A Novel Smart Home Lightweight Authentication Protocol using IoT Applications

HANA A.RABABAH[1], AHMAD Y. ALHUSENAT[2], KHALED A.MAHAFZAH[1]
[1]Department of Electrical Engineering, Al-Ahliyya Amman University, Amman, JORDAN
[2]Department of Network Engineering and Security, Jordan University of Science and Technology, Irbid, JORDAN

Abstract: - The Internet of Things (IoT) introduces innovative real-time applications that use sensors to collect data that exchange between things to things and things to humans through the network. In this aspect, security and privacy is the primary concern for researchers to protect these systems. This paper proposes a real-time authentication algorithm based on the one-time pad (OTP) principle. The keys are dynamically exchanged, and the data is encrypted via dynamic encryption, depending on random sensors' data. The key is generated and exchanged dynamically using the dynamic encryption technique, thus enhancing the users' data privacy and security. Moreover, a lightweight key generation, exchange, and authentication protocol are proposed for data collecting from smart home sensors. The proposed protocol guarantees security and privacy demand, which are the user's primary concern. The proposed protocol is developed for smart home applications with interfacing requirements, which makes the system real and applicable. The operation principle of the proposed protocol is illustrated sufficiently if there is any desynchronization or emergency.

Key-Words: - Lightweight algorithm, Internet of Things (IoT), One-time pad (OTP), Privacy, Authentication, Dynamic key exchange, Real-Time application, Smart Home.

Received: October 16, 2021. Revised: September 18, 2022. Accepted: October 17, 2022. Published: November 24, 2022.

1 Introduction

Cyber-Physical System (CPS) is a new digital system for securing IoT applications related to physical, computational, and communications elements. The IoT real-time applications of CPS are implemented in many areas that require high security and privacy in the exchange of data, such as industry, smart homes, smart grids of power systems, and medical devices, [1], [2]. IoT applications exchange vast amounts of secure and private data within heterogeneous networks, but they are vulnerable to attack in both the hardware and the software because due to many cyber and physical interfaces, Attacks may come from these interfaces; Indeed, security is the main burden for cyber-physical systems. Nowadays, energy management in home appliances has become a crucial issue. To overcome this issue, a smart home is presented in, [3]. In this home, the user can control energy consumption remotely through smartphone applications in which the Internet of Things plays an essential role, [4]. Smart homes rely on different sensors thus home automation devices need to be decorated due to the rapid development of numerous new wireless communication technologies, [5], [6]. As seen in Fig.1, the overall system comprises a home equipped with different sensors such as a humidity sensor, temperature sensor, fire/smoke detector, and light sensor, [7]. Moreover, these sensors are controlled remotely using a mobile application with different features. Both sides of this system are connected using an IoT server. IoT information security concerns are becoming more complex and vital. In a single network context, traditional and present security cannot provide expanded secure data sharing for IoT, [8]. A user's identification is verified by an authentication process using various tools, including a password, identity certificate, smart cards, or biometrics, [9]. However, because of inherent weaknesses or carelessness on the user's part, many authentication techniques are vulnerable to compromise, [10], [11]. Some proposed conventional authentication methods also call for administrator setup beforehand, user intervention for identity clarification, and permission. They are, therefore, inappropriate for mobile environments. This problem highlights the necessity for a seamless authorization solution incorporating context information to improve static authentication methods. In the end, this approach would reduce the need for the user to provide verification information each time they want to access the necessary service. Any information describing an entity's circumstance, such as a person, location, or object,

is context, [12], [13], [14]. This work proposes a smart home authentication protocol inspired by the random nature of IoT real-time applications. The proposed protocol improves the security and privacy of the data ultimately. Moreover, the paper presents a new lightweight algorithm that utilizes the random nature of real-time data and exchanges the dynamic encryption keys in order to improve security and privacy. The proposed algorithm can classify and manage data dynamically, this feature is significant for smart home applications depending on the One-Time Pad (OTP), which is the most robust lightweight encryption technique; Using unpredictable random keys, and used only for one time. The paper is organized as follows: Section 2 discusses the proposed protocol and its dynamic encryption. Section 3 presents the authentication algorithm technique. Interfacing requirements as a mobile application for smart home applications are presented in Section 4. Finally, Section 5 concludes the paper, and future work will be given.

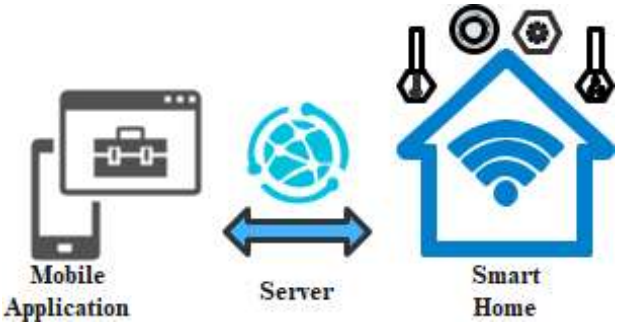

Fig. 1: Smart Home connection with IoT.

2 The proposed Protocol and Dynamic Encryption

2.1 Security Requirements

This section presents security and privacy requirements for real-time application systems, and the proposed authentication and key exchange algorithm. User privacy and sensitivity are critical and significant concerns in implementing these IoT applications in real life (smart home, smart car, human body, etc.). Using the Advanced Encryption Standard (AES) to encrypt real-time applications' data requires many static keys for each user and system, which requires huge storage for these keys, which are under threat. Also, it suffers from the critical key exchange, [15], and privacy issues result from using only one key for all systems and applications. As well as, if RSA (Rivest–Shamir–Adleman) is applied for real-time applications, it suffers from choosing between private and public keys regarding privacy issues or multi-private and public keys regarding storage and keys exchange issues, [15]. In the presented lightweight real-time authentication technique, a dynamic key exchange stage is proposed which changes and updates the keys between the administrator and server. Enhancing security and privacy by exchanging active keys with Hash functions, including unique identification for the administrator and server (ID_a, and ID_S, respectively), permitting the user to manage and ensure the privacy, integrity, and authentication of their applications data, the authentication technique will be discussed in details. Also, a sequence number is generated within the server and sent to the administrator to be used in the following stage message to prevent replay attacks and synchronization. Moreover, the protocol provides the ability to manage the family or emergency response applications to eliminate who, when, where, and what data is received.

Table 1. Abbreviations and cryptography functions.

V_i	Initial vector
ID_a	Administrator identity
ID_S	Server identity
S	data sensor
D	data group
M	message
Seq	Sequence number
Ak	Acknowledgment
$Hash$	One-way Hash function
⊕	Exclusive-OR operation

2.2 Authentication Protocol

The protocol has an administrator side and a server side within three stages: the initial stage, the normal stage, and the dynamic stage, as shown in Fig.2, Fig.3, and Fig.4. Table 1 shows the required authentication protocol abbreviations and cryptography functions.

2.2.1 Initial Stage

The initial stage is the first contact between the administrator and the server. In this stage, the administrator can generate sensors' data that they want to use as key $K_1$and send M_1 to the server using V_i. The server will use V_i to ⊕ it with M_1 and save K_1, which can be used in dynamic encryption and decryption, as shown in Fig.2.

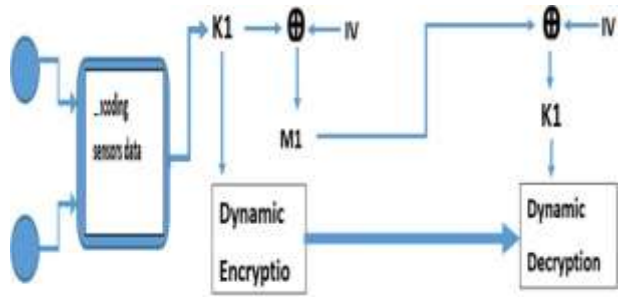

Fig. 2: Protocol Initial stage.

2.2.2 Normal Stage

The normal stage is the second contact between the administrator and the server. In this stage, the administrator generates sensors' data that they want to use as a new key K_2 and send M_2 to the server using K_1. K_1 is used by the server to be $\oplus$ with M_2 and save K_2, which can be used in dynamic encryption and decryption, as shown in Fig. 3.

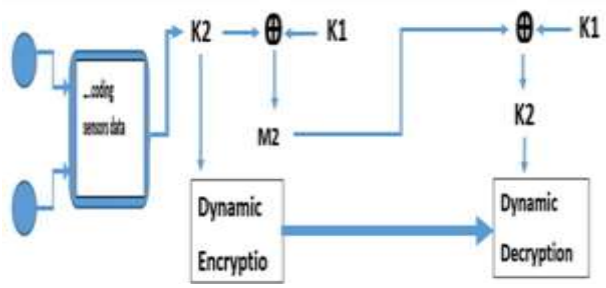

Fig. 3: Protocol Normal stage.

2.2.3 Dynamic Stage

At this stage, the administrator can generate new sensors' data that they want to use as a unique key K_n and send M_n to the server using $K_{(n-1)}$, and then the server will use $K_{(n-1)}$ to $\oplus$ it with M_n and save K_n, which can be utilized in dynamic encryption and decryption, as shown in Fig.4. In this stage, the two sides will exchange the key dynamically without the need to save all keys or stack them in just one key.

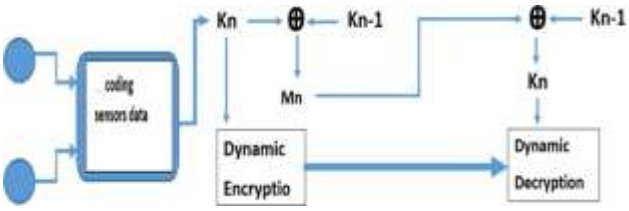

Fig. 4: Protocol Dynamic stage.

3 Dynamic Algorithm Solution

3.1 Initial Stage Algorithm

Algorithm 1 represents the administrator side's initial stage, it collects the sensors' K_1, and the combined data from the chosen sensors' group. Then sends ($M_1 = K_1 \oplus V_i$), Hash ($K_1 \oplus ID_a$), and cipher data, which is encrypted by K_1 using dynamic encryption. On the other side, algorithm 2 receives $M_1 = K_1 \oplus V_i$; Hash ($K_1 \oplus ID_a$) and cipher data, then calculates ($K_1 = M_1 \oplus V_i$) to authenticate the administrator if the result of the calculated hash value at algorithm 2 is the same as the received one. Finally, the server authenticates the administrator message and generates Seq_1, and sends it to the administrator as an acknowledged message and sends ($Seq_1 \oplus K_1$; Hash ($Seq_1 \oplus ID_S$)) as an acknowledged message and decrypts the cipher data using K_1 and save K_1. The computational complexity in algorithms 1 and 2 is O(1) because we have just one message with two lightweight liner operations, ⍰ and a hash function. Therefore, we need low storage to save ID_a, ID_S, V_i, dynamic updated key K_1, and updated Seq_1.

Algorithm 1 Initial stage Administrator side

Input: Select group of sensors from 1 to n.
Collect the data Sensor K_1= data combines from sensors group chosen
Output: Send $M_1 = D_i$//Hash($K_1 \oplus ID_a$)
1: Calculate $D_i = K_1 \oplus V_i$
2: Calculate Hash($K_1 \oplus ID_a$)
3: Send the $M_1 = D_i$//Hash($K_1 \oplus ID_a$)
4: Encrypt data using K_1
5: Send Cipher Data

Algorithm 2 Initial stage Server side

Input: $M_1 = D_i$//Hash($K_1 \oplus ID_a$) and cipher Data
Output: send (Ak//Hash($Seq_1 \oplus ID_S$))
1: Calculate $K_1 = M_1 \oplus V_i$
2: Calculate Hash($K_1 \oplus ID_a$)
3: If the same result hash received then
4: Accepts the authenticated message
5: Set $K_d = K_1$
6: Generate random Seq_1
7: Calculate Ak = $Seq_1 \oplus K_1$
8: Calculate Hash($Seq_1 \oplus ID_S$)
9: Decrypt the cipher data
10: Send (Ak//Hash($Seq_1 \oplus ID_S$))
11: Else discard the message
12: End if

3.2 Normal Stage Algorithm

Algorithm 3 at the administrator side normal stage collects the sensors' K_2, and the combined data from the chosen sensors group. Then sends $M_2 = K_2 \oplus K_1$, Hash ($Seq_1 \oplus ID_a$), and cipher data.

Where data is encrypted by K_2, using dynamic encryption, after authentication, the server acknowledges the message by solving ($Seq_1 \oplus K_1$; Hash ($Seq_1 \oplus ID_S$)) and calculate the hash value. On the other side, algorithm 4, at the server side normal stage, receives $M_2 = K_2 \oplus K_1$, hash ($Seq_1 \oplus ID_a$) and ciphers data, then calculate ($K_2 = M_2 \oplus K_1$) and Hash ($K_1 \oplus ID_a$) to authenticate the administrator if the same resulted hash value is received. It generates a random Seq_2 and sends ($Seq_2 \oplus K_2$); Hash ($Seq_2 \oplus ID_S$)) as acknowledge message, decrypts the cipher data using K_2 and saves K_2. If K_1 does not authenticate M_2, try by V_i and update the key, else discard the message. The computational complexity in algorithms 3 and 4 is O(1) because we have just one message with two lightweight liner operations, Xor and Hash function. We need low storage to save ID_a, ID_S, V_i , dynamic updated key K_2, and updated Seq2.

Algorithm 3 Normal stage Administrator side

Input: Ak//Hash($Seq_1 \oplus ID_S$)
1: Authenticate the server If ID_S True
2: else discard the message
3: collect the sensor data group K_2= data combines from sensors group chosen
Output: send the M2 = D_i//Hash($Seq_1 \oplus ID_a$) and Cipher Data
1: calculate $D_i = K_2 \oplus K_1$
2: calculate Hash($ID_a \oplus Seq_1$)
3: send the M2
4: Encrypt using Dynamic encryption by K_2
5: send cipher Data

Algorithm 4 Normal stage Server side

Input: $M_2 = D_i$//Hash($Seq_1 \oplus ID_a$) and cipher data
Output: send (Ak//Hash($Seq_2 \oplus ID_S$))
1: Calculate $K_2 = K_1 \oplus D_i$
2: Calculate Hash($Seq_1 \oplus ID_a$)
3: If the same result Hash received then
4: Accept the authenticated message
5: Set $K_d = K_2$;
6: Generate random Seq_2
7: Calculate Ak = $Seq_2 \oplus K_2$
8: Calculate Hash($Seq_2 \oplus$IDs)
9: Send (Ak//Hash($Seq_2 \oplus$IDs))
10: Else
11: Calculate $K_2 = D_i \oplus V_i$
12: Calculate Hash($K_2 \oplus ID_a$)
13: If the same result Hash received then
14: Accepts the authenticated message
15: Set $K_d = K_2$
16: Generate random Seq_2
17: Calculate Ak = $Seq_2 \oplus K_2$
18: Calculate Hash($Seq_2 \oplus ID_S$)
19: Send (Ak//Hash($Seq_2 \oplus ID_S$))
20: Decrypt using dynamic encryption by K_2
21: Else discard the unauthenticated message
22: End if
23: End if

3.3 Dynamic Stage Algorithm

Algorithm 5 is at the administrators' side dynamic stage, it collects sensors' K_n, and the combined data from the chosen sensors group. Then send $M_n = K_n \oplus K_{(n-1)}$, hash ($Seq_{(n-1)} \oplus ID_a$), and cipher data. Where data is encrypted by K_n using dynamic encryption after authenticating, the server acknowledges that message by solving ($Seq_{(n-1)}$) $\oplus K_{(n-1)}$; Hash ($Seq_n \oplus ID_S$)) and calculate the hash value. On the other side, algorithm 6 dynamic stage server side, receives ($M_n = K_n \oplus K_{(n-1)}$), Hash ($Seq_n \oplus ID_a$) and cipher data, then calculate $K_n = M_n \oplus K_{(n-1)}$and Hash ($K_{(n-1)} \oplus ID_a$) to authenticate the administrator if the same resulted hash value received. It generates a random Seq_n and sends ($Seq_n \oplus K_n$; Hash ($Seq_n \oplus ID_S$)) as an acknowledged message, decrypts the cipher data using K_n and saves K_n. If Mn is not authenticated by $K_{(n-1)}$, try by V_i and update the key, else discard the message. The computational complexity in algorithms 5 and 6 is O(n) because we have n message with two lightweight liner operations, Xor and Hash function. We need low storage to save ID_a, ID_S, V_i, dynamic updated key K_n, and updated $Seq_{(n-1)}$.

Algorithm 5 Dynamic stage Administrator side

Input: Ak//Hash($Seq_2 \oplus ID_S$).
Collect the data group K_n= data combined from chosen sensors group
Output: ($M_n = D_{(n-1)}$//Hash($Seq_{(n-1)} \oplus ID_a$)) (Cipher Data)
1: Calculate $D_{(n-1)} = K_n \oplus K_{(n-1)}$
2: Calculate Hash($ID_a \oplus Seq_{(n-1)}$
3: Send the M_n
4: Encrypt using dynamic encryption by K_n
5: Send cipher Data

Algorithm 6 Dynamic stage Server side

Input: $D_{(n-1)}$Hash($Seq_{(n-1)} \oplus ID_a$ and (Cipher Data)
Output: Send (Ak//Hash ($Seq_n \oplus ID_S$))
1: Calculate $K_n = K_{(n-1)} \oplus D_{(n-1)}$
2: Calculate Hash ($Seq_{(n-1)} \oplus ID_a$)
3: If the same result that received then

4: Accepts the authenticated message
5: Set $K_d = K_n$
6: Decrypt using dynamic encryption by K_n
7: Generate random Seq_{n}
8: Calculate Ak = $Seq_{\mathrm{n}} \oplus K_n$
9: Calculate Hash($Seq_{\mathrm{n}} \oplus ID_S$)
10: Send (Ak//Hash($Seq_{\mathrm{n}} \oplus ID_S$))
11: Else
12: Calculate $K_n = K_{(n-1)} \oplus V_i$
13: Calculate Hash($K_n \oplus ID_a$)
14: If the same result hash received then
15: Accept the authenticated message
16: Set $K_d = K_n$
17: Generate random Seq_{n}
18: Calculate Ak = $Seq_{\mathrm{n}} \oplus K_n$
19: Send (Ak//Hash($Seq_{\mathrm{n}} \oplus$ IDs))
20: Decrypt using dynamic encryption by K_n
21: Else discard the message not authenticate
22: End if
23: End if

4 Smart Home Authentication

Multiple sensors are used in IoT real-time applications for various purposes, such as smart homes, smart cities, smart cars, smart grids, etc., [16], [17], [18]. Their real-time data can be used as a random key generated by the administrator that manages the user applications and sends these data to the server, where the data will process and react to implement the IoT application.

In a smart home application, the overall system comprises a home equipped with different sensors such as a humidity sensor, temperature sensor, fire/ smoke/ gas leakage detector, and light sensors indicating LDR and motion sensors, [7]. Moreover, these sensors are controlled remotely using a mobile application with different features. Both sides of this system interact using an IoT server. In this case, the home administrator can manage the user's data by giving each user unique identification and initial vector and sending the data for each authentication user while the key exchanges dynamically, preventing any user from knowing any unauthorized data. The administrator gathers all data from the sensors, then manages that data by grouping it and sending each group of sensors' data as a key to the server, where their destination authentication user can see the smart home application information and interact with the system situation and use these keys for dynamic encryption.

For example, the smart home provides data for three accounts, which requires three- different unique identification (ID_S) and initial vectors for each user. The first one is for parents, with full access and privilege to all smart home features. This information must be available just for parents and not available for anybody else; in this case, we will use a secret initial vector V_i for this account and send the sensor data as a key to these users for authentication and encryption, which enhances privacy and security for users, that dynamic key is updated for each user individually. The second account is for children, where there is limited access and privilege, children can control and use some smart home features by using another initial vector V_i for these users, allowing them to authenticate and decrypt authorized application data, and the last account is for emergency cases that can send critical information to the nearest emergency center and family members, which uses public initial vector V_i that allows reserving and decryption that message it if needed. The administrator manages the data based on selected and programmed criteria in advance based on users' and applications' demands and requests. Moreover, the user can manually add these options to eliminate who, when, where, and what data is received.

5 Conclusion and Future work

The IoT real-time applications of CPS are implemented in many areas of industries. For example, intelligent Cars, Medical Devices, Power Grid Systems, Home-based Arrangements, and other similar regions. These applications need high security and privacy in the data exchange. This paper proposes a real-time authentication and a dynamic key exchange protocol that changes and updates the keys between the administrator and server every time. This will enhance security and privacy. This real-time authentication algorithm technique gives key exchange techniques for dynamic encryption, which depends on the random sensor data. The protocol has a low power consumption feature and limited storage required with a lightweight complexity algorithm, facilitating the implementation and distribution of the IoT real-time applications. In future work, the realization of the proposed authentication method will be developed. The smart home model, mobile application, and programmed GUI will be established. Then, real-time data will be presented and discussed thoroughly; the authors will work on realizing the proposed authentication protocol. Finally, a smart home with at least three prototype sensors will be built, and the effectiveness of the proposed authentication method will be verified.

References:

[1] M. Wankhade and S. V. Kottur, "Security Facets of Cyber Physical System" 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020.Author, *Title of the Book*, Publishing House, 200X.

[2] Li, W., Yigitcanlar, T., Erol, I., & Liu, A. Motivations, barriers and risks of smart home adoption: Froma systematic literature review to conceptual framework. Energy Research & Social Science, 80, 102211. 2021.

[3] L. Liu, Y. Liu, L. Wang, A. Zomaya and S. Hu, "Economical and Balanced Energy Usage in the Smart Home Infrastructure: A Tutorial and New Results," in IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 4, pp. 556-570, Dec. 2015.

[4] M. Collotta and G. Pau, "A Novel Energy Management Approach for Smart Homes Using Bluetooth Low Energy," in IEEE Journal on Selected Areas in Communications, vol. 33, no. 12, pp. 2988-2996, Dec. 2015.

[5] G. Song, F. Ding, W. Zhang and A. Song, "A wireless poK1r outlet system for smart homes," in IEEE Transactions on Consumer Electronics, vol. 54, no. 4, pp. 1688-1691, November 2008.

[6] P. Franco, J. M. Martínez, Y. -C. Kim and M. A. Ahmed, "IoT Based Approach for Load Monitoring and Activity Recognition in Smart Homes," in IEEE Access, vol. 9, pp. 45325-45339, 2021.

[7] Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. Smart home security: challenges, issues and solutions at different IoT layers. The Journal of Supercomputing, 77(12), 14053-14089. 2021.

[8] J. T. Kim, "Analyses of secure authentication scheme for smart home system based on internet on things," 2017 International Conference on Applied System Innovation (ICASI), 2017.

[9] Almutairi, O., & Almarhabi, K. Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia. International Journal of Advanced Computer Science and Applications, 12(4). 2021.

[10] Y. Ashibani, D. Kauling and Q. H. Mahmoud, "A context-aware authentication service for smart homes," 2017 14th IEEE Annual Consumer Communications and Networking Conference (CCNC), 2017.

[11] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," 2015 International Symposium on Consumer Electronics (ISCE), 2015.

[12] V. O. Nyangaresi and S. O. Ogundoyin, "Certificate Based Authentication Scheme for Smart Homes," 2021 3rd Global Power, Energy and Communication Conference (GPECOM), 2021.

[13] S. -H. Chang, T. William, W. -Z. Wu, B. -C. Cheng, H. Chen and P. -H. Hsu, "Design of an authentication and key management system for a smart meter gateway in AMI," 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), 2017.

[14] S. Yu, A. K. Das and Y. Park, "Comments on "ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes"," in IEEE Access, vol. 9, pp. 49154-49159, 2021.

[15] C. Tan, Haodong Wang, Sheng Zhong and Qun Li, "IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks", IEEE Transactions on Information Technology in Biomedicine, vol. 13, no. 6, pp. 926-932, 2009.

[16] A. Y. Alhusenat and B. A. Alsaify, "Body Sensors Network Management Protocol," 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), 2021.

[17] M. Fanlin and Y. Wei, "Summary of Research on Security and Privacy of Smart Grid," 2020 International Conference on Computer Communication and Network Security (CCNS), 2020.

[18] A. Brisson, "Deterministic random number generation for one time pads: Creating a Whitenoise super key", 2017 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computed, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2017.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

All authors have contributed equally to the creation on this article.