IJTBI
International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/19
DOI: https://doi.org/10.5281/zenodo.19131591

PRIVACY-PRESERVING AND EFFICIENT MESSAGE AUTHENTICATION FOR IOT SYSTEMS

[#1]**SD. KHAJA PASHA,** ***Assistant Professor,***
[#2]**AMBEERA HIMAVARSHITHA,** ***B.Tech Student,***
[#3]**VEGOLAPU SAI GEETHANJALI,** ***B.Tech Student,***
[#4]**VENGALA KAVYA,** ***B.Tech Student,***
[#5]**MANUPATI MANITEJA,** ***B.Tech Student,***
Department of AIML,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: The Internet of Things (IoT), a crucial element of the next-generation Internet, has rapidly developed in recent years. Massive volumes of data are generated and collected by IoT devices, which may be used for a number of purposes, including enhancing people's lives, by machine learning and big data analytics. Since the Internet of Things depends on machine-to-machine (M2M) communication, data security and privacy are important issues that need to be resolved to stop different types of cyberattacks (including impersonation and data pollution/poisoning). However, the variety of IoT devices and the restricted processing power make it challenging to develop lightweight and varied IoT security solutions. In this work, we propose an effective, secure, and privacy-preserving message authentication system for IoT. Because our method allows for offline/online computation and supports IoT devices with different cryptography settings, it is more flexible and effective than previous solutions.

Keywords: Internet of Things, hop-by-hop authentication, integrity, source privacy.

1. INTRODUCTION

The Internet of Things (IoT) enables the construction of systems from numerous independent components, all of which contribute uniquely to the overall. Machine learning has the potential to greatly reduce the amount of human intervention required for computer-to-computer data sharing and retrieval. After personal computers and the World Wide Web, this is the IT industry's third most significant innovation.

Everyone can now be online at all times thanks to the interplay between the Internet of Things and various sectors of industry and society. Not only that, but this also allows humans to communicate with inanimate objects and, even more importantly, with other people and inanimate objects that are associated with them. Many new academic disciplines have emerged as a result of the proliferation of connected devices and the Internet of Things (IoT), including big data, machine learning, smart home systems, intelligent transportation systems, and many more.

The majority of network traffic in the future will come from machine-to-machine (M2M) communication, particularly amongst several Internet of Things (IoT) devices. It is critical that the massive volumes of data transmitted and received by IoT devices be authentic and trustworthy for uses such as machine learning and big data analytics, among

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/19
DOI: https://doi.org/10.5281/zenodo.19131591

many others. Misleading predictions and inferences might result from data that has been artificially enhanced or altered. Verifying the accuracy and use of machine learning and big data analysis relies on maintaining the integrity and authenticity of the acquired data.

In the realm of the Internet of Things, symmetric-key and public-key communication protocols are available for secure message exchange. Since symmetric-key operations are quicker than public-key operations, the symmetric-key technique requires less computing power. However, using symmetric-key based approaches in a large and diverse IoT network makes cryptographic key management very difficult. Additionally, the intermediary forwarding nodes in the IoT network cannot verify the message's validity if the authentication process solely depends on the sender's and recipient's shared key. Only the person who is supposed to receive the data will be able to detect if it was corrupted or distorted in transit.

Alternatively, these issues can be mitigated using a public-key approach, where any individual can verify the veracity of a message using the public key. Since anybody may easily verify the authenticity of an authentication token using the sender's public key, public-key approaches pose serious privacy risks. Additionally, keep in mind that public-key procedures are very resource intensive.

It's worth noting that safeguarding the privacy of the data source can be as crucial in certain instances, particularly when a person is linked to a wearable device. Knowing the source of a data stream allows an attacker to prevent its transmission, for instance by launching a denial-of-service attack. Consequently, the accuracy of the machine learning prediction or judgment would suffer. We need to develop a secure, efficient, and privacy-aware message authentication method that can effectively manage hop-by-hop verification if we are to overcome the issues mentioned above in the realms of Machine-to-Machine (M2M) and Internet of Things (IoT) communications. One novel approach that Li et al. presented, source anonymous message authentication (SAMA), could work here. They reasoned that their system would be more cost-effective than the current methods of authenticating and concealing message sources.

2. SYSTEM DESIGN

The addition of the offline/online paradigm to our system's architecture facilitates its interaction with IoT devices. Practical uses of the Internet of Things, such as smart grids, factory automation, and environmental monitoring, place a premium on efficiency. The proposed method requires the smart device to perform the costly public-key procedures only during message preparation time. This way, you may put the resources to better use when the device isn't in use. Notably, we can reduce calculation costs by combining RSA and ElGamal types of systems, as opposed to relying solely on the ElGamal technique as demonstrated in. The ElGamal system outperforms the RSA approach in terms of speed, which may appear unusual given that it employs Elliptic Curve Cryptography (ECC). Since the RSA public exponent e can be very small, our hybrid approach can quickly verify RSA signatures—all that is required

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/19
DOI: https://doi.org/10.5281/zenodo.19131591

of most RSA nodes. Both the creation and verification of signatures are handled more quickly by the new SAMA system compared to its predecessor. To demonstrate the superiority of our method, we employed a Raspberry Pi in conjunction with a laptop.

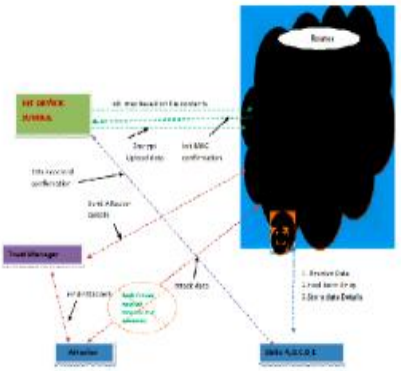

Fig 1. Architecture Diagram

3. RELATED WORK

Data transmission security against various threats has been the subject of research into public-key and symmetric-key approaches, which use two keys. To verify the authenticity of a message, two methods were proposed. A pioneer in its field, the TESLA protocol allowed the sender to choose a release time and used a one-way key chain. The provided language satisfies the requirements of the MAC. The synchronizing of devices over a large network, however, presents TESLA with a significant challenge. The non-repudiation security feature is available to users of the second system, which is named EMSS. Secure hash algorithms and public-key methods are the building blocks of the system. Interleaved hop-by-hop authentication prevents malicious actors or compromised nodes from injecting the network with false data.Message validation codes (MACs) are used by many sensor nodes in symmetric-key systems to verify the accuracy of reports or messages. This is essential for message verification. This tactic adheres to a crucial guideline in the field. Ye came up with a polynomial-based mechanism for message authentication (year). To verify the authenticity of the data being transmitted, this technique makes use of polynomials. Some of the benefits of this method are how simple it is to implement and how difficult it is to alter. A novel approach to the message authentication problem is shown in the research by Li et al., which makes use of ring signatures. The method used by this system is called "ring signature," and it is based on an ElGamal signature scheme that has been modified. In comparison to its predecessors, this system has a number of significant advantages. Since an attacker can create a ring in any way they like and alter an existing ring signature to create a true one, the suggested ring signature approach is not secure. This research suggests a way to achieve the same goal without adding extra communication or processing complexity. Experts in ring signatures have investigated the aforementioned attack vector. Systems that authenticate users and agree on keys while protecting their privacy have been the subject of much research in recent years for application in wireless sensor networks (WSNs) and the Internet of Things (IoT).

Distant user authentication, as opposed to hop-by-hop message authentication, is the subject of this research. Investigation into easy-to-implement, secure authentication methods for the Internet of Things (IoT) and wireless sensor networks has increased in tandem with rising worries about the physical security of these devices. Even if

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/19
DOI: https://doi.org/10.5281/zenodo.19131591

an attacker manages to take over a sensor node, the physical layer can be protected with the help of the Link Quality Indicator (LQI), which displays the parameters of the wireless channel, and Physically Unclonable Functions (PUFs). For IoT and Wireless Sensor Networks (WSNs), there are a plethora of lightweight verification approaches accessible today.

4. IMPLEMENTATION

IOT Device Source

The content is sent to the end users (a, b, c, e, and f) by the router after the Source component has enabled navigation to the requested file, started the nodes with a digital signature, and given it.

Router

Fast and precise data transmission to its final destination is the primary function of the router. All of the router nodes' Media Access Control (MAC) addresses are displayed by the numerals n1, n2,..., n13. The node's bandwidth is communicated by this address. Any suspect nodes, whether malicious or just traffic nodes, will be reported by the router to the IDS Manager. The router provides visibility into the identifiers, injections, digital signatures, bandwidth use, and node health of the network. Our ability to modify node statuses and distribute bandwidth more equitably depends on this data.

IDS Manger

The IDS administrator is the individual responsible for overseeing the Intrusion Detection System (IDS). Examining and removing any suspicious or harmful stuff that enters or exits the network is their primary responsibility. The IDS manager divides the time in half based on the router's performance.

Training Phase:

Normal Profile Generation creates and stores the normal profiles for various types of valid traffic data throughout the Training Phase.

Test Phase:

Building profiles for different kinds of traffic discovered during testing is possible with the Tested Profile Generation tool. The Attack Detection module compares the evaluated profiles to their standard database versions once it has them.

Sinks

The router is able to forward the data file from the service provider to the correct location if the module identifies a malicious or traffic node. Following data collection from the router, the IDS Manager applies filters before creating an attacker profile.

Forgery Attacker and Packet Droppers

The Attack Detection module can identify Denial-of-Service (DoS) attacks by distinguishing between malicious nodes or traffic and legitimate traffic using a threshold-based classifier. When testing, a potentially dangerous actor could, for instance, create a false signature and transmit it to any router node they want using a threshold-based classifier. This biased statement can be seen on an updated criminal profile.

5. CONCLUSION

The system that verifies messages and maintains the privacy of users' information is found to have a vulnerability. We have included a solution that can potentially reduce unforeseen expenses. Additionally, we demonstrated a novel method for message authenticity verification that further prioritizes secrecy and anonymity.

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/19
DOI: https://doi.org/10.5281/zenodo.19131591

Since this approach is compatible with many different security protocols and configurations, it simplifies the process of connecting various smart devices to IoT networks. We also used a combination of online and offline calculation approaches to improve the efficiency and scalability of the first proposal.

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.

[11] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

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

[13] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-byhop authentication scheme for filtering of injected false data in sensor networks," in Security and Privacy (S&P), IEEE Symposium on, 2004, pp. 259–271.

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

[15] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and