

## Securing IoT edge device communication with efficient ECC middleware for resource-constrained systems

Zainatul Yushaniza Mohamed Yusoff<sup>1</sup>, Mohamad Khairi Ishak<sup>1,2</sup>, Lukman AB Rahim<sup>3</sup>

<sup>1</sup>School of Electrical and Electronic Engineering, Universiti Sains Malaysia, Pulau Pinang, Malaysia

<sup>2</sup>Department of Electrical and Computer Engineering, College of Engineering and Information Technology, Ajman University, Ajman, United Arab Emirates

<sup>3</sup>Faculty of Science and Information Technology, Universiti Teknologi Petronas, Seri Iskandar, Malaysia

### Article Info

#### Article history:

Received Sep 26, 2023

Revised Apr 29, 2024

Accepted May 17, 2024

#### Keywords:

Authentication

Confidentiality

Integrity

Internet of things

Lightweight cryptography

Servlet technology

### ABSTRACT

The internet of things (IoT) rapidly grows into various parts of life. However, it has significant obstacles during setup and deployment, particularly in terms of network segmentation, administration, and security at all tiers, from physical to application. While IoT provides several advanced features and benefits, it is also vulnerable to security threats and flaws that must be thoroughly investigated to avoid misuse. Cryptographic approaches are routinely used to address these security concerns. Message queuing telemetry transport (MQTT), an application layer protocol, is vulnerable to various known and undisclosed security flaws. Integrating encryption techniques within the MQTT protocol to provide secure data flow is a potential strategy for increasing security. This study provides a middleware broker that improves authentication processes, securing connections between cloud servers and resource-constrained devices. Using a Java Servlet and the elliptic curve cryptography (ECC) technique, the study creates a system for creating encrypted identification keys within a web-based transaction framework. This system intends to provide asymmetric authentication that is energy and resource-efficient, with a focus on cost minimization. It also includes a security feature to protect users from common internet threats. The system's efficacy, including its low energy usage of only 4 mJ per device, is thoroughly tested, proving it meets the original protocol criteria.

This is an open access article under the [CC BY-SA](#) license.



### Corresponding Author:

Mohamad Khairi Ishak

Department of Electrical and Computer Engineering, College of Engineering and Information Technology

Ajman University

Ajman, United Arab Emirates

Email: m.ishak@ajman.ac.ae

## 1. INTRODUCTION

The internet of things (IoT) refers to a vast network of interconnected software and hardware components that are used in various industries, including production and energy management, agriculture, e-commerce, logistics, healthcare, satellite imagery, building and infrastructure automation, large-scale projects, and transportation [1]. Smart homes have become a prominent application within the vast realm of the IoT, facilitating the linking of intelligent gadgets to improve data exchange and interaction, as depicted in Figure 1. This improvement enhances user convenience in managing, controlling, and accessing diverse gadgets [2]. However, the extensive connectivity of smart homes raises concerns about security and privacy. IoT systems have substantial security obstacles at the application layer, such as ensuring data access,

authentication, privacy, and identity protection. The challenge of ensuring the security of smart home devices arises from the wide range of possible vulnerabilities and attack routes that can be exploited [3]. Creating and executing strong security frameworks to reduce the impact of these changing threats is crucial. In the absence of adequate safeguards, adversaries have the potential to breach message routing, intercept data, modify transmissions, obstruct access for authorized users, and potentially disrupt the IoT network by escalating power consumption, generating routing loops, or falsifying identities [4]. The interconnectedness of IoT devices, frequently facilitated by fog computing nodes, underscores the necessity for a comprehensive security strategy that prioritizes authentication, availability, and privacy. Cryptography techniques are crucial for attaining these security objectives [5].

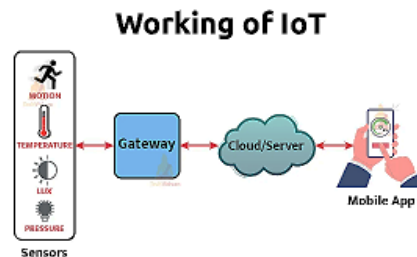


Figure 1. Interdevice system in IoT

Our research makes a substantial contribution to improving the security of IoT, specifically in the context of smart homes, through various important initiatives: i) our implementation utilizes servlet technology to provide a robust security and privacy identification (SPID) system designed specifically for IoT devices with limited resources in smart homes. This system guarantees authentication, confidentiality, integrity, and resilience against cyber threats; ii) elliptic curve cryptography (ECC) employs concise keys to ensure effective security, posing a formidable challenge for potential attackers attempting to breach the system. This technique entails the sender and receiver producing a pair of public and private keys using ECC, augmenting the security level; iii) the authentication and communication phase parameters are transmitted over a secure channel by calculating a hash value. Finally, all received parameters are recalculated to ensure stability and security; and iv) by implementing ECC into the communication protocols of smart home devices, we greatly enhance the security system of IoT ecosystems, effectively protecting against a wide range of vulnerabilities and threats.

This work aims to secure the IoT landscape through ongoing innovation and security advancements, ensuring the integrity and reliability of smart home ecosystems and the broader IoT network. The remainder of this article is organized as follows. Section 2 discusses some recently proposed related studies and preliminary literature on ECC. Section 3 details the proposed protocol. A security and performance analysis in section 4. A conclusion in section 5.

## 2. RELATED WORKS AND PRELIMINARIES

This study section describes the work related to the proposed work and identifies the critical preparatory work required for this document.

### 2.1. Related works

Research by [6], [7] emphasizes the vulnerability of contemporary primary care physicians to many types of cyberattacks, including shoulder surfing, brute force, and smear efforts. A template-based authentication method was developed [8]. However, it is still vulnerable to corruption attacks. Another attempted solution intended to be both efficient and secure, but it did not adequately address common threats such as man-in-the-middle (MitM) and phishing attempts, which also significantly impact processing time. Comparable restrictions are seen in the technique described in reference [9]. The paired-key structure, as shown in [10], is susceptible to the threat of physical hacking, which has the potential to compromise the authentication keys. The dual-key protocol described in [11] is susceptible to vulnerabilities arising from probable failures in its key distribution function, which can disrupt the relationships between entities. The approach described in [12] requires significant processing resources due to its strong dependence on cryptographic operations. However, the methodology described in [13] does not guarantee complete confidentiality or adequately protect against serious attacks and denial of service (DoS) threats. The authentication scheme described in [14] is ineffective against attacks that exploit the use of keys, does not

provide guarantees of message relevancy, and is excessively intricate. The session key generation mechanism described in [15] is vulnerable to replay and time synchronization attacks and it does not adequately safeguard anonymity or relevance. The method based on physical unclonable functions (PUFs) described in [16] imposes substantial computational and connectivity challenges. On the other hand, the approaches presented in [14], [15], [17] lack sufficient anonymization and non-traceability capabilities, thereby restricting their usefulness in advanced surveillance scenarios.

The self-signing and access control systems described in [18] effectively safeguard against data leakage and unauthorized code alterations. However, their implementation necessitates the involvement of a certifying authority. The simplified approach described in [19] relies on a trusted authority, which introduces a possible vulnerability due to the presence of a single point of failure. The user and password system in [20] is susceptible to many attacks due to weaknesses in session information. The provision of anonymity and non-traceability in [21], [22] requires the use of additional accounts and communication, which increases complexity. Implementing a three-step authentication process in [23] incurs additional expenses in data storage and processing, as it involves a two-factor authentication mechanism. The approach proposed in [5], which relies on fingerprint authentication, mitigates the risk of online and MitM attacks but incurs greater initial costs for implementation. Despite its basic design for home security, the cost-effective system in [24] cannot effectively prevent online hacking attempts. According to research conducted in [25], it is recommended to prioritize installing a home security system that addresses physical risks rather than online ones. The V2V authentication approach utilizing ECC in [26] improves the real-time flow of information between vehicles. However, it also leads to higher transit and storage expenses due to safety regulations. The procedure described in [27] demonstrates resilience against attacks but necessitates intricate and multi-step calculations. The facial recognition security system implemented in [28] for IoT devices, utilizing Raspberry Pi 3, focuses on enhancing performance and energy efficiency. However, it neglects cyberattack countermeasures and incurs significant expenses for installation and maintenance. Furthermore, the home automation protection system in [29] is still susceptible to cyber threats because of a lack of sufficient preventive measures.

## 2.2. Elliptic curve cryptography

ECC a variant of public-key cryptography, relies on the mathematical framework of elliptic curves within finite fields. Independently introduced by Koblitz and Victor Miller during the mid-1980s, ECC keys typically span 256 bits, offering comparable security to a 3072-bit Rivest–Shamir–Adleman (RSA) key while providing superior defense against attacks. Furthermore, ECC surpasses RSA in speed, enhancing efficiency and minimizing server resource utilization. A comparison of these encryption schemes is detailed in Table 1 [30]. Consequently, ECC encryption finds particular utility in securing IoT devices with constrained resources and demanding robust security. The security of cryptographic systems hinges on the inherent complexity of mathematical problems, with algorithms impervious to polynomial-time solutions deemed secure.

Table 1. Comparison item between ECC and RSA

No.	Comparison item		ECC	RSA
1	Key length	256 bits		2,048 bits
2	CPU usage	Less		Higher
3	Memory usage	Less		Higher
4	Network usage	Less		Higher
5	Efficiency	High		Normal
6	Anti-attack	High		Normal
7	Compatibility	Support new browsers and OS (some platforms, such as cPanel are not supported)		Supports all

## 3. PREVIEW OF DANG-SCHEME

This study enhances the Dang-Scheme, an authentication framework first presented by Dang *et al.* [31], in our research. This is an enhancement of a protocol developed by Wang *et al.* [32] to strengthen the authentication of IoT devices with limited resources, specifically emphasizing increased security. Comprehending the Dang-Scheme is essential as it establishes the foundation for our improved protocol. The Dang-Scheme is organized into three primary phases, illustrated in Figure 2. Phase 1 is enrollment, during this stage, the system integrates devices by registering their distinct identifiers with the server. After the registration, the server creates and maintains necessary authentication data, while the device provides secure cookie data for future authentication procedures. Phase 2 is authentication between server and device, before allowing network access, a verification process occurs between the server and the device to confirm the device's credentials or cookie data, thereby verifying the authenticity of both the device and the server. The completion of this essential process results in the generation of a session key, demonstrating mutual

authentication. Phase 3 is authentication between two devices, due to the widespread occurrence of device-to-device interactions in IoT ecosystems, devices must authenticate one another before exchanging data. Like the second phase, this stage confirms the identities of the devices and establishes a secure session key for secure communication.

Figure 2 depicts the authentication workflow of the Dang-Scheme, which employs a centralized management approach to oversee connectivity, verification, and access within IoT environments. This method is particularly suitable for devices with limitations in processor capability, storage capacity, and energy resources. The system utilizes an ECC-based mutual authentication mechanism to authenticate devices. A notable aspect of this method is that device 2 (the responder) independently acquires the authentication key from the server. However, this approach channels all inter-device connections through the Device, potentially leading to bottlenecks. To address this, we introduce a novel protocol that enhances security by employing fluid protocols, albeit without specifically targeting brute-force attacks. Our solution aims to optimize and refine the authentication process, mitigating the inefficiencies present in the original Dang-Scheme while maintaining its security.

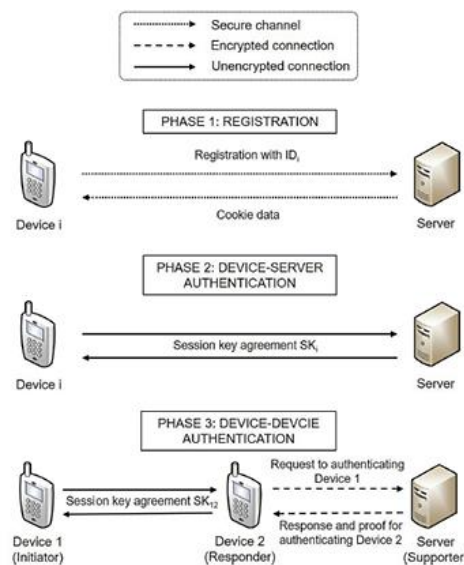


Figure 2. Authentication workflow of the Dang-Scheme

#### 4. METHOD

Our system incorporates a modified version of the Dang *et al.* [31] technique designed to enhance the security assurance of authenticating resource-constrained devices in the IoT environment. The Dang-Scheme authentication protocol comprises three primary phases: i) phase 1 involves registration; ii) phase 2 entails device-server authentication; and iii) phase 3 encompasses device-device authentication. However, their proposal entails a protocol in which each device can authenticate the identity of the other device as a server via the responder registration device. Conversely, the responder obtains authentication from the server of the IoT system, requiring both parties to mutually verify each other's credentials before establishing communication. The objective of our proposed protocol is to transition the authentication process from mutual to asymmetric.

IoT systems consist of interconnected components capable of communication and interaction. These components range from large entities such as servers, home appliances, vehicles, and gateways, to smaller devices like smartphones and sensors. Our approach leverages these components, with a secure middleware broker positioned above the foundational layers to manage devices, enrollment, service contracts, and transactions. This middleware is an additional protective layer complementing existing security measures, offering a tangible, scalable, and centrally manageable solution, illustrated in Figure 3. Using servlet technology, the security framework provides a fundamental middleware solution suitable for parallel and distributed deployments. Figure 3 shows the categorized security roles and concerns into a three-tier model: collection domain, network domain, and application domain. The ECC algorithm employs keys to encrypt identification data, securing web traffic using public and private keys. As a practical coding technique, ECC presents a viable alternative to RSA. Elliptic curves ensure the necessary level of security for public-key cryptography. Algorithm 1 exemplifies the implementation of the system model.

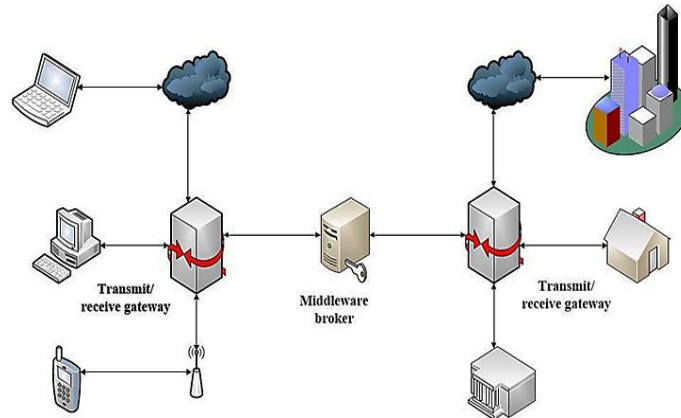


Figure 3. The method proposed a middleware security broker key for enhanced security and device or network isolation

#### Algorithm 1. Calculate system model application

```

On connect (client, userdata, flags, rc):
  RC ← str (rc)
  client.subscribe ← smarthome/light
  Ec=newEllipticCurve (newsecp256r1())
  ECCryptoSystemcs=newECCryptoSystem (ec)
  EncryptedOnOFF=cs.encrypt (bytes, bytes.length,
  privateKeys.elementAt (index))
  Command+ =encryptedOnOFF
On message (client, userdata, msg):
  Msg ← str (msg.payload)
  Size (bytes) ← str (sys.getsizeof (msg.payload))
  Starttime ← int (round (time.time ()×1000))
  Message ← str (msg.payload.decode ("utf - 8"))
  cmd ← echo + message|ecc - d - sk
  Stream ← os.popen (cmd)
  Output ← stream.read ()
  Output ← stream.read ()
  Output ← stream.read ()
  If output.replace is ON then
    output.replace ← lightON
  End if
  os.system ← (/home/pi/turnoff.sh)
  Durationtime ← int (round (time.time ()×1000)) -
  Start time
  Duration (ms) ← str (duration time)

```

#### 4.1. Servlet technology

Servlets are server-side technologies and applications written in Java that facilitate efficient data flow between clients and a web server. They enable dynamic interactions and manipulation of data on web pages. They function from the server's side, autonomously from any graphical user interface, enabling interactive online content without requiring client-side computation. When a client, such as a web browser or any web-enabled program, sends a request to a web server, servlets become active. The requests are processed, and dynamic responses are created, using servlet request and response objects to represent the incoming inquiries and outgoing replies, respectively. Servlets can handle multiple client requests concurrently and effectively manage and coordinate these interactions. In addition, they can redirect requests to alternative servers or servlets, enhancing their adaptability in web applications. Clients communicate with a servlet by sending a URL command that specifies the server's hosting directory or simulates local access. Servlets written in Java are highly skilled at executing intricate business logic. Servlets are well-suited for building advanced business applications that involve real-time data processing and presentation, as they enable powerful interactions with relational databases through dynamic web pages.

## 5. RESULT AND DISCUSSION

In this section, we prove that the proposed authentication protocol is secure and resistant to various attacks by performing a comprehensive security analysis of the security scheme. While making the proposed protocol resistant to various attacks, another critical aspect to look at is power consumption performance.

## 5.1. Security analysis

### 5.1.1. Security properties

Asymmetric authentication is the authentication transaction key serves as the transaction key for communication among IoT devices. Upon determining the device ID, network ID, and application ID, the ECC algorithm generates a unique identifying transaction key, which is then transmitted to the gateway receiver. As both public and private keys adhere to a 256-bit elliptic curve, each generated identity transaction key possesses uniqueness. Subsequently, the transaction identification key is forwarded to the user-requested destination. Confidentiality is concerning encryption algorithms, key agreements, and the privacy of personal device data, the proposed protocol effectively addresses these requirements. During the middleware broker process, the system examines the device ID, network ID, and application ID, prompting the user to generate a private key before encrypting the user's device. Despite the utilization of the device's private data during the authentication phase, the protocol ensures data confidentiality by employing a random key for each operation and encapsulating the end with an ECC function. Consequently, even if an attacker intercepts the data during transmission, they are unable to reuse or access the secret session key. Perfect forward/backward secrecy is in the proposed protocol, every session is uniquely identified by a random number generated independently by each device. Consequently, the session key varies randomly, ensuring it differs with each session. These characteristics effectively thwart attempts by attackers to predict the key in subsequent sessions. Additionally, the key is incapable of decrypting messages from past or future sessions, thus demonstrating the capability of our scheme to offer perfect forward/backward secrecy.

### 5.1.2. Resistance to attacks

Impersonation attack is in this case, the attacker sends a connection request using the ID of another device and impersonates that device. The broker middleware does not support an attacker who does not have the correct session key and cannot construct a valid message. So, attacking the edge of the device is impossible. Brute force attack for this attack to be successful, the attacker would have to guess the correct username and password from the middleware agent. Even if they get these values, they cannot do a private/public key session on the device. MitM attack is an attack in which an attacker secretly sends messages between two devices that believe they communicate directly, potentially modifying the messages. Attackers can eavesdrop on user names and passwords. But the attacker can't do anything without the public and private keys. For ECC encryption, guessing  $K$  from  $K_a = A_{priv} * B_{pub}$  and  $K_b = B_{priv} * A_{pub}$  is impossible.

## 5.2. Performance analysis

As highlighted throughout the article, any scheme designed for the IoT must be suitable for power-constrained devices. The protocol fails if such a design cannot be tested in practice. The analysis primarily focuses on endpoints that are considered resource-constrained entities.

### 5.2.1. Computational costs

The first analyzes each device's computational effort in the proposed authentication protocol. The operation of the evaluated scheme is the elliptic curve point multiplication.

### 5.2.2. Energy consumption

To further assess the computational burden of both protocols, the study evaluates their power consumption costs. Given that the proposed protocol employs ECC, the analysis utilizes a specific configuration of these algorithms. Table 2 outlines the configuration details of this cryptographic algorithm, including the estimated energy consumption for operation in both schemes. According to the findings from the Dang-Scheme, which utilizes curve m-221, the energy consumption for operation amounts to 9480  $\mu J$ . In contrast, the proposed scheme, employing the same cryptography (ECDLP and ECDH) but utilizing the curve depicted in Figure 4 for the elliptic curve, exhibits a significantly reduced operating energy of only 3456  $\mu J$ . The equation below shows the equation of this curve:  $a=-5.4$ ,  $b=16.8$ , curve:  $y^2=x^3+(-5.4)x+16.8$ , PointP=(3.2|5.68), PointK=(-1.6|-4.62), and PointL=P+K=(3.007|-5.267). Figure 5 shows a 46% power consumption difference between the two schemes. It shows that the proposed method is more efficient in D2D authentication applications using ECC.

Table 2. Summary of the power consumption

Notation	Protocol	Energy consumption ( $\mu J$ )
ECC	Proposed protocol	3,456
	Dang-Scheme	9,480

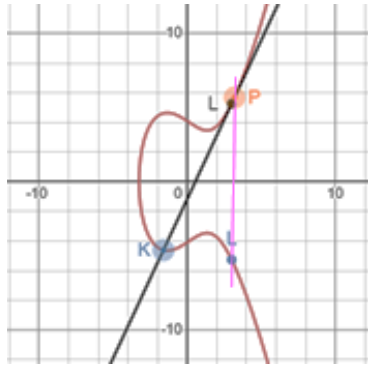


Figure 4. Elliptic curve

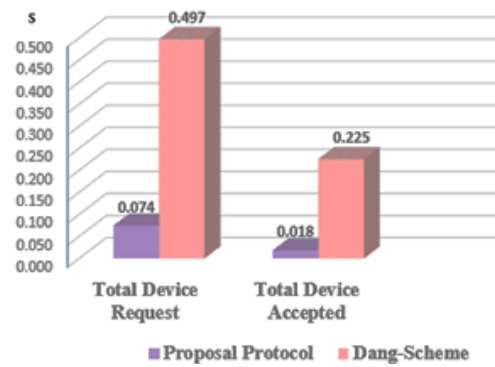


Figure 5. Power consumption difference between the two schemes

### 5.2.3. Processing time

Furthermore, this study conducted experiments to gauge the processing time required by each device when utilizing the proposed protocol. The implementation was coded in Javascript and Python and executed on a 2.90 GHz×16 Intel i7-10700U processor. Table 3 outlines the average processing time for each protocol per device. Figure 6 provides a comparison of circuits, particularly focusing on the D2D stage. The findings indicate that employing the proposed protocol necessitates only 0.074 s for the device to complete all authentication tasks with the server. In contrast, the proposed method achieves a reduction in device authentication time to 0.018 s. Conversely, Dang *et al.* [31] require slightly longer durations for device operations, specifically 0.497 s for the initiating device and 0.225 s for device authentication.

Table 3. Processing time of devices in seconds

Phase	Device	Proposal method (s)	Dang-Scheme (s)
D2D authentication	Total device request	0.074	0.497
	Total device accepted	0.018	0.225

### ELLIPTIC CURVE CRYPTOGRAPHY

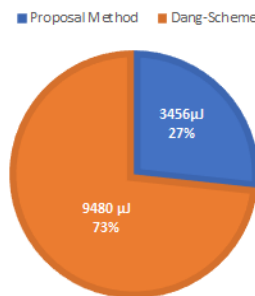


Figure 6. The processing time required by the schemes for the D2D authentication phase

## 6. CONCLUSION

The rapid progress of smart homes, smart cities, and many sectors of the IoT is unquestionably crucial to the future direction of the digital era—the attributes of IoT present novel security concerns that differ from those encountered in previous technological advancements. The objective of this research has been to address these problems by creating a novel authentication technique that enables asymmetric authentication, simplifying the communication between devices and servers in IoT networks. The authentication procedure reaches its highest point when the middleware security agent confirms the legitimacy of the device, allowing communication between two devices. Implementing this strategy greatly reduces the computing burden on servers and decreases their reliance on embedded devices, which is a critical part of our methodology. Our contribution centres around a recently developed authentication system that achieves a balance between simplicity and strength by utilizing ECC and efficient operating procedures. This study has conducted comprehensive security evaluations to comprehensively evaluate the resilience of our strategy against prevalent cyber-attacks in the IoT domain. In addition, our approach exhibits remarkable



energy efficiency, consuming only 4 mJ during device authentication. These results highlight the practical feasibility of our approach, particularly for modern applications in diverse sectors such as smart urban development and environmental sustainability. Ensuring the security and operational effectiveness of IoT is crucial as its proliferation persists. Our authentication system is a notable advancement in this ever-changing and demanding environment, providing a paradigm of creativity and resilience.

## ACKNOWLEDGEMENTS

The authors express gratitude to Ajman University, United Arab Emirates, Universiti Sains Malaysia and the Ministry of Higher Education Malaysia for their support through the research grant, Fundamental Research Grant Scheme (FRGS – Grant No: FRGS/1/2020/TK0/USM/02/1), which facilitated the completion of this study.

## REFERENCES




- [1] A. C. Jose and R. Malekian, "Improving smart home security: integrating logical sensing into smart home," *IEEE Sensors Journal*, vol. 17, no. 13, pp. 4269–4286, 2017, doi: 10.1109/JSEN.2017.2705045.
- [2] S. Saponara and T. Bacchillone, "Network architecture, security issues, and hardware implementation of a home area network for smart grid," *Journal of Computer Networks and Communications*, 2012, doi: 10.1155/2012/534512.
- [3] M. Q. Aldossari and A. Sidorova, "Consumer acceptance of internet of things (IoT): smart home context," *Journal of Computer Information Systems*, vol. 60, no. 6, pp. 507–517, 2020, doi: 10.1080/08874417.2018.1543000.
- [4] M. Husamuddin and M. Qayyum, "Internet of things: a study on security and privacy threats," in *2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017*, 2017, pp. 93–97, doi: 10.1109/Anti-Cybercrime.2017.7905270.
- [5] T. D. P. Bai, K. M. Raj, and S. A. Rabara, "Elliptic curve cryptography based security framework for internet of things (IoT) enabled smart card," in *Proceedings - 2nd World Congress on Computing and Communication Technologies, WCCCT 2017*, 2017, pp. 43–46, doi: 10.1109/WCCCT.2016.20.
- [6] R. Sarmah, M. Bhuyan, and M. H. Bhuyan, "SURE-H: a secure IoT enabled smart home system," in *IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings*, 2019, pp. 59–63, doi: 10.1109/WF-IoT.2019.8767229.
- [7] A. Ali, H. Rafique, T. Arshad, M. A. Alqarni, S. H. Chauhdary, and A. K. Bashir, "A fractal-based authentication technique using sierpinski triangles in smart devices," *Sensors (Switzerland)*, vol. 19, no. 3, 2019, doi: 10.3390/s19030678.
- [8] K. Irfan, A. Anas, S. Malik, and S. Amir, "Text-based graphical password system to obscure shoulder surfing," *2018 15th International Bhurban conference on applied sciences and technology (IBCAST)*, pp. 422–426, 2018.
- [9] W. Meng, W. Li, L. F. Kwok, and K. K. R. Choo, "Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones," *Computers and Security*, vol. 65, pp. 213–229, 2017, doi: 10.1016/j.cose.2016.11.010.
- [10] M. Hossain, S. Noor, and R. Hasan, "SC-IoT: a hardware and software co-verification based authentication scheme for internet of things," in *Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017*, 2017, pp. 109–116, doi: 10.1109/MobileCloud.2017.35.
- [11] P. Poramabage, P. Kumar, C. Schmitt, A. Gurtov, and M. Ylianttila, "Certificate-based pairwise key establishment protocol for wireless sensor networks," in *Proceedings - 16th IEEE International Conference on Computational Science and Engineering, CSE 2013*, 2013, pp. 667–674, doi: 10.1109/CSE.2013.103.
- [12] S. Sciancalepore, G. Piro, G. Boggia, and G. Bianchi, "Public key authentication and key agreement in IoT devices with minimal airtime consumption," *IEEE Embedded Systems Letters*, vol. 9, no. 1, pp. 1–4, 2017, doi: 10.1109/LES.2016.2630729.
- [13] S. Patel, D. R. Patel, and A. P. Navik, "Energy efficient integrated authentication and access control mechanisms for internet of things," in *2016 International Conference on Internet of Things and Applications, IOTA 2016*, 2016, pp. 304–309, doi: 10.1109/IOTA.2016.7562742.
- [14] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain," *Journal of Information Security and Applications*, vol. 45, pp. 156–175, 2019, doi: 10.1016/j.jisa.2019.02.003.
- [15] S. Dey and A. Hossain, "Session-key establishment and authentication in a smart home network using public key cryptography," *IEEE Sensors Letters*, vol. 3, no. 4, pp. 1–4, 2019, doi: 10.1109/LSSENS.2019.2905020.
- [16] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and secure session-key establishment scheme in smart home environments," *IEEE Sensors Journal*, vol. 16, no. 1, pp. 254–264, 2016, doi: 10.1109/JSEN.2015.2475298.
- [17] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2019, doi: 10.1109/IIOT.2018.2846299.
- [18] S. Sciancalepore, A. Caposelle, G. Piro, G. Boggia, and G. Bianchi, "Key management protocol with implicit certificates for IoT systems," in *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*, 2015, pp. 37–42, doi: 10.1145/2753476.2753477.
- [19] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Human centric Computing and Information Sciences*, vol. 7, no. 1, 2017, doi: 10.1186/s13673-017-0087-4.
- [20] M. Wazid, A. K. Das, V. B. K., and A. V. Vasilakos, "LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment," *Journal of Network and Computer Applications*, vol. 150, 2020, doi: 10.1016/j.jnca.2019.102496.
- [21] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016, doi: 10.1016/j.adhoc.2015.05.014.
- [22] S. Challa *et al.*, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017, doi: 10.1109/ACCESS.2017.2676119.
- [23] C. D. M. Pham, T. L. P. Nguyen, and T. K. Dang, "Resource-constrained IoT authentication protocol: an ECC-based hybrid scheme for device-to-server and device-to-device communications," pp. 446–466, 2019, doi: 10.1007/978-3-030-35653-8\_30.
- [24] S. S. Chowdhury, S. Sarkar, S. Syamal, S. Sengupta, and P. Nag, "IoT-based smart security and home automation system," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, Oct. 2019, pp. 1158–1161, doi: 10.1109/UEMCON47517.2019.8992994.






- [25] A. Singh, D. Gupta, and N. Mittal, "Enhancing home security systems using IoT," in *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, Jun. 2019, pp. 133–137, doi: 10.1109/ICECA.2019.8821833.
- [26] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for V2V communication in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6709–6717, 2020, doi: 10.1109/TVT.2020.2986585.
- [27] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3548–3557, 2020, doi: 10.1109/TII.2019.2944880.
- [28] A. Kumar, P. S. Kumar, and R. Agarwal, "A face recognition method in the IoT for security appliances in smart homes, offices, and cities," in *Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019*, 2019, pp. 964–968, doi: 10.1109/ICCMC.2019.8819790.
- [29] K. L. Raju, V. Chandrani, S. K. S. Begum, and M. P. Devi, "Home automation and security system with node MCU using internet of things," in *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, 2019, pp. 1–5, doi: 10.1109/ViTECoN.2019.8899540.
- [30] Z. Vahdati, S. M. D. Yasin, A. Ghasempour, and M. Salehi, "Comparison of ECC and RSA algorithms in IoT devices," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 16, pp. 4293–4308, 2019.
- [31] T. K. Dang, C. D. M. Pham, and T. L. P. Nguyen, "A pragmatic elliptic curve cryptography-based extension for energy-efficient device-to-device communications in smart cities," *Sustainable Cities and Society*, vol. 56, 2020, doi: 10.1016/j.scs.2020.102097.
- [32] K. H. Wang, C. M. Chen, W. Fang, and T. Y. Wu, "A secure authentication scheme for internet of things," *Pervasive and Mobile Computing*, vol. 42, pp. 15–26, 2017, doi: 10.1016/j.pmcj.2017.09.004.

## BIOGRAPHIES OF AUTHORS






**Zainatul Yushaniza Mohamed Yusoff**    received a B.Eng. degree in electrical, and electronic engineering (communication) from Universiti Selangor (Unisel), Malaysia, in 2011, and a M.Sc. degree in wireless communication engineering from the University Putra Malaysia (UPM), Malaysia, in 2018. She is currently pursuing a Ph.D. degree with Universiti Sains Malaysia (USM), Malaysia. She can be contacted at email: zainiza75@student.usm.my.



**Mohamad Khairi Ishak**    received a B.Eng. degree in electrical and electronics engineering from the International Islamic University Malaysia (IIUM), Malaysia, an MSc. in embedded systems, from the University of Essex, the United Kingdom and Ph.D. from the University of Bristol, United Kingdom. He is a member of IEEE and a registered graduate engineer with the Board of Engineers Malaysia (BEM). Currently, he is an Associate Professor Lecturer at the Department of Electrical and Computer Engineering, College of Engineering and Information Technology, Ajman University, Ajman, United Arab Emirates. His research interests are embedded systems, real-time control communications and the internet of things (IoT). Emphasis is given towards the development of theoretical and practical methods which can be practically validated. Recently, significant research has been directed towards important industrial issues of embedded networked control systems and IoT. He can be contacted at email: m.ishak@ajman.ac.ae.



**Lukman AB Rahim**    received a Bachelor of Arts (Second Class Hons.) in English from Srinakharinwirot and received a Ph.D. degree from Lancaster University, with a project verifying model transformations using model checking. He is currently a Core Researcher at the High-Performance Cloud Computing Center and a Senior Lecturer in Computer and Information Sciences at Universiti Teknologi Petronas (UTP). His current research interests are in formal verification, software and system modelling, and software architecture. His current research is focused, in particular, on adopting model-driven engineering and formal verification in cloud computing. Some of the projects he is presently working on are: using architecture-driven modernization and model-driven engineering in deploying engineering simulation software as a cloud service; formal verification of cloud security mechanisms using model checking; and domain-specific modelling languages for educational games. Apart from these projects, he is also involved in research projects related to system engineering and big data, i.e., real-time cloud platforms, the correlation between scheduling and job workload and energy consumption, and secure data transmission for big data applications. He is also working on consultancy projects for corrosion monitoring using acoustic technology and pipeline integrity systems; playing the role of project leader and system engineer. He can be contacted at email: lukmanrahim@utp.edu.my.