AN EFFICIENT PRIVACY PRESERVING MESSAGE AUTHENTICATION SCHEME FOR INTERNET-OF-THINGS

T.Anil Karuna Kumar, Assistant Professor, Dept.of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP, India
O.Vineetha, PG Scholar, Dept.of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP, India

Abstract

Internet of Things devices are responsible for collecting and transmitting data in smart cities, assisting smart cities to release greater potential. As Internet of Things devices are increasingly connected to smart cities, security and privacy have gradually become important issues. Recently, research works on mitigating security challenges of Internet of Things devices in smart cities mainly focused on authentication. However, in most of the existing authentication protocols, the trustworthiness evaluation of Internet of Things devices in smart cities is ignored. Considering the trustworthiness evaluation of Internet of Things devices is an important constituent of data source authentication, in this article, a cloud- aided trustworthiness evaluation mechanism is first designed to improve the credibility of the Internet of Things devices in smart cities. Furthermore, aiming at the problem that the user's privacy is easy to leak in the process of authentication, an anonymous authentication and key agreement scheme based on non-interactive zero knowledge argument is proposed. The proposed scheme can ensure the privacy preservation and data security of Internet of Things devices in smart cities. The security analysis demonstrates that the proposed scheme is secure under q-SDH problem. The experi- mental simulation indicates that the performance of the proposal is greatly improved compared with other similar schemes.

Keywords: Smart cities, non-interactive zero knowledge, trustworthiness evaluation, anonymous authentication

Introduction

With the continuous increase of population in cities and the formation of new urban agglomerations, the problems caused by urbanization, such as traffic jams, environmental degradation, lack of resources, and the decline of residents' quality of life, have become increas- ingly prominent. The concept of smart cities was pro- posed to realize the sustainable development of the cities.[1] Information and communication technologies are showing an increasingly accelerating development trend in the world.[2] A series of key technologies, such as 5G network, Internet of Things (IoT), cloud comput- ing, big data analysis, new generation geographic

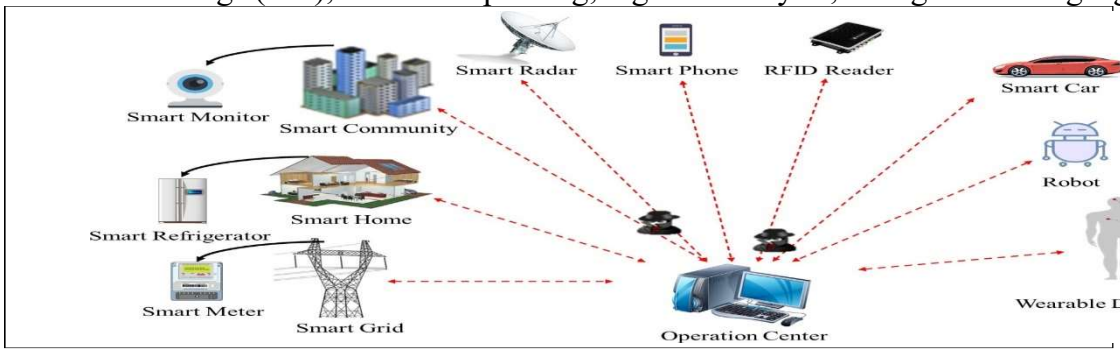


Figure 1. IoT devices in smart cities transmitting data to the operation center in the presence of adversaries.

In the architecture of smart cities, the terminal per- ception layer provides the ability of intelligent percep- tion of the physical environment and realizes the identification, data collection, monitoring, and control of the infrastructure within the scope of the city through sensing devices and sensor networks.[4] With the rapid development of IoT and mobile communication technologies, smart meters, smart cameras, wear- able embedded devices, smart home appliances, and other terminal devices come into family life. Although a large number of IoT terminal devices provide people with convenient life, they also provide a broader attack platform and environment for attackers.[5] As shown in Figure 1, in smart cities, most of the data collected by these IoT devices is sensitive, attackers may eavesdrop or tamper with these data to obtain benefits, which may bring serious consequences. For example, smart meters collect electricity consumption data, which will expose the user's life behavior track once leaked; wear- able embedded devices collect people's physiological data, which will endanger people's lives once leaked or tampered in the transmission process. To ensure the security of terminal communication services in smart cities, prevent the data collected by IoT devices from being eavesdropped on or tampered in the process of transmission, and avoid the damage or major security

Main contributions

The main contributions of this study can be summarized as follows:

1. *A cloud-aided trustworthiness evaluation mechanism is designed.* Trustworthiness evaluation provides reliable authorization basis for identity authentication. However, due to the limited computing and storage resources of IoT device, the trustworthiness evaluation cannot be com- pleted by itself. Considering the powerful com- puting resources and storage capacity, cloud server is introduced to evaluate the reliability of IoT devices. The operation center will decide whether to authorize the IoT device according to the trustworthiness level value calculated by the cloud server, so as to achieve mutual trust between the IoT device and the operation center.
2. *An anonymous authentication and key agreement protocol with privacy preservation is proposed*. A non-interactive zero knowledge (NIZK) scheme is constructed to realize anonymous authentica- tion and key agreement between operatiion cen- ter and IoT devices. As the properties of NIZK, the proposed scheme can protect the data secu- rity and privacy of IoT devices in smart cities.
3. *Formal security analysis and experimental simu- lation are presented*. Security analysis demon- strates that the proposed protocol can meet many security requirements such as anonymity, privacy preservation, mutual authentication, forward security, and unlinkability. Performance analysis shows that the proposed protocol requires much less time overhead than similar protocols, so the proposed protocol is more suitable for deployment in smart cities.

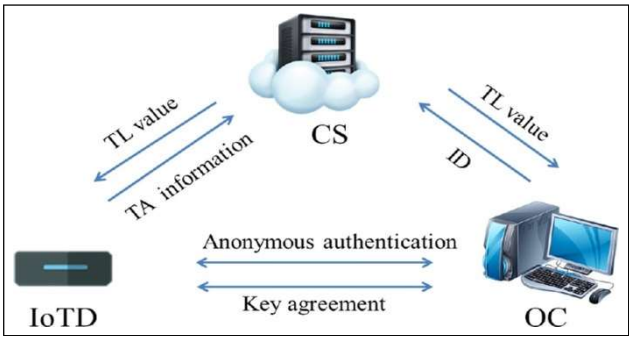
Related works

In recent years, IoT devices are widely used in various fields of smart cities. Its security has also received great attention.[13–17] For the secure authentication of IoT devices, scholars have done a lot of research. Now, the related work is sorted out as follows.

In 2014, aiming at security issues of implantable medical devices in wireless body area network environ- ment, Liu et al.[18] proposed an authentication scheme based on certificateless signature. The scheme is proved to be secure against the existence forgery of adaptive chosen message attack in random oracle model. However, Xiong[19] pointed out that Liu et al.'s scheme could not resist the public key replacement attack and proposed an extensible certificateless remote authenti- cation protocol with anonymity and forwarding secu- rity to solve this problem, but this scheme has the problem of member revocation. To solve this problem, in 2015, Xiong and Qin[20] proposed a remote authenti- cation scheme which was constructed by incorporating an efficient revocation certificateless encryption scheme for short-term key disclosure and a certificateless

signa- ture scheme. The security analysis shows that the scheme satisfies anonymity, key escrow resistance, and revocability. However, Shim[21] pointed that the scheme was insecure against the adversary who knows a secret value. According to the secret value, the adversary can forge signatures. That is the scheme cannot resist signature forgery attack. In 2021, Wei et al.[22] proposed an efficient, secure, and privacy-preserving message authentication scheme. The scheme supports IoT devices in smart cities with different encryption systems (whether RSA or ElGamal), and allows offline/online computing, making it more versatile and efficient than previous solutions.

However, the process of identity authentication may reveal users' privacy. To protect the privacy of users, more and more scholars focus on anonymous authenti- cation. In 2017, Dimitriou and Karame[23] proposed an anonymous authentication scheme based on the blind signature and the hash chain. Blind signature technol- ogy has the characteristic that the signer is invisible to the message signed by him, so as to protect the privacy of the sender. But this scheme cannot trace malicious senders. To solve this problem, Kong et al.[24] proposed an anonymous authentication scheme based on blind group signature. In this scheme, the group manager can trace the group signatures generated by the group members by using the group private key. But the scheme needs multiple interactions to ensure the secu- rity of authentication, resulting in huge computation and communication costs. Aiming at the low efficiency of authentication and resisting load modification attacks on the smart meter, Boyapally et al.[25] proposed an authentication scheme based on physically unclon- able functions(PUF). The scheme uses lightweight cryptographic primitives, which makes the scheme fea- sible in resource-constrained IoT devices. Vasco et al.[26] proposed an authentication scheme based on oblivious pseudo random functions (OPRF), and further



System model

It needs to collect its own trustworthiness attribute(TA) information and send it to the CS. The CS calculates its trustworthiness level(TL) and returns it to the IoTD. Second, the IoTD signs the TL and sends the report to the OC. To prevent cheating, the OC requests the TL of the device from the CS for comparison. And the authorized tag is granted to the IoTD whose TL falls within its acceptable range. Among them, the CS is semi-trusted, it may deliberately reduce the TL value of the IoTD to prevent the authentication and key agree- ment between legitimate IoTD and OC; the IoTD is semi-trusted, it may deliberately improve its TL value to cheat the OC; the OC is also semi-trusted, it may be curious about the privacy of data in the IoTD.

Performance analysis

In this section, first, a comparison about features of the proposed scheme with those of other schemes is given. Second, the communication overhead of the proposed scheme is analyzed. Finally, the computational cost is discussed and the time cost of authorized tag generra- tion and session key exchange is described.

Features comparison

In this subsection, the comparison between the pro- posed scheme, revocable and scalable certificateless remote authentication (RSCR[20]), threshold-based anonymous identification (TAI[32]), and conditionally anonymous ring signature (CRS[33]) is given. As dis- played in Table 2, only the proposed scheme can satisfy all of these features. By generating NIZK proofs, the proposed scheme satisfies the mutual authentication and privacy-preserving. As the hash function is colli- sion resistant, the data integrity is guaranteed in the proposed scheme. As the q-SDH assumption holds in G, the proposed scheme can resist forgery attack.

Conclusion

In this article, we first propose a cloud-aided trust- worthiness evaluation mechanism. According to the trustworthiness evaluation calculated by CS, the OC decide whether to authorize tag to IoTD, hence mutual trust between IoTD and OC is guaranteed in the pro- posed scheme. In addition, an efficient anonymous authentication and key agreement scheme based on non-interactive zero knowledge is proposed. Based on this scheme, the OC can authenticate the validity of IoTD without revealing its identity, hence privacy pre- servation of IoTD is guaranteed in the proposed scheme. And the session key prevents attackers acquir- ing data in plaintext, hence data security of IoTD is guaranteed in the proposed scheme. Security analysis indicates that the proposal can satisfy many security properties, such as anonymity, privacy preservation, mutual authenticaition, forward security, and unlink- ability. The result of performance evaluation demon- strates that the proposal is more suitable for deployment in smart cities.

However, how to seek a balance between privacy protection and regulation is a problem worthy of dis- cussion in the data security protection of the smart city. In the future, we will study how to design a revocation mechanism which can revoke malicious entities while keeping the anonymity of legitimate entities in smart cities.

References

1. Shen M, Tang X, Zhu L, et al. Privacy-preserving sup- port vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet Things J* 2019; 6(5): 7702–7712.
2. Xie J, Tang H, Huang T, et al. A survey of blockchain technology applied to smart cities: research issues and challenges. *IEEE Commun Surv Tut* 2019; 21(3): 2794–2830.
3. Hammi B, Khatoun R, Zeadally S, et al. IoT technolo- gies for smart cities. *IET Netw* 2018; 7(1): 1–13.
4. Alavi AH, Jiao P, Buttlar WG, et al. Internet of things- enabled smart cities: state-of-the-art and future trends. *Measurement* 2018; 129: 589–606.
5. Hui TKL, Sherratt RS and Sa´nchez DD. Major require- ments for building smart homes in smart cities based on internet of things technologies. *Fut Gener Comput Syst* 2017; 76: 358–369.
6. Penchalaiah, P., & Rajasekar, P. An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence for Highly Secure Data. International Journal of Future Generation Communication and Networking (WoS), ISSN, 2233-7857.

Author's Profile:

Talamala.Anil Karuna Kumar has received his PG degree in Master of Computer Applications from R.V.R & J.C College of Engineering, affiliated to Acharya Nagarjuna University from Guntur-Andhra Pradesh.

Oduru.Vineetha has received her degree B.Sc Computers (2016-2019) from Duvvuru ramanamma women's College-Gudur which is affiliated to VSU, Nellore. And now Persuing MCA (2019- 2021) at Narayana Engineering College-Gudur which is affiliated to JNTU Anantapoor**.**

.