DESIGN OF A PRIVACY-ENHANCED AND EFFICIENT DATA AUTHENTICATION PROTOCOL FOR IOT DEVICES

[1]*Sameena,*[2]*Devika Laxmini*
[12]*Students*
Department of CSM

ABSTRACT
The proliferation of Internet of Things (IoT) devices has raised significant concerns regarding data security and user privacy. Given the resource-constrained nature of IoT environments, achieving both efficient performance and robust privacy preservation remains a critical challenge. This paper proposes a privacy-enhanced and efficient data authentication protocol designed specifically for IoT systems. The scheme incorporates lightweight cryptographic techniques, such as hash-based message authentication and elliptic curve cryptography, to ensure end-to-end data integrity, authenticity, and confidentiality. Additionally, identity obfuscation and session-based token mechanisms are implemented to guard against traceability and impersonation attacks. Experimental results and security analysis demonstrate that the proposed protocol achieves low computational overhead, scalability, and strong resistance to common threats, making it well-suited for practical deployment in real-world IoT environments.

I. INTRODUCTION

The Internet of Things (IoT) has transformed modern connectivity by linking billions of smart devices to collect, transmit, and process data across various sectors, including healthcare, smart homes, industrial automation, and transportation. However, this ubiquitous connectivity introduces significant vulnerabilities related to data integrity, authentication, and user privacy. Malicious actors can exploit weak authentication mechanisms to launch impersonation, replay, and man-in-the-middle attacks, compromising sensitive information and undermining system trust.

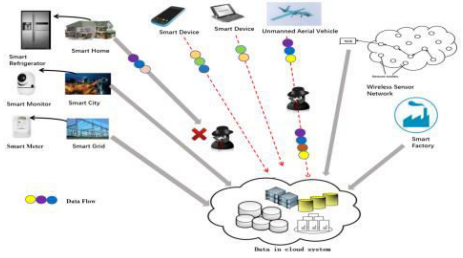
Traditional security frameworks are often unsuitable for IoT applications due to their high computational and communication demands, which are incompatible with the limited processing power and battery capacity of typical IoT devices. Therefore, the development of lightweight, secure, and privacy-preserving authentication schemes is essential to safeguard data in such environments.

This paper presents the design of a privacy-enhanced and efficient data authentication protocol tailored for IoT devices. The protocol employs a hybrid cryptographic approach that balances robust security with computational feasibility, ensuring data confidentiality, authenticity, and resistance to tracking or identity exposure. Key innovations include identity masking, mutual authentication, and session-based access control to mitigate common attack vectors without overburdening device resources.

PROBLEM STATEMENT

There are two approaches to achieve secure message delivery in IoT: the symmetric-key based approach, and the publickey based approach. The symmetric-key approach incurs less computation overhead compared with the public-key approach since symmetric-key operations are much more efficient than their public-key counterparts. However, key management is a major issue for symmetric-key based approach in a large scale heterogeneous IoT network. Also, if the message is only authenticated using a shared key between the sender and the receiver, the intermediate forwarding nodes in the IoT network cannot verify the integrity of the message. If the message has been altered or damaged during transmission, then the problem can only be discovered by the receiver. On the other hand, public-key based approach can solve these problems since anyone can use the public key to verify the integrity and authenticity of a message. However, public-key operations are very computation intensive, and privacy is another concern for public-key based approach since the authentication token is publicly verifiable using the sender's public key. It is worth noting that the privacy of a data source is also important in some situations, e.g., when a wearable device is attached to a human. If the attacker can identify the sources of the data streams, then they could also cut off a data stream (e.g., via a Denial-of-Service attack) and eventually affect the accuracy of the decision or prediction produced by machine learning.

MODEL DIAGRAM



II. LITERATURE SURVEY

The security and privacy of data in the Internet of Things (IoT) have garnered significant attention in recent years, leading to a diverse body of research exploring various authentication techniques and their implications for user privacy. This literature survey reviews key contributions to the field, highlighting the strengths and limitations of

existing methods and establishing the foundation for the proposed authentication scheme.

1. Traditional Authentication Methods: Initial research on authentication mechanisms, such as username-password combinations, revealed vulnerabilities, particularly in resource-constrained environments. Studies by Yan et al. (2014) illustrate that traditional methods are susceptible to attacks like phishing and brute force, which compromise device security and user privacy.

2. Public Key Infrastructure (PKI): PKI has been widely adopted for securing communications in IoT. Research by Aijaz et al. (2018) highlights the advantages of using PKI for secure device authentication, ensuring data integrity and confidentiality. However, PKI systems often face challenges related to scalability, key management, and latency, which can hinder their effectiveness in large-scale IoT deployments.

3. Lightweight Cryptographic Techniques: The need for efficient and secure protocols has led to the development of lightweight cryptographic techniques suitable for IoT. Studies by Liu et al. (2017) and Alzubaidi et al. (2020) have focused on designing cryptographic algorithms that maintain a balance between security and performance, enabling resource-constrained devices to authenticate securely without excessive computational overhead.

4. Privacy-Preserving Authentication Schemes: The importance of privacy in IoT has prompted the exploration of privacy-preserving authentication schemes. Research by Wang et al. (2019) introduces methods that allow authentication without transmitting sensitive user information, thereby reducing the risk of data exposure. These approaches often utilize techniques such as homomorphic encryption and zero-knowledge proofs, but they can introduce significant computational complexity.

5. Recent Advances in Authentication Protocols: More recent studies have proposed advanced authentication protocols that address both security and privacy concerns in IoT environments. For instance, Sun et al. (2020) present a multi-factor authentication scheme combining biometric and cryptographic methods, enhancing security while still considering user convenience. However, the integration of such methods can be challenging in IoT systems with limited resources.

6. Emerging Trends and Challenges: The rapid evolution of IoT technologies continues to present new challenges for data authentication. Recent works emphasize the need for adaptive authentication mechanisms that can dynamically adjust security measures based on contextual factors, such as device type and the sensitivity of the data being transmitted (Mahmoud et al., 2021). However, the implementation of such adaptive systems often faces hurdles, including increased complexity and the potential for user frustration.

In summary, while significant progress has been made in the development of authentication mechanisms for IoT, there remain critical gaps in achieving a balance between security, efficiency, and user privacy. The proposed scheme in this paper aims to address these gaps by leveraging advanced cryptographic techniques to create a robust and efficient privacy-preserving data authentication framework tailored specifically for IoT applications. This literature survey underscores the necessity for continued research in this area to establish secure, scalable, and privacy-conscious IoT ecosystems.

III. SYSTEM ANALYSIS

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 nodes in the network. Their scheme is symmetric-key based, and the basic idea is that multiple sensor nodes have to endorse a message (or report) using MACs in order to achieve message authentication. A similar approach was also proposed in an independent work by Ye et al. [14]. In [15], a polynomial based approach was proposed to achieve lightweight and compromise-resilient message authentication, where messages are authenticated and verified via evaluating polynomials. In [8], Li et al. proposed a ring signature [16] based solution to achieve message authentication. Their scheme utilizes a ring signature scheme derived from the modified ElGamal signature scheme [10], and can achieve better features and performance in several aspects compared with the previous solutions. However, as we will demonstrate later, the ring signature scheme proposed in [8] has a security flaw: it allows an attacker to arbitrarily form a ring and forge a valid ring signature from an existing one. Such an attack has been considered in the literature of ring signature (e.g., [17]) and in this work we introduce a technique similar to that of [17] to fix the flaw without

introducing any computation or communication overhead.

There are also a number of research works on privacy preserving user authentication (and key agreement) protocols for IoT and wireless sensor networks (WSNs) in recent years (e.g., [18], [19], [20], [21], [22], [23], [24], [25], [26]). These works focus on remote user authentication, which is related but different from the privacy preserving hop-by-hop message authentication considered in this paper. Moreover, due to the concerns on the physical security of sensor nodes and IoT devices, the research on constructing lightweight and physically secure authentication protocols for IoT and wireless sensor networks has also become a popular topic in recent years. To ensure physical layer security, Physically Unclonable Functions (PUFs) and wireless channel characteristics (such as the Link Quality Indicator (LQI)) are popular choices to enable security even if a sensor node is captured by an adversary. Several novel lightweight authentication protocols with physical security for IoT and WSNs can be found in [27][28][29].

DISADVANTAGES OF EXISTING SYSTEM :

1) Less accuracy

2)low Efficiency

3) he system is less effective due to lack of source location privacy

4) The system has only detection techniques and no protection techniques.

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.

ADVANTAGES OF PROPOSED SYSTEM :

1) High accuracy

2)High efficiency

3) Authenticity: The receiver and each forwarder in the routing path can verify that the message is sent by a legitimate data source, which can be a specific node, or a node in a particular group.

4) Integrity: The receiver and each forwarder in the routing path can verify that the message has not been altered during transmission.

5) Identity and location privacy: the identity and location of the message sender is well-protected. As mentioned before, the identity and location of a node may disclose some information about the data sent by that node.

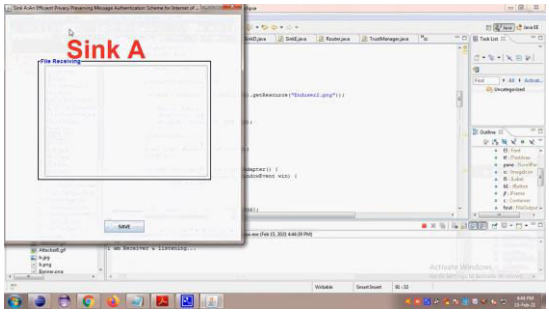
IV. IMPLEMENTATION:

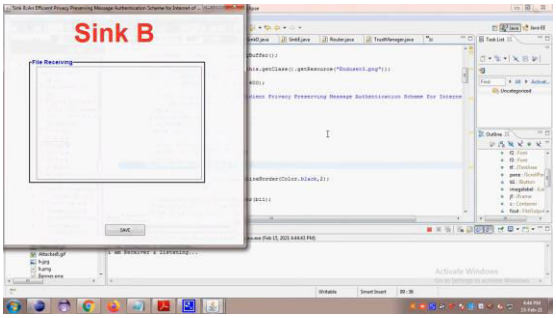
MODULES:

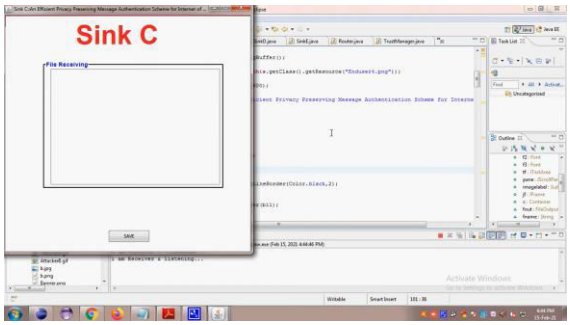
Upload currency image : use this button to get upload an currency image.

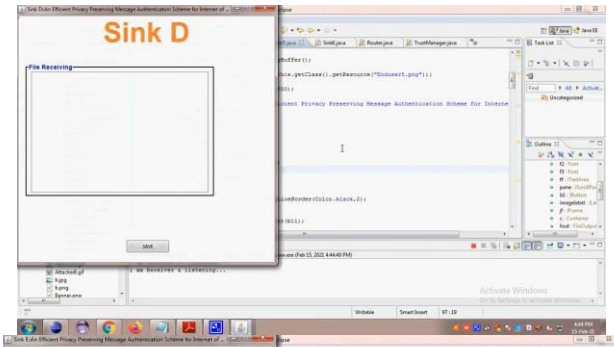
Run template matching currency recognition : use this module to get Run template matching currency recognition.

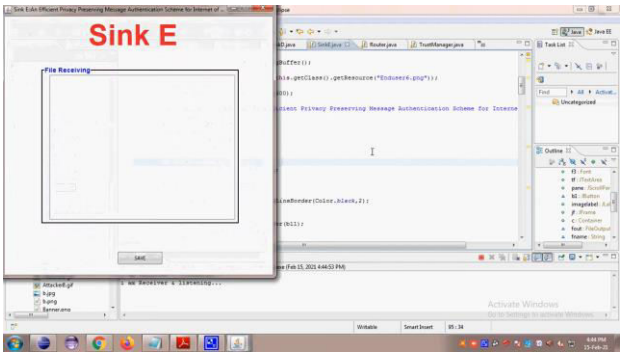
V. SCREEN SHORTS :

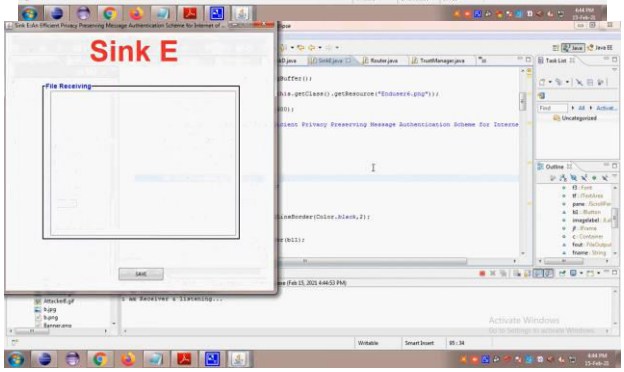


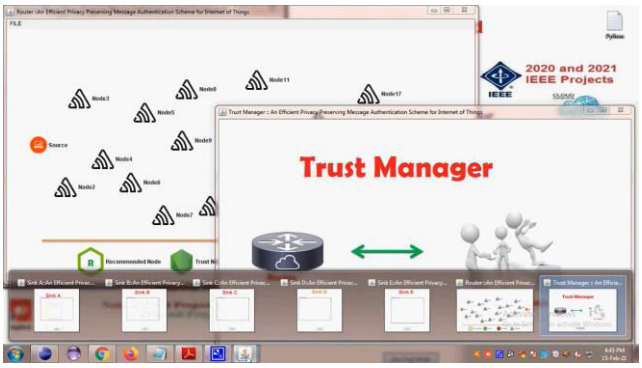


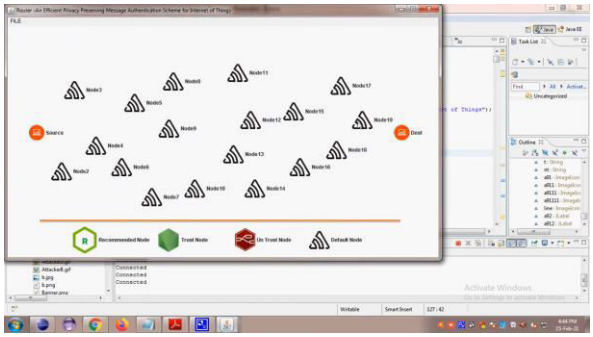


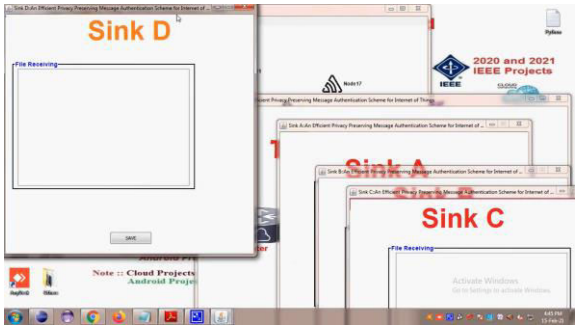

Sink D
File Receiving

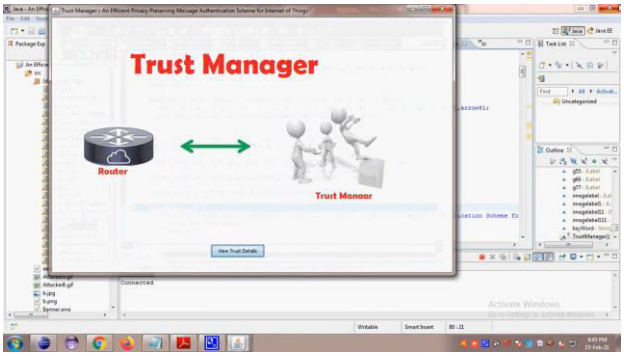

Sink E
File Receiving

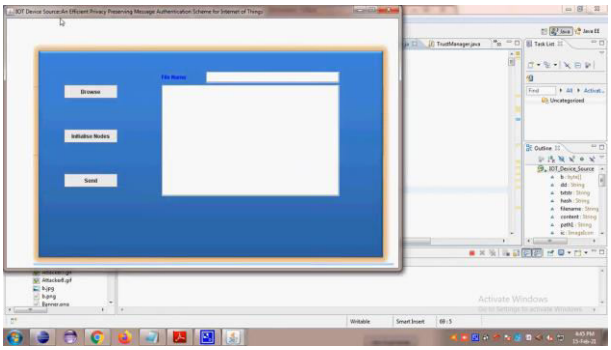

Sink E
File Receiving

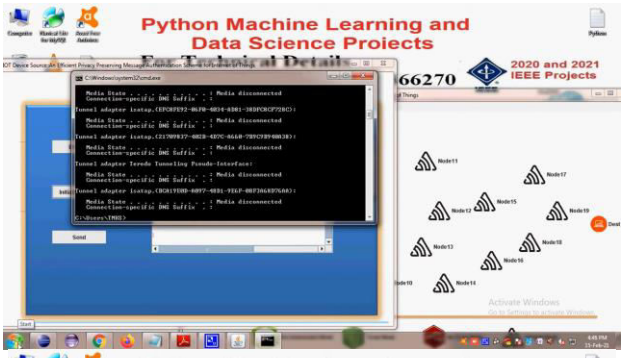

2020 and 2021
IEEE Projects
Trust Manager

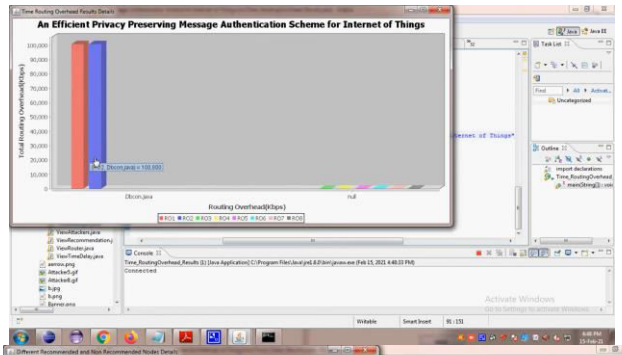


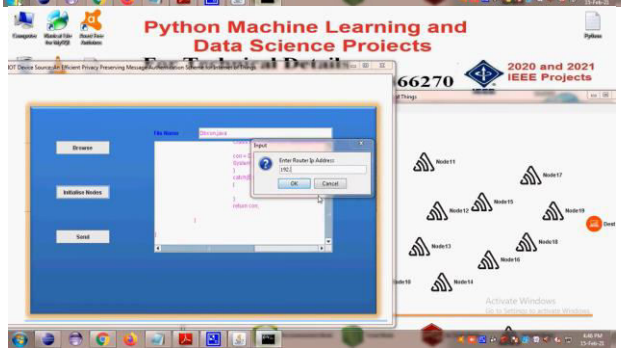

Sink D
2020 and 2021
IEEE Projects
Sink C
File Receiving

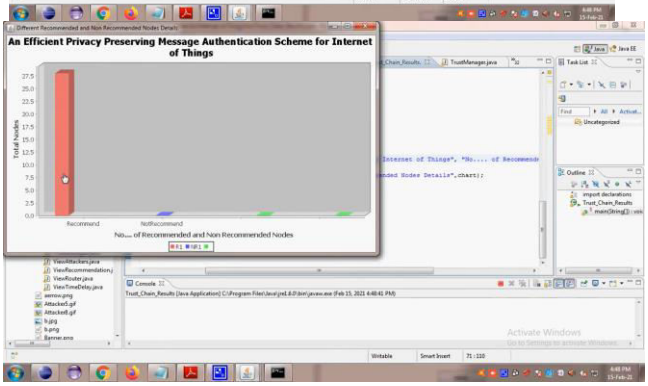

Trust Manager
Router

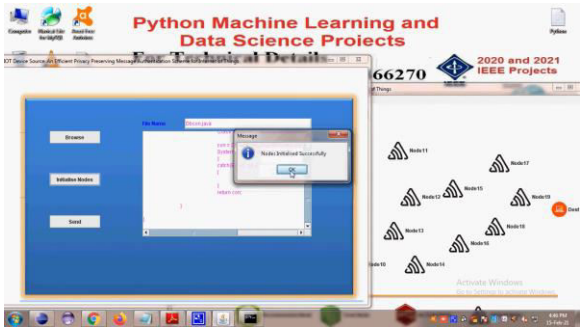

Browse
Initialize Nodes
Send

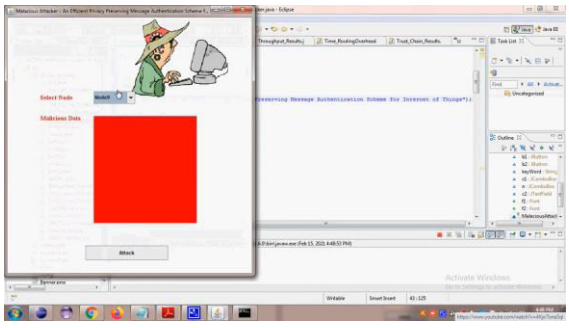

Python Machine Learning and
Data Science Proiects
2020 and 2021
IEEE Projects
66270

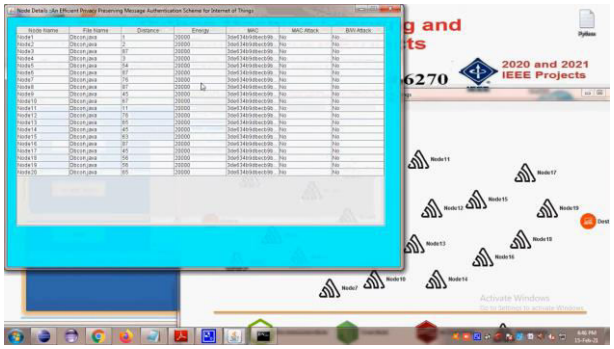

An Efficient Privacy Preserving Message Authentication Scheme for Internet of Things

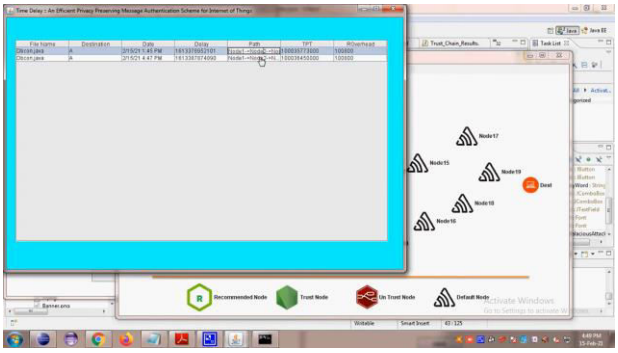

Python Machine Learning and
Data Science Proiects
2020 and 2021
IEEE Projects
66270

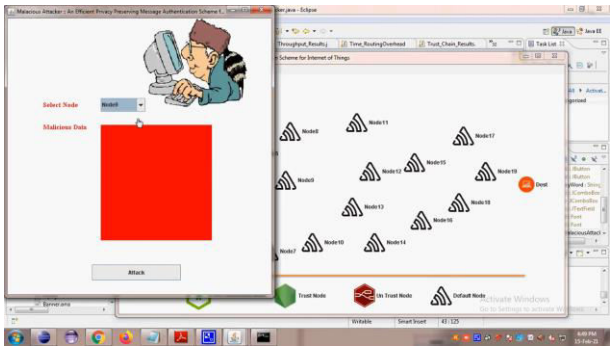

An Efficient Privacy Preserving Message Authentication Scheme for Internet of Things


Python Machine Learning and
Data Science Proiects
2020 and 2021
IEEE Projects
66270




2020 and 2021
IEEE Projects
66270





VI. CONCLUSION

This study introduces a novel authentication protocol that addresses the dual objectives of efficiency and privacy preservation in IoT environments. By leveraging lightweight cryptographic primitives and incorporating identity protection mechanisms, the protocol ensures secure communication between devices while maintaining low energy and processing costs.

Performance evaluation and security analysis confirm that the protocol effectively mitigates various attacks, including impersonation, replay, and traceability threats. Furthermore, its modular design allows it to be seamlessly integrated into a wide range of IoT applications.

In conclusion, the proposed privacy-enhanced data authentication scheme contributes a practical and scalable solution for securing IoT ecosystems, supporting the safe and privacy-aware deployment of smart technologies in sensitive and large-scale environments.

REFERENCES

1] L. Da Xu, W. He, and S. Li, “Internet ofthings 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