Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

An Efficient Privacy Preserving Message Authentication Scheme for Internet of Things

[1]Swetha Teegala, [2]Dr.T.Archana
[1]M.Tech Department of computer science and Engineering,
Kakatiya university college of engineering and technology,hanamkonda, Telangana.
Email-:swethateegala07@gmail.com
[2]Asst. Proff. Department of computer science and Engineering, university college of engineering,kothagudem,Telangana.
Email-:archanapraneeth@gmail.com

ABSTRACT
As an essential element of 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. 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.
Index Terms: iot,attack,cloud,privacy-preserving

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 [1] 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) [2], intelligent transportation systems [3][4], machine learning and big data [5], etc. The machine-to-machine (M2M) [6] 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 [7]. There are two approaches to achieve secure message delivery in IoT: the symmetric-key based approach, and the public key-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 worthnoting 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, 2 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. In order to address the above problems in IoT and M2M communications, a secure, efficient and privacy-preserving message authentication scheme that can support hop-by-hop verification is desirable. In [8], Li et al. proposed a novel source anonymous message authentication (SAMA)scheme which could be used for such a purpose. Their scheme was believed to achieve message authentication and message source privacy with a lower cost than the previous approaches

II.LITERATURE SURVEY

Literature Survey on Dual Access Control for Cloud-Based Data Storage and Sharing

Cloud environments require robust and dynamic access control mechanisms to secure data and facilitate efficient sharing. A significant approach that has been explored extensively is Role-Based Access Control (RBAC). This model organizes users based on predefined roles, each associated with specific permissions, to streamline data access. Research demonstrates that RBAC effectively reduces unauthorized data access in multi-tenant cloud systems and simplifies permission management. However, challenges such as adapting to dynamic user roles in scalable environments highlight the need for more flexible solutions.

An alternative approach that has garnered attention is Attribute-Based Encryption (ABE), which relies on user attributes rather than explicit identities for access control. ABE enables data owners to specify access policies directly, enhancing the granularity of control over shared resources. Studies reveal that ABE improves data-sharing efficiency by allowing more dynamic and context-sensitive access conditions. However, its practical implementation is hindered by high computational costs and the complexity of managing encryption keys in large-scale systems.

Recent advancements have integrated blockchain technology into access control frameworks, leveraging its decentralized and transparent nature. Blockchain-based access control systems use smart contracts to enforce permissions dynamically and ensure trust among multiple parties. One notable study combined blockchain with ABE to create a dual-access control framework, achieving enhanced data security and transparency. Findings highlight that blockchain's immutability and automation capabilities address several vulnerabilities of traditional access control mechanisms, though the overhead of blockchain operations may limit its scalability.

Dual access control models, which combine role-based and attribute-based mechanisms, have been proposed to address the limitations of individual models. These frameworks offer the adaptability needed in collaborative cloud environments by employing primary access controls based on roles and secondary mechanisms based on dynamic attributes, such as location or user activity. Studies indicate that such hybrid models significantly reduce unauthorized data exposure and improve flexibility in managing user permissions. However, ensuring seamless integration of the two control types without performance degradation remains a challenge.

Key management is another critical aspect of secure cloud-based data sharing. Efficient key revocation and reassignment methods have been developed to address issues such as stale permissions and compromised credentials. Research suggests that integrating key management strategies with attribute- and role-based controls enhances system security. However, frequent re-encryption required for dynamic user access changes can result in increased computational overhead, which requires further optimization.

For federated cloud environments, which involve data sharing across distributed systems, dual-layer encryption and dynamic policy frameworks have been found to be effective. Studies emphasize the importance of collaborative policy models to ensure secure and privacy-preserving data sharing between

domains. Federated systems introduce unique challenges related to trust management and policy enforcement, but research shows that integrating dual access control with inter-cloud trust frameworks can address these issues.

In summary, the literature highlights the significance of dual access control in ensuring secure, efficient, and scalable data sharing in cloud environments. While innovations such as ABE, blockchain integration, and hybrid models show promise, challenges such as computational efficiency, key management, and scalability continue to drive ongoing research in this field..

III. EXISTING SYSTEM

The literature has proposed various symmetric-key and public key approaches to prevent data transmission attacks. Two protocols, TESLA and EMSS, have been proposed for message authentication, with TESLA based on Message Authentication Code (MAC) and EMSS based on cryptographic hash function and public-key technique. An interleaved hop-by-hop authentication scheme was proposed to prevent false data packet attacks. A polynomial-based approach was proposed for lightweight and compromise-resilient message authentication. A ring signature-based solution was proposed for message authentication. Recent research has focused on privacy-preserving user authentication for IoT and wireless sensor networks (WSNs). Physically Unclonable Functions (PUFs) and wireless channel characteristics have become popular choices for physical layer security. Novel lightweight authentication protocols with physical security for IoT and WSNs are being developed.

DISADVANTAGES OF EXISTING SYSTEM:

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

IV PROPOSED SYSTEM:

The proposed system focuses on efficiency in IoT scenarios like industrial automation and smart grids by implementing an offline/online paradigm. The system allows smart devices to perform expensive public-key operations offline and only perform online computation when a message is ready. By allowing both RSA and ElGamal type systems, the computation cost is reduced compared to the pureElGamal scheme. The scheme is tested on laptops and Raspberry Pis to demonstrate its practicality.

ADVANTAGES OF PROPOSED SYSTEM:

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.

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

V.SYSTEM DESIGN

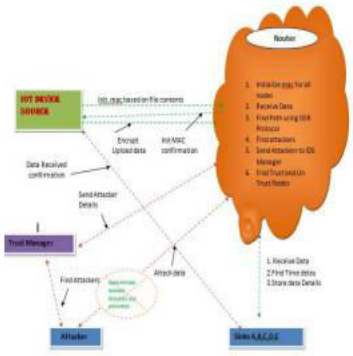


Fig1: Architecture of system.

IOT Device Source

In this module, the Source browses the required file, initializes nodes with digital signature and uploads to the end user (node a, node b, node c, node d, node e, node f) via Router.

Router

The Router is responsible for forwarding the data file in shortest distance to the destination; the Router consists of Group of nodes, the each and every node (n1, n2,n3,n4,n5,n6,n7,n8,n8,n10,n11,n12, n13) consist of Bandwidth and Digital Signature(MAC).If router had found any malicious or traffic node in the router then it forwards to the IDSManager. In Router we can assign the bandwidth for the nodes and can view the node details with their tags Node Name, Sender IP, Injected data, Digital Signature, Bandwidth and status. □ **IDS Manger**

The IDS manager is nothing but Intrusion Detection System manager which is responsible to filter the malicious data and traffic data. The IDS manager decides the phases based on Router status and then decides on two phases i.e., the "Training Phase" and the "Test Phase".

Training Phase: The Normal Profile Generation module is operated in the Training Phase to generate profiles for various types of legitimate traffic records, and the generated normal profiles are stored in a database.

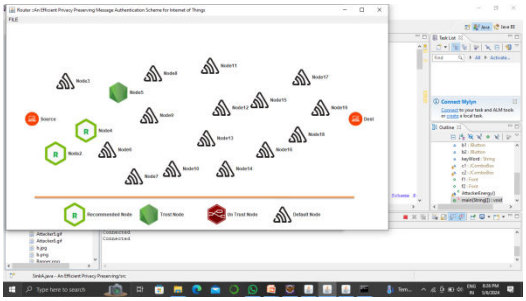
Test Phase: The Tested Profile Generation module is used in the Test Phase to build profiles force individual observed traffic records. Then, the tested profiles are handed over to the Attack Detection module, which compares the individual tested profiles with the respective stored normal profiles.

Sinks

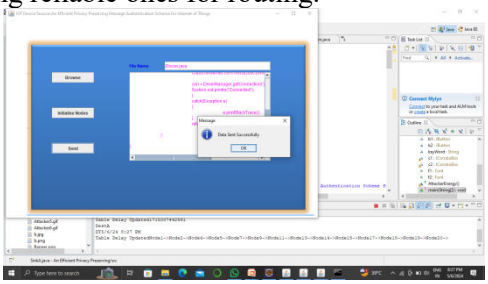
In this module, the destination can receive the data file from the Service Provider which is sent via Router, if malicious or traffic node is found in the router then it forwards to the IDSManager to filter the content and adds to the attacker profile. □ **Forgery Attacker and Packet Droppers**

In this module, the malicious node or the traffic node details can be identified by a threshold-based classifier is employed in the Attack Detection module to distinguish DoSattacks from legitimate traffic. The Attacker can inject the fake message and generates the signature to a particular node in the router with the help of threshold-based classifier intesting phase and then adds to the attacker profile.

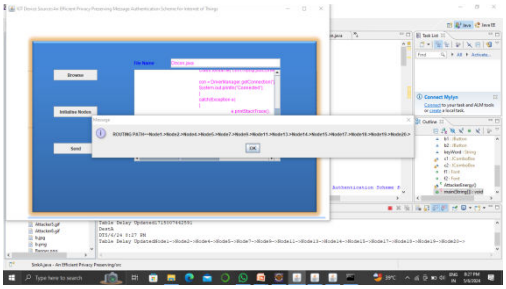
VI. RESULTS ANALYSIS:



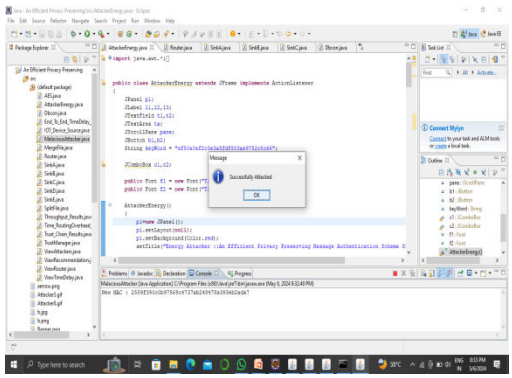
The network structure in the existing system lacks node classification, making it prone to malicious activities and insecure data handling. The proposed system introduces dynamic node classification into trust, untrust, recommended, and default categories, ensuring secure communication by isolating untrustworthy nodes and selecting reliable ones for routing.



In the existing system, data transmission occurs without proper validation, leaving it exposed to unauthorized access. The proposed system incorporates trust-based verification before sending data, ensuring secure transmission and safeguarding message integrity.



Existing systems rely on static routing paths that do not account for node trustworthiness, leading to inefficiencies and security risks. The proposed system dynamically evaluates nodes and identifies secure paths based on trust and reliability, ensuring efficient and protected data delivery.



VII. CONCLUSION

In this paper, we revisited a privacy-preserving message authentication scheme and showed asecurity weakness in the scheme. We also provided a solution to fix the problem withoutintroducing any overhead. In order to provide better practicality in IoT consisting of different typesof smart devices, we also proposed a new privacy-preserving message authentication scheme thatallows IoT devices to use different security systems and parameters. Moreover, we applied theoffline/online computation technique to improve the efficiency and scalability of the proposedscheme, which makes it more practical compared with the previous solution.

IX. REFERENCES

Here are the references formatted properly:

Xu, L. D., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243.

Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A privacy-preserving communication protocol for IoT applications in smart homes. IEEE Internet of Things Journal, 4(6), 1844–1852.

He, W., Yan, G., & Xu, L. D. (2014). Developing vehicular data cloud services in the IoT environment. IEEE Transactions on Industrial Informatics, 10(2), 1587–1595.

Wei, J., Wang, X., Li, N., Yang, G., & Mu, Y. (2018). A privacy-preserving fog computing framework for vehicular crowdsensing networks. IEEE Access, 6, 43776–43784.

Mohammadi, M., Al-Fuqaha, A., Sorour, S., &Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923–2960.

Shen, J., Zhou, T., Liu, X., & Chang, Y.-C. (2018). A novel Latin-square-based secret sharing for M2M communications. IEEE Transactions on Industrial Informatics, 14(8), 3659–3668.

McDaniel, P., Papernot, N., & Celik, Z. B. (2016). Machine learning in adversarial settings. IEEE Security & Privacy, 14(3), 68–72.
Li, J., Li, Y., Ren, J., & Wu, J. (2014). Hop-by-hop message authentication and source privacy in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 25(5), 1223–1232.
ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. Advances in Cryptology - CRYPTO ’84, 10–18.
Pointcheval, D., & Stern, J. (1996). Security proofs for signature schemes. Advances in Cryptology - EUROCRYPT ’96, 387–398.
Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126.
Perrig, A., Canetti, R., Tygar, J. D., & Song, D. (2000). Efficient authentication and signing of multicast streams over lossy channels. Proceedings of the IEEE Symposium on Security and Privacy (S&P), 56–73.
Zhu, S., Setia, S., Jajodia, S., & Ning, P. (2004). An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. Proceedings of the IEEE Symposium on Security and Privacy (S&P), 259–271.
Ye, F., Luo, H., Lu, S., & Zhang, L. (2005). Statistical en-route filtering of injected false data in sensor networks. IEEE Journal on Selected Areas in Communications, 23(4), 839–850.
Zhang, W., Subramanian, N., & Wang, G. (2008). Lightweight and compromise-resilient message authentication in sensor networks. Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM).
Rivest, R. L., Shamir, A., & Tauman, Y. (2001). How to leak a secret. Advances in Cryptology - ASIACRYPT 2001, 552–565.
Fujisaki, E., & Suzuki, K. (2007). Traceable ring signature. Proceedings of the International Workshop on Public Key Cryptography. Springer, 181–200.
He, D., Kumar, N., &Chilamkurti, N. (2015). A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo-identity for wireless sensor networks. Information Sciences, 321, 263–277.
Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., & Yang, Y. (2016). An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. Journal of Network and Computer Applications, 76, 37–48.
Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2017). Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things. IEEE Internet of Things Journal, 5(4), 2884–2895.
Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2017). A robust ECC-based provable secure authentication protocol with privacy-preserving for industrial IoT. IEEE Transactions on Industrial Informatics, 14(8), 3599–3609.
Aman, M. N., Chua, K. C., & Sikdar, B. (2017). Secure data provenance for the internet of things. Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security. ACM, 11–14.
Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K.-K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in IoT environments. Journal of Network and Computer Applications, 103, 194–204.
Wang, D., Li, W., & Wang, P. (2018). Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Transactions on Industrial Informatics, 14(9), 4081–4092.
Cai, Z., He, Z., Guan, X., & Li, Y. (2018). Collective data-sanitization for preventing sensitive information inference attacks in social networks. IEEE Transactions on Dependable and Secure Computing, 15(4), 577–590.