Vol 13 Issue 02, June 2023
ISSN NO: 0364-4308

A Secure and Privacy-Enhanced Message Authentication Scheme for IoT Devices

Mr.T V Seshu Kiran[1]., Gaddam Keerthi [2]
1 Assistant Professor, Department of CSE, Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India
2, B.Tech CSE (20RG1A0519),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT

As an essential element of the next generation Inter- net, Internet of Things (IoT) has been undergoing an extensive development in recent years. In addition to the enhancement of people's daily lives, IoT devices also generate/gather a massive amount of data that could be utilized by machine learning and big data analytics for different applications. Due to the machine-to-machine (M2M) communication nature of IoT, data security and privacy are crucial issues that must be addressed to prevent different cyber attacks (e.g., impersonation and data pollution/poisoning attacks).

Nevertheless, due to the constrained computation power and the diversity of IoT devices, it is a challenging problem to develop lightweight and versatile IoT security solutions. In this paper, we propose an efficient, secure, and privacy-preserving message authentication scheme for IoT. Our scheme supports IoT devices with different cryptographic configurations and allows offline/online computation, making it more versatile and efficient than the previous solutions.

Keywords: *privacy,encryption,text.*

I.INTRODUCTION

THE Internet of Things (IoT) provides a self-establishing network of highly coupled heterogeneous objects, such as smart devices, RFID tags, sensors, etc. It allows devices to simplify the retrieval as well as the exchange of data without human involvement in various applications and has a considerable position in the growth of information technology after the computer science and the Internet. IoT brings a pervasive digital appearance by engaging society and industries, and enables a series of interactions between human to human, human to thing, and more importantly, thing to thing. The development of IoT has led to enormous applications, such as smart home systems (SHSs), intelligent transportation systems, machine learning and big data , etc. The machine-to-machine (M2M)

communication among massive numbers of IoT devices will dominate future communication network traffic. The integrity and authenticity of the massive amount of data collected and transmitted by the IoT devices are crucial in some applications such as machine learning and big data analytics. Maliciously injected or modified data can cause biased or wrong decision making and prediction. Therefore, in order to ensure the correctness and accuracy of machine learning and big data analysis, the integrity and authenticity of the collected data must be retained.The increasing integration of location-based services and the ubiquitous generation of spatiotextual data pose a critical challenge to individual privacy. In particular, the computation of spatio-textual skylines, which involves the aggregation of location data, raises significant concerns regarding the exposure of sensitive information. Existing privacy-preserving techniques for spatial data often fall short in addressing the unique challenges posed by spatiotextual skylines, necessitating novel approaches. Balancing the trade-off between utility and privacy in the context of location aggregation remains a formidable task, exacerbated by the dynamic nature of spatio-textual data and evolving privacy threats. A comprehensive solution is required to ensure robust privacy preservation while maintaining the practical utility of spatio-textual skylines for diverse applications, contributing to the responsible and secure utilization of location-based services in our interconnected world.

II.EXISTING SYSTEM

In order to prevent various types of attacks in data transmission, both symmetric-key and public-key approaches have been proposed in the literature. In [12], two different message authentication protocols were proposed. The first protocol, named TESLA, is based on Message Authentication Code (MAC), and the design utilizes a one-way key chain and timed release of keys by the sender. However, the TESLA protocol requires synchronization among devices, which is difficult to implement in a large scale network. The second protocol in [12], named EMSS, is based on cryptographic hash function and public-key technique, and can achieve the security property of non repudiation. In [13], an interleaved hop-by-hop authentication scheme was proposed to prevent the injected false data packet attack by attackers or compromised

Existing system and disadvantages

- The system is less effective due to lack of source location privacy.
- The system has only detection techniques and no protection techniques.

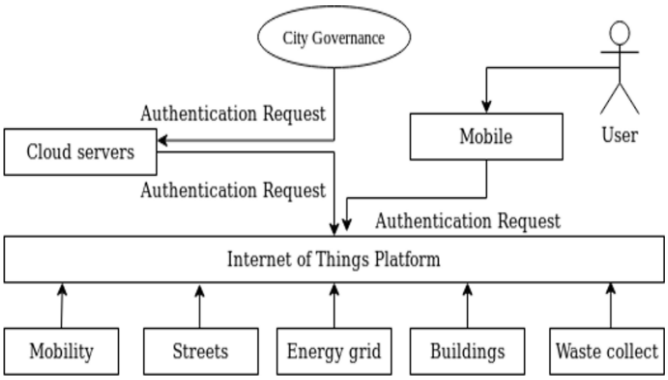
III.PROPOSED SYSTEM

Moreover, considering the low computation power of the IoT devices, we also apply the offline/online paradigm in the design of our system. Efficiency is extremely important in practical IoT scenarios such as industrial automation, environmental monitoring, smart grids, etc. In proposed scheme, a smart device can perform some expensive public-key operations offline (e.g., when it is idle), and only does the online computation when the message to be sent is ready. Interestingly, we find that by allowing both RSA and ElGamal type systems in our scheme, we are able to reduce the computation cost compared with the pure ElGamal scheme proposed in [8]. This may look counterintuitive since it is known that the ElGamal system (implemented using Elliptic Curve Cryptography, or ECC for short) is much faster than the RSA system. The reason of this counterintuitive fact is that in our hybrid scheme, for most of the RSA nodes, we only need to do RSA signature verification, which is very fast since the RSA public exponent e can be very small. The proposed new SAMA scheme is compared with the previous scheme in terms of its execution time during signature generation and verification. We also implement our scheme in a laptop and in a Raspberry Pi to demonstrate its practicality.

IV.LITERATURE REVIEW

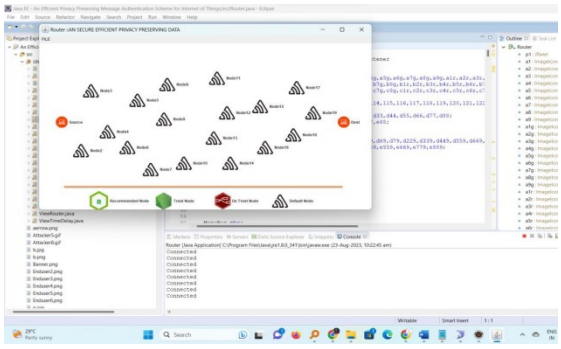
Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio frequency identification (RFID), and wireless, mobile, and sensor devices. A wide range of industrial IoT applications have been developed and deployed in recent years. In an effort to understand the development of IoT in industries, this paper reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and identifies research trends and challenges. A main contribution of this review paper is that it summarizes the current state-of-the-art IoT in industries systematically Internet of things is the trending direction when it comes to designing smart living environment. One of the popular applications of Internet of things is the smart home system. A smart home system usually consists of various types of connected sensors,

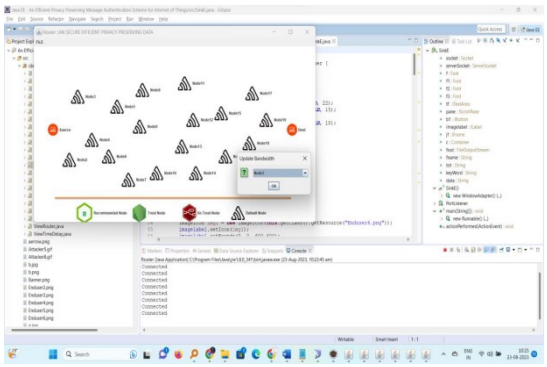
actuators, appliances and a controller. The controller analyzes the data reported by the sensors and sends out messages to electric appliances and other sensors to ask them to behave accordingly. There are a lot of smart home designs proposed in the literature to make the systems smarter and more comfortable. However, little work has considered the security and privacy issues in smart home systems. In this paper, we analyze the differences of security and privacy issues that lie in the smart home systems, smart grid, and wireless sensor networks. Further, we propose our own solutions that achieves privacy preservation during the communications between end sensors and appliances and the controller. Recently, the study of road surface condition monitoring has drawn great attention to improve the traffic efficiency and road safety. As a matter of fact, this activity plays a critical role in the management of the transportation infrastructure. Trustworthiness and individual privacy affect the practical deployment of the vehicular Crowd sensing network. Mobile sensing as well as the contemporary applications are made use of problem solving. The fog computing paradigm is introduced to meet specific requirements, including the mobility support, low latency, and location awareness. The fog-based vehicular crowdsensing network is an emerging transportation management infrastructure. Moreover, the fog computing is effective to reduce the latency and improve the quality of service. Most of the existing authentication protocols cannot help the drivers to judge a message when the authentication on the message is anonymous. In this paper, a fog-based privacy-preserving scheme is proposed to enhance the security of the vehicular crowdsensing network. Our scheme is secure with the security properties, including non-deniability, mutual authentication, integrity, forward privacy, and strong anonymity. We further analyze the designed scheme, which can not only guarantee the security requirements but also achieve higher efficiency with regards to computation and communication compared with the existing schemes.

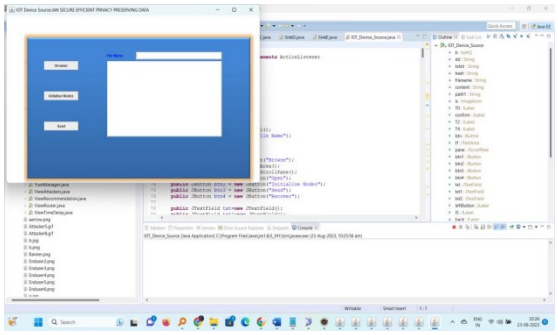


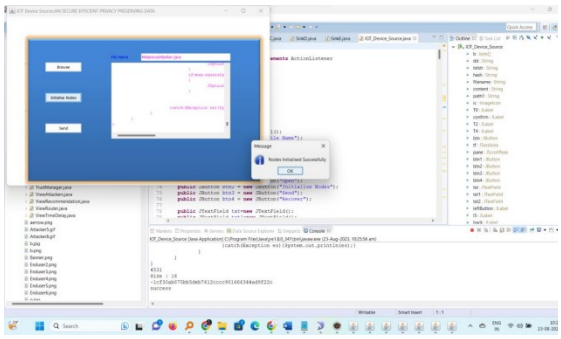
System architecture

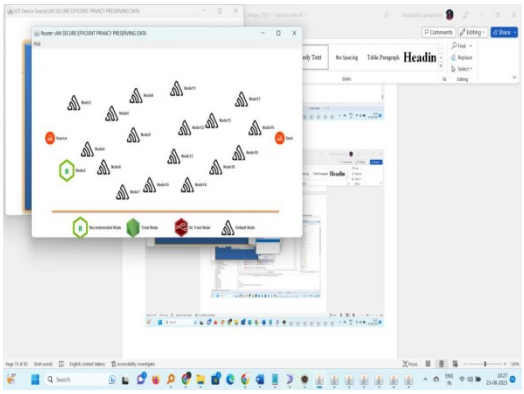
V.Result :











VI. CONCLUSION

In this paper, we revisited a privacy preserving message authentication scheme and showed a security weakness in the scheme. We also provided a solution to fix the problem without introducing any overhead. In order to provide better practicality in IoT consisting of different types of smart devices, we also proposed a new privacy-preserving message authentication scheme that allows IoT devices to use different security systems and parameters. Moreover, we applied the offline/online computation technique to improve the efficiency and scalability of the proposed scheme, which makes it more practical compared with the previous Solution.

VII.FUTURE SCOPE

The next generation Internet, Internet of Things (IoT) has been undergoing an extensive development in recent years. In addition to the enhancement of

people's daily lives, IoT devices also generate/gather a massive amount of data that could be utilized by machine learning and big data analytics for different applications. Due to the machine-to-machine (M2M) communication nature of IoT, data security and privacy are crucial issues that must be addressed to prevent different cyber attacks (e.g., impersonation and data pollution/poisoning attacks). Nevertheless, due to the constrained computation power and the diversity of IoT devices, it is a challenging problem to develop lightweight and versatile IoT security solutions.

VIII.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 privacy preserving 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 services in the iot environment," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1587– 1595, 2014.

[4] J. Wei, X. Wang, N. Li, G. Yang, and Y. Mu, "A privacy-preserving fog computing framework for vehicular crowdsensing networks," IEEE Access, vol. 6, pp. 43 776–43 784, 2018.

[5] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for iot big data and streaming analytics: A survey," IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 2923–2960, 2018.

[6] J. Shen, T. Zhou, X. Liu, and Y.-C. Chang, "A novel latin-squarebased secret sharing for m2m communications," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3659– 3668, 2018.

[7] P. McDaniel, N. Papernot, and Z. B. Celik, "Machine learning in adversarial settings," IEEE Security Privacy, vol. 14, no. 3, pp. 68–72, 2016.

[8] J. Li, Y. Li, J. Ren, and J. Wu, "Hop-by-hop message authentication and source privacy in wireless sensor networks," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 5, pp. 1223–1232, 2014.

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

[10] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in Advances in Cryptology - EUROCRYPT '96, 1996, pp. 387–398.