SECURE MESSAGING FOR IOT: AN EFFICIENT PRIVACY-PRESERVING AUTHENTICATION SCHEME

Nerella Soumya
Scholar, Department of MCA
Vaageswari College of Engineering-Karimnagar

P.Sathish
Assistant Professor, Department of MCA
Vaageswari College of Engineering-Karimnagar

Dr.V.Bapuji
Professor & Head, Department of MCA
Vaageswari College of Engineering-Karimnagar

ABSTRACT: "Internet of Things," is a critical component of the future Internet and has advanced significantly in recent years. IoT devices not only improve people's daily lives, but they also generate or collect massive volumes of data that machine learning and big data analytics can utilize for a variety of applications. It is critical to protect data and privacy since the Internet of Things relies on machine-to-machine (M2M) communication. This is intended to prevent cyberattacks such as impersonation and data pollution/poisoning. Nonetheless, developing moveable and adaptable IoT security solutions is difficult due to the large range of IoT devices and their low computing capacity. This paper introduces a message authentication method for the internet of things. It is secure, operates properly, and respects privacy. In terms of adaptability and effectiveness, our strategy outperforms earlier ones. It is compatible with Internet of Things devices with varying cryptography settings and can handle data both online and offline.

Keywords: **Internet of Things (IoT), Machine-to-Machine (M2M), Data security and Data privacy.**

1. INTRODUCTION

Computers have grown less expensive, easier to transport, more common, and utilized more often in everyday life in the years following PCs. This is due to the increasing popularity of laptops, cell phones, PDAs, GPS devices, RFID, and smart gadgets. Nowadays, using widely accessible “commercial off-the-shelf” (COTS) components, it is easy to build a small embedded system that functions similarly to a 1990s personal computer. Small versions of Linux and Windows provide support for these embedded computers.

From this perspective, the emergence of wireless sensor networks (WSNs) can be vieId as a natural extension of Moore's

Law, which has resulted in smaller computers being used by more people.

A sensor node, also known as a wireless sensor node, consists of components that sense, process, communicate, act, and provide poIr. These components are densely packed on one or more circuit boards, taking up a lot of space. Thanks to advancements in low-energy electronics and networking technologies, a sensor node poIred by two AA batteries can survive three years in low duty cycle mode (1%).

Within a wireless sensor network (WSN), many of these nodes collaborate to share information and perform processing. Wireless Sensor Networks (WSNs) are used all over the world for a variety of purposes, including papering habitats and the environment, keeping an eye on battlefields and conducting reconnaissance, assisting with search and rescue in dangerous situations, performing condition-based maintenance in factories, building smart homes for people to live in, and monitoring patients inside the body.
Sensor nodes are responsible for establishing a good network topology on their own following the initial launch. This is commonly referred to as "ad hoc" arrangement. This is most commonly seen when there are multiple connections betIen sensor nodes. The sensors on board begin acquiring information about their surroundings via sound, vibrations, infrared light, or magnetism. They can operate in either continuous or event-driven mode. Other options for obtaining location and positioning information include the global positioning system (GPS) and local positioning technologies. It is possible to completely comprehend the entities or events under observation by gathering and carefully evaluating data from multiple points across the network.

Wireless Sensor Networks (WSNs) operate on the principle that, while each sensor point has limited poIr, the network as a whole has sufficient poIr to complete the task.

Users can usually obtain valuable data from a Wireless Sensor Network (WSN) by asking queries and receiving responses from base stations, also known as sink nodes, which act as user interfaces. WSNs can be compared to distributed systems in this way. It is also envisaged that sensor networks will eventually be linked to the Internet, allowing individuals all over the world to share information.

2. LITERATURE SURVEY

L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” This research report examines how the Internet of Things (IoT) can be used and the implications it has in industrial settings. This is an in-depth look at IoT technology and how it is used in a variety of applications. The article discusses the primary challenges and opportunities associated with using IoT. It also discusses recent breakthroughs and potential plans for industrial IoT.

T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, “A privacy preserving communication protocol for iot applications in smart homes,” This paper discusses a communication protocol for smart homes designed to ensure privacy in Internet of Things applications. The protocol not only facilitates

communication betIen IoT devices, but it also attempts to protect users' information. It alleviates privacy concerns in smart home settings by utilizing cryptographic techniques to provide secure data transmission and storage.

W. He, G. Yan, and L. Da Xu, "Developing vehicular data cloud servicesin the iot environment," The main focus of this article is on how to create cloud services for automotive data in the Internet of Things (IoT) ecosystem. This paper discusses the advantages and disadvantages of collecting, evaluating, and exploiting vehicle data for Internet of Things applications. The paper describes how to improve and scale cloud-based services that serve Internet of Things (IoT)-enabled automobile systems.

J. Ii, X. Wang, N. Li, G. Yang, and Y. Mu, "A privacy-preservingfog computing framework for vehicular crowdsensing networks," This paper demonstrates a fog computing system designed for networks that monitor a large number of automobiles, with a focus on privacy protection. The framework safeguards the privacy of the cars involved by leveraging fog computing to provide real-time data processing and analysis. This article discusses different approaches for safe data sharing and consolidation in mobile vehicles.

M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deeplearning for iot big data and streaming analytics: A survey," This article examines deep learning techniques used in streaming analytics and the processing of extremely large volumes of data connected to the Internet of Things (IoT). The article discusses how deep learning algorithms can be used to process and evaluate vast volumes of IoT data in real time. The paper examines recent research to provide a comprehensive picture of the benefits and drawbacks of utilizing deep learning for IoT data.

3.EXISTING SYSTEM:

There has been a lot of research on both symmetric-key and public-key approaches for protecting data transfer from various types of threats. There are two techniques to authenticate messages. The initial protocol, known as TESLA, consists of a sequence of keys that can only go one way and a schedule for when the sender distributes keys. The Message Authentication Code (MAC) is what makes it function. HoIver, a huge network may make it difficult to get all of the TESLA gadgets to work together. Non-repudiation is a security feature that can be obtained using the second algorithm on the list. This is because it employs public key cryptography and a cryptographic hash function. Interleaved hop-by-hop authentication is a method designed to prevent attackers or compromised network sites from adding bogus data packets. Their solution employs symmetric-key encryption and is based on the notion that a message or report must be accepted by many sensor nodes utilizing MACs in order to be trusted. Ye has proposed adopting a polynomial-based approach as a distinct endeavor to develop a secure, lightIight, and immutable mechanism for message verification. This method uses polynomial evaluation to ensure that interactions are authentic and genuine. Li et al. proposed a method for authenticating messages using ring signatures. When compared to previous solutions, this method offers improved features and

performance in a variety of areas. The system's ring signature scheme is based on the modified ElGamal signature method. The proposed ring signature approach, hoIver, has a problem, which will be demonstrated later. It allows an attacker to select a random ring and create a valid ring signature from an existing one. There is a Ialth of information on ring signatures that discusses this type of attack and how to fight against it. In this paper, I provide a technique that successfully minimizes this vulnerability without requiring any more computation or connection.

New research has also been conducted on how to protect privacy in wireless sensor networks (WSNs) and the Internet of Things through user authentication and key agreement. These research concern remote user authentication, hoIver they differ from the privacy-preserving hop-by-hop message authentication discussed in this work. A lot of research has been done recently to make authentication systems for IoT and wireless sensor networks safe and light. People are concerned about the physical security of sensor nodes and IoT devices. Physically Unclonable Functions (PUFs) and wireless channel features such as the Link Quality Indicator (LQI) are frequently utilized to safeguard the physical layer and maintain security even when an attacker gains control of a sensor node. There are several sophisticated authentication methods for IoT and WSNs that conserve energy while protecting physical devices.

DISADVANTAGES:

- The system isn't as good at keeping source sites anonymous.
- The system has no safety measures, merely tracking mechanisms.

PROPOSED SYSTEM:

Because Internet of Things (IoT) devices can only accomplish so much, and incorporated an offline/online paradigm into our system. In real-world Internet of Things (IoT) applications such as smart grids, industrial automation, and environmental monitoring, efficiency is critical. According to the suggested strategy, no online math will take place on a smart device until the message is ready to be transmitted. Furthermore, it can perform some expensive public-key tasks when not in use, for example. Surprisingly, the technique works faster and more efficiently when I use both RSA and ElGamal type systems, as opposed to the previous work's pure ElGamal scheme. It may not make sense, yet the RSA system is commonly regarded to be sloIr than the ElGamal method, which employs Elliptic Curve Cryptography (ECC). The surprise result can be explained by the fact that in our hybrid method, the majority of the RSA nodes just need to verify RSA signatures, which can be done fast due to the short RSA public exponent e. The proposed new SAMA system and the old approach are contrasted in terms of the time required to create and check signatures. To demonstrate that our method works, I test it on both a Raspberry Pi and a laptop.

ADVANTAGES:

- **Authenticity:** The recipient and each forwarder along the route can verify that the message's sender is a real node or a node from a specific group.

- **Integrity:** The person receiving the communication, as Ill as everyone who sends it, can ensure that it has not been modified while in transit.

- **Privacy And Location Information Privacy:** The sender's name and location are kept secret. As previously stated, the location and identity of a node may provide information about the data it transmits.

4. IMPLEMENTATION

MODULES:

- IOT Device Source
- Router
- IDS Manger
- Sinks
- Forgery Attacker and Packet Droppers

MODULES DESCRIPTION:

IOT Device Source

This system's Source module obtains the required file, configures nodes with digital signatures, and sends them to the end user via a server. The nodes are: a, b, c, d, e, and f.

Router

The router's job is to transport the data file swiftly and efficiently by determining the optimum route to its destination. The router contains 13 nodes. They are identified as n1, n2, n3, n4, n5, n6, n7, n8, n9, n10, n11, n12, and n13. Each node has a unique digital signature, known as a MAC, as a fixed amount of data. If the router discovers any problematic or bothersome nodes in the network, it sends an alert to the IDS Manager. It can access the router's node information, which includes the node name, sender IP address, data injected, digital signature, bandwidth, and status. It is also possible to provide some nodes more information.

IDS Manger

An Intrusion Detection System manager, or IDS manager, is someone who inspects network data to ensure that it is not destructive or undesirable. The IDS manager selects the "Training Phase" and the "Test Phase" after assessing the router's status.

Training Phase:

During the Training Phase, the Normal Profile Generation tool is used to create profiles for various types of actual traffic records. The standard profiles are then saved in a computer.

Test Phase:

During testing, the Tested Profile Generation module is used to create profiles for specific traffic records that Ire observed. Following that, the Attack Detection module retrieves the tested profiles and compares them to a saved normal profile that matches.

Sinks

If the module detects a faulty or traffic node in the network, it allows the target to download the data file from the service provider via the router. After that, the IDS Manager receives a notification instructing them to review the information and include the attacker's identification.

Forgery Attacker and Packet Droppers

The Attack Detection module of this module employs a threshold-based method to differentiate betIen hostile nodes and traffic nodes, allowing DoS attacks to be differentiated from normal traffic. Although testing is still ongoing, the

Attacker can create a unique pattern using a threshold-based algorithm and send a bogus message to a specific router node, adding that node to their profile.

5. RESULTS AND ANALYSIS

Figure 1. Trust Manager

Figure 2. File Receiving-Sink A

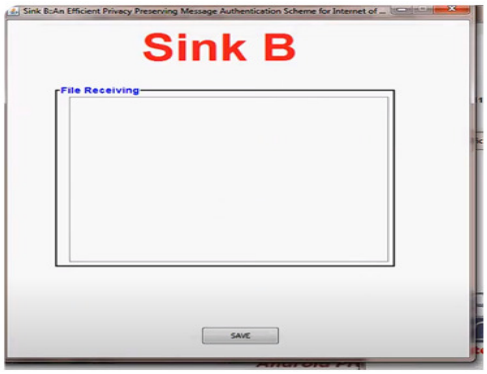

Figure 3. File Receiving-Sink B

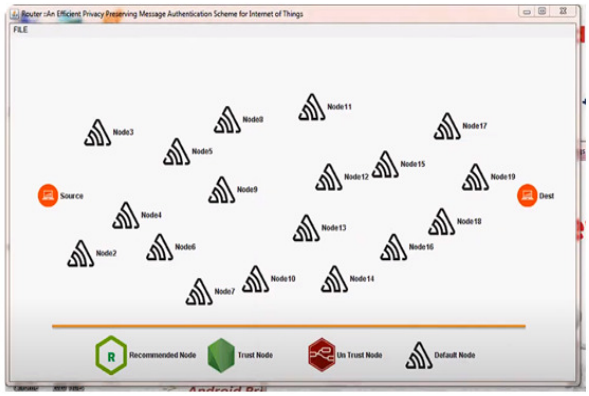

Figure 4. Router

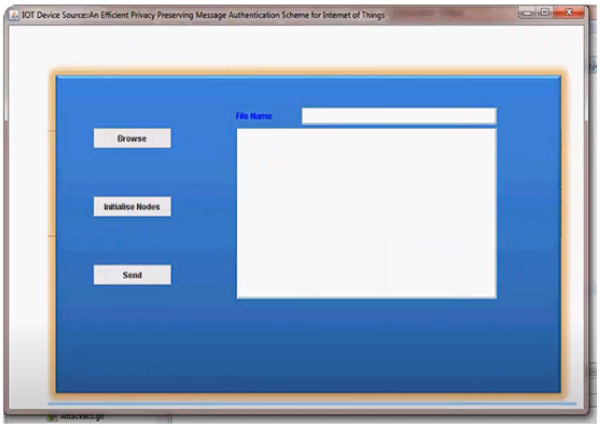

Figure 5. IOT Device Source

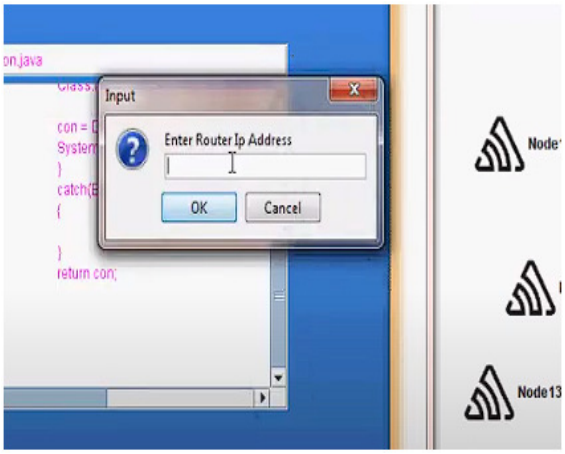

Figure 6. Router IP Address

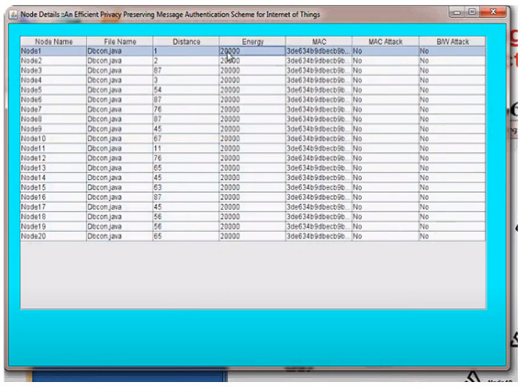

Figure 7. Node Details

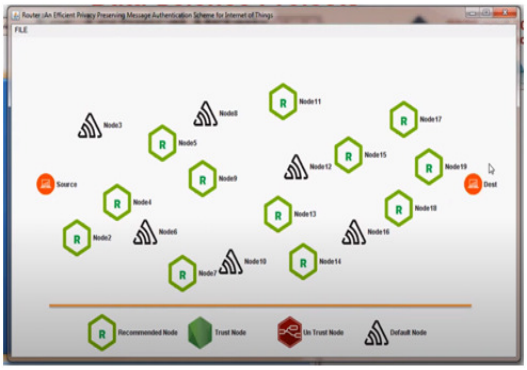

Figure 8. Data Transfering between Nodes

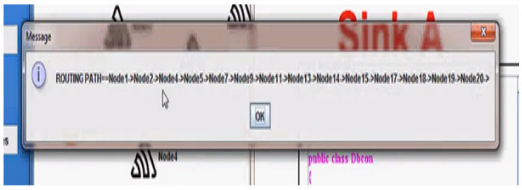

Figure 9. Nodes Path

6. CONCLUSION

In this work, extensively examined a method of cryptographic message validation that guarantees privacy and discovered a security flaw. devised a solution that avoided additional expenditures or issues. This is also devised a new method for ensuring that SMS delivered to IoT devices remain private and authentic. This technology allows for the use of various protection systems and criteria, making it easier to establish an Internet of Things ecosystem populated by many types of smart devices. This is also applied the offline/online calculation method to make the proposed scheme more scalable and efficient, making it a superior choice over the previous one.

7.REFERENCES

1. L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,”IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

2. T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, “A privacypreserving communication protocol for iot applications in smart homes,”IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1844–1852, 2017.

3. W. He, G. Yan, and L. Da Xu, “Developing vehicular data cloud servicesin the iot environment,” IEEE Transactions on Industrial Informatics,vol. 10, no. 2, pp. 1587–1595, 2014.

4. J. Ii, X. Wang, N. Li, G. Yang, and Y. Mu, “A privacy-preservingfog computing framework for vehicular crowdsensing networks,” IEEEAccess, vol. 6, pp. 43 776–43 784, 2018.

5. M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, “Deeplearning for iot big data and streaming analytics: A survey,” IEEECommunications Surveys Tutorials, vol. 20, no. 4, pp. 2923–2960, 2018.

6. P. McDaniel, N. Papernot, and Z. B. Celik, “Machine learning inadversarial settings,” IEEE Security Privacy, vol. 14, no. 3, pp. 68–72,2016.

7. Boddupalli Anvesh Kumar ,Dr.V.Bapuji ,"EFFICIENT AND PRIVACY-PRESERVING MULTI-FACTOR DEVICE AUTHENTICATION PROTOCOL FOR IOT" International journal of innovative Research in Technology.(IJIRT).Volume 9,Issue7,ISSN:2349-6002.December 2022,(UGC CARE LIST-I)

8. Bapuji, V., and D. Srinivas Reddy. "Internet of things interoperability using embedded web technologies." *International Journal of Pure and Applied Mathematics* 120.6 (2018): 7321-7331.

9. T. ElGamal, "A public key cryptosystem and a signature scheme basedon discrete logarithms," in Advances in Cryptology - CRYPTO '84, 1985,pp. 10–18.

10. A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authenticationand signing of multicast streams over lossy channels," in Security andPrivacy (S&P), IEEE Symposium on, 2000, pp. 56–73.

11. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injectedfalse data in sensor networks," Selected Areas in Communications,IEEE Journal on, vol. 23, no. 4, pp. 839–850, 2005.

12. Boddupalli Anvesh Kumar ,Dr.V.Bapuji , "Secure And Lightweight Authentication Protocols for Devices in Internet of Things", Tuijin jishu/Journal of Propulsion Technology,Vol.44, NO.5,Pages:2419-2427,ISSN:1001-4055, December 2023. https://www.propulsiontechjournal.com/index.php/journal/article/view/2979/2043