International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys.13, No.1 (May-23)

http://dx.doi.org/10.12785/ijcds/1301110

An Intelligent Encrypt/Decrypt Algorithm in IoT Regarding Home Data Privacy and Security

Yousra Abd Mohammed[1] **and Shayma Wail Nourildean**[1]

[1]*Communication Engineering Department, University of Technology, Baghdad, Iraq*

Received 8 Sep. 2022, Revised 2 May. 2023, Accepted 14 May. 2023, Published 30 May. 2023

Abstract: Citizens and urban settings have benefited significantly from major advances in new life and services provided by smart homes (SHs), which are fully capable of controlling physical objects in real time, collecting very sensitive information, and delivering intelligent data to citizens in many fields, such as transportation, healthcare, smart buildings and parking, public safety, traffic systems, and smart agriculture. The architecture, on the other hand, may encounter a variety of security and privacy challenges at multiple levels.It is in the applied experimental session testing the performance of various machine learning (ML) models for threat detection that one may get a thorough grasp of where and how Data Science can offer value to IoT network security. The findings serve as a foundation for illustrating the advantages of integrating new technology for the purpose of forecasting risks and concerns. Implementing machine learning into intelligent security systems, in addition, increases the requirement for a multi-disciplinary strategy and data infrastructure to manage the whole lifespan of a security product (Software Engineering end-to-end, including ML and Data DevOps). In this paper, we give an intelligent security algorithm for home data privacy and security in IoT. Experiments using the publicly available IoT-23 dataset, which contains labeled information on malicious and benign IoT network traffic, are used to complete the case study. The benign situations were received directly from the actual hardware and were not faked in any way or form. This enabled real-time network activity to be observed and evaluated. Therefore, models provide accurate outputs that may be used to forecast and identify vulnerabilities on Internet of Things-based systems. Furthermore, the lab might be expanded to accommodate the development of commercial and industry demos to demonstrate the benefits of building intrusion detection systems that use machine learning algorithms.

Keywords: Intelligent security algorithm, IoT, encryption, decryption

1. INTRODUCTION

The population of metropolitan regions has been growing at an alarming rate in recent decades. According to a study published by the United Nations Population Fund, over half of the world's people live in cities [1], according to the UN Population Fund. With its stringent standards and practical basis in an urbanized environment, the notion of a "smart home"[2] has drawn far too much interest from both academics and business. Numerous towns and communities have started to build their own plans geared toward the notion of Smart homes in order Improve the life quality and provide the best facilities to people. Several nations with rapidly increasing populations are spending major money in smart home-related initiatives [3]. Smart homes infrastructure includes many devices and interconnected systems that can be used in a variety of applications. A networking paradigm known as information-centric networking (ICN) is one that is capable of maintaining packet delivery even in unreliable situations. As a result, in smart homes, ICN might be seen as a viable alternative to IP-based networking systems [4]. In addition to IP-based techniques, which are provided in [5]'s work, ICN solutions may be used to accelerate the establishment of the Internet of Things and its associated applications. Rather of relying on IP host IDs to identify and find content, ICN is defined as an architectural paradigm to label content and place information in the architecture's heart [6]. The central concept is to radically restructure the internet into a more general and straightforward design.

A lot of research articles on "security and privacy of smart homes" have been released. Kazlauskas K, for example, discusses an algorithm for S-box formation in his paper [7]. The secret key is used to generate the S-box in this case. A lot of S-boxes are created by altering the shared secret key. However, the encryption and decryption processes take longer. The introduction to new "pseudo-random S-box". The development of key-dependent S-box was explained in [8]. [9], [10] looked at the differences between current cryptography and traditional cryptographic techniques. It concludes that contemporary cryptographic methods have a positive avalanche effect. A new strategy for improving the avalanche effect in cryptography is described in [11],

E-mail address: yousra.a.mohammed@uotechnology.edu.iq, Shayma.W.Nourildean@uotechnology.edu.iq

[12]. A new approach to symmetric encryption/decryption using crossover and mutation processes is described in [13]. The usage of genetic operators is detailed in [14], and it plays an important part in key formation that is resistant to various attacks. [15] Explains how to generate pseudo-random sequences and cryptographic algorithms using genetic algorithm operations. smart home privacy has identified technological and design issues [16] as well as potential attacks to identify people and activities from information acquired from smart environments [17], [18], [19] in response a number of studies have developed design and analytic frameworks [20], [21] as well as data management and visualization systems [22], [23], [24] in smart settings. [25], [26], [27] established the algorithm that explains fundamental ideas, technology, IoT difficulties, and device security. In [28], this paper has been proposed a framework for providing effective services in smart cities that is safe and privacy-conscious. The suggested smart city paradigm safeguards the stakeholders' privacy and the integrity of services, such as preventing rogue SPs from misusing public data. This study [29] used the ZigBee communication protocol to examine the security of devices and IoT networks. To secure IoT data while it is being stored and transported, a paper introduced the Flexible encryption Technique (FlexenTech), a new scalable encryption method [30]. A proof of concept for an IoT-based HAN "Home Area Network" in a worldwide setting employing ZigBee protocol as a smart data gathering component. The ZigBee network platform is used in a simulation research with various topologies and configurations that takes place in a worldwide setting is presented in [31]. The main goal of this survey [32] is to provide an overview of continuous authentication techniques used in an Internet of Things environment. Blockchain-related solutions offered in this context are also explored [33], [34]. In [35] three exemplary ABE schemes designed for the worst-case scenario on two well-known IoT platforms, ESP32 and RE-Mote, were examined in terms of their performance in typical IoT constrained devices. [36] is summarized recent research on IoT-enabled smart city applications with a focused on highlighting resource limitations, including restricted processing, limited (energy, storage, and bandwidth). Finally in [37] This study suggested a blockchain-based fog-based secure data exchange framework for Internet of Things devices.

The following is a breakdown of the paper's structure. Section 2 summarizes the overall Smart home architecture, giving a high-level overview of the architecture's levels, followed by a more in-depth assessment of each layer. Sections 3&4 introduce security and privacy considerations, as well as security techniques for smart home devices. Sections 5 and 6 contain the methodology and experimental results. Finally, in Section 7, conclusions are formed.

2. SMART HOME'S ARCHITECTURE

This part is presented an Internet of Things-based architecture with a strong emphasis upon privacy and security challenges that smart homes provide. Architecture, shown in Figure 1, is based on the design suggested in [38] and is built atop it. The following points offer a high-level overview of architecture's layers, followed by a more in-depth examination of each layer.

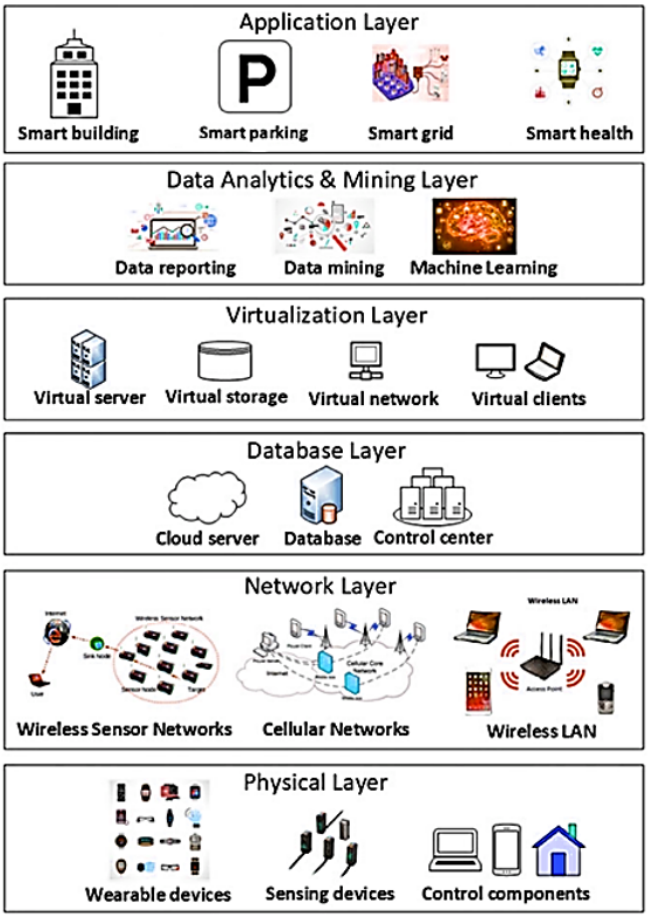

Figure 1. IoT–based architecture

- Physical layer : This layer consider as the systems base often known as the perception layer or the lowest architectural layer that contains heterogeneous hardware such as sensors and actuators which gather and transmit data to the architectures top tier (network layer) to be processed[39].
- Network layer (NL): Serves as foundation of IoT-based architecture. Primary job of NL is passages the data acquired by physical layer and links hardware on the web such as smart devices and servers together [40].
- Database layer (support layer): it operates closely with top layers of the architecture. It involves of database servers and intellectual computing systems. This layer's major role is to meet application requirements using intelligent computing technologies like (cloud/edge) computing [41].

- Virtualization layer: offers the technology known as virtual network, which allows network capabilities hardware and software and to be integrated into a single program entity that can be adjusted conceptually, rather than physically. In order to be effective, network virtualization [42] may need the use of both platform virtualization and resource virtualization.

- Mining and Data analytics layer: In this layer, Raw data is transformed to useful information that may be used to enhance the performance of the network and forecast future occurrences, such as system failures. For data analysis, this layer utilizes different data mining analytics approaches, like MLAs [43].

- Application layer: There are many layers to the secure IoT-based architecture, and this is the most important of them, it is in charge to provide an intelligent apps and facilities to consumers depending on their particular needs [44].

3. SECURITY AND PRIVACY ISSUES IN SMART HOME APPLICATIONS

There are various uses and services the Internet of Things (IoT) can provide including smart cities and houses. IoT smart devices connect with other parts, such as proxy, mobile platforms, as well as data collectors, providing governance, information sharing, and other duties relating to the service being delivered. Whereas these components provide people new, cutting-edge services and contribute towards addressing a number of difficulties, their limited processing capability exposes them to well-known security and privacy risks.

Several threats, both internal and external, have been identified in smart homes applications. The majority of these threats, for example, are due to residents' lack of knowledge about the security and solutions available in their own homes. In addition, companies those make or provide smart home apps don't verify that security criteria are met in order to avert attacks [45], where Smart homes are vulnerable to software vulnerabilities like Eavesdropping, Modification of data, Attacks using passwords.

4. SECURITY HOMES SECURITY

Smart Homes Devices could make quick decisions for detecting and fixing problems whenever a problem or a stranger enters the sensor working area ring, or when something inside or outside the house which not functioning properly. Algorithms are therefore utilized in smart homes to gradually design systems that are high in performance and reliable. New algorithms are continually being developed by designers, as we will demonstrate in this survey:

A. Machine-learning algorithms (MLAs)

MLAs are intelligent in the sense, they can recognize a wide range of internal and exterior concerns and communicate them to the home's owners. And they may be utilized for a variety of tasks such as event identification, energy conservation, anomalous behavior detection, and image-to-speech recognition. By using these algorithms, the requirement for passwords should be considerably reduced since there is simply speech or video identification, and devices will continue to operate as usual [46]. Learning algorithms are often used in smart home systems for tasks such as Identification of actions, prediction of behavior, recognized of faces, and other similar tasks. MLAs are heavily reliant on face recognition in the majority of their working principles. It was claimed in [47] that these algorithms operate similarly to the human mind.
Researchers in [48] talk about object motion detection in smart homes technology, which is accomplished via the use of machine learning algorithms. The greatest benefit of machine learning is that it allows for safe controlled access to smart homes, security in every piece of hardware, and the prevention of physical assaults by persons in the neighborhood without the consent of the home's owner.

B. Real-time algorithms (RTAs)

RTAs are designed for more controlling machinery in line with human motions inside a specific zone or possibly an angle of placed sensors. RTAs use to connect lights to other appliances like heaters, air conditioners, alarms, and other like devices. When somebody is approached or opened the bedroom's door, the air conditioning, lights, and curtains will all automatically switch on and open. Alternatively, if somebody enters the bathroom, both the heating and the lights will switch on. [49] The setups of these devices enable gadgets to communicate data to the Internet of Things, allowing home inhabitants to make configurations using their mobile phones. Two factors determine the object behavior accuracy in RTAs, first, the logical outcomes of the calculations, and second the physical moment at which results are created [50].

C. Deep learning algorithms (DLAs)

Only during the day can video security cameras be employed, and it has never been simple to detect activities at night [51]. Because employing DLAs will improve human aspect recognition, an alarm will sound when someone who isn't registered in that home system enters the area.

D. Prediction algorithms (PAs)

The primary goal of these algorithms is to develop a universal predictor or estimator that can be used to forecast the next action taken by the user. For gathering data depending on movement history contexts, or phrases, a zone IDs dictionary viewed as character symbols are established. [52], which are then used to generate reports.
These algorithms examine the objects' previous and present states in the given situation. If an item has altered its activities from its previous state, prediction algorithms are concerned with identifying the causes for the change in behavior of the object. In the second situation, a prediction method is used to ensure that trusted judgments are replicated. Moreover, as previously said, there are various security needs for smart homes. These include confidentiality, integrity, and availability [53], [54].

E. Identity-based encryption

To safeguard connections among devices having limited capabilities, a secure and effective system must be developed for usage with smart home technologies. This includes the use of encryption and identity-based signatures, which are digital signature techniques for authentication. The ability to manage such systems, especially having devices with self-conscious processing abilities is difficult to achieve despite the existence of a variety of cryptographic algorithms for safeguarding communication among IoT devices. As a result, devices used in the process of home security must interact with the companies that make the devices in order to obtain permission for authentication, which can occasionally make things impossible. As a result, permission is only necessary during the installation or when registration [55], [56].

5. METHODOLOGY

The algorithm that is used for both encryption and decryption is introduced in this section. The sender and recipient share a secret key known only to them as the "key". The pseudo-random numbers are responsible for the construction of the S-box and the arrangement of the components inside the S-box. A program written in Matlab that simulates the entire process of encoding, decrypting, and decoding a message was developed based on the NTRUEncrypt protocol and its detailed formulation in the textbook "An Introduction to Mathematical Cryptography". The program makes use of Matlab's vectorization for faster encryption- and decryption-processes. Public key and private key pairs that will be used for encryption and decryption can be generated from public parameters. To encrypt a message, the transmitter will use a public key, and to decode a message, the receiver will need a private key (a form of assymetric cryptography).

After we have converted a text into its ASCII numeric values (there may be a more efficient protocol, but we only want to find one that works for us so that we can rapidly test the complete encryption system), we can begin encoding it. After that, we add padding to ensure that all ASCII values are three letters in length. When we convert a base 10 number to a base 3 number, if the very first digit in the message is 0, the information contained in the message will be lost (encrypting purposes). In this particular example, we turn the very first 0 into a number nine (No ASCII value will reach 900 so this can be easily converted back during decoding).

We will next divide the whole sequence 97303210811111818101032117033 into 15-digit blocks (Matlab's precision is set to 16 digits by default), with each block having 15 digits. This is the equivalent of 5 characters per block in the game. The following examples show how zero padding will be applied at the end of the final block: 973032108111118 and 101032117033000. This array is converted into fully random coefficients by utilizing the NTRUEncrypt protocol, which is implemented in Matlab. As a result of selecting N = 47 and the fact that NTRU is based on Polynomial Rings, our encrypted message will be represented as a n x 47 array (block size of 47).

- Decryption and decoding: If the encrypted communication is returned to us for decryption, we can quickly transform it back to the original post-encoded message, which saves time. Then, using the required block number information, we may restructure the data such that it can be decoded properly. A form of Public Key Cryptography Figure 2. :

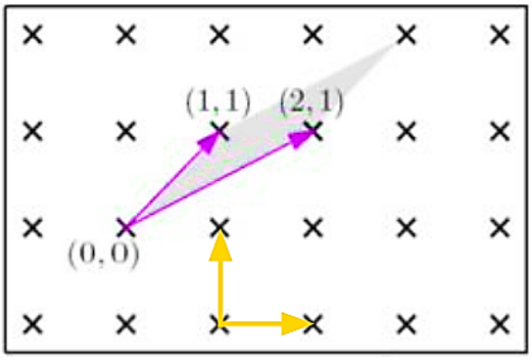

Figure 2. Summary of the NTRU Public Key Cryptosystem

- Key generator: generates a public key and a private key with the security settings that have been specified (N, p, q, d). An encryption algorithm is a mathematical that generates a ciphertext from a message and a public key.

Decryption algorithm accepts a private key and a ciphertext and either outputs the same message as the private key or does not (if successful)

This is the first cryptographic construction based on Quotients of Polynomial Rings, which is most effectively understood in terms of algebraically organized lattices Integer N and two moduli p and q result in the convolution function.

$$R = \frac{Z[x]}{(x^N - 1)}, \quad R_p = \frac{\left(\frac{Z}{pZ}\right)[x]}{(x^N - 1)}, R_q = \frac{\left(\frac{Z}{pZ}\right)[x]}{(x^N - 1)} \qquad (1)$$

By lowering the coefficients of a polynomial a(x) ∈ R modulo p or q, a polynomial a(x) R may be logically transferred to Rp and Rq. The center-lift technique is used to shift items from Rp or Rq to R, as well as the other way around. Ternary polynomials are polynomials that have the form T(d_1, d_2):

$$T(d_1, d_2) = \begin{cases} a(x) \ \textit{has } d_1 \textit{ coefficients equal to } 1. \\ a(x) \ \textit{has } d_2 \textit{ coefficients equal to } -1. \\ a(x) \ \textit{has all other coefficients equal to } 0. \end{cases}$$

Where a(x) ∈ R

6. EXPERIMENTAL RESULT

The plain text 'I love Iraq', the private key was 2x47 digits and the public key was 1x47 digits cipher text was Row1 [60 57 18 54 75 74 13 40 2 52 11 2 70 66 76 68 119 69 13 84 10 123 21 32 36 113 5 12 72 67 6 31 96 113 37 116 7 54 53 21 9 70 118 104 0 107 106]
Row2 [65 105 114 16 0 106 16 54 66 77 40 41 113 100 46 3 53 116 85 56 48 47 37 74 26 20 27 25 61 89 53 45 110 82 16 106 20 104 16 113 69 104 33 52 39 108 23]
Row3 [18 72 28 20 86 110 41 30 16 17 42 100 82 61 45 99 76 31 64 59 112 15 90 65 7 2 45 3 17 75 0 59 5 125 104 3 99 14 67 33 43 117 36 31 50 12 104].
In our algorithm and from Figure 3. We notice the many randomness in the ciphertext and also the division of this text into three rows and the large random distribution, which gives it high protection even for post-quantum computer attacks,

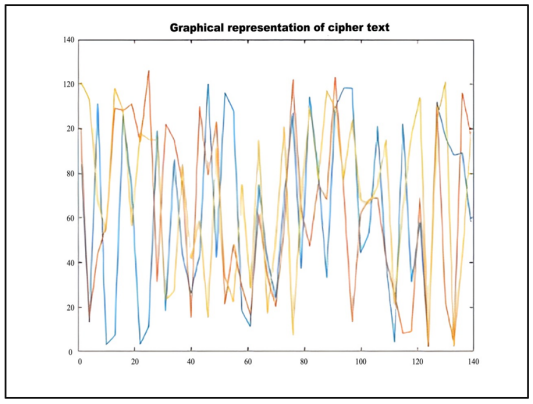

Figure 3. Summary of the NTRU Public Key Cryptosystem

We utilized the following materials for all tests (Figures 3-5), N as safe primes are used as independent variables (11, 23, 47), Constants include the following: maximum number of rounds of GAME: 10; maximum number of trials: 20.

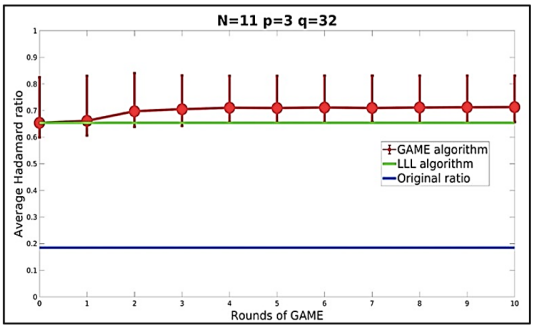

Figure 4. (N = 11) Both LLL and GAME (all 10 hits) did well. GAME increased the Hadamard ratio from 8.25 percent to 9.25 percent. The smallest vector is 85.7 percent the length of the longest vector when

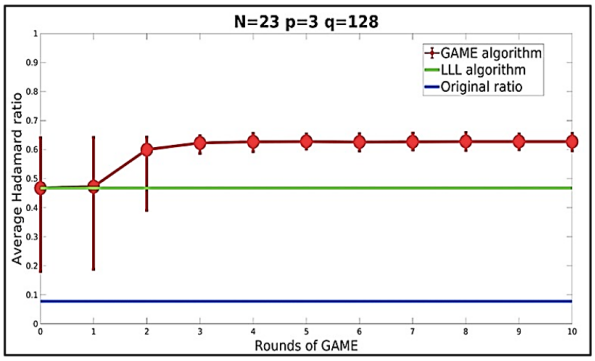

Figure 5. (N = 23) When compared to LLL, GAME (all 10 hits) exhibits a substantial improvement of 34.12 percent in terms of performance. The smallest vector is 81.1 percent the length of the longest vector when using the best basis (f, g).

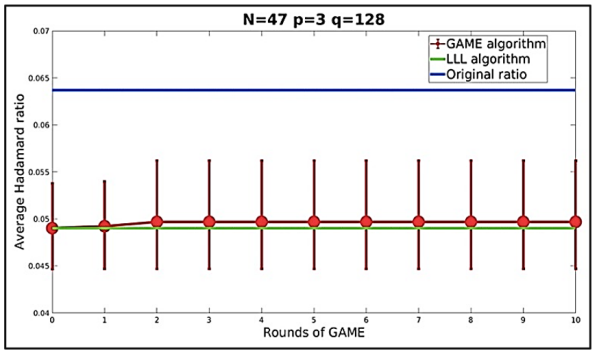

Figure 6. (N = 47): A "better" base is no longer possible with either LLL or GAME (just 1 hit). GAME outperforms LLL by a factor of 1.36 percent. The smallest vector is 1700 percent the length of the longest vector using the returned basis (f, g).

7. CONCLUSION

Urban areas' functionality as well as individuals' overall quality of life and wellbeing could be improved by smart homes. The installation of several smart technologies has brought security and privacy concerns to light. These issues need efficient and effective solutions to be resolved. Furthermore, while designing and implementing new smart systems, it is essential to take into account the security and privacy risks that may arise. This paper is submitted a proposal to strengthen the security of IoT, an artificial intelligence method for data encryption in the IoT is presented. The IoT data unit value is encrypted using an artificial intelligence technique that creates a three-dimensional transformation matrix. Additionally, in order to increase the security performance of IoT edge data, it is necessary to then, for the nodes of the scrambling sequence, an artificial intelligence access strategy is developed, and a random-access route is constructed for the components of the scrambling sequence. It allows them to minimize the cost of computing while also increasing the operational efficiency of Internet of Things devices.

ACKNOWLEDGMENT

The authors are profoundly grateful to the University of Technology (UOT), and Communication Dept., for supporting this research work.

REFERENCES

[1] Y. Cui, S. Gao, C. Xie, Q. Zhang, H. Wang, H. Zhu, and H. Zhou, "Analysis of the matrilineal genetic structure of population in the early iron age from tarim basin, xinjiang, china," *Chinese Science Bulletin*, vol. 54, no. 21, pp. 3916–3923, 2009.

[2] E. Ever, F. M. Al-Turjman, H. Zahmatkesh, and M. Riza, "Modelling green hetnets in dynamic ultra large-scale applications: A case-study for femtocells in smart-cities," *Computer Networks*, vol. 128, pp. 78–93, 2017.

[3] N. Alharbi and B. Soh, "Roles and challenges of network sensors in smart cities," in *IOP Conference Series: Earth and Environmental Science*, vol. 322, no. 1. IOP Publishing, 2019, p. 012002.

[4] M. Wang, J. Wu, G. Li, J. Li, Q. Li, and S. Wang, "Toward mobility support for information-centric iov in smart city using fog computing," in *2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*. IEEE, 2017, pp. 357–361.

[5] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE wireless communications*, vol. 20, no. 6, pp. 91–98, 2013.

[6] A. V. Vasilakos, Z. Li, G. Simon, and W. You, "Information centric network: Research challenges and opportunities," *Journal of network and computer applications*, vol. 52, pp. 1–10, 2015.

[7] K. Kazlauskas, G. Vaicekauskas, and R. Smaliukas, "An algorithm for key-dependent s-box generation in block cipher system," *Informatica*, vol. 26, no. 1, pp. 51–65, 2015.

[8] B. Maram and J. Gnanasekar, "A block cipher algorithm to enhance the avalanche effect using dynamic key-dependent s-box and genetic operations," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 10, pp. 399–418, 2018.

[9] P. Ganesh, A. Nitin, and T. Sitendra, "A block based encryption model to improve avalanche effect for data security," *International Journal of Scientific and Research Publications*, vol. 3, no. 1, pp. 1–4, 2013.

[10] J. Gnanasekar, "Light weight cryptographic algorithm to improve avalanche effect for data security using prime numbers and bit level operations," *International Journal of Applied Engineering Research*, vol. 10, no. 21, pp. 41 977–41 983, 2015.

[11] J. P. Bhoge and P. N. Chatur, "Avalanche effect of aes algorithm," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 3, pp. 3101–3103, 2014.

[12] A. Singh, "A new approach to enhance avalanche effect in aes to improve computer security," *Journal of Information Technology & Software Engineering*, vol. 5, no. 1, p. 1, 2015.

[13] B. Maram, J. Gnanasekar, G. Manogaran, and M. Balaanand, "Intelligent security algorithm for unicode data privacy and security in IoT," *Service Oriented Computing and Applications*, vol. 13, no. 1, pp. 3–15, 2019.

[14] R. Roy Chowdhury, A. Che Idris, and P. E. Abas, "Internet of things device classification using transport and network layers communication traffic traces," *International Journal of Computing and Digital Systems*, vol. 12, no. 1, pp. 545–555, 2022.

[15] S. Dutta, T. Das, S. Jash, D. Patra, and P. Paul, "A cryptography algorithm using the operations of genetic algorithm & pseudo random sequence generating functions," *International Journal*, vol. 3, no. 5, 2014.

[16] J. Bugeja, A. Jacobsson, and P. Davidsson, "On privacy and security challenges in smart connected homes," in *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 2016, pp. 172–175.

[17] N. Apthorpe, D. Reisman, and N. Feamster, "A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic," *arXiv preprint arXiv:1705.06805*, 2017.

[18] M. Conti, M. Nati, E. Rotundo, and R. Spolaor, "Mind the plug! laptop-user recognition through power consumption," in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*. New York, NY, USA: Association for Computing Machinery, 2016, p. 37–44.

[19] J. Obermaier and M. Hutle, "Analyzing the security and privacy of cloud-based video surveillance systems," in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*. New York, NY, USA: Association for Computing Machinery, 2016, p. 22–28.

[20] A. Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015, pp. 727–732.

[21] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-design framework for assessing internet of things applications and platforms," in *Proceedings of the 6th International Conference on the Internet of Things*, 2016, pp. 83–92.

[22] B. Carminati, P. Colombo, E. Ferrari, and G. Sagirlar, "Enhancing user control on personal data usage in internet of things ecosystems," in *2016 IEEE International Conference on Services Computing (SCC)*. IEEE, 2016, pp. 291–298.

[23] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[24] J. Wu, J. Liu, X. S. Hu, and Y. Shi, "Privacy protection via appliance scheduling in smart homes," in *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. ACM, 2016, pp. 1–6.

[25] M. Abdel-Basset, M. Gunasekaran, M. Mohamed, and F. Smarandache, "A novel method for solving the fully neutrosophic linear programming problems," *Neural Computing and Applications*, vol. 31, no. 5, pp. 1595–1605, 2019.

[26] M. Abdel-Basset, G. Manogaran, A. Gamal, and F. Smarandache, "A hybrid approach of neutrosophic sets and dematel method for developing supplier selection criteria," *Design Automation for Embedded Systems*, vol. 22, no. 3, pp. 257–278, 2018.

[27] M. Abdel-Basset, G. Manogaran, A. E. Fakhry, and I. El-Henawy, "2-levels of clustering strategy to detect and locate copy-move

forgery in digital images," *Multimedia Tools and Applications*, vol. 79, no. 7, pp. 5419–5437, 2020.

[28] K. Tabassum and A. Ibrahim, "A secure and privacy-aware framework for future smart cities," *International Journal of Computing and Network Technology*, vol. 7, no. 1, 2019.

[29] I. Vaccari, E. Cambiaso, and M. Aiello, "Evaluating security of low-power internet of things networks," *International Journal of Computing and Digital Systems*, vol. 8, no. 02, pp. 101–114, 2019.

[30] S. Medileh, A. Laouid, E. M. B. Nagoudi, R. Euler, A. Bounceur, M. Hammoudeh, M. AlShaikh, A. Eleyan, and O. A. Khashan, "A flexible encryption technique for the internet of things environment," *Ad Hoc Networks*, vol. 106, p. 102240, 2020.

[31] E. A. Asonye, S. M. Musa, C. M. Akujuobi, M. N. Sadiku, and J. Foreman, "Realizing an IoT-based home area network model using zigbee in the global environment." *International Journal of Computing and Digital Systems*, vol. 9, no. 6, pp. 1131–1142, 2020.

[32] F. H. Al-Naji and R. Zagrouba, "A survey on continuous authentication methods in internet of things environment," *Computer Communications*, vol. 163, pp. 109–133, 2020.

[33] M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Information Processing & Management*, vol. 58, no. 3, p. 102482, 2021.

[34] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture," *Energy Reports*, vol. 7, pp. 8075–8082, 2021.

[35] P. Perazzo, F. Righetti, M. La Manna, and C. Vallati, "Performance evaluation of attribute-based encryption on constrained IoT devices," *Computer Communications*, vol. 170, pp. 151–163, 2021.

[36] S. Zahoor and R. Naaz Mir, "An IoT enabled smart city: Assessing the applications, resource constraints, existing solutions and research directions," *International Journal Of Computing and Digital System*, vol. 12, no. 1, pp. 271–283, 2021.

[37] D. Mohapatra, S. K. Bhoi, K. K. Jena, S. R. Nayak, and A. Singh, "A blockchain security scheme to support fog-based internet of things," *Microprocessors and Microsystems*, vol. 89, p. 104455, 2022.

[38] L. Tan and N. Wang, "Future internet: the internet of things. advanced computer theory and engineering (icacte)," in *2010 3rd International Conference on*, vol. 5, 2010, pp. V5–V376.

[39] T. Yu, T. Li, Y. Sun, S. Nanda, V. Smith, V. Sekar, and S. Seshan, "Learning context-aware policies from multiple smart homes via federated multi-task learning," in *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2020, pp. 104–115.

[40] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, "Investigating smart home security: Is blockchain the answer?" *IEEE Access*, vol. 8, pp. 117 802–117 816, 2020.

[41] Y. Cui, S. Gao, C. Xie, Q. Zhang, H. Wang, H. Zhu, and H. Zhou, "Analysis of the matrilineal genetic structure of population in the early iron age from tarim basin, xinjiang, china," *Chinese Science Bulletin*, vol. 54, no. 21, pp. 3916–3923, 2009.

[42] I. Hwang and D. Shin, "Application level network virtualization using selective connection," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2018, pp. 1–2.

[43] C. V. Nguyen, M. T. Nguyen, T. V. Quyen, A. M. Le, A. Masaracchia, H. T. Nguyen, H. P. Nguyen, L. D. Nguyen, H. T. Nguyen, and V. Q. Nguyen, "Hybrid solar-rf energy harvesting systems for electric operated wheelchairs," *Electronics*, vol. 9, no. 5, p. 752, 2020.

[44] R. El-Azab, "Smart homes: Potentials and challenges," *Clean Energy*, vol. 5, no. 2, pp. 302–315, 2021.

[45] J. J. Palop, L. Mucke, and E. D. Roberson, "Quantifying biomarkers of cognitive dysfunction and neuronal network hyperexcitability in mouse models of alzheimer's disease: depletion of calcium-dependent proteins and inhibitory hippocampal remodeling," in *Alzheimer's Disease and Frontotemporal Dementia*. Springer, 2010, pp. 245–262.

[46] J. Mao, Q. Lin, and J. Bian, "Application of learning algorithms in smart home IoT system security," *Mathematical foundations of computing*, vol. 1, no. 1, p. 63, 2018.

[47] I. A. Berg, O. E. Khorev, A. I. Matvevnina, and A. V. Prisjazhnyj, "Machine learning in smart home control systems-algorithms and new opportunities," in *AIP Conference Proceedings*, vol. 1906, no. 1. AIP Publishing LLC, 2017, p. 070007.

[48] J. Jaihar, N. Lingayat, P. S. Vijaybhai, G. Venkatesh, and K. Upla, "Smart home automation using machine learning algorithms," in *2020 International Conference for Emerging Technology (INCET)*. IEEE, 2020, pp. 1–4.

[49] S. A. Khan, A. Farhad, M. Ibrar, and M. Arif, "Real time algorithm for the smart home automation based on the internet of things," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, no. 7, pp. 94–99, 2016.

[50] B. Das, D. J. Cook, N. C. Krishnan, and M. Schmitter-Edgecombe, "One-class classification-based real-time activity error detection in smart homes," *IEEE journal of selected topics in signal processing*, vol. 10, no. 5, pp. 914–923, 2016.

[51] Y. Peng, J. Peng, J. Li, and L. Yu, "Smart home system based on deep learning algorithm," in *Journal of Physics: Conference Series*, vol. 1187, no. 3. IOP Publishing, 2019, p. 032086.

[52] A. Dixit and A. Naik, "Use of prediction algorithms in smart homes," *International Journal of Machine Learning and Computing*, vol. 4, no. 2, p. 157, 2014.

[53] C. S. Kouzinopoulos, G. Spathoulas, K. M. Giannoutakis, K. Votis, P. Pandey, D. Tzovaras, S. K. Katsikas, A. Collen, and N. A. Nijdam, "Using blockchains to strengthen the security of internet of things," in *International ISCIS Security Workshop*. Springer, Cham, 2018, pp. 90–100.

[54] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.

[55] Y. Guo, Z. Wang, X. Yin, X. Shi, J. Wu, and H. Zhang, "Incremental deployment for traffic engineering in hybrid sdn network," in *2015*

IEEE 34th international performance computing and communications conference (IPCCC). IEEE, 2015, pp. 1–8.

[56] K. Sharma, D. Anand, M. Sabharwal, P. K. Tiwari, O. Cheikhrouhou, and T. Frikha, "A disaster management framework using internet of things-based interconnected devices," *Mathematical Problems in Engineering*, vol. 2021, 2021.

Yousra Abd Mohammed is a lecturer at the Communication Engineering Department, University of Technology- Baghdad, Iraq since 2005. She received her B.Sc. in Electronic and Communication Engineering from Technology University/Baghdad, Iraq in 1992 and her M.Sc. degree in Computer Engineering from Technology University/Baghdad in 2004. Her research interests include Control Systems, Encryption and Decryption Algorithms.

Shayma Wail Nourildean is a lecturer (a member of an academic staff) in Communication Engineering department in University of Technology (UOT), Baghdad–Iraq. She Holds a M.Sc. degree in Control and Computer Engineering with specialization in Computer Engineering since 2006 and she received B.Sc. degree in Computer Engineering from Baghdad University in 2002. Her research areas are Computer Networks, Data Communication and Wireless Sensor Networks. She published a number of papers in national and international journals and participated in multiple national and international conferences.