography to create a lightweight and secure three-factor authentication framework for IoT. Mutual authentication is achieved between nodes using publish-subscribe patterns such as message queue telemetry transfer (Saqib et al., 2020). The general design allows mutual authentication between the subscriber, broker, and publisher, allowing the subscriber to access publisher data via the broker.

Simple and easy–to–break passwords are used in the classic password-based remote user authentication process. For IoT-based critical applications, multifactor remote user authentication approaches (Das, 2011, Chang et al., 2010) that use a combination of identities and passwords entered in a smart card are recommended. An adversary will find it difficult to guess the identity and password since they have high entropies.

Motivation and contribution

The Internet of Things framework is a collaboration between a remote user, a gateway, and a sensor node. In IoT jargon, the sensor node is referred to as a publisher, the remote user as a subscriber, and the gateway as a broker. The majority of authentication protocols are only intended for mutual authentication between a remote user and a gateway node. Researchers have not fully solved mutual authentication between the gateway and the IoT node, to our knowledge. Because mutual authentication is missing, attackers can use this flaw to insert rogue or shadow IoT devices into the network and perform active and passive attacks.

The sensor node is referred to as a publisher in IoT lingo, while the remote user is referred to as a subscriber and the gateway is referred to as a broker. The majority of authentication protocols are

ISSN 2828-1500 (Online) | 2828-1985(Print)

designed to allow a remote user and a gateway node to mutually authenticate. Researchers have not yet successfully handled mutual authentication between IoT nodes and gateways, to our knowledge. Because there is no reciprocal authentication, attackers can use this flaw to introduce rogue or shadow Internet of Things devices onto the network and launch active and passive assaults.

In this context, our suggested three-factor authentication architecture is built on the publish-subscribe pattern, which is similar to message queue telemetry transport (MQTT), and aims to provide the following benefits:

1)It uses three-factor authentication based on a password, identity, and low-cost digital signature to provide mutual entity authentication of the gateway with both remote users (subscribers) and IoT nodes (publishers), making it ideal for implementing IoT-based critical applications in the health care domain, for example.
2) Session key creation based on nonces is dynamic, meaning that it can change from session to session, making the scheme immune to known session key assaults and ensuring pure forward secrecy.
3) The architecture is designed using computationally cheap hash chains and safe elliptical curve cryptography.
4) The scheme has been properly confirmed using the Scyther tool and is resistant to the majority of commonly used attacks.

The following is the structure of the remainder of the paper: The literature review for the suggested protocol is illustrated in Section II. Section III uses elliptical curve encryption to create a secure, lightweight, signature-based three-factor authentication framework for IoT. The suggested framework's security is examined informally in Section IV. Section V shows how to use the Scyther simulation tool to perform formal security verification on the framework. The performance of the framework is compared in Section VI to that of other relevant current protocols. The paper is finally summarized in Section VII.

LITERATURE REVIEW

The various key agreement and authentication mechanisms important to sensor networks and IoT security are explained in this section.

Yeh et al. (2011) proposed an authentication method for distant users based on elliptical curve cryptography in 2011. However, when compared to other procedures, the computational cost was significant. In 2012, Xue et al. (2013) introduced a time-related credibility-based framework that provided strong authentication between the parties and agreed on a common key for continued communication. However, Xue et al. (2013)'s approach was discovered to be vulnerable to a variety of attacks, including smart card theft and server spoofing.

Chang et al. developed a secure and reliable authentication technique in 2013 that protected users' privacy. Das and Goswami (2013), on the other hand, established in 2013 that their approach could not provide multiple levels of security or safe authentication. Furthermore,

ISSN 2828-1500 (Online) | 2828-1985(Print)

conventional authentication approaches are ineffective for distributed systems with multiple servers, such as the IoT framework, because remote users who want to utilize the IoT framework's services must know the same number of identities and passwords as the number of servers. (Kumari et al., 2017, Chatterjee et al., 2018).

In 2014, Turkanovi et al. proposed an important arbitration and authentication mechanism for the Internet of Things architecture. However, in 2016, Amin and Biswas (2016) demonstrated that Turkanovic et al. design. 's process contains numerous security flaws, including a DOS attack, sensor node capture attack with malicious node formation, inefficient login and authentication phases, hash function calculation problem, identity theft attack, and offline identity and password guessing attack.

Amin and Biswas devised a security mechanism for multi-gateway WSNs. In 2016, Amin and Biswas suggested distributed cloud framework authentication architecture based on smart cards. Registered users can have secure access to secret data from all private cloud servers using this protocol.

In 2016, Das et al. (2016) proposed a three-factor multi-gateway WSN user authentication mechanism. Das et al. proposed a multi-gateway framework for WSNs since generic WSNs add a lot of overhead to the gateway and use a lot more power than multi-gateway wireless sensor networks. They also demonstrated that the system they proposed is resistant to a variety of cryptographic attacks, including sensor capture and impersonation. However, Das et al. technique .'s are vulnerable to user tracking attacks, according to Kazmi et al. (2019), because the session key is not the same for all three participants.

Amin and Biswas's protocol is vulnerable to sensor capture, disclosure of session key, desynchronization attack, impersonation attack, and offline guessing attack, according to Wu et al. (2017). They also demonstrated that the technique proposed by Amin and Biswas is vulnerable to user tracking attacks and that mutual authentication is not achieved. For multiple-gateway WSNs, Wu et al. proposed a key exchange and mutual authentication system. Srinivas et al. (2017) discovered security flaws in Amin and Biswas' scheme in 2017. Srinivas et al. also demonstrated that sensor nodes have limited battery, memory, and power. Srinivas et al. followed up with a more reliable and effective remote user authentication mechanism for multi-gateway WSNs ideal for IoT frameworks.

In 2017, Bae and Kwak (2020) proposed a reliable and efficient smartcard-based authentication technique in a multi-gateway IoT framework to reduce communicational and computing overhead. Their authentication approach, on the other hand, is vulnerable to attacks such as traceability, impersonation, anonymity, spoofing of gateway nodes, and disclosure of session keys, and it does not provide secure mutual authentication.

In 2017, Kazmi et al. (2019) proposed the concept of Smart Grid, in which appliances are made intelligent enough to communicate with one another via Electromagnetic Compatibility and even control a smart house's power use. By combining two existing heuristic approaches, this paper offers a new hybrid algorithm known as harmony search differential evolution (HSDE). Enhanced differential evolution and harmony search are the algorithms that were used. Peak to average

ISSN 2828-1500 (Online) | 2828-1985(Print)

ratio, power cost, user comfort, and energy usage are all factors that are considered while evaluating their performance.

On the basis of a wireless sensor network, Mishra et al. (2018) suggested a multimedia communication authentication mechanism for the IoT framework. The efficiency of this plan is very good. The wireless sensor network framework, on the other hand, has a history of security issues. Wu et al. proposed an authentication architecture for WSN in order to address this security issue. To satisfy security requirements such as confidentiality in IoT, the authentication technique is based on key exchange and biometrics for WSNs.

Hassan et al. (2018) examined recent advances in edge computing technologies and their implications for the Internet of Things. They outlined the necessary conditions for a successful edge computing deployment in the IoT and looked at a few key edge computing scenarios.

Shin and Kwon (2019) found security flaws in the Jung et al. technique. 's (Jung et al., 2017) and proposed a three-factor authentication and key exchange mechanism for wireless sensor networks. The proposed architecture uses the XOR operation and hash functions to meet a variety of security requirements.

3. Methodology:

The first step in preventing or resolving a shadow IoT problem is to gain visibility.

According to the Shadow IoT security issues, the IoT devices linked to the network are unknown, resulting in just a threat.

To reduce the shadow IoT security concerns, take the following steps:

- Sanctioned
- Authorized (not sanctioned yet irrelevant)
- Prohibited (not sanctioned and dangerous)

Block Diagram:

ISSN 2828-1500 (Online) | 2828-1985(Print)

Working Definition of Shadow IOT:

Shadow IoT refers to the Internet of things (IoT) devices or sensors that are in use without the knowledge of IT within a business.

Employees used personal smartphones or other mobile devices for work functions before the days of bringing your own device (BYOD) laws.

"Shadow IoT is a continuation of shadow IT on a much larger scale," explains Mike Raggo, CSO of 802 Secure.

"It is due to the increasing number of devices per employee, as well as the sorts of gadgets, functionalities, and purposes."

Consider the case of Shadow IoT Involved in real-time:

1. Germany's telecoms regulator, the Federal Network Agency, banned a connected doll (i.e., a doll connected to the Internet), dubbed "My Friend Cayla," since it was designated as an "illegal espionage device."

2. In 2017, hackers used an internet-connected fish aquarium to get access to business networks and steal 10 GB of data from a North American casino.

3. Wiki-leaks released information about a CIA gadget known as Weeping Angel, which reveals how an agent may turn a Samsung smart TV into a live microphone.

Blow-fish is a symmetric encryption technique that was created to take the role of DES. It divides messages into 64-bit chunks and encrypts each one separately.

The fact that Blowfish is freely available in the public domain is one of the key reasons for its continued appeal. That isn't to say that it isn't still a good encryption method. Many people believe it has never been defeated.

Blowfish has been used to encrypt user passwords and secure online payments, among other things. It's regarded as one of the most user-friendly and adaptable encryption algorithms available.

CONCLUSION AND FUTURE RESEARCH

The technique serves as a foundation for a more comprehensive methodology for a variety of scenarios. It serves as a foundation for furthering the energy efficiency service for smart coasters and other devices.

ACKNOWLEDGEMENTS

The Berlin Senate and the European Union-funded the "Berlin Center for Digital Transformation" project (EFRE 1.8/01-05), which the authors gratefully acknowledge.

ISSN 2828-1500 (Online) | 2828-1985(Print)

REFERENCES

M. Abramovici, “Smart Products,” in CIRP Encyclopedia of Production Engineering, T. I. A. f. Produ, L. Laperrière, and G. Reinhart, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 1–5.
W. Kritzinger, M. Karner, G. Traar, J. Henjes, and W. Sihn, "Digital Twin in manufacturing: A categorical literature review and classification," IFAC-PapersOnLine, vol. 51, no. 11, pp. 1016–1022, 2018, doi: 10.1016/j.ifacol.2018.08.474.
R. Stark and T. Damerau, "Digital Twin," in CIRP Encyclopedia of Production Engineering, Berlin, Heidelberg: Springer Berlin Heidelberg; Imprint: Springer, 2019, pp. 1–8.
F. Tao et al., "Digital twin-driven product design framework," International Journal of Production Research, vol. 57, no. 12, pp. 3935–3953, 2019, doi: 10.1080/00207543.2018.1443229.
A. Tukker and U. Tischner, "Product-services as a research field: past, present and future. Reflections from a decade of research," Journal of Cleaner Production, vol. 14, no. 17, pp. 1552–1556, 2006, doi: 10.1016/j.jclepro.2006.01.022.

ISSN 2828-1500 (Online) | 2828-1985(Print)