Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

EFFICIENT MESSAGE AUTHENTICATION FOR PRIVACY PRESERVING INTERNET OF THINGS

[#1]MUPPU SANDHYARANI, Department of *MCA*,
[#2]Dr.V.BAPUJI, *Associate Professor& HOD*,
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT: In recent years, the Internet of Things (IoT) has evolved fast as a key component of the next generation Internet. IoT devices generate/collect massive amounts of data that machine learning and big data analytics can use for a variety of purposes, including improving people's lives. Because IoT relies on machine-to-machine (M2M) communication, data security and privacy are critical challenges that must be addressed in order to prevent various cyber assaults (such as impersonation and data pollution/poisoning). Nonetheless, building lightweight and diverse IoT security solutions is a difficult challenge due to limited processing power and the diversity of IoT devices. We present an efficient, safe, and privacy-preserving message authentication mechanism for IoT in this work. Our technique is more versatile and efficient than prior systems since it supports IoT devices with varied cryptography settings and enables for offline/online computing.

Index Terms—Internet of Things, hop-by-hop authentication, integrity, source privacy.

1. INTRODUCTION

The Internet of Things (IoT) makes it possible to build a system out of many disparate parts, each of which contributes to the whole in some way. With machine learning, data may be easily shared and retrieved among programs with little to no human intervention required. After the development of computers and the Internet, this innovation is the third most important in the field of information technology. Interactions between the IoT and various sectors of society and the economy pave the way for the development of a pervasive online existence. That way, people can talk to things and, more crucially, to other people and things that are connected to them. Several new fields of study have emerged thanks to the Internet of Things (IoT), such as smart home systems (SHSs), intelligent transportation systems (ITSs), machine learning, big data, and others.

Machine-to-machine (M2M) communication, specifically between a massive number of IoT devices, will be the main form of network traffic in the future. Machine learning and big data analytics, to name just two examples, rely heavily on the authenticity and reliability of the massive amounts of data collected and transmitted by IoT devices. Data that has been intentionally introduced or manipulated can result in incorrect forecasts and choices. Therefore, it is crucial to maintain the validity and integrity of the gathered data to ensure the veracity and precision of machine learning and big data analysis.

Both a public-key based strategy and a symmetric-key approach have emerged to guarantee safe message delivery in the IoT domain. Since symmetric-key operations are more efficient than public-key operations, the computational cost of the symmetric-key methodology is lower than that of the public-key method. However, in the context of symmetric-key based techniques inside a heterogeneous and extensive IoT network, the management of cryptographic keys presents a considerable difficulty. Furthermore, the intermediate

forwarding nodes within the IoT network lack the capability to verify the integrity of the message if the authentication of the message is confined to a shared key established between the sender and the recipient. In the event that information is corrupted or garbled while being transmitted, only the intended recipient will be able to recognize any problems.

However, these problems can be overcome with the help of a public-key approach, as anyone can use the public key to ensure the truthfulness and reliability of a message. With public-key methods, the authentication token can be verified publicly using the sender's public key, which raises serious privacy concerns. It's also important to remember that public-key operations need a lot of processing power.

It is important to remember that protecting the privacy of the data source is equally important in some cases, especially when a wearable gadget is connected to an individual. If an attacker can determine where a data stream is coming from, they can disrupt its transmission, for example by launching a denial-of-service assault. The conclusion would be a decrease in the precision of the machine learning verdict or forecast. Developing a safe, efficient, and privacy-conscious technique of message authentication that can efficiently handle hop-by-hop verification is crucial for overcoming the aforementioned challenges in the field of Internet of Things (IoT) and Machine-to-Machine (M2M) communications. A novel method, source anonymous message authentication (SAMA), was introduced by Li et al. and may be applicable here. They hypothesized that their method would be cheaper than existing methods of message authentication and message source secrecy.

2. RELATED WORK

Both symmetric-key and public-key techniques, which use a pair of keys, have been discussed in the literature as means to secure data transmission against a wide range of assaults. There were two methods proposed for determining whether or not a communication was genuine. With a one-way key chain and a sender-determined release time, the TESLA protocol was the first of its kind. The given phrase conforms to the specifications of the MAC. However, TESLA has a serious issue in synchronizing devices across a wide network. The second system, referred to as EMSS, allows users to achieve the non-repudiation security feature. The system is functional because of the use of public-key techniques and secure hash algorithms. To prevent attackers or compromised nodes from seeding the network with bogus data, an interleaved hop-by-hop authentication mechanism can be implemented.

Many sensor nodes in a symmetric-key-based system employ MACs (Message validation Codes) to validate the veracity of a message or report. In order to verify messages, this is required. This technique adheres to one of the basic principles in the industry. Polynomial-based message authentication was developed by Ye (year). Polynomials are used in this technique to ensure the authenticity of transmitted data. This approach has the advantages of being simple to implement and challenging to alter. In their study, Li et al. demonstrate a novel application of ring signatures to the problem of message authentication. The system in question employs a technique known as "ring signature," which is derived from an adjusted version of the ElGamal signature scheme. This system improves upon its predecessors in a number of key respects. This research will demonstrate that the proposed ring signature approach is insecure due to the fact that an attacker can construct a ring in any way they see fit and create a valid ring signature by modifying an existing ring signature. This paper proposes a solution that does not involve any more computational or communication complexity while accomplishing the same goal. Researchers in the realm of ring signatures have discussed the aforementioned method of attack. Privacy-preserving user authentication and key agreement systems for the Internet of Things (IoT) and wireless sensor networks (WSN) have been the subject of extensive research in recent years.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

This study primarily focuses on remote user authentication, which is similar to but distinct from hop-by-hop message authentication. There has also been a rise in research towards simple yet secure authentication methods for IoT and wireless sensor networks in response to growing concerns about the physical security of sensor nodes and IoT devices. Even if an attacker has seized control of a sensor node, the physical layer can be secured with the help of Physically Unclonable Functions (PUFs) and the Link Quality Indicator (LQI), which displays the parameters of the wireless channel. There are a variety of lightweight current verification methods in the realms of the Internet of Things (IoT) and Wireless Sensor Networks (WSNs).

3. SYSTEM DESIGN

To further accommodate the restricted processing power of IoT devices, we incorporate the offline/online paradigm into our system's architecture. Efficiency is paramount in real-world Internet of Things applications like industrial automation, environmental monitoring, smart grids, etc. In the proposed approach, the smart device only does the online calculation when the message to be transmitted is being prepared, freeing up resources for other uses while the device is not in use to handle the expensive public-key activities. In contrast to the pure ElGamal approach provided in [8], we are able to lower the computation cost by permitting both the RSA and ElGamal type systems, which is an intriguing observation. It may seem contradictory, given that it is well-known that the ElGamal approach, which uses Elliptic Curve Cryptography (ECC), is far faster than the RSA technique. Because the RSA public exponent e can be rather modest, our hybrid technique only needs to perform RSA signature verification for the majority of RSA nodes, which is a relatively quick procedure. The new SAMA scheme's speed is compared to the old scheme's speed during signature generation and verification. To further show the efficacy of our approach, we implemented it on a laptop and a Raspberry Pi..

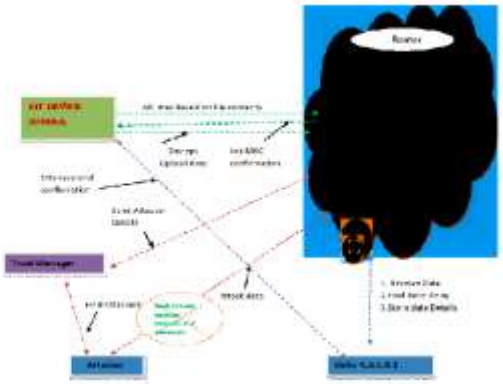

Fig 1. ARCHITECTURE DIAGRAM

4. IMPLEMENTATION

IOT Device Source

After the Source component has allowed navigation to the given file, launched the nodes with a digital signature, and transferred the material, it is forwarded to the end users (a, b, c, e, and f) via the Router.

Router

The router's primary function is to quickly and efficiently transmit data to its eventual destination. Each of the router's nodes, denoted by the numbers n1, n2, n3, n4, n5, n6, n7, n8, n10, n11, n12, and n13, receives a certain amount of bandwidth that is determined by its Media Access Control (MAC) address. The router will notify the IDS Manager of any suspicious nodes it has identified, whether they be malicious or traffic nodes. The router provides visibility into network nodes' identities, injections, digital signatures, bandwidth usage, and status. Using this information, we may fine-tune node statuses and share out bandwidth more evenly.

IDS Manger

The Intrusion Detection System (IDS) is managed and monitored by the IDS administrator. Their primary function is to examine incoming and outgoing network traffic for suspicious or harmful material and eliminate it. Depending on the state of the router, the IDS manager splits the time into two periods.

Training Phase:

During the Training Phase, the normal profiles for the various forms of valid traffic data are generated and stored using the Normal Profile Generation component.

Test Phase:

With the help of the Tested Profile Generation feature, profiles may be made for certain types of traffic that were discovered during the testing phase. The Attack Detection module then obtains the assessed profiles and checks them against their regular counterparts in the database.

Sinks

If the router detects a malicious or traffic node, the module gives it permission to forward the data file given by the Service Provider to the destination. The router forwards the information to the IDS Manager, which does the content filtering and subsequently creates the profile of the attacker.

Forgery Attacker and Packet Droppers

The Attack Detection module can identify Denial-of-Service (DoS) attacks by distinguishing between malicious nodes or traffic and legal traffic using a classifier based on thresholds. The employment of a threshold-based classifier by a prospective threat actor to generate a fake signature and inject a spoofed message into a selected router node during testing is one scenario. Their criminal profile can be updated to reflect this biased message.

5. CONCLUSION

We analyze a message authentication system that also safeguards user privacy and pinpoint its flaw. We've also included a solution that should make it such that there are fewer hidden expenses. We also shared a novel method of message authentication that gives further importance to privacy and confidentiality. By accommodating a wide range of security protocols and configurations, this strategy facilitates the incorporation of diverse smart devices into IoT networks. In addition, we employed a combination of offline and online calculating methods to boost the original proposal's efficiency and scalability.

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