IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 10, No. 4, August, 2023, pp. 1352-1358
Journal homepage: http://iieta.org/journals/mmep

A Secured Multi-Stages Authentication Protocol for IoT Devices

Ahmad Y. Alhusenat[1*], Hamza Abu Owida[2], Hana A. Rababah[3], Jamal I. Al-Nabulsi[2], Suhaila Abuowaida[4]

[1] Department of Network Engineering and Security, Faculty of Computer and Information Technology, Jordan University of Science and Technology, Irbid 22110, Jordan
[2] Department of Medical Engineering, Faculty of Engineering Al-Ahliyya Amman University, Amman 19111, Jordan
[3] Department of Electrical Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman 19111, Jordan
[4] Department of Computer Science, Prince Hussein Bin Abdullah Faculty of Information Technology, Alal-Bayt University, Mafraq 25113, Jordan

Corresponding Author Email: ayalhusenat18@cit.just.edu.jo

https://doi.org/10.18280/mmep.100429

Received: 20 February 2023
Revised: 10 April 2023
Accepted: 2 May 2023
Available online: 30 August 2023

Keywords:
Internet of Things (IoT), authentication protocol, dynamic key exchange, real-time application, One-Time Pad (OTP)

ABSTRACT

The Internet of Things (IoT) facilitates the deployment of sensing devices for data acquisition and transmission across networks and systems, thus enabling innovative real-time applications. Securing these platforms remains paramount due to the high value placed on data privacy. This study proposes a novel real-time authentication method, fundamentally grounded in a One-Time Pad (OTP) concept. Data are encrypted using dynamic encryption, the parameters of which are determined by data from randomly distributed sensors. Encryption keys are dynamically transmitted, allowing for on-the-fly key generation and exchange. This enhances the security and privacy of user data. A lightweight technique for key creation, exchange, and authentication is presented for data collection from sensors used in real-time applications. This protocol ensures data privacy and security throughout the data collection process. The proposed protocol's efficacy is demonstrated through a discussion of how it meets these criteria, and an example illustrating its operation at each tier in the event of desynchronization or an incident.

1. INTRODUCTION

To secure the physical, computational, and communications aspects of IoT applications, a novel digital system known as a Cyber-Physical System (CPS) has been designed. Real-time Internet of Things solutions provided by CPS are being used in many industries. Things like smart cars, medical equipment, electrical grids, house setups, and similar things [1]. A high standard of security and privacy in data transmission is required for these applications. IoT apps transmit massive amounts of data over heterogeneous networks, yet they can be compromised at multiple levels. The key difficulty of cyber-physical systems [2] is managing security, which can be compromised through any of the many cyber and physical connections that IoT applications involve. This study presents the authentication protocols for real-time Internet of Things applications affected by stochastic factors. These protocols, which were inspired by randomness, will help ensure the privacy and security of IoT users in the long run. We will be creating the overarching protocol and putting it into practice in several contexts, including the deployment of smart grids and the integration of medical equipment [3, 4]. To improve the security of symmetric encryption, our lightweight algorithm provides a new method of operation. Since the information used in real-time applications is inherently uncertain, we can apply a novel approach to exchanging dynamic encryption keys. Then, we'll start using these authentication techniques to bolster our security and personal safety.

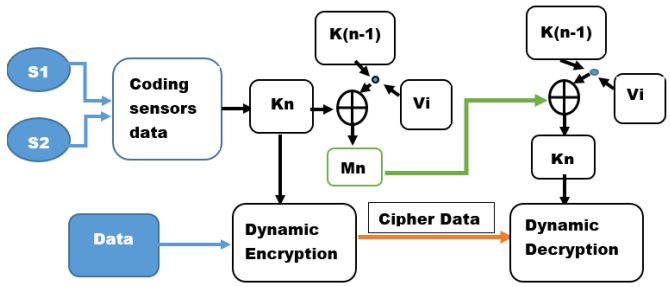


Figure 1. A dynamic OTP key

In addition to dynamic data classification and management, our innovative authentication technique based on the unpredictable nature of IoT applications like Smart Cars, Medical Devices, and Power Grid Systems [5, 6] will demonstrate how to design a custom protocol for each of these niche areas. Proposed One-Time Pad (OTP), is the strongest and lightest encryption method, but random keys are hard to come by, and keys used just once are not predictable [7, 8]. In this research, we offer a low-overhead method of key generation, exchange, and authentication that may be used for OTP-based authentication and data collection from sensors embedded in real-time applications, as shown in Figure 1. In this scenario, we assume that the data from the real-time application has been encrypted using the Advanced Encryption Standard (AES) stand-alone. To use this method, you will need a large number of static keys, one for each user and system, which puts a strain on storage space. Moreover,

there is a severe issue with exchanging keys [9] and confidentiality concerns if they utilize a single key for all their devices and software. In addition, if you employ Rivest-Shamir-Adleman (RSA) stand-alone for real-time applications, you'll have to decide between using a single set of private and public keys, which presents privacy concerns, and using a set of numerous private and public keys, which presents storage and key exchange problems [9]. The suggested authentication method includes a dynamic key exchange stage, which regularly rotates and refreshes the keys used to communicate between the administrator and the server. Privacy and safety will be improved. Key exchange is possible in real time with this authentication process. The lightweight real-time authentication protocol enhances user privacy by exchanging dynamic keys with Hash functions, including unique identification for the administrator and server (ID_a, ID_s, respectively), which makes the user manage and ensures the privacy, integrity, and authentication of their applications data, the authentication technique will be discussed in detail.

The vast majority of the currently available systems described in the research literature for the Internet of Things (IoT) and settings similar to it are either insecure against a variety of known attacks or wasteful in communication and processing [10]. They have their fingers crossed to eliminate the tiny cracks in the current user authentication mechanisms by proposing a novel secure, lightweight anonymous authentication protocol for the IoT environment using physically unclonable function (PUF) that can inhibit imitation of dysfunctional smart devices as well to opposing other well-known attacks necessary for IoT security. The suggested approach consists of five unique steps: (1) initialization, (2) device activation, (3) user identification, (4) mutual authentication and session key agreement, and (5) maintenance. Users' identities are transmitted through a secure channel during the registration process, which is both challenging to implement and vulnerable to attacks. However, our proposed protocol uses a dynamic key and hash function to transmit the ID between the administrator and the user, making registration simple and secure.

Aman et al. [11] developed lightweight mutual authentication techniques for IoT systems using Physical Unclonable Functions (PUFs). Besides being secure against a wide range of attacks, this method also uses extremely few resources (CPU time, memory, power, and network traffic, among other things). Nonetheless, to put these protocols to use in contexts where speed is of the essence, like automotive networks, it would be preferable to further minimize the latency of authentication by reducing the number of messages exchanged between the entities. However, these protocols should be utilized in contexts where punctuality is of the utmost importance, such as in vehicular networks.

A three-factor user authentication scheme was presented by Li et al. [12]. This set of authentication protocols is both secure and low-power. Since this method involved the user communicating directly with sensor nodes, it was determined to be inappropriate for Internet of Things (IoT) use cases due to its negative impact on the sensor network lifetime.

Authentication is a crucial and complex issue for protecting the rapidly expanding industrial IoT. Secure device-to-device communication in low-resource settings is addressed by several authentication systems [13-17]. There are many security flaws in these techniques, though. Most are also incompatible with IoT contexts since they have significant processing, storage, and communication needs. To guarantee safe communication between IoT devices, it is crucial to create an adequate security architecture. We, therefore, present a practical authentication mechanism for protecting the interoperability of IoT gadgets. The suggested scheme authenticates a smart sensor with an administrator and server using minimal computational, storage, and network resources. Our proposal does not rely on any methodology taxing on system resources; instead, we make effective use of hashing and Xor operations to arrive right forward and reliable method. This algorithm involves the use of randomly generated sensor data, which is passed through a lightweight complexity algorithm to generate secure encryption keys. The design of the complexity algorithm is aimed at reducing the amount of processing power necessary for the authentication protocol. As a result, power consumption is minimized, and system load is lowered, making it an ideal choice for use in environments with limited resources. To minimize power and usage, the authentication protocol uses lightweight techniques such as Physical Unclonable Functions (PUFs), and bitwise operations like Xor and Hash. The computational complexity of the algorithm is optimized to reduce the O(n) complexity on both ends of the data transmission process, further enhancing the overall efficiency of the authentication mechanism.

The objective of this research is to propose a concise authentication protocol that can generate and exchange keys suitable for sensors in real-time applications. The protocol aims to meet the requirements of users for privacy and security. The proposed research work aims to enhance the security of real-time applications through the introduction of a more robust and secure authentication protocol. The suggested authentication method includes a dynamic key exchange stage for dynamic encryption, which enhances the security of the data transmission process. The program allows users to have complete control over the information stored, giving them the ability to modify and select recipients as well as set conditions under which the information can be shared. The proposed protocol's primary value lies in its capacity to manage user application data using an unlimited number of randomly generated keys that can be easily distributed and exchanged. This allows the application to regulate the actions of authorized users, including who has access, when they can access, and what they can do. As a result, the protocol improves both the security and privacy of users' data. In addition, the proposed protocol could work at each tier in the occurrence of a desynchronization or incident.

Section 2 provides an in-depth explanation of the methods used for authentication protocol stages and dynamic encryption. The proposed protocol's synchronization and emergency procedures, power consumption, and complexity analysis are discussed in Section 3. In the final section, make conclusive remarks the concluding part.

2. PROBLEM FORMALIZATION

2.1 Initial stage

In this stage, the administrator creates the first key K_1 and sends $M_1=K_1 \oplus V_i$, Hash $(K_1 \oplus ID_a)$ to authenticate the administrator on the server side and exchange the key at the same time using the initial vector V_i. Then the server side sends acknowledge ($Seq_1 \oplus K_1$, Hash ($Seq_1 \oplus ID_s$)) after generating sequence number Seq_1 to authenticate the server on the administrator side, also use the Seq_1 for synchronization in

the next message. Dynamic encryption is used after authentication to decrypt and decrypt the data using K_1, as shown in the flowchart Figure 2.

2.2 Normal stage

In the normal stage, the administrator creates the second key K_2 and sends $M_2=K_2 \oplus K_1$, Hash $(Seq_1 \oplus ID_a)$ to authenticate the administrator on the server side and exchange the key at the same time using the first key K_1. Then the server side sends acknowledge $(Seq_2 \oplus K_2$, Hash $(Seq_2 \oplus ID_s))$ after generating sequence number Seq_2 to authenticate the server on the administrator side, also using the Seq_2 for synchronization in the following message. Dynamic encryption is used after authentication to decrypt and decrypt the data using K_2, as shown in the flowchart Figure 3.

2.3 Dynamic stage

As shown in the flowchart Figure 4, in the dynamic stage, the administrator creates the new key K_n and sends $M_n=K_n \oplus K_{n-1}$, Hash $(Seq_{n-1} \oplus ID_a)$ to authenticate the administrator on the server side and exchange the key at the same time using the first key K_{n-1}. Then the server side sends acknowledge $(Seq_n \oplus K_n$, Hash $(Seq_n \oplus ID_s))$ after generating sequence number Seq_n to authenticate the server on the administrator side, also using the Seq_n for synchronization in the following message. Dynamic encryption is used after authentication to decrypt and decrypt the data using K_n.

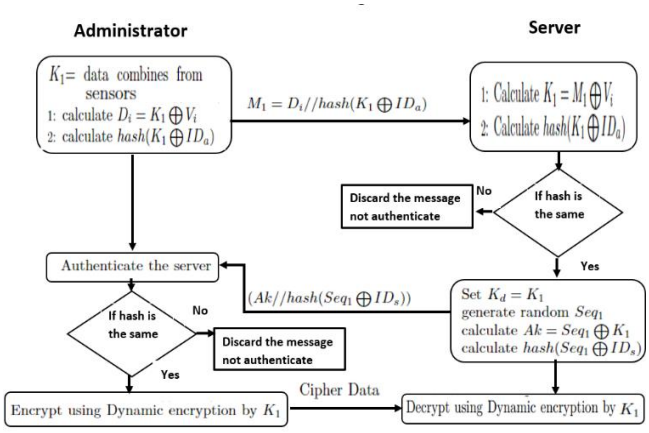


Figure 2. Initial stage

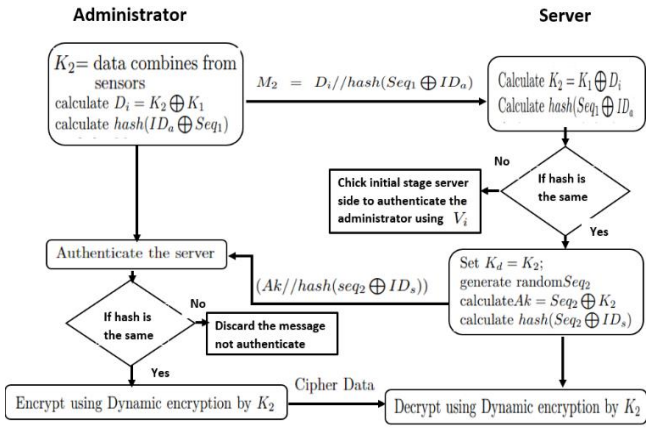


Figure 3. Normal stage

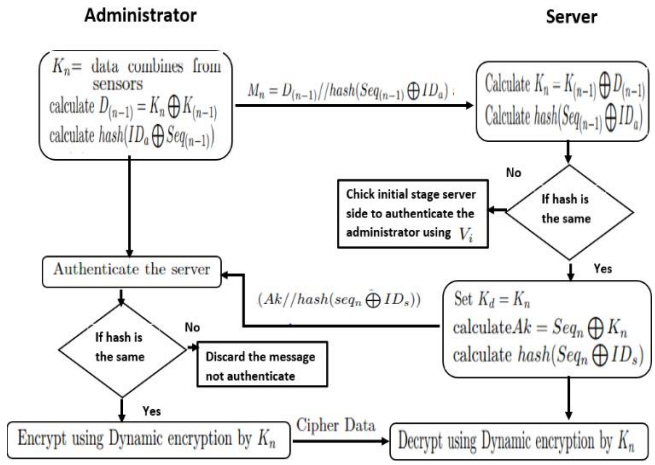
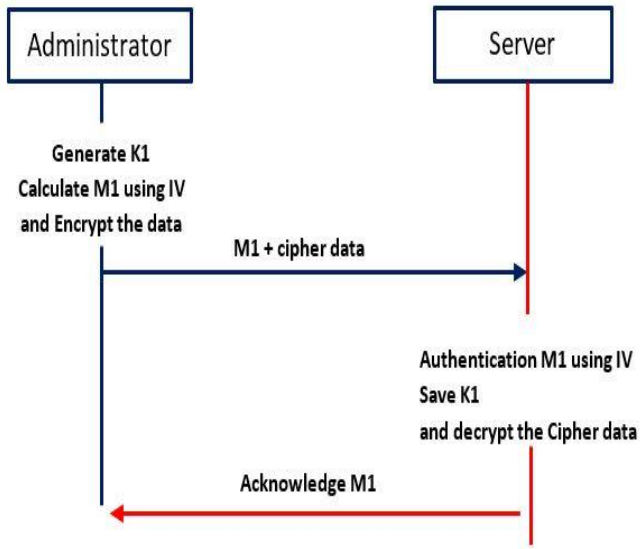
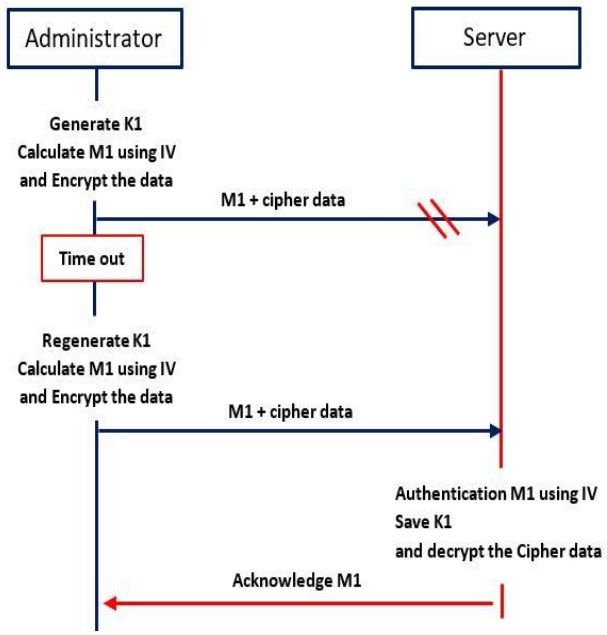


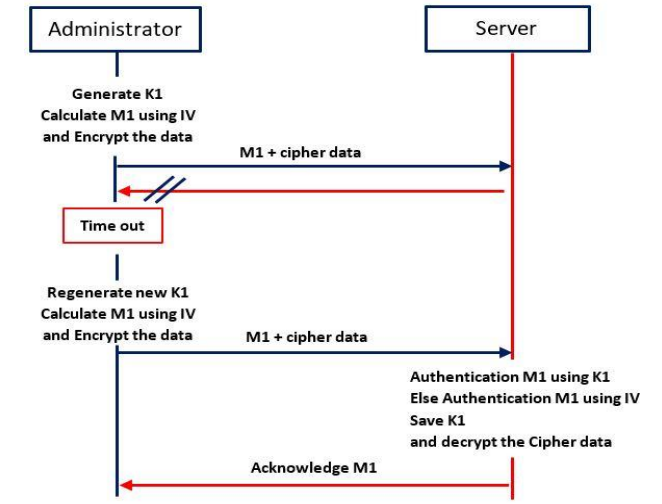
Figure 4. Dynamic stage



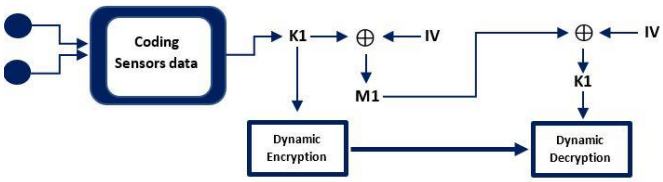
(a) Initial protocol without missing a message



(b) Initial protocol with missing the first message

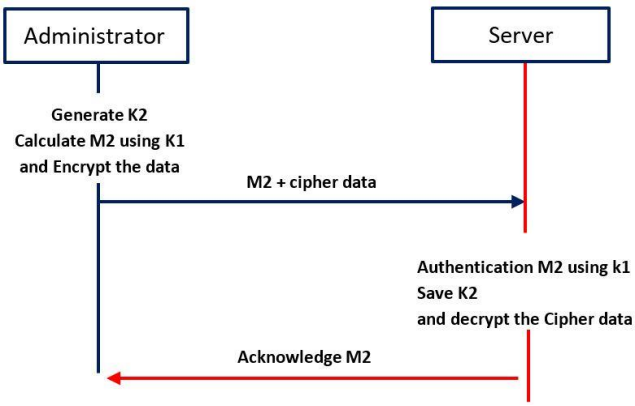


(c) Initial protocol with a missing acknowledgment message

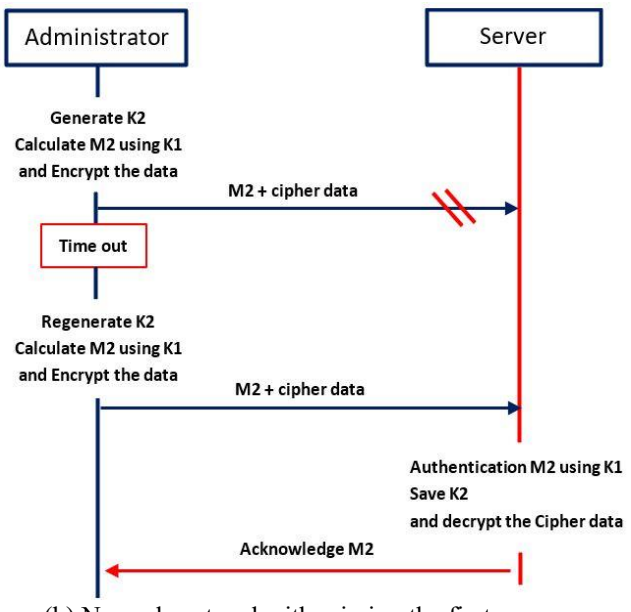


(d)

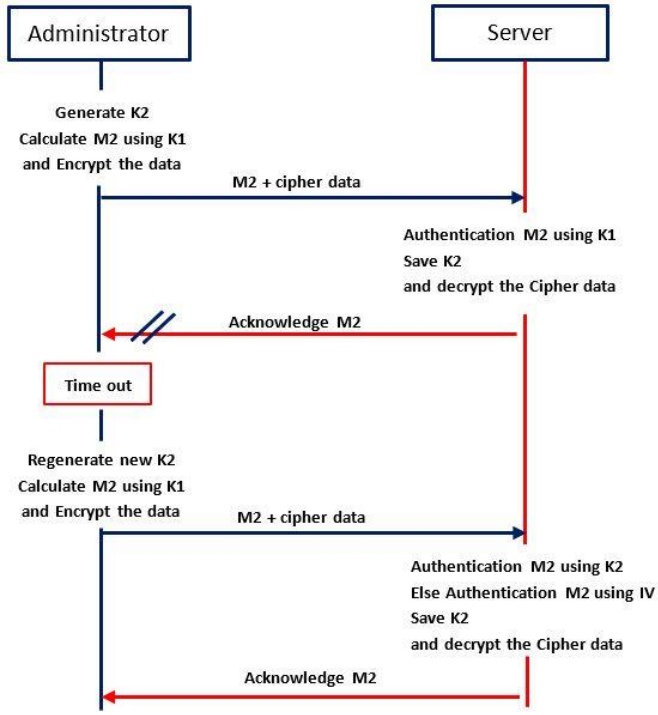
Figure 5. Initial protocol



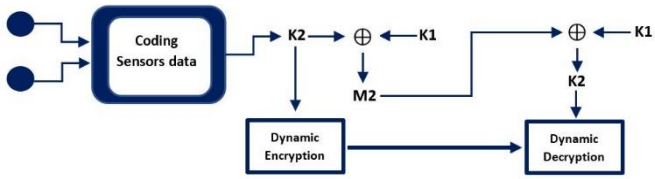
(a) Normal protocol without missing a message



(b) Normal protocol with missing the first message



(c) Normal protocol with a missing acknowledgment message



(d)

Figure 6. Normal protocol

3. ALGORITHM TRANSACTION EXAMPLE, POWER CONSUMPTION, AND COMPLEXITY ANALYSIS

This section describes how our protocol reacts with sequence messages between the administrator and server sides and shows how we can update the key and the miss synchronization cases. Also, we study power consumption and complexity analysis for the proposed real-time authentication algorithm.

3.1 Initial protocol

Figure 5(a) shows how the administrator side generates the first key and uses the initial vector to send it, and uses the first key for dynamic encryption and decryption but Figure 5(b) shows if the message is not received from server the administrator wait for the acknowledgment message for a specific time, then if not receive the acknowledgment the administrator will regenerate new key and send it by initial vector again, as seen in Figure 5(c).

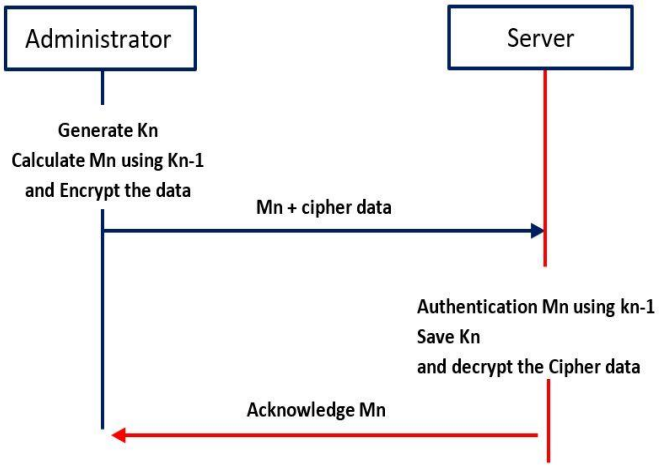
3.2 Normal stage protocol

Figure 6(a) shows how the administrator side generates the second key and uses the first key to send it, and uses the second key for dynamic encryption and decryption but Figure 6(b) shows if the message is not received from server the administrator wait for the acknowledgment message for a

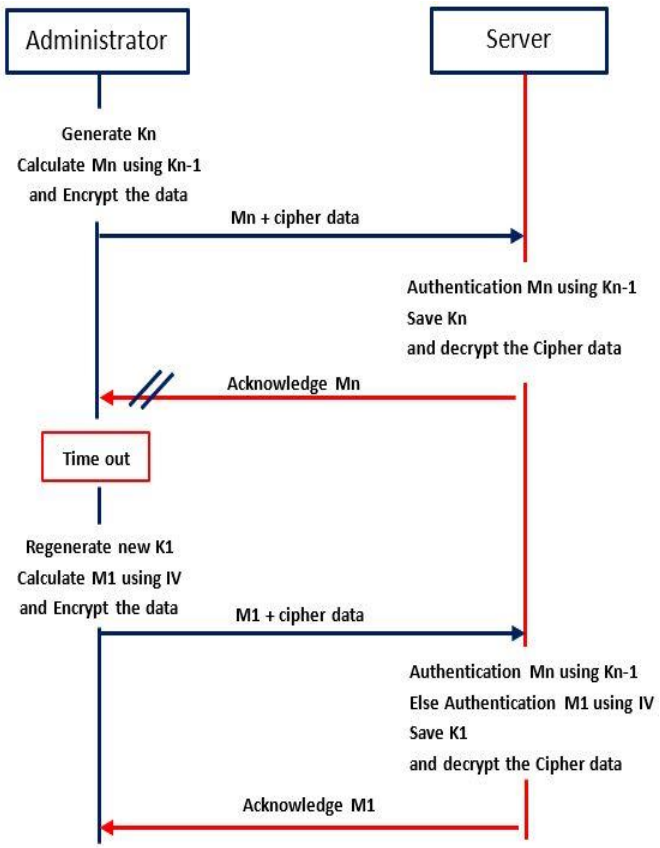
specific time, then if not receive the acknowledgment the administrator will regenerate new key and send it by initial vector again, as seen in Figure 6(c).

3.3 Dynamic stage protocol

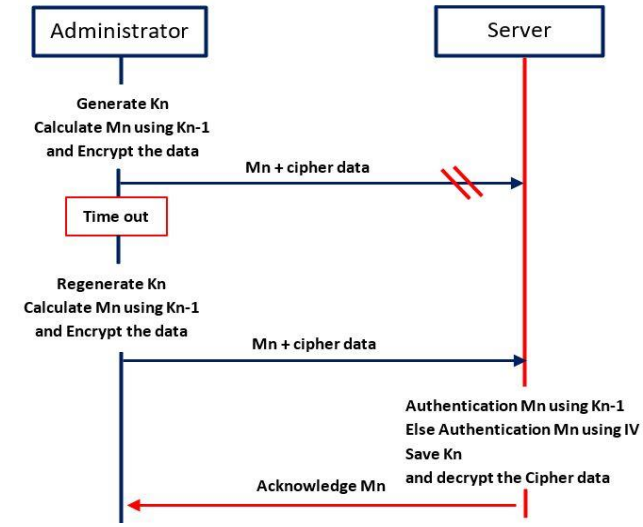
Figure 7(a) shows how the administrator side generates the dynamic key and uses the previous key to send it, and uses the active key for dynamic encryption and decryption but Figure 7(c) shows if the message is not received from server the administrator wait for the acknowledgment message for a specific time, then if not receive the acknowledgment the administrator will regenerate new key and send it by initial vector again, as seen in Figure 7(b).



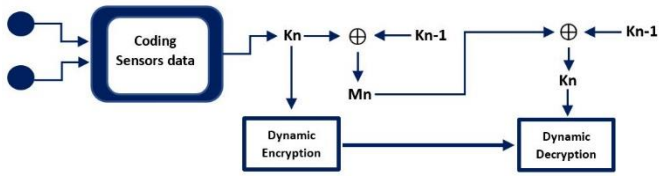
(a) Dynamic protocol missing the first message



(b) Dynamic protocol with a missing acknowledgment message



(c) Dynamic protocol missing the first message



(d)

Figure 7. Dynamic protocol

3.4 Power consumption and complexity analysis

To improve the security of the data transmission process, the authentication protocol utilizes various cryptographic techniques, including Xor and Hash functions. The Xor function is a bitwise operation that produces a binary 1 when the input bits differ and a binary 0 when they are the same. It is commonly used in cryptography to create a secure encryption key. Additionally, the Hash function is a mathematical function that transforms input data into a fixed-size output value, also referred to as a hash value or message digest. This function is useful in ensuring that the data has not been tampered with during transmission and in maintaining its integrity. In the proposed real-time authentication protocol, we use two main light power consumption functions (Xor, Hash(.)) for each message. The single message complexity is O(1). If we need to send n message, the complexity is O(n), so we have lightweight authentication and key exchange algorithm with a limited size required, which will minimize the power consumption also where it has been concluded [18] that the size of the message (mainly increasing the size of the message) in the algorithm instructions is the main factor affecting power consumption. The storage size needed is shallow because we dynamically update the key and do not need to save all keys. We have to keep the secret initial vector only.

4. CONCLUSIONS AND FUTURE WORK

Real-time Internet of Things (IoT) applications are increasingly being adopted across a broad range of sectors, including smart vehicles, medical devices, electrical grids, and smart homes and offices. To ensure secure and private communications within these interconnected systems, we

propose a real-time authentication mechanism complemented by a dynamic key exchange protocol. This system pivots on the regular rotation and refreshing of keys, used for dynamic encryption.

The algorithm integrates randomly generated sensor data, which is processed through a lightweight complexity algorithm to generate secure encryption keys. The proposed protocol's primary value is its ability to efficiently manage user application data. Moreover, it can effectively operate at each tier in the event of desynchronization or an incident.

The lightweight algorithm's design aims to minimize the processing power required for the authentication protocol, thereby reducing power consumption and system load. This makes it an ideal choice for environments with limited resources and facilitates the easy creation and deployment of IoT applications.

We have optimized the computational complexity of the algorithm to lower the O(n) complexity at both ends of the data transmission process. The proposed authentication mechanism will be implemented through the development of a smart home prototype, a mobile application, and a Graphical User Interface (GUI) prototype. The insights garnered from this implementation will be explored and discussed expeditiously.

This innovative solution for securing IoT applications holds the potential to drive transformative changes across various sectors, with applications in remote medical monitoring, smart homes, smart grids, and other sensor-based systems.

REFERENCES

[1] Wankhade, M., Kottur, S.V. (2020). Security facets of cyber physical system. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE, 359-363. http://doi.org/10.1109/ICSSIT48917.2020.9214079

[2] Lounis, K., Zulkernine, M. (2021). T2T-MAP: A PUF-based thing-to-thing mutual authentication protocol for IoT. IEEE Access, 9: 137384-137405. http://doi.org/10.1109/ACCESS.2021.3117444

[3] Chang, S.H., William, T., Wu, W.Z., Cheng, B.C., Chen, H., Hsu, P.H. (2017). Design of an authentication and key management system for a smart meter gateway in AMI. In 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), IEEE, 1-2. http://doi.org/10.1109/GCCE.2017.8229288

[4] Yu, S.J., Das, A.K., Park, Y. (2021). Comments on "ALAM: anonymous lightweight authentication mechanism for SDN enabled smart homes". IEEE Access, 9: 49154-49159. http://doi.org/10.1109/ACCESS.2021.3068723

[5] Fanlin, M., Wei, Y. (2020). Summary of research on security and privacy of smart grid. In 2020 International Conference on Computer Communication and Network Security (CCNS), IEEE, 39-42. http://doi.org/10.1109/CCNS50731.2020.00017

[6] Rababah, H.A., Alhusenat, A.Y., Mahafzah, K.A. (2022). A novel smart home lightweight authentication protocol using iot applications. WSEAS Transactions on Systems and Control, 17: 477-482. http://doi.org/10.37394/23203.2022.17.52

[7] Alhusenat, A.Y., Baha'A, A. (2021). Body sensors network management protocol. In 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), IEEE, 1-6. http://doi.org/10.1109/ICCSPA49915.2021.9385768

[8] Brisson, A. (2017). Deterministic random number generation for one time pads: creating a whitenoise super key. In 2017 IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), IEEE, 1-5. http://doi.org/10.1109/UIC-ATC.2017.8397605

[9] Tan, C.C., Wang, H.D., Zhong, S., Li, Q. (2009). IBE-Lite: A lightweight identity-based cryptography for body sensor networks. In IEEE Transactions on Information Technology in Biomedicine, 13(6): 926-932. http://doi.org/10.1109/TITB.2009.2033055

[10] Banerjee, S., Odelu, V., Das, A.K., Chattopadhyay, S., Rodrigues, J.J., Park, Y. (2019). Physically secure lightweight anonymous user authentication protocol for internet of things using physically unclonable functions. IEEE Access, 7: 85627-85644. http://doi.org/10.1109/ACCESS.2019.2926578

[11] Aman, M.N., Chua, K.C., Sikdar, B. (2017). Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet of Things Journal, 4(5): 1327-1340. http://doi.org/10.1109/JIOT.2017.2703088

[12] Li, X., Peng, J.Y., Niu, J.W., Wu, F., Liao, J.G., Choo, K.K.R. (2017). A robust and energy efficient authentication protocol for industrial internet of things. IEEE Internet of Things Journal, 5(3): 1606-1615. http://doi.org/10.1109/JIOT.2017.2787800

[13] Jiang, Q., Zeadally, S., Ma, J.F., He, D.B. (2017). Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access, 5: 3376-3392. http://doi.org/10.1109/ACCESS.2017.2673239

[14] Li, N., Liu, D.X., Nepal, S. (2017). Lightweight mutual authentication for IoT and its applications. IEEE Transactions on Sustainable Computing, 2(4): 359-370. http://doi.org/10.1109/TSUSC.2017.2716953

[15] Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F.B., Rodriguez, J., Bicaku, A., Maksuti, S., Tauber, M.G., Schmittner, C., Bastos, J. (2017). A lightweight authentication mechanism for M2M communications in industrial IoT environment. IEEE Internet of Things Journal, 6(1): 288-296. http://dx.doi.org/10.1109/JIOT.2017.2737630

[16] Adeel, A., Ali, M., Khan, A.N., Khalid, T., Rehman, F., Jararweh, Y., Shuja, J. (2022). A multi-attack resilient lightweight IoT authentication scheme. Transactions on Emerging Telecommunications Technologies, 33(3): e3676. https://doi.org/10.1002/ett.3676

[17] Eldefrawy, M.H., Pereira, N., Gidlund, M. (2018). Key distribution protocol for industrial Internet of Things without implicit certificates. IEEE Internet of Things Journal, 6(1): 906-917. http://doi.org/10.1109/JIOT.2018.2865212

[18] Al Sibahee, M.A., Lu, S.F., Hussien, Z.A., Hussain, M.A., Mutlaq, K.A.A., Abduljabbar, Z.A. (2017). The best performance evaluation of encryption algorithms to reduce power consumption in WSN. In 2017 International Conference on Computing Intelligence and Information System (CIIS), IEEE, 308-312. http://doi.org/10.1109/CIIS.2017.50

NOMENCLATURE

D	Data
Hash	Hash function
ID_a	Identification for the administrator
ID_s	Identification for the server
K	Key
M	Message
O()	The algorithm's worst-case complexity
Seq	Sequence number
//	And
$\oplus$	Xor

Subscripts

AES	Advanced Encryption Standard
CPS	Cyber-Physical System
CPU	Cintral Prossising Unit
IoT	Internet Of Things
OTP	One-Time Pad
PUF	Physical Unclonable Functions
RSA	Rivest-Shamir-Adleman
GUI	Graphical user interface