MAK HILL Publications Research Journal of Applied Sciences

Research Article
doi: rjas.2022.1.6

An Secure Mutual Authentication and Key Agreement Protocol That Preserves Internet of Things (IoT) Modules

[1]Saeed QY Al-Khalidi, [2]Prakash Kuppuswamy, [2]Syed Ameen Saadullaha Hussaini Quadri, [2]Mohammad Khamruddin Shamshuddin and [3]Ahamed Ali Shaik Meeran

[1]*Department of Management Information System, King Khalid University, Abha Kingdom of Saudi Arabia*

[2]*Department Computer Network and Engineering, College of CS and IT, Jazan University, Jazan, Kingdom of Saudi Arabia*

[3]*Department of Information Technology, College of CS and IT, Jazan University, Jazan, Kingdom of Saudi Arabia*

ABSTRACT

IoT systems need a high security to protect information exchanged between devices and users. Securing the information and providing authentication are the most significant features of end-user devices on vulnerable and open network infrastructure. Thus, it is more often and significant to reinforce and modernize the security protocol for IoT devices headed for security perception. The security concern of IoT devices can be fulfilled with effective cryptography algorithm techniques. Several private and public cryptography techniques provide an extensive choice of services to protect users' information in the form of scrambled text, that can be authenticated only by authorized users or devices. Particularly, end user-device authentication is essential for the internet of things (IoT). The IoT devices are linked via the internet and they are deployed in open and public places, which creates them susceptible activity by unauthorized agents. Thus, it is significant to design an effective and strong authentication protocol to protect the end user-device with affordable cost and rapid communication. In the proposed work, the linear matrix-based, block cipher cryptography protocol scheme is used. The protocol encrypts confidential data using cryptography to generate a different scenario of the same text. In contrast to simple block cipher algorithms based on linear matrix algorithms, symmetric cryptography reduces encryption time but is not concerned about security. The objective of the research paper is to establish secure links for end-to-end communication with a proper and high speed authentication scheme.

OPEN ACCESS

Key Words

IoT security, cryptography, authentication, encryption, decryption, smart device

Corresponding Author

Prakash Kuppuswamy

Department of Computer Network and Engineering, College of CS and IT, Jazan University, Jazan, Kingdom of Saudi Arabia

Received: 4 January 2022
Accepted: 12 March 2022
Published: 5 April 2022

Citation: Saeed QY Al-Khalidi, Prakash Kuppuswamy, Syed Ameen Saadullaha Hussaini Quadri, Mohammad Khamruddin Shamshuddin and Ahamed Ali Shaik Meeran, 2022. An Secure Mutual Authentication and Key Agreement Protocol That Preserves Internet of Things (IoT) Modules. Res. J. Applied Sci., 17: 1-6, doi: rjas.2022.1.6

INTRODUCTION

The IoT is a new technological paradigm that aims "to access anything and anyone at anytime and anywhere". The rapid increase of IoT enabled applications that open up multiple business opportunities and lead to new business models[1]. The IoT is technology connected with Internet connectivity and it enables intelligent device-to-device communications. The IoT has begun to shape our modern world, where smart devices interact not only with humans but also with other smart devices, objects, environments and infrastructure[2]. The IoT uses physical devices that are uniquely identified and that can be assigned an IP address dynamically and it has ability to transfer data over the network. The basic purpose of IoT includes an autonomous connection between devices and applications (Fig. 1)[3].

The device, intelligently connected and observed real-time environment that enables the IoT, bringing it to life and delivering intelligence everywhere. The real-time interactivity is the greatest opportunity within the IoT will be in the transformational shift arising from the computing link to highly intelligent nodes, where intelligence is significantly scaled and where nodes have the power to learn, adapt and communicate[3].

Today the demand for security in compact devices such as sensors with wireless communication functions is most needed in real-world applications. However, the end device has limited information processing resources in their memory or processing unit and low power consumption technology is extremely required. The lightweight cryptographic community is paying attention to this phenomenon. Over the past few years, a number of lightweight cryptographic algorithms have been proposed that are primarily aimed at low-resource devices[4]. A data transfer takes place whenever two devices communicate with each other. It can also be very sensitive and personal. Hence, the IoT network must encrypt these sensitive data packets when they are moving from device to device. It also helps to prevent data theft. It is easy to encrypt data using cryptography, which is the process of converting simple text into an unintelligible form. Secrecy, integrity, non-repudiation and authentication are the primary objectives of cryptography.

In addition to the IoT market's new opportunities, it introduces a wealth of problems, among which security is usually among the most prominent. Moreover, this concern will only grow exponentially, as the global number of connected physical devices is forecast to grow by 12% annually, reaching 125 billion by 2030[5]. Due to this, security issues will arise as the ecosystem of connected devices becomes increasingly complex and fragmented[5,6].

There have been numerous authentication schemes proposed in recent years. Nevertheless, the majority of these schemes Li *et al*.[7] Yu and Kin[8] are focused on the user. This study is organized as follows: In section 3, we discuss the IoT and related security issues. The proposed authentication protocol is described in section 4, Then the evaluation of security is discussed in section 5. In addition, efficiency and comparison scheme of proposed algorithm with existing scheme is discussed in section 6. Finally, we concluded in section 7.

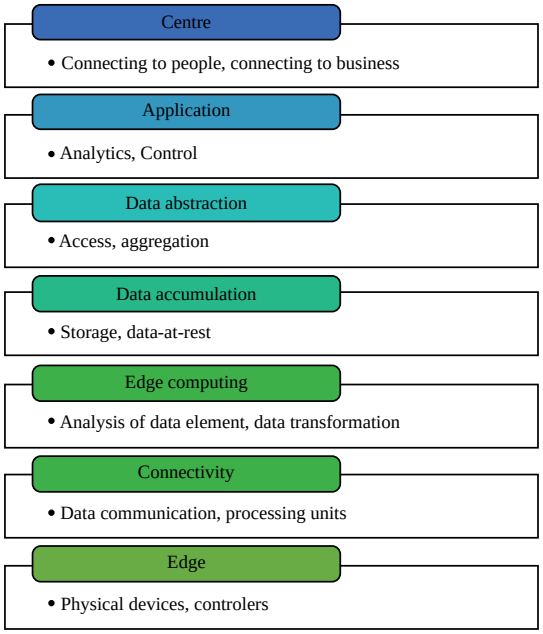

Fig. 1: IoT communication model

Internet of things communication layer model, 7 layers consist centre, application, data abstraction, data accumulation, edge computing, connectivity, edge

BACKGROUND STUDY

Authors discussed obstacles to applying the data encryption method used in conventional personal systems to IoT wireless devices due to the storage capacity and performance of the processor chip. Moreover, applying RSA encryption and similar type of encryption schemes consumes more time to encrypt the message and it causes the functional speed of IoT devices. Due to the above reason, the author suggested a new encryption scheme TPRNG (True prime random number generator), trying to reduce the encryption scheme prime numbers generator. The significant benefit of a new method is that it cannot be predicted through other scheme[8].

The author discussed cloud server-based IoT device security concept. Basically, integration of technology finds always security issues. Here, they proposed an authentication scheme based on the Elliptic curve cryptography scheme for the cloud servers and IoT components. The protocol scheme shows better security and performance reports while

it is compared with other related cryptography algorithms. Study acknowledged preventing various attacks from malware. Performance and security analyses show that the method is well designed to counter various attacks on IoT-based cloud environments[9].

In this study author's discussed a two-factor authentication scheme for IoT components. Further, conversed about the vulnerability of physical and cloning attacks faced by the open IoT devices due to the limited storage and computational capacity of the methods. So, it is significant to protect the IoT components from a vulnerable adversary with an efficient encryption scheme. The authors introduced a new scheme of two authentication methods that preserved lightweight and privacy for IoT devices. The significant benefit of the two-way authentication method provides the benefits, that the components of the IoT device are not possible to clone the device to use malfunction. The performance and security study shows to be strong enough against malware but also very efficient in terms of computational efficiency. The suggested protocol allows an IoT device to anonymously communicate with the server located at the data and control unit[10].

In this study, the authors discussed a new cryptography technique based on the block cipher scheme (linear matrix). The aim of this research article is to identify the significant method of data protection to prevent unauthorized access. The proposed scheme works on arbitrary data working on modulo 37. The protocol scheme of security mechanisms provides data confidentiality, data authentication and data access control. In this research article, there are considerable security aspects that should be taken into justification in-depth in order to have suitable data privacy and security on open and wireless channels[11].

Authors discussed the scope and limitations of (IoT) infrastructure. Though IoT provides significant benefits to the internet community, it has a lack of trust between various entities of the system and a single point of failure can cause significant damage to the entire structure of IoT. The article provides a blockchain-based trusted network for IoT security. It is a decentralized scheme to avoid a single point of failure. Suggesting a unique digital crypto-token, that controls mechanism of prevent any unauthorized access to IoT devices. Designing the scheme, using blockchain techniques provides continuous security acknowledgment from IoT devices without any user intervention. Block chain-based security authentication schemes accelerate the commercial type of application[12].

This scheme provides enhanced embedding efficiency, advanced data hiding capacity could able to be reached. Moreover, the protocol scheme used Adaptive Firefly optimization, which can be capable of transferring huge volumes of data over the IoT network. The protocol scheme performance is evaluated with different parameters, such as embedding efficiency, PSNR, carrier capacity, time complexity and MSE. Results were compared to existing methods, such as OMME, FMO and LSB[13].

Perceptual layer security: A perception layer has sensors for sensing the environment and gathering information about it. Sensors in the perception layer gather information about smart objects in the network:

- Node tampering
- Fake node
- Side channel attack
- Malicious code injection
- Protecting sensor data
- Mass node authentication
- Physical damage

Network layer security: There are basically two sublayers in the network layer, the routing layer, which handles the transfer of packets between sources and destinations and the encapsulation layer:

- Heterogeneity problem
- Network congestion
- RFID's interference
- Node jamming in WSN
- Eavesdropping attack
- Routing attacks
- Denial of service
- RFID spoofing
- Sybil attack

Support layer security: The fourth layer is considered a support layer that lies between the perception and network layer of IoT conventional architecture. A perception layer has sensors for sensing the environment and gathering information about it. Sensors in the perception layer gather information about smart objects in the network:

- Data security
- Interoperability and portability
- Business continuity and disaster recovery
- Cloud audit
- Tenants security
- Virtualization security

Application layer security: Order to pass messages between layers, the application layer determines a set of protocols for message passing:

- Data access and authentication
- Phishing attacks
- Malicious active X scripts
- Malwares attack

MATERIALS AND METHODS

The proposed scheme assumes that communication between IoT devices uses an authenticated channel and that its confidentiality is guaranteed. The protocol used for securing IoT authentication is based on the Linear Block Cipher algorithm (LBC). We proposed a novel method to increase the security concern. We used modulo 37 instead of modulo 26. The equation of the hill cipher or linear matrix cipher modulo 26 and the extending version of modulo 37 are mentioned below. Proposed security model designing based on a symmetric key algorithm using simple text and numerals. The major advantage of symmetric cryptography is to use the same keys for encryption and decryption. The authentication approach is based on a simple mathematical calculation based suitable for small-scale devices. The general diagram of the IoT device authentication process is mentioned in Fig. 2. The processing and accessing method between the IoT devices described in Fig. 3.

The authentication process that is performed during the request by an application service and the flow of authentication by the service request are shown in Fig. 3. The system authentication processing has three stages, first steps initialization process, key generation and finally access verification process.

The key space of modulo 26 hill cipher is mentioned in Eq. 1 and it's (5×5) hill cipher based key size about 114 bits.

$$\text{Log}_2 (26n^2) = 4.7n^2\text{-}1.7 \quad (1)$$

Proposed algorithm based on modulo 37, it is a prime number, therefore the order of the general linear group is as follows:

$$GL(n, Z_{37}) \text{ is } 37n^2(1\text{-}1/37)\ (1\text{-}1/37^2)\ldots(1\text{-}1/37^n) \quad (2)$$

The key space of modulo 37 proposed block cipher is mentioned in Eq. 3 and it's based on (6×6) square matrix and its key size is about 164 bits:

$$\text{Log}_2 (37n^2) = 5.3n^2\text{-}2.1 \quad (3)$$

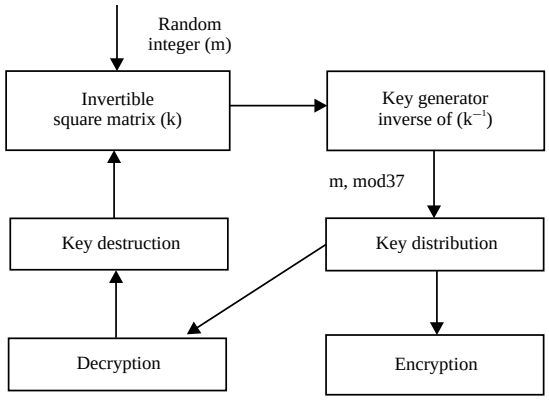

Fig. 2: Device authentication process using LBC
A key distribution process and key destruction are involved in the authentication scheme module of Encryption/Decryption, Linear Block Cipher

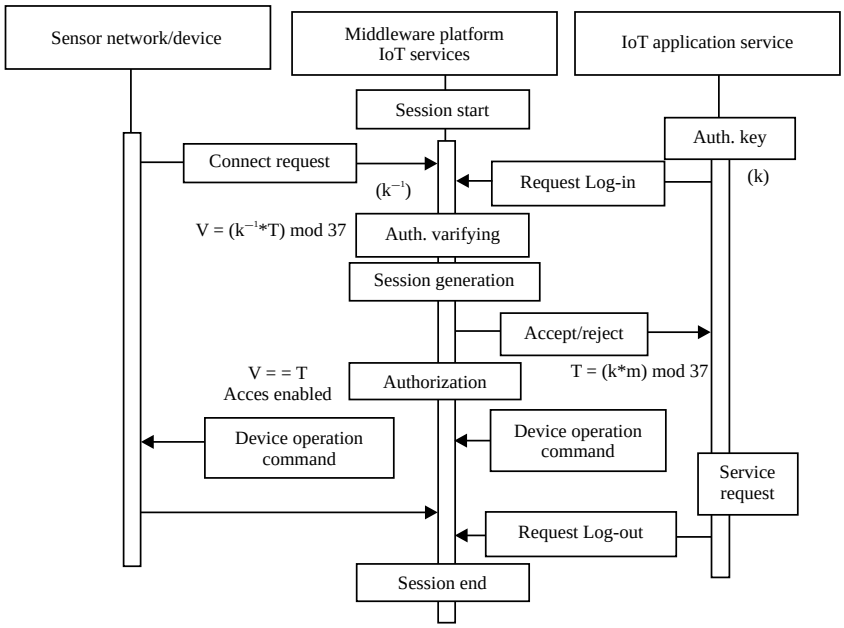

Fig. 3: Device authorization process
The authorization process is completed by IoT hardware devices through Sensor Networks, Middleware applications and IoT application services

Initialization phase: The Application service first generates by chosen random integer 'k' and its equivalent inverse using mod 37 called as k^1. These key can be used to generate the verification of the device and authentication.

Key generation process: Each and every end-device can be allocated by a unique id, it can be capable of being created by companies using any alphabets and integer combination. This device authentication scheme is done by the T = (k*m) mod 37.

Authentication process: Authorization device can verify the device information using V =(k^{-1}*T) mod 37. device-id 'T' and authentication message 'V' is equal then access can be allowed and connection between IoT devices can be established.

We herein propose a new linear matrix-based block cipher mechanism applicable to small wireless enable devices such as IoT. Conventional algorithms use a very large key size, which requires large hardware areas and expensive arithmetic calculations. Because of this, traditional encryption may not be appropriate for IoT devices. It is being proposed that an authentication scheme should have an extremely small key but compensate for this problem by changing it continuously with an unexpected random number. As the proposed new algorithm does not suffer from any problems with existing public-key encryptions, which impede data transmission, it is ideal for IoT devices that perform many-to-many communications. Benefits of the proposed protocol scenario

The race between system developers and hackers should never end. The second group will always seek unauthorized access to steal data by intruding into a system. There is a possibility that an attacker will try to access the legitimate embedded IoT device. The proposed scheme's security has been examined in this section by considering an attack model. It is important to consider communication and computation costs when performing authentication. Because it is based on random nonce values, the scheme is very secure and efficient. As it doesn't use time stamps, there is no time synchronization issue. This new architecture design allows the IoT devices to be relieved of the heavy computation and processing involved in authentication, monitoring and connecting to the network. By providing sound authentication, access control and data encryption schemes, the security goals of confidentiality, integrity and availability can be achieved. Further, the proposed authentication scheme supports the addition of new nodes (or end-users), as well as mobility of edge devices and end-users. Unlike the utilization of commercialized explicit certificates, it has not yet been matured and standardized to customize implicit certificates in WSN security applications.

Table 1: Evaluation of authentication scheme

Features	Hill cipher algorithm (mod 26)	Proposed algorithm (mod 37)
Letters	A-Z (26 letters)	A-Z and 0-9 (36 letters)
Key size	114 bits	164 bits
Block size	(2×2) to (5×5)	(2×2) to (6×6)
Modular Metrics	Mod 26	Mod 37

RESULTS AND DISCUSSIONS

Proposed authentication scheme's efficiency mentioned in the following comparison Table 1. The various comparison features such as letters, key size, block size modular type and its metrics are mentioned in the below table. The reason for selecting linear block will not produce same kind of result for the repeated text variable. Also, as we mentioned in the table, it can construct 2, 3 and 6 block square matrix. Another significant benefits of choosing these authentication scheme, it will support negative variable for constructing a square matrix, so it is quite complicated for the unauthorized entities.

The proposed new protocol system is fully secure for large scale data encryption. It can be enhanced and applied in various applications such as E-commerce, security system, Iot system security, one time password generation, Money transfer, Block Chain and Government and Federal security service etc.

CONCLUSION

With the enormous increase of IoT-connected devices, the importance of security risks is raised by the academic and professional community as any connected object becomes a computing device and a potential target for an attack. In this study, we have proposed Mutual authentication schemes that reduce traffic by eliminating faults and fake packets. This system provides security against unauthorized users. It improves performance and reduces bandwidth consumption. Further work will develop into research that surges area and power efficiency even with greater key size. Data transmissions and receptions in real time can be accomplished with this method. As part of the proposed authentication model, the edge devices and end-users obtain cryptographic credentials and both parties authenticate mutual communication. The end users can authenticate themselves directly with the sensor nodes and acquire the data and services they need by using these authentication protocols. As we mentioned in the previous section, the security of the proposed scheme shows authentication solution achieves security goals and is resilient against known attacks such as eavesdropping, replay and Denial of Service. The goal of the project is to create a functional prototype of the IoT system involving real-time application devices that utilize cloud and fog-based connectivity with a novel linear block cipher scheme.

SIGNIFICANCE STATEMENT

Security is the basic requirement of any user of digital communication. An internet user will share his confidential and important information only on a reliable network medium. With the emergence of IoT technology, the security demands of its users also increased. Despite the maturity of existing network security solutions, it is not feasible to apply them in the context of IoT due to the size and heterogeneity of the IoT networks and the resource constraints on their end devices. The Internet of Things is a new paradigm and always uses open-access internet medium along with smart devices placed in open geographical areas, so it has low-security mechanisms and is susceptible to all kinds of attacks and malware. The threats to IoT can range from sophisticated to insider since they can operate remotely or from within an organization. There are many security issues associated with IoT end devices, which are discussed below.

REFERENCES

1. Weber, R.H., 2010. Internet of things-new security and privacy challenges. Comput. Law Secur. Rev., 26: 23-30.
2. Khan, R., S.U. Khan, R. Zaheer and S. Khan, 2012. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. 10th International Conference on Frontiers of Information Technology, December 17-19, 2012, IEEE, Islamabad, Pakistan, pp: 257-260.
3. Park, N. and N. Kang, 2015. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. Sensors, Vol. 16. 10.3390/s16010020.
4. Ding, L., C. Jin and J. Guan, 2015. Slide attack on standard stream cipher enocoro-80 in the related-key chosen IV setting. Pervasive Mobile Comput., 24: 224-230.
5. Xu, H., J. Ding, P. Li, F. Zhu and R. Wang, 2018. A lightweight rfid mutual authentication protocol based on physical unclonable function. Sensors, Vol. 18 .10.3390/s18030760.
6. Amin, R., S.H. Islam, M.K. Khan, A. Karati, D. Giri and S. Kumari, 2017. A two-factor rsa-based robust authentication system for multiserver environments. Secur. Commun. Networks, Vol. 2017 .10.1155/2017/5989151.
7. Li, X., D. Yang, X. Zeng, B. Chen and Y. Zhang, 2019. Comments on "Provably secure dynamic Id-based anonymous two-factor authenticated key exchange protocol with extended security model". IEEE Trans. Inform. Forensics Secur., 14: 3344-3345.
8. Yu, H. and Y. Kim, 2020. New RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices. Electronics, 9: 246-0.
9. Kumari, S., M. Karuppiah, A.K. Das, X. Li, F. Wu and N. Kumar, 2017. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J. Supercomput., 74: 6428-6453.
10. Gope, P. and B. Sikdar, 2019. Lightweight and privacy-preserving two-factor authentication scheme for iot devices. IEEE Internet Things J., 6: 580-589.
11. Kuppuswamy, P., Shanmugasundaram and R. John, 2020. A Novel Approach of Designing E-Commerce Authentication Scheme Using Hybrid Cryptography Based On Simple Symmetric Key And Extended Linear Block Cipher Algorithm. 2020 International Conference on Computing and Information Technology (ICCIT-1441), September 09-10, 2020, IEEE, pp: 1-6.
12. Agrawal, R., P. Verma, R. Sonanis, U. Goel, A. De, S.A. Kondaveeti and S. Shekhar, 2018. Continuous Security in IoT Using Blockchain. 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), April 20- September 13, 2018, IEEE, Calgary, AB, Canada, pp: 6423-6427.
13. Khari, M., A.K. Garg, A.H. Gandomi, R. Gupta, R. Patan and B. Balusamy, 2020. Securing data in internet of things (IoT) using cryptography and steganography techniques. IEEE Trans. Syst., Man, Cybern.: Syst., 50: 73-80.