Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1341–1354
DOI : 10.47974/JDMSC-1750

A mathematical model for secure Cloud-IoT communication: Introducing the revolutionary lightweight key mechanism

Gaikwad Vidya Shrimant *
K. Ravindranath †
Gudapati Syam Prasad §
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram
Andhra Pradesh
India

Abstract

Internet of Things (IoT) is a new technology in telecommunications that focuses on wireless, remote communication. It involves connecting various smart devices to build a network that can transfer data through the cloud. In this type of environment, challenges such as device life span of battery, space needed for storage, consumption of power, and data security for cloud IoT have been identified. This work presents the design and implementation of a secure lightweight key establishment system for the integration of IoT Cloud. A Symmetric Lightweight Algorithm is utilized to enhance the security of Cloud IoT. To improve the efficiency of key setup time, the Advanced Encryption Standard (AES) is applied. The use of AES algorithm in combination with Cloud and IoT Security ensures efficient and consistent performance across software and hardware platforms in various environments. This integration allows for the connection of various smart devices and sensors to Cloud IoT services, facilitating the sharing of sensor readings while addressing security concerns. Before any data is transferred, we securely authenticate both the cloud server and IoT device and generate unique session keys for each new communication session. We conclude by discussing about how cloud computing helps IoT technology achieve secure connection by overcoming various security challenges.

Subject Classification: *94A60 Cryptography.*

Keywords: *Mathematical modeling, Cloud IoT, Security, Lightweight key mechanism, AES, ESP8266.*

* *E-mail:* **gaikwad.vidya30@gmail.com (Corresponding Author)**
† *E-mail:* **ravindra_ist@kluniversity.in**
§ *E-mail:* **syamprasad.gudapati@gmail.com**

1. Introduction

The proposed key establishment mechanism aims to provide a lightweight and secure solution for handshaking of Cloud Server with Smart IoT Devices .The proposed mechanism resolves security threats by using AES (advanced encryption standard) for data encryption and data decryption and by authenticating the cloud server and the IoT devices before communication takes place.

The proposed mechanism uses a fresh current session key for every fresh current session between the Smart IoT Device and cloud server to ensure the protection of the transmit. Additionally, cloud server and every smart IoT device are assigned with unique identifiers which are used to authenticate them before the communication takes place, making it more difficult for unauthorized entities to access the network.

The scheme also includes the use of random nonce and random numbers to add randomness to the data, making it more difficult for an attacker to predict or guess the authentication token. The token needed for authentication and token needed for session with device are transferred by Smart IoT device to the cloud server , where the cloud server verifies the authenticity of the tokens and decrypts the Device Session Token using the key of encryption key, nonce, and random number.

The token of device session is received by cloud server and decrypts by it and compares it with the Authentication Token computed at the cloud server. If the tokens match, the IoT device is considered to be securely authenticated.

Once the authentication is done, session key is computed at the cloud server and it is send to the smart IoT device. The key of session is decrypted by the device and it is used it to check the whether the cloud server is authenticated or not. This means only authentiucated entities are allowed for secure communication.

2. Literature survey

Research in [1], [2],[3], [4], has focused on the netwrok and physical layers of IoT systems by considering and implementing lightweight encryption and low-cost encryption. This can include using lightweight cryptographic primitives, such as lightweight block ciphers, lightweight key exchange protocols, and lightweight authentication protocols.

Susha Surendran [5], the purpose of lightweight cryptography designs is to provide efficient encryption for limited resource devices such as IoT devices.

Authors have studied various types of attacks on these lightweight ciphers to identify vulnerabilities and weaknesses.

Pallavi K N [6] discussed a secured data transfer between the cloud and IoT can include various lightweight cryptographic algorithms. These algorithms can include symmetric algorithms such as AES-128, AES-192 and AES-256, as well as lightweight block ciphers like PRESENT, PRINCE, and SPECK. Each algorithm has its own performance parameters, such as key size, sapce needed for storage and rounds number.

Saurabh Singh in [7] has discussed the basics of lightweight cryptography and its applications in IoT, focusing on lightweight hash functions, block ciphers, stream ciphers, and the specific requirements for low-resource IoT devices.

Pejman Panahi in [8] has conducted simulations on popular IoT devices such as the Raspberry Pi 3 and the Arduino Mega 2560. By evaluating the performance of encryption and decryption on these devices, it can be beneficial to choose on the correct IoT platform and cryptographic encryption algorithm for their specific use case.

Jatinder Singh in [9] has conducted an study of the current scenario of Cloud IoT Security by considering different stakeholders, such as cloud providers, end users and cloud tenants. The research has considered the different security factors for IoT in terms of the different IoT technologies being used.

L. Minh Dang in [10] conducted a study of literature survey for the recent progress in Cloud IoT Security.Bottom of Form

Gudapati, S.P., Gaikwad, V., 2021 [18], the proposed scheme aims to provide secure data transfer between the IoT cloud commnication in a smart home network by implementing mutual authentication, message confidentiality and integrity, and lightweightness properties.

Vidya. S. Gaikwad, 2018 [19], study of cloud security awareness done by the authors.

N. P. Sable 2019 [27], proposed algorithm of encryption for searching data security into cloud.

Nilesh Sable 2018 [28], proposed algorithm of encryption for audit data sharing on cloud.

Wankhede et.al. 2021 [29] proposed and implement survival prediction of glioma brain tumour approach on dynamic architecture using FRCNN deep learning algorithm.

Nilesh Sable 2016, done survey of searching multi keyword preserving privacy using cloud.

3. Proposed Scheme

Table 1 represents the symbols and desscription of our proposed mechanism.

1. In order to provide adequate security in a smart device communication with cloud, it is important to ensure that the smart IoT devices and the cloud server are authenticated entities and they are connected securely with each other.
2. The cloud server and smart IoT device are using symmetric cryptography for message encryption,message decryption and hash function.

The Proposed scheme is divided into two steps

i. Setup of System

ii. Lightweight Key Establishment and Authentication

i. *Setup of System*

It is important for each smart IoT device and the AWS cloud to have a unique identifier (ID) to help ensure the security of the system. A json file is used to store the Identity of the cloud server and smart IoT device, the system can use these IDs to verify the authenticity of the devices and the server.

The use of unique IDs, along with the use of encryption keys (EK) to secure the communications between the devices and the cloud server, helps to protect against masquerade and other types of attacks by ensuring that only authorized entities are able to communicate with the system.

Additionally, by specifying the DI(Identifier for Device), GI(Identifier for Cloud Server), and EK(Key for Encryption) and Port No., this ensures that the keys are long enough to provide a high level of security and to resist against brute-force attacks. The DI, GI, EK are 128bits long in size mentioned in Figure 1.

ii. *Lightweight Key Establishment and Authentication in represented in Figure 2.*

Step 1: Model for Smart IoT Device-A (SD-A)

- Generating a NONCE[S] (a unique value used for authentication) at the smart IoT device (SD-A) and including a "r1" i.e random number in the calculation of the message authentication token can help to improve the security of the system.

  AT_A=h (CIA || DI_A || r1) where AT_A=Authentication Token of Smart IoT Device A

Table 1

Symbols and Description of proposed mechanism

Symbols	Description
EK_A	Encryption Key for Smart Device-A
CI_A	Cloud Identifier for Smart Device-A
DI_A	Device Identifier for Smart Device-A
E	Encrypt Message m for Smart Device-A
D	Decrypt Message m for Smart Device-A
h( )	Hash Function
||	Concatenation Operation
DST_A	Device Session token for Smart Device-A
AT_A	Authentication Token for Smart Device-A
SK	Session Key
CST	Cloud Session Token for Cloud Server

- By including the cloud identifier (CI_A) of the cloud server to which the IoT device is connected, the smart device identifier (DI_A) of the smart IoT device and the "r1" random number in the data being hashed, the system can ensure that the token is unique for each message and cannot be easily guessed or predicted by an attacker.
- Randomness is created by adding the "r1" with function of hash, it prevents from attack.

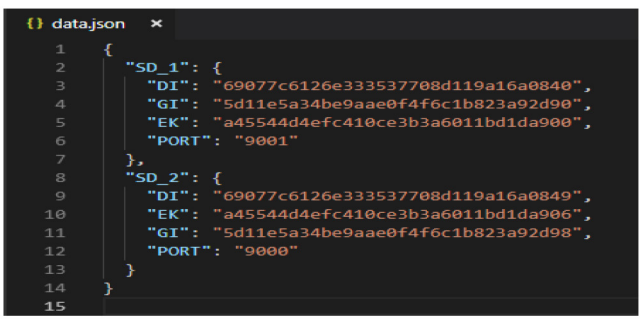

Figure 1

Json file containing DI, GI, EK and Port no.

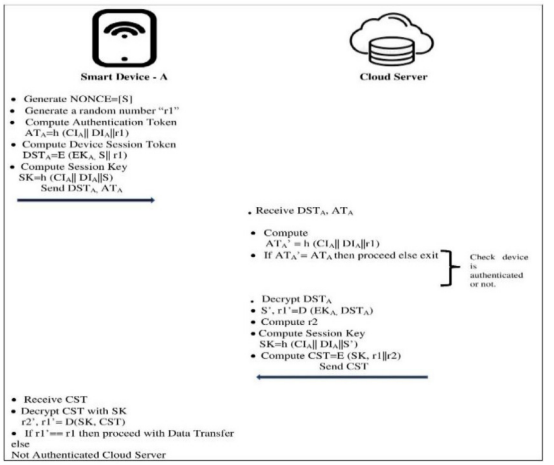

Figure 2

Key Establishment and Authentication proposed mechanism

- Compute a DST_A (Device Session Token) using an encryption key (EK_A) for the smart IoT device (SD-A) with a NONCE=S and a random number=r1, the system can establish a secure session between the device and the cloud server.
- By encrypting the data (S) and the "r1" (random number) using the encryption key (EK_A), it ensures that the information is kept confidential and only authorized entities with the key can decrypt it.

  DST_A = E(EKA, S | |r1) Where DST_A is Calculation of Device Session token

Step 2: Model for Cloud Server Operations

- The server of Cloud receives the token of Device Session (DST_A) and the token of Authentication (AT_A) generated by the Smart IoT device (SD-A).
- The Cloud server decrypts the DST_A using the encryption key to obtain the nonce (S') and the random number (r1').

  $$S', r1' = D (EK_A, DSTA)$$

- The Cloud server calculates the Authentication Token (AT_A') using the Cloud Identifier (CI_A), the Device Identifier (DI_A), and the random number (r1) and compares it with the received Authentication Token (AT_A). If $AT_A' = AT_A$ then the Smart IoT Device is Authenticated, if

the values do not match, then the Smart IoT device is not an trusted/ authentic device.

$$AT_A' = h\ (CI_A\ ||\ DI_A\ ||\ r1)$$

- The Cloud server generates a new random number (r2) and calculates the Session Key (SK) using a hash function with the Cloud Identifier (CIA), the Device Identifier (DIA) and the nonce (S').

$$SK = h\ (CI_A\ ||\ DI_A\ ||\ S')$$

- The Cloud server calculates the Cloud Server Token (CST) using the generated session key (SK), the random number (r1) and the new random number (r2) as input, and encrypts this data.

$$CST = E\ (SK, r1\ ||\ r2)$$

- The Cloud server sends the CST to the IoT device (SD-A).

By following these steps, the Cloud server can authenticate the Smart IoT device and establish a secure session key for communication between the Smart IoT Device and Cloud Server. The Cloud server token (CST) is verifying the whether the Cloud Server is authenticated or non-authenticated.Top of Form

Step-3: Model for Smart IoT Device-A

- Once the IoT device receives the Cloud Session Token (CST) from the Cloud Server, it will decrypt the CST with the Session Key (SK).

$$\mathbf{r1', r2' = D(SK, CST)}$$

If the random numbers r1' and r1 match, then the IoT device proceeds with data transfer by This ensures that the communication between the IoT device and the Cloud Server is secure and only authorized entities can access the data.

If the random numbers do not match, then the IoT device will determine that the Cloud Server is not authenticated and will not proceed with the data transfer, this is to avoid any potential security risks or malicious access.Top of Form

4. Analysis of Performance

The focus of this section is to discuss the analysis of performance of the proposed mechanism and then compare with [20]-[23].

5. Experimentation Environment:

The proposed mechanism is implemented on a ESP8266 platform..

This paper has chosen Symmetric Key Algorithm, Advanced Encryption Standard (AES) for the encryption and decryption.

Figure 3 shows ESP8266 is connected to four sockets in which we can connect an electric bulb, any type of charger. When we click/toggle between ON and OFF buttons present on the web browser then an electric bulb will go glow on and off. Even the charger will get on and off. This is handled through the AWS instance running on AWS cloud.

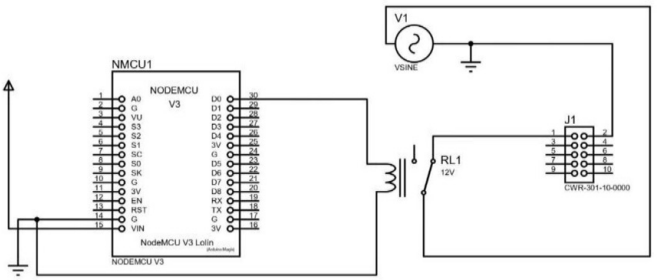

Figure 3

ESP8266 connected with socket

The steps of proposed mechanism are shown in below images.

1. The proposed mechanism shown in Figure 4 represents the process of handshaking between a smart device (SD-1) and a cloud server. This includes the authentication of the smart device and the computation of a session key.

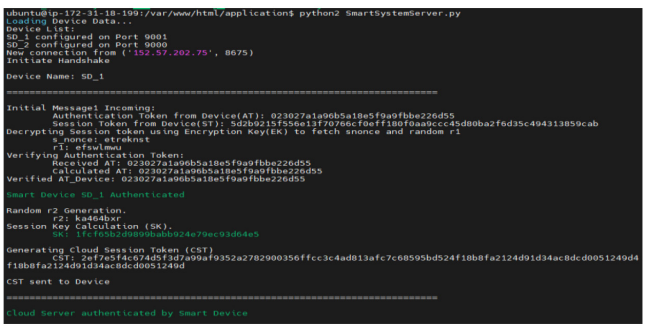

Figure 4

Proposed mechanism outcome using AES

3. Figure 5 represents the outcome of instance on browser. In the browser Public IP address of the running AWS instance is given. To toggle the ON and OFF led connected to ESP8266 use ON and OFF buttons displayed on web browser.

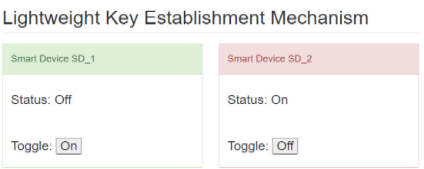

Figure 5

Instance outcome on Browser using public IP address

In the case of the ESP8266 device, energy consumption can be measured by monitoring the power consumption of the device while the cryptographic operations are being performed.

As mentioned in [24],[25] and [26] we have used the formula E=V*I, to calculate the energy "E" consumed by the smart IoT device. Where V is the voltage of ESP8266 and I is the circuit current.

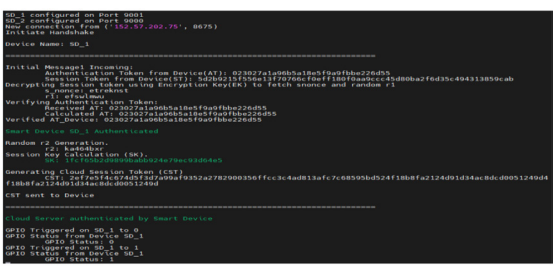

Figure 6

Smart IoT device status after clicking ON and OFF button on browser

Figure 6: represents the smart IoT device status after clicking ON and OFF button on browser.

We have referred datasheet of ESP8266, Voltage for ESP8266 is 3.3V (volt) and 80mA(milliampere) respectively in the working/active mode. Multiply the values (V*I), we get the consumption of energy for cryptographic steps, like encryption, hashing, decryption. We get total energy consumption for proposed mechanism 264 micro-Joule.

4) Figure 7 Represents for every new handshaking session new current random number and session.

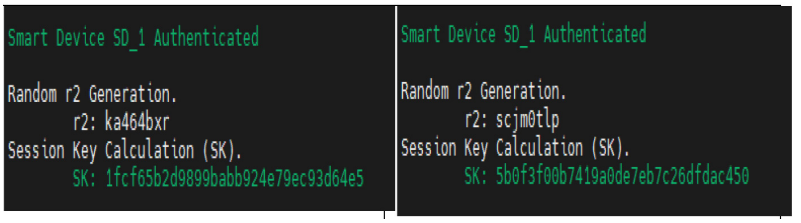

Figure 7

Fresh new Random Number and Session Key computed for every current fresh session

The Table 2 Compares the cost of computation of proposed mechanism, which is compatible to device, it requires one encryption and one decryption, one message authentication code, and two hashing functions are needed for cryptographic operations.

Table 2

Comparison of Computation Cost

Mechanisms	[20]	[21]	[22]	[23]	Proposed
Cryptosystem	1E+1D	-	4E+4D	1E+1D	1E+1D
MAC	1 MAC	-	7 MAC	-	1 MAC
Hash Operation	1H	4H	5H	4H	2H
Point Multiplication	2t	2t	-	4t	-

Figure 8 represents the comparison of communication cost in terms of number of messages exchanged,[20] needs four messages,[21] needs

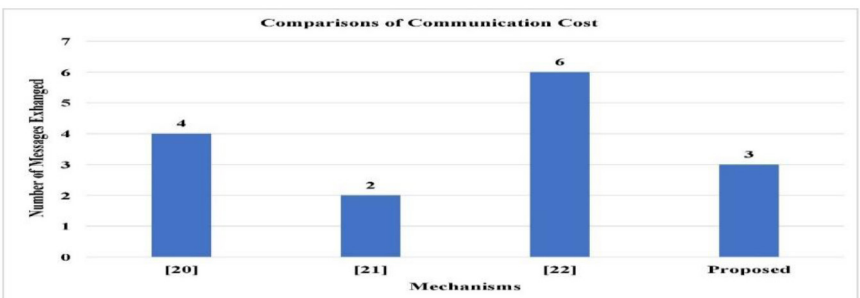

Figure 8

Communication cost comparison with proposed mechanism in terms of number of messages exchanged

two messages,[22] needs six messages, whereas proposed mechanism needs three messages, (one for token of device session, one for token of authentication and last one for token of cloud server) for the whole cryptographic steps. Thus, proposed mechanism can be a good option for securing smart IoT device and cloud server communication.

6. Conclusion

As the interconnected nature of smart IoT devices and cloud server's systems makes them vulnerable to various types of cyber-attacks. The proposed scheme addresses this challenge by providing secure data transfer and communication, authentication between the cloud server and smart IoT devices in the smart IoT cloud applications. The use of AES algorithm for encryption and the implementation of mutual authentication, message confidentiality and integrity, and lightweightness properties help to ensure the security of the Smart IoT Cloud Application.

The proposed scheme is just one aspect of securing a smart home, smart light systems, house climate control systems, safety and security applications.

In this paper, a lightweight algorithm of cryptography is used to provide security for data transfer and secure communication between Smart IoT device and Cloud Server. By considering the smaller size of key, low computation power, low consumption of energy, a less messages are exchanged, the lightweight key establishment mechanism is proposed. Before the connection establishment the authenticity of smart IoT device and cloud server is done. The nonce, random number, session key is computed newly for every current/fresh connection. In the future work, proof of concepts for the safeguard of various attacks will be provided.

References

[1] S. Singh, "Advanced lightweight encryption algorithms for IoT devices : survey , challenges and solutions," *J. Ambient Intell. Humaniz. Comput.*, vol. 0, no. 0, p. 0 (2017).

[2] A. K. Nain, J. Bandaru, M. A. Zubair, and R. Pachamuthu, "A Secure Phase-Encrypted IEEE 802 . 15 . 4 Transceiver Design," vol. 66, no. 8, pp. 1421–1427 (2017).

[3] M. Mangia, F. Pareschi, and R. Rovatti, "Low-Cost Security of IoT Sensor Nodes With Rakeness-Based Compressed Sensing : Statistical and Known-Plaintext Attacks," vol. 13, no. 2, pp. 327-340 (2018).

[4] Z. Mahmood, H. Ning, and A. U. Ghafoor, "A polynomial subset-based efficient multi-party key management system for lightweight device networks," Sensors (Switzerland), vol. 17, no. 4 (2017).

[5] Surendran, S., Nassef, A., & Beheshti, B. D. A survey of cryptographic algorithms for IoT devices. 2018 IEEE Long Island Systems, Applications and Technology Conferenc (LISAT) (2018). https://doi.org/10.1109/lisat.2018.8378034.

[6] K N Pallavi, V Ravi Kumar, & S Srikrishna. Comparative Study of Various Lightweight Cryptographic Algorithms for Data Security Between IoT and Cloud. 2020 5th International Conference on Communication and Electronics Systems (ICCES) (2020).

[7] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H., Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*. (2017) https://doi.org/10.1007/s12652-017-0494-4.

[8] Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S., Performance evaluation of lightweight encryption algorithms for IoT-based applications. *Arabian Journal for Science and Engineering*, 46(4), 4015-4037 (2021). https://doi.org/10.1007/s13369-021-05358-4.

[9] Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D., Twenty security considerations for cloud-supported Internet of things. *IEEE Internet of Things Journal*, *3*(3), 269-284 (2016). https://doi.org/10.1109/jiot.2015.2460333.

[10] Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H., A survey on Internet of things and cloud computing for healthcare. Electronics, 8(7), 768 (2019). https://doi.org/10.3390/electronics8070768.

[11] Dilip Kumar Sharma, Neeraj Baghel, & Siddhant Agarwal. (n.d.). Multiple Degree Authentication in Sensible Homes based on IoT Device Vulnerability. 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC).

[12] Valmiki Siddhartha, Gurjot Singh Gaba, & Lavish Kansal. A Lightweight Authentication Protocol using Implicit Certificates for

Securing IoT Systems [Paper presentation]. International Conference on Computational Intelligence and Data Science (2020, April).

[13] Hittu Garg, Nit Kurukshetra, & Mayank Dave. (n.d.). Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware. 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU).

[14] Khan, M. A., & Salah, K., Cloud adoption for E-lEarning: Survey and future challenges. Education and Information Technologies, 25(2), 1417-1438 (2019). https://doi.org/10.1007/s10639-019-10021-5.

[15] Hahn, D., Munir, A., & Behzadan, V., Security and privacy issues in intelligent transportation systems: Classification and challenges. IEEE Intelligent Transportation Systems Magazine, 13(1), 181-196 (2021). https://doi.org/10.1109/mits.2019.2898973.

[16] Hategekimana, Festus & Whitaker, Taylor & Pantho, Md & Bobda, Christophe. IoT Device Security Through Dynamic Hardware Isolation With Cloud-Based Update. *Journal of Systems Architecture.* (2020). 109. 101827. 10.1016/j.sysarc.2020.101827.

[17] Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos. 2017. Security and Privacy for Cloud-Based IoT: Challenges. Comm. Mag. 55, 1, 26-33 (January 2017). DOI:https://doi.org/10.1109/MCOM.2017.1600363CM.

[18] Gudapati, S.P., Gaikwad, V., Light-Weight key establishment mechanism for secure communication between IoT devices and cloud. In Intelligent System Design (pp. 549–563). Springer, Singapore (2021).

[19] G. S. Prasad and V. S. Gaikwad, (2018) "A survey on user awareness of cloud security", *Int. J. of Engineering and Technology*, vol. 7, no. 2.32, pp. 131-135 (May 2018).

[20] Y. Li, "Design of a key establishment protocol for smart home energy management system," in Proc. 5th Int. Conf. Comput. Intell., Commun. Syst. Netw. (CICSyN), pp. 88-93 (Jun. 2013).

[21] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in Proc. IEEE Int. Conf. Consum. Electron. (ICCE), pp. 787-788 (Jan. 2011).

[22] K. Han, J. Kim, T. Shon, and D. Ko, "A novel secure key paring protocol for RF4CE ubiquitous smart home systems," Pers. Ubiquitous Comput., vol. 17, no. 5, pp. 945-949, (Jun. 2013).

[23] Jebri, S., Ben Amor, A., Abid, M. et al. Enhanced Lightweight Algorithm to Secure Data Transmission in IoT Systems. Wireless Pers Commun 116, 2321-2344 (2021). https://doi.org/10.1007/s11277-020-07792-3.

[24] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," Comput. Netw., vol. 54, no. 17, pp. 2967-2978 (Dec. 2010).

[25] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638-4646 (Sep. 2013).

[26] G. Ateniese, G. Bianchi, A. Capossele, and C. Petrioli, "Low-cost standard signatures in wireless sensor networks: A case for reviving pre-computation techniques?" in Proc. NDSS, San Diego, CA, USA, (Feb. 2013).

[27] D. P. Gadekar, N. P. Sable, A. H. Raut, "Exploring Data Security Scheme into Cloud Using Encryption Algorithms", *International Journal of Recent Technology and Engineering* (IJRTE), Volume-8 Issue-2 (July 2019).

[28] Ashvini Jangam, Nilesh Sable, "Data Security Scheme:Share and Audit Our Data into Cloud using Encryption, "*International Journal of Innovative Research in Science, Engineering and Technology*, Vol 7, Issue 3 (2018).

[29] Disha Sushant Wankhede, R. Selvarani, Dynamic architecture based deep learning approach for glioblastoma brain tumor survival prediction, Neuroscience Informatics, Volume 2, Issue 4 (2022), 100062, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2022.100062.

[30] Nilesh Sable, Shreejit Pillai, Gaurav Ransing, Navanath Ransing, Sumit Markad, "Survey on Privacy Preserving Multi Keyword Search in Cloud Computing", *International Journal of Advanced Research in Computer and Communication Engineering*, vol 5, Issue 11 (2016).