International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Fuzzy Intrusion Detection Method and Zero-Knowledge Authentication for Internet of Things Networks

[1]Elangovan Muniyandy, [2]Iratus Glenn A. Cruz, [3]Dr Mansoor Farooq, [4]Dr. Yeruva. Jaipalreddy, [5]Dr.Rakesh Kumar, [6]Vivek KumarPandey

Submitted: 05/02/2024 **Revised**: 13/03/2024 **Accepted**: 19/03/2024

Abstract: One of the encouraging trends that has contributed to the exponential rise in human progress over the last decade is the Internet of Things (IoT). Interconnection of physical objects for the purpose of data exchange is the next frontier of the internet, known as the Internet of Things (IoT). Everything from household appliances to cars to buildings to animals is part of the Internet of Things (IoT). The Internet of Things (IoT) has become the de facto standard because to its many useful uses in business, medicine, agriculture, and other fields. The Internet of Things (IoT) integrates wireless, pervasive, and ubiquitous technology to solve problems. Things with sensors implanted in them and linked over the internet make it up. Data is collected and shared by these networked devices. Many applications rely on the monitoring and analysis of data originating from heterogeneous devices. Fuzzy logic is used in this study to create a new, lightweight intrusion detection system (IDS) for Internet of Things (IoT) applications based on the MQTT protocol. Using fuzzy variables, the IDS detects network irregularities. In conclusion, this study offers a fresh security framework to solve the problems with current algorithms in an Internet of Things setting. This study also provides an application layer security that smart environments may use to avoid DoS attacks.

Keywords: *Internet of Things (IoT), Intrusion Detection, fuzzy logic. Networks*

1. Introduction

The Internet of Things (IoT) is a preeminent networking system that enables items to interact with one another via the use of pervasive connection. In the year 1999, Kevin Ashton was the first person to use the term "Internet of Things." He did so by establishing a connection between the supply chain idea of RFID Ashton (2009). In recent times, the Internet of Things revolution has brought about an acceleration in the development of novel communication protocols and cyber-physical systems. Traditional networks, such as wireless sensor networks, omnipresent networks, cyber-physical systems, and ubiquitous networks, have been supplanted by the innovations that have been made in the Internet of Things in recent years [1]. A cell phone, electrical equipment, traffic lights, and almost anything else that is used in daily life may all be considered Internet of Things devices. Generally speaking, Internet of Things devices that have limited processors, memory, and energy are considered to be resource-constrained. The Internet of Things (IoT) is a network in which every gadget is linked to the internet and has the capability to do computations. Data is collected and shared by sensors and actuators that are integrated in all physical devices. The manner in which these devices are utilized and the environment in which they function determine how they do so[2, 3]. At regular intervals of one minute, the sensors continuously transmit data on the operational status of the equipment. There are applications for the Internet of Things in practically every industry, from agriculture to aeronautics, and it has opened up new business prospects and chances for new businesses. This has led to the development of new apps and services for users that do not need human participation [4]. In turn, this necessitates the development of innovative and pertinent solutions for communication, computing, and networking. The quality of life of the user is improved by these cutting-edge Internet of Things apps. A wide variety of applications, including those in the government, the military, and smart surroundings, make use of the Internet of Things devices [4, 5], [6]. All of the information that is flowing from these gadgets is

1Department of Biosciences, Saveetha School of Engineering. Saveetha Institute of Medical and Technical Sciences,Chennai, T.N., India, Email: muniyandy.e@gmail.com
2Instructor 1, CMISO Coordinator, College of Communication and Information Technology, President Ramon Magsaysay State University, Castillejos Campus, Philippines, Email: iratusglenncruz@gmail.com
3Assistant Professor IT, Department of Management Studies, University of Kashmir, Kashmir, India, Email: mansoor.msct@uok.edu.in
4Assistant Professor, Department of Electronics and Communication Engineering, Narasaraopeta Engineering College, Andhra Pradesh, India, Email: y.jaipalreddy@gmail.com
5Assistant Professor, Department:Electronics and Communication Engineering, I K Gujral Punjab Technical University, Kapurthala, Punjab, India, Email: drrakeshbanga@gmail.com
5 Research Scholar, Department of Electronics and Communication, University of Allahabad, Uttar Pradesh, India, Email: vivek5confidential@gmail.com
6Assistant Professor, Department of Computer Science and Engineering, United College of Engineering and Research, Prayagraj, Uttar Pradesh, India, Email: vivek5confidential@gmail.com

really important and crucial. Emergent autonomous applications are the outcome of the Internet of Things devices working together to complete the job that has been allocated to them in settings that are data-centric. Some examples of these applications are mentioned below:

When it comes to the consumer sector, the Internet of Things (IoT) is an essential component of home automation systems. It is possible to link any household appliance to the Internet of Things device in order to guarantee that they are used in the most effective manner. A classic illustration of this would be the Apple Watch. There are also other advantages, such as protection insurance and electricity savings. It is [7]. Internet of Things (IoT)-enabled home solutions provide assistance to elderly people and others who need particular care. In the case of individuals who have difficulties seeing, it is possible to integrate voice-controlled Internet of Things. Consequently, the technology that is used in smart homes provides its consumers with an improved quality of life[8].

• Application in Industries: The Internet of Things has the ability to connect differently designed manufacturing equipment that is equipped with sensing, recognizing, processing, communicating, actuating, and networking capabilities in a seamless manner. The capacity to build a whole new firm and market possibilities for manufacturing based on such an incredibly integrated intelligent cyber-physical world is made possible by this [9].

• Applications in Agriculture: Internet of Things applications allow for the accurate measurement of data that is essential to agriculture, such as temperature, wind speed, humidity, and other such factors. In the long run, this will lead to a reduction in risk and waste, as well as an improvement in quality and quantity, among other things [10].

Engineering applications include the requirement for ongoing attention and monitoring of a variety of infrastructures, including big buildings, bridges, railway lines, and other similar types of structures. Using devices that are guided by the Internet of Things, it is possible to monitor the operation of structures such as these to ensure that they operate effectively and to ease the installation of high-quality infrastructure. In order to achieve greater efficiency, Internet of Things automation may also be included into waste management systems [11].

2. Challenges in Iot

Massive Scaling: The IoT suffers from a fragmentation of the platform and a lack of technical norms. This results in a situation wherein the plethora of readily accessible IoT technologies makes it hard to create applications that work continually between separate, incompatible technology ecosystems in terms of both hardware and software differences. The number of connected devices is expected to be 50 billion[12][13]. The massive amount of data collection, storage, addressing, and naming these devices, etc. are major challenges with the increasing number of smart devices. Architecture: With the design and management of IoT improving day by day, IoT solutions must be devised to avoid improper scalability. The need for adequate architecture, which provides connectivity and communication in different IoT applications is another challenge. Standardization: Several efforts have been made by different work groups of the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF) to standardize IoT activity. A collaboration of these, and similar, workgroups is essential to bring about a full-strength IoT[14]. Naming and Addressing Issues: The ability to identify the nodes is a key component in any network. The rise in scalability issue affects effective naming and addressing[15].

Security and Privacy: The IoT is susceptible to attacks of all sorts because of the minimalist characteristics of the devices themselves. Moreover, the openness of the system results in frequent communication failures. The self-healing property of IoT requires high computation and large storage, and connecting with a range of enabling technologies for the IoT results in new challenges

The IoT’s inherent characteristic of anytime anywhere anything connectivity of massive devices increases the complexity of security mechanisms of the IoT system. Traditional cryptographic algorithms are not efficient in such scenarios where devices with low processing power are used. Hence, the need for lightweight algorithms is essential requirements in establishing a secure end-to-end connectivity. This research work focuses on implementing a novel lightweight algorithm provide authentication, group key agreement, and IDS in an IoT environment[16]. A vital challenge in IoT security is that devices in operation must be able to determine that assorted devices in the network are authorized to obtain information during secure communication. Most effective way to validate the authenticity of devices is the cryptographic hash technique, which provides secure communication from one device to other devices. Generally, single-factor authentication is applied to achieve network integrity. Single password authentication mechanisms are susceptible to side-channel and dictionary attacks. Furthermore, the increased use of IoT in commercial applications keeps demanding an underlying secure multicast communication [17]. Secure group communication is another challenge in the IoT, given its dynamic group membership, with the high-frequency entry of new members and exit of old ones. The characteristic of dynamic membership demands that shared cryptographic material be refreshed often to provide both backward and forward secrecy. Secure group communication in IoT can be enforced only by forming a secret group key through computationally efficient methods. The M2M communication in IoT is accomplished with application protocols such as Constrained Application Protocol (CoAP), and Message Queuing Telemetry Transport (MQTT). MQTT is predominantly implemented in secure IoT applications such as health monitoring. The bluntness of these protocols results in various types of attacks including Denial of Service (DoS) attack. This facilitates the need for efficient Intrusion Detection System (IDS) method in MQTT-based application. The existing algorithms for secure end-to-end communication are still needed to be modified to meet the security requirements of security in IoT. The identity authentication that prevents malicious devices in participating in communication is not suitable for most of the IoT applications[18]. A multifactor authentication and session key agreement schemes need to be addressed properly for constrained devices. Besides, a lightweight group key agreement protocol for multicasting is becoming another challenge in the field of IoT. Additionally, since most IoT applications demand the prevention of DoS attacks, an intelligent IDS that detects DoS attacks early is to be incorporated into them

In this research work, the overall goal is to design a system where lightweight algorithms for authentication, group key agreement, and IDS are implemented for constrained devices in IoT. The following are the objectives of the proposed work: To design a novel lightweight mutual authentication scheme for constrained devices in the IoT networks to design a secure authentication scheme by incorporating multiple factors into the identity of the device. To provide secure sessions by establishing a shared session key among the devices using simple computation steps. To design and develop a secure hierarchical group key agreement protocol based on Elliptic Curve Diffie-Hellman (ECDH) using B-tree for multicasting in IoT networks. To have the proposed group key agreement provide the group forward and backward secrecy.

To devise a group key agreement that adapts to smart environments by significantly reducing the computation and storage needed, while ensuring the highest levels of security. To design a lightweight IDS using fuzzy logic to prevent the DoS attack in the application layer protocol such as MQTT, CoAP, etc. To design efficient methods to detect the flooding of publisher and subscriber messages that culminates in DoS attacks. To design a lightweight rule base to enable computationally efficient decision making in fuzzy inference engine. This research identifies and addresses the limitations present in the authentication, group key agreement, and IDS in constrained devices in IoT. In the research work, a zero-knowledge authentication scheme is proposed. This scheme allows the party to prove the other party at the end that it has the credentials without revealing anything else. The proposed scheme is technically distinct from zero-knowledge proof. This is because of the narrower definition of a zero-knowledge authentication scheme than that of the zero-knowledge. The proposed group key agreement addresses the key management problems due to the scalability in the network. IDS play a major role in defending computer technologies and network environments against various cyber-attacks. Modern DoS attacks including ordinary and malicious network traffic considerably improve the frequency of false alarms, thus challenging IDS efficacy. This research work aims to provide the solutions to the issues in authentication, group key agreement and IDS for smart environments. The lightweight algorithms which enhance the authentication, multicast communication and DoS attack prevention for the smart things are the major contributions of this research work. The communication model of the proposed work is shown in Figure 1.

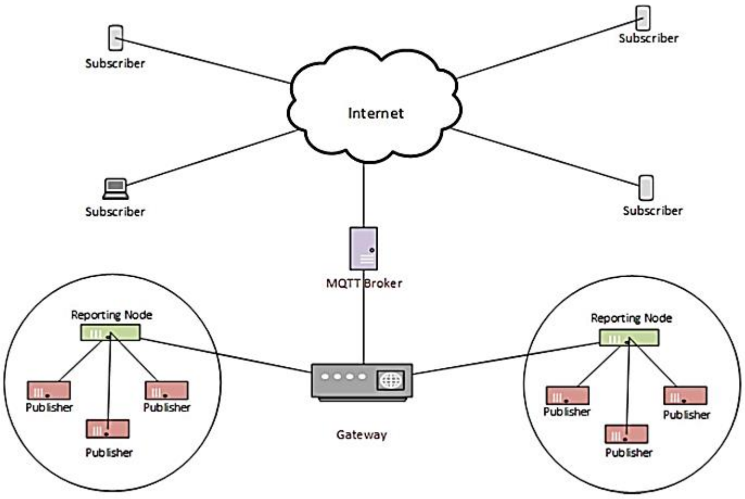

Fig .1 Communication Model

In the Internet of Things communication paradigm that has been suggested, the most important components are the publisher, the subscriber, the reporting node, the gateway, and the MQTT broker. As Internet of Things devices, the publisher and the subscriber are regarded to be. The data are detected by the publisher, who then transmits them to the reporting node. These data are compiled by the reporting node, which then transmits them to the gateway. Due to the fact that the data that is published may include sensitive information, it is necessary for the publisher and the reporting node to have effective authentication in this circumstance. For this reason, a location-based authentication technique, also known as LBAS, is presented in this thesis as a means of establishing secure communication.

The inherent scalability features of Internet of Things situations need the use of effective multicasting in order to transmit the same message to a collection of devices. It is common practice to do multicasting via the use of encrypted group communication. It is possible for those publisher nodes that are required to take part in the multicasting to become members of the group. For the purpose of establishing a secure group communication relationship between the devices, a group key is established.

The purpose of this study is to provide a B-tree-based group key agreement technique as a potential solution to the problem of scalability that exists in smart environments. The reporting node serves as the group controller in this configuration, and each of the publishing devices makes an equal contribution to the generation of the group key using this approach. Following the establishment of the secure connection, the publisher becomes transparent to a great number of apps. For the purpose of establishing an end-to-end connection, this work takes into consideration MQTT as the application layer protocol. On top of the TCP transport layer is where the MQTT protocol operates. Through the use of MQTT, the handshaking process that is part of TCP guarantees that communication is reliable. Nevertheless, MQTT is not capable of providing secure data exchange from beginning to finish. If an attacker is able to successfully conduct a Denial of Service (DoS) attack, they will have successfully compromised the MQTT broker. In the third part of this thesis, an intrusion detection system (IDS) is presented as a means of preventing denial of service attacks in MQTT brokers. The suggested architecture of the system, which includes the elements of location-based authentication, hierarchical group key agreement, and fuzzy-based intrusion detection systems among its components

An innovative technique that employs the user's location and identity as authentication elements has been developed to overcome the security problems that are present in Internet of Things authentication. The security is improved as a result of this since it eliminates the weaknesses that are present in the single factor authentication. Due to the fact that it is based on ECC calculation, the suggested authentication procedure is designed to be both lightweight and straightforward. Within the context of smart environments, the problem of scalability is also handled by taking into consideration hierarchical structures.

During the course of this study, the B-Tree-based group key agreement was proposed as a solution to secure multicasting, which is another significant security issue in the Internet of Things. There is also a reduction in the amount of calculation and communication overhead in restricted devices as a result of the ECC-based computations that are used in the suggested methods. Additionally, the use of BTree in key management contributes to the enhancement of the scalability of secure multicasting in an intelligent environment. Following the deployment of the network, the intrusion detection system (IDS) is required in order to keep an eye out for any hostile devices that may be present. This paper presents a fuzzy-based intrusion detection system (IDS) by taking into consideration the features and problems of Internet of Things (IoT) security. The use of fuzzy rule interpolation techniques results in a significant reduction in the density of the rule base. Because of this, it is suitable for use with very small devices in the network. The description of the functions of the different components that make up the system architecture is provided in the next section.

Location-Based Authentication Scheme

Single factor authentication or one factor authentication methods are often used for authentication purposes in order to accomplish the goal of achieving security in the networks. Users are required to provide a username and password for the majority of single-factor authentication. The authentication method that relies on a password is susceptible to attack by an attacker. Several distinct scenarios of Internet of Things applications make use of multi-factor authentication techniques that are based on a password, biometric information, and a smart card. There have been reports of flaws in such techniques, including the ability to eavesdrop on the password, clone the smart card, and duplicate the biometric information. When it comes to information security and access management, the location of the device adds a new dimension at each and every one of these scenarios. It is possible to utilize the physical location of a device as an extra authentication factor in order to prevent fraudsters from deceiving the user.

Verification of data access from a place that has been authorized may be accomplished using the device's location information. When it comes to Internet of Things applications such as geo-fence monitoring and location discovery IoT services, the position of the devices is an extremely important factor. One component, the position of the device, is taken into consideration by the majority of the location-based authentication techniques that are now in use. These works consider location to be the one and only piece of information that each node has, making it more vulnerable to a range of different types of assaults. There are just a handful of methodologies that make use of location for multi-factor authentication in smart environments. These methodologies take use of the fact that users are using smart phones and send location information to users via the smart phone.

The smart phones may not always be with the user, or they may not be functioning properly. This is something that has been seen. In situations like these, it is not possible to rely on the techniques that were outlined before. The ECC algorithm is used in LBAS for the purpose of authenticating the stated location of Internet of Things (IoT) nodes in security areas. Following this, shared secure session keys are calculated between the Sensing node (SN) and the Reporting node (RN) for the purpose of encrypting data. Internet of Things devices such as RFID, sensor nodes, or smart phones may all serve as the SN. The self-certified public key system is used by the LBAS in order to perform authentication. The overhead that is spent in certificate-based authentication procedures is eliminated by self-certified public, which removes the need for certificate production and distribution. By using Zero-knowledge proof, the Registered Nurse (RN) is able to produce the public key of the Social Network (SN) without having any prior knowledge of the SN's private key during the registration process. Additionally, the location of the SN is checked as an extra authentication in addition to that. The computation of a session key follows the completion of this two-level authentication process. This session key is used for the purpose of encrypting and decrypting messages in order to ensure safe communication between the SN and the RN. RN is responsible for managing secure connections and transmitting the data that has been detected to the base station.

B-Tree Based Group Key Agreement

The Internet of Things presents a number of challenges, one of which is the attainment of secure group communication. This is because the membership of the group is constantly changing, with new members joining and old members leaving the group at a fast rate. When a group is generating periodic multicast data, the establishment of a group key and the preservation of that key are both very important factors. An Internet of Things network consisting of sensor nodes and a gateway are features of the communication model. This network is made up of a number of different secure multicast groups. Additionally, the sensor network assists in the development of multicast groups and facilitates group transactions. Each multicast group is comprised of a collection of Internet of Things devices, of which they all share a common set of information. The gateway is responsible for controlling the Internet of Things network and collecting data from the various devices. For the purpose of group creation and group-oriented activities in the Internet of Things, the contributory group key generation technique, which is based on ECC, is used for the production of group keys. The B-tree is used to effectively describe the group structure, which simplifies the process of often updating group keys in a way that is both scalable and safe.

Fuzzy Based IDS For MQTT Protocol

Due to the fact that it is both simple and scalable, MQTT is a frequently utilized application layer protocol for the purpose of transmitting data between the many devices that make up the Internet of Things. MQTT communication between Internet of Things devices is accomplished via the use of three fundamental components: the publisher, the subscriber, and the broker. Through the use of a revolutionary fuzzy logic-based intrusion detection technique, Secure-MQTT is able to identify malicious behavior that is carried out by nodes inside the MQTT broker.

Over the course of a period of time, the behavior of MQTT publishers' network traffic is analyzed, and certain traffic aspects become learned. With the help of a technique that is based on fuzzy logic, Secure-MQTT is able to identify malicious behavior on nodes that are part of the MQTT broker. The technique that is based on fuzzy logic is used for the processing of the selected traffic characteristics. In accordance with the fuzzy rules included inside the rule base, the malicious node is successfully identified. The fuzzy inference engine then makes a determination on whether or not the MQTT message must be acknowledged.

The complicated nature of the fuzzy model is simplified by the use of dynamic fuzzy interpolation techniques. It is also helpful in improving the efficiency of the updated rule base, which ultimately leads to an improvement in the overall performance of the intrusion detection system (IDS). The work is carried out utilizing dynamic fuzzy interpolation rather than dense rule basis, which results in the task being more lightweight. Compared to the current MQTT-S, which uses SSL/TLS to offer security, the Secure-MQTT is a more secure alternative. Despite the fact that it responds to assaults in a timely manner, Secure-MQTT has been seen to not compromise the greater communication rate. As a result, Secure-MQTT demonstrates its effectiveness in identifying attacks without negatively impacting the performance of the network.

Location-Based Authentication Scheme

The purpose of this study is to offer a new Location-Based Authentication Scheme (LBAS) for Internet of Things devices. This scheme makes use of a self-certified two-factor authentication protocol that is computationally efficient. The identity and location of a device are used to produce public keys in this self-certified authentication system. These keys are then used to authenticate the device. The generation of a session key follows the authentication process, which is done in order to create a secure connection between the devices. The LBAS is made up of two innovative algorithms that are both safe and lightweight. These algorithms are based on ECC and are intended for authentication and the production of session keys. In addition to this, the LBAS utilizes a hierarchical topology structure, which contributes to the increased scalability of the network. The LBAS is designed to avoid potential attacks such as location duplication, replays, and node captures. This is made possible by the use of the zero-knowledge approach, which is utilized to create the public keys.

As the Internet of Things (IoT) becomes more prevalent in business applications, there is a growing need for a secure multicast communication system. It is recommended that a group be created if a device wants to transmit the same message to many nodes over the network.

By reducing the amount of computing overhead and the amount of time it takes for communication to take place, group communication helps to improve the network's capacity for communication. On the other hand, in order to provide safe communication between a large number of nodes, it must repeatedly undertake a large number of mutual authentication procedures, which results in a significant increase in performance overhead. A similar modification is required for the session key agreement in mutual authentication techniques in order to accommodate a group of devices.

After the mutual authentication has been completed in this study, a group key is produced for the device in order to determine whether or not it wishes to take part in a group. When it comes to the Internet of Things (IoT), the only way to ensure secure group communication is to generate a secret group key using techniques that are computationally efficient. In order to maintain confidentiality, the suggested method for group key agreement takes into account both the activities performed by the group and any future modifications made to the group key. In this context, we are thinking about two different operations: the addition of new members and the departure of members from the group. Due to the dynamic membership features of smart environments, it is necessary to often update the cryptographic materials that are communicated in order to maintain the confidentiality of the group key, as well as to maintain both backward and forward secrecy.

The secrecy of the group key guarantees that computational infeasibility is maintained in such a manner that the intruder is unable to discover the solution. It is impossible for a new member to deduce or access the prior set of group keys from the new group key if backward secrecy is in place. The new group key should not be derived from the prior group keys in the same way that it should not be found when members leave the group. This kind of confidentiality is known as advance secrecy. For the purpose of this chapter, a new group key agreement procedure that is based on ECC is explored. Through the use of ECC, the protocol is able to dramatically reduce the amount of calculations that are performed inside a node, therefore saving both time and energy. As an additional benefit, the use of a B-Tree structure for the purpose of organizing the group membership results in a reduction in the quantity of messages that are sent in order to accomplish both backward and forward secrecy. The protocol is efficient in an Internet of Things setting because it reduces the amount of round operations required to maintain the group structure, performs point multiplication, and enjoys the inherent benefits of ECC.

3. Secure-Mqtt

One of the most important aspects of any Internet of Things application that is built on MQTT is the MQTT broker since it provides customers with a wide range of services. The most significant vulnerability of the MQTT protocol is that it may be inundated, which can ultimately result in a denial of service attack. At some point during the denial of service assault, the attacker is able to compromise the broker, which causes fake control or data packets to be sent. Significant security issues in the MQTT protocol include, among other things, the capacity to automatically recover from a denial of service attack, the amount of time required to recover from such an assault, and the effect of a broker failure on an Internet of Things application.

As a countermeasure against a denial of service attack in the MQTT protocol, certificate-based SSL/TLS authentication is one of the countermeasures. However, it is not recommended for Internet of Things devices since certificate management increases the amount of computation and communication overhead. Additionally, the speed of the MQTT is negatively impacted by the production and distribution of session keys inside the SSL/TLS protocol. The use of throttling, which prevents the attacker from discovering regularly subscribed topics and flooding them with fake messages in the broker, is another security precaution that reduces the severity of a denial of service assault.

Thasting, on the other hand, is incapable of withstanding distributed denial of service assaults on a broad scale, which means that it does not offer sufficient security for smart settings. During the process of throttling, there is a high probability that critical messages will be abandoned, which is something that has to be addressed. When an intruder launches a botnet assault, they take control of devices connected to the Internet of Things (IoT) by installing malware on a compromised node in order to corrupt the broker. The classic intrusion detection system (IDS) is used in the methods that are meant to identify and prevent the assaults that were outlined before. However, this IDS does not provide effective results in all IoT network settings. This is largely due to the dynamic network properties of the Internet of Things as well as the minimal setup requirements of IoT devices. As a result, there is a requirement for a lightweight intrusion detection system (IDS) for the MQTT protocol in order to guarantee safe communication for Internet of Things devices that have limited resources.

4. Conclusion

An innovative authentication method for Internet of Things devices with limited resources has been suggested and put into practice as a result of this study. The authentication technique that has been suggested is innovative in that it combines the extra authentication element with an implementation that is computationally efficient. Taking into account the weaknesses of Internet of Things security methods and the features of devices that are part of the network, the authentication system takes into account the location of the item as an extra component. In addition, the thesis has made significant progress in the development of a group key agreement protocol that is computationally efficient by taking into consideration the huge scaling features of the smart environment. When it came to implementing the frequent joining and departing of devices in the network, the group key agreement took into consideration the use of B-tree-based key management. In addition, the thesis proposes a lightweight intrusion detection system (IDS) that can accommodate a small number of devices in the Internet of Things (IoT). The thesis proposed a lightweight fuzzy-based DoS attack detection technique, which is essential to the security of the internet of things, rather than constructing a generic intrusion detection system.

References

[1] Kaushik, A., Al-Raweshidy, H. A novel intrusion detection system for internet of things devices and data. Wireless Netw 30, 285–294 (2024). https://doi.org/10.1007/s11276-023-03435-0

[2] Rui, K., Pan, H. & Shu, S. Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking (SDN) and Machine Learning techniques. *Sci Rep* **13**, 18003 (2023). https://doi.org/10.1038/s41598-023-44764-6

[3] Alexey Finogeev, Michael Deev, Danila Parygin & Anton Finogeev (2022) Intelligent SDN Architecture With Fuzzy Neural Network and Blockchain for Monitoring Critical Events, Applied

Artificial
Intelligence, 36:1, DOI: 10.1080/08839514.2022.2145634

[4] Kavitha, S, Alphonse, PJA & Reddy, YV 2019, 'An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System', Journal of medical systems, vol. 43, no. 8, p. 260.

[5] Lee, J, Yu, S, Park, K, Park, Y & Park, Y 2019, 'Secure Three-Factor Authentication Protocol for Multi-Gateway IoT Environments', Sensors, vol. 19, no.10, pp. 2358-2362

[6] Mohammed, AJ & Yassin, AA 2019, 'Efficient and Flexible MultiFactor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device', Cryptography, vol. 3, no. 3, pp. 24.

[7] Qikun, Z, Yongjiao, L, Yong, G, Chuanyang, Z, Xiangyang, L & Jun, Z 2019, 'Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication', IEEE Access, vol. 7, pp. 87085-87096

[8] Yaqoob, I, Hashem, IAT, Ahmed, A, Kazmi, SA & Hong, CS 2019, 'Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges', Future Generation Computer Systems, vol. 92, no. 2019, 265-275

[9] Cuka, M, Elmazi, D, Bylykbashi, K, Spaho, E, Ikeda, M & Barolli, L 2019, 'Implementation and performance evaluation of two fuzzy-based systems for selection of IoT devices in opportunistic networks', Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 2, pp. 519-529.

[10] Kavitha, S, Alphonse, PJA & Reddy, YV 2019, 'An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System', Journal of medical systems, vol. 43, no. 8, p. 260

[11] Ammar, M, Giovanni, R & Bruno, C 2018, 'Internet of Things: A survey on the security of IoT frameworks', Journal of Information Security and Applications, vol. 38, no. 2018, pp. 8-27.

[12] Arain, QA, Memon, I, Deng, Memon, MH, Mangi, FA & Zubedi 2018, 'A Location monitoring approach: multiple mix-zones with location privacy protection based on traffic flow over road networks', Multimedia Tools and Applications, vol. 77, no. 5, pp. 5563-5607.

[13] Chien, HY 2018, 'Group-Oriented Range-Bound Key Agreement for Internet of Things Scenarios', IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1890-1903

[14] Choi, W, Jo, HJ, Woo, S, Chun, JY, Park, J & Lee, DH 2018, 'Identifying ecus using inimitable characteristics of signals in controller area networks', IEEE Transactions on Vehicular Technology, vol. 67, no. 6, pp. 4757-4770.

[15] Dhillon, PK & Kalra, S 2018, 'Multi-factor user authentication scheme for IoT-based healthcare services', Journal of Reliable Intelligent Environments, vol. 4, no. 3, pp. 141-160

[16] Alaba, FA, Othman, M, Hashem, IAT & Alotaibi, F 2017, 'Internet of Things security: A survey', Journal of Network and Computer Applications, vol. 88, no. 2017, pp. 10-28.

[17] Bilal, M & Kang, SG 2017, 'A secure key agreement protocol for dynamic group', Cluster Computing, vol. 20, no. 3, pp. 2779-2792

[18] Chen, CH, Lin, MY & Guo, XC 2017, 'High-level modeling and synthesis of smart sensor networks for Industrial Internet of Things', Computers & Electrical Engineering, vol. 61, no. 2017, pp. 48-66.