Connection Science

ISSN: 0954-0091 (Print) 1360-0494 (Online) Journal homepage: www.tandfonline.com/journals/ccos20

Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system

Mounika Jammula, Venkata Mani Vakamulla & Sai Krishna Kondoju

To cite this article: Mounika Jammula, Venkata Mani Vakamulla & Sai Krishna Kondoju (2022) Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system, Connection Science, 34:1, 2431-2447, DOI: 10.1080/09540091.2022.2124957

To link to this article: https://doi.org/10.1080/09540091.2022.2124957

Published online: 23 Sep 2022.

CONNECTION SCIENCE
2022, VOL. 34, NO. 1, 2431–2447
https://doi.org/10.1080/09540091.2022.2124957

Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system

Mounika Jammula[a], Venkata Mani Vakamulla[b] and Sai Krishna Kondoju[a]

[a]Department of Electronics and Communication Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, India; [b]Department of Electronics and Communication Engineering, National Institute of Technology, Warangal, India

ABSTRACT

Internet of Things (IoT) devices require lower power consumption with higher security, which can be achieved by using lightweight cryptography (LWC) approaches. Attribute-based encryption (ABE) provides a fine-grained access control policy over encrypted data, making it useful in IoT-based cloud storage for allowed data protection. However, the conventional ABE approaches resulted in poor security performance against various attacks in the IoT environment. So, in this paper, the LWC-ABE method is proposed to enhance the security performance against various attacks in the IoT environment. The proposed LWC-ABE contains only multiple trusted authority environments, which is a bottleneck in IoT servers and IoT devices. The proposed LWC-ABE method supports high expressiveness, access policy updates, large attribute domains, and white box traceability properties. The simulation results shows that the proposed LWC-ABE resulted in reduced encryption and decryption times for multi users, different message sizes scenarios as compared to conventional approaches. The numerical outcomes of the proposed method are much better based on performance of encryption and decryption times as 0.000835 and 0.000310 respectively.

ARTICLE HISTORY
Received 30 June 2022
Accepted 11 September 2022

KEYWORDS
Internet of things; lightweight cryptography; attribute-based encryption; ChaCha; playfair encryption; cloud service provider

1. Introduction

Recently, IoT technology and wireless communications are rapidly growing, and users have been using light-weight devices and small computing devices (Fu et al., 2022). The reasons behind this are that these devices are cheaper, smaller, more powerful, and more efficient in handling. Further, resource-constrained devices like RFID tags, contactless smart cards, smart phones, wireless patient monitoring systems, and wireless sensor networks are widely suffering from higher security issues (Rasori et al., 2022). The study of tradable investment products known as assets is known as security research. It focuses on determining the appropriate value of certain commodities (i.e. stocks and bonds). These are often categorised as either derivative contracts, equity, or a combination of the two. Shareholders also include tradable financial futures. One of the most significant changes in information and

CONTACT Mounika Jammula jmounika_ece@cbit.ac.in Department of Electronics and Communication Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India

communication technology (ICT) is the reduction of size at a sustainable cost. As a result, advances in ICT are enabling new services that benefit from the reduction in the size of computing devices (Oberko et al., 2022). The future landscape of ICT in this competition includes not just merging a variety of applications into one universal compact device, but also a large number of restricted devices communicating with one another across a network. The use of ICT to improve educational participation and results. In order to improve educational access and learning results for adolescents with disabilities, information and communication technology (ICT) technologies can be utilised as a catalyst. The success of this process is based not just on technological advancements but also on user and network security (Tu et al., 2021). Since resource constrained devices have limited power (battery) supply and less computing capability, due to these limitations, it is challenging to implement traditional cryptographic primitives (La Manna et al., 2021) on these small devices. Moreover, these small computing devices do not perform better when conventional cryptographic standards (Guo et al., 2021a) are applied to these lightweight devices. Conventional encryption is a type of cryptography where the sender and receiver both use the same key to encrypt and decode messages. It was the only kind of encryption in use until public-key encryption was established. An intruder can assault the network or computer system and render it inoperable. Cryptography cannot guarantee high availability, one of the core components of information security. It motivates researchers to invent cryptographic primitives that can be satisfactorily implemented on these ubiquitous small devices. Thus, LWC (Xiang & Zhao, 2022) is an emerging area of cryptography for the last decade, which is commonly defined for resource-constrained devices. The LWC was initially implemented for small devices, but nowadays, LWC targets a very wide variety of devices. It entails the creation and analysis of cryptographic primitives for resource-constrained devices. It is, in fact, a hybrid of two fields: cryptography and hardware technology. Instead of totally reinventing the new cryptographic method, the majority of the building components were adapted from traditional cryptography with minor changes. A few cryptographic methods (Rana et al., 2022) like block cyphers, stream cyphers, hash functions, and message authentication codes are the four types of LWC (like any other cryptographic primitive). A block cipher is a way of encrypting data in blocks in order to generate ciphertext using a cryptographic key and algorithm. In contrast to stream ciphers, which encrypt data one bit at a time, block ciphers handle fixed-size blocks concurrently. A stream cipher is an encryption technique that encrypts and decrypts a certain quantity of data using a symmetric key. A symmetric cipher key is an encryption tool that is utilised in both encryption and decryption as compared to an asymmetric cipher key. Any function that may be used to transform information of arbitrary size to fixed-size values is referred to as a hash function. Hash values, hash codes, metabolise, or just hashes are the terms used to refer to the results of a hash function. The values are often used to index a hash table, which is a fixed-size table. The message Authentication Code (MAC), often known as a tag, is used to verify the origin and type of a message. The authenticity of data communicated over a network or transferred from one person to another is confirmed by MACs using authentication technology.

A symmetric key cypher is one in which an unvarying size block of plain text is processed via a changeable function with a key as a parameter to produce cypher text. The symmetric key cypher and stream cypher (Jammula et al., 2022) store a string of bits of plaintext with a stream of bits generated by a key when it is passed through a function, resulting in a bit string of cypher text. The hash function is a cryptographic primitive that takes a given

sized block of plaintext and converts it into a unique string of bits using a one-way function. One-way functions are essential components of many tools used in contemporary cryptography. They are utilised in message authentication, digital signatures, and pseudorandom generators. Furthermore, a one-way hash function is built in such a way that identifying a text that hashes to a given value is problematic. The MAC system employs a technique that encrypts messages using session encryption and the delivered regular text communication. The information is next processed by the MAC method, which creates identification labels with a specified distance. The message's MAC is the consequence of the data processing. Message authentication codes (Kumar et al., 2022a) are cryptographic primitives that take a key and a lengthy string of bits from a message as input and output a unique shorter string of bits. It is also known as the keyed hash function.

Three essential characteristics, namely security, cost, and performance, have posed considerable obstacles in constructing lightweight cyphers (Prakasam et al., 2022). The fundamental focus of modern lightweight cypher design is to create imaginative and unorthodox structures that result in a cypher with a compact footprint, adequate speed, low power consumption, and appropriate security. Several primitives (Zitouni et al., 2022) were developed during the conference in response to the absence of acceptable cyphers that are both efficient and secure for very limited contexts. With the growing popularity of creating new lightweight primitives, it is critical to assess and quantify the cryptographic security (Adeel et al., 2022) of these new structures. Even though extensive attempts have been made in recent years to conduct a third-party examination of new designs, the process of examining the security of novel architectures is still ongoing. One of the most important fields of research in the theory of LWC is block cypher designator (Kumar, V., et al, 2022b). A lot of work has been done in this direction and developed the ABE methods. However, the problems presented in the conventional ABE methods are affecting the security standards. Initially, an ABE with outsourced decryption is chosen to reduce the user's calculation cost since the high cost of decryption increases with the complexity of the access policy. Secondly, when a user's attributes are changed, ABE must allow attribute revocation in order to update the user's access privileges in a timely and effective manner. Third, if the data owner changes the access control policy, the policy update requirement must be satisfied while creating the ABE. The proposed LWC-ABE scheme can provide whitebox traceability as well as policy updates to tackle the three challenges listed above and, as a result, can address the anticipated needs of IoTs. RFID tags, detectors, as well as contactless smart cards are examples of compact, low-power, and low-footprint devices that can benefit more from the usage of lightweight cryptography. In order to guarantee safety and confidentiality in IoT applications, it can be employed. Securing the keys is the most essential factor in IoT applications with respect to ciphertext authentication model. However, in the existing systems, the problems are elliptic curve discrete logarithm problem, security hashing functions, security attacks and so on.

The major contributions of this work are:

- A novel flexible and useful LWC-ABE method is developed by adopting the ChaCha and Playfair encryptions for high secured IoT environment.
- The proposed LWC-ABE scheme supports simultaneous policy updating, attribute revocation and outsourcing decryption properties.

- The proposed LWC-ABE contains only multiple trusted authority environment, which is a bottleneck in IoT servers and IoT devices has the flexibility to change their access policy.
- The simulation results shows that the proposed LWC-ABE resulted in reduced encryption and decryption times for multi users, different message sizes scenarios as compared to conventional approaches.

Rest of the paper is organised as follows: section 2 deals with the survey on conventional encryption and cryptographic methods with problem statement. section 3 deals with the detailed analysis of proposed LWC-ABE method. Section 4 deals with the results and discussion with performance analysis. Section 5 deals with the conclusion and future enhancements.

2. Literature survey

This section gives a survey of conventional encryption and cryptographic methods used in the IoT environment. An enhanced secure IoT (ESIT) (Nayak & Swain, 2022) has been developed by using hybrid elliptic curve cryptography (HECC) methods. Asymmetrical public-key cryptography using a shared secret key type is required as the hyper elliptic curve cryptographic technique (HECC). Each client has a set of public and private keys. While a public key is employed to secure data and verify signatures, a secret key is utilised to decipher or generate signatures. Hyper elliptic curves (HECC) are elliptic curves that are especially suitable to cryptography. A generalisation of elliptic curves, are algebraic curves. It differs from the HECC in that it must show that it is aware of the lightweight cryptography realisation application restrictions and change needs accordingly. Size, performance, safety, and energy are examples of such limits. Further, an LWC-based authentication scheme has been developed in (Zhang et al., 2022), which is based on consortium blockchain for cross-domain IoT environment. As a result, it can be used to create security features that are equivalent. The stiffness of the discrete logarithmic problem determines the cryptographic strength of ECC-based LWC. This idea, combined with a security protocol, can be utilised to offer key installation, authentication, encryption, and service signature. It is used in Lightweight and Anonymous Mutual Authentication Protocol (Wang et al., 2022). For periphery IoT networks with physically unclonable functionality, a compact, anonymously reciprocal authentication system is used, including zero secret key storing as well as a massive number of pseudonyms. The preparation of the sample, the enrolment process, as well as the case of security make up the system's three overall processes. A lightweight and anonymous mutual authentication protocol is utilised for edge IoT nodes with physically unclonable functionality, with zero shared secret storage and a high number of pseudonyms. To adapt to the noisy environment, the protocol employs the reverse fuzzy extractor, and the additional subprotocol is included to improve resistance to the desynchronisation threat. Sensors are used to safely gather medical information from the patient's body and transmit it to the healthcare system. Different applications call for varying levels of security, where a resource's scarcity is a key factor. The ideal candidate algorithm for the proposed healthcare system is inferred from the investigation (Alassaf et al., 2017). These solutions can then be applied in the limited environment for applications such as health care, defense, military, and security. In order to maximise security applications, (Alkhudaydi & Gutub, 2020) suggests fusing enhanced Arabic text steganography with lightweight encryption. Using every

frequent diacritic that occurs naturally in Arabic, the study attempts to conceal encrypted secret information within Arabic stego-cover writings.

Researchers further concentrated on different types of ABE (Perazzo et al., 2021) methods that are lightweight and suitable for applications with limited resources. One reason for adoption of ABE is that it minimises weight generation during key generation, while the other could be design and implementation decisions. Cryptographers examine which ECC implementations are most commonly used and deemed lightweight. But the conventional ABE methods are suffering from the various attacks. Therefore, modern cryptography extensively using Ciphertext-Policy ABE (CP-ABE) was proposed (Chinnasamy et al., 2022). It uses a very small set of encryption and decryption keys to provide the same level of security as RSA. The security of CP-ABE suffers from the elliptic curve discrete logarithm problem. Distinct types of pairing, like Weil pairing, Tate pairing, and bilinear pairing models, are also not supported by CP-ABE, which resulted in reduced security standards.

Alassaf and Gutub (2019) analyzes the effectiveness of three reliable candidate encryption algorithms, notably AES, SPECK, and SIMON. With the availability of internet of things (IoT) support, short-term monitoring and emergency notification of healthcare signals are becoming more inexpensive. Data confidentiality is essential, necessitating the use of encryption. The robust encryption method is in conflict with the limits on memory, calculation speed, power consumption, and compact device sizes. Multimedia data sharing via unsecured networks will become more necessary as the Internet of Things (IoT) develops. The limited resources of an IoT platform prevent the use of traditional methods for data encryption (Alassaf et al., 2019). The suggested method was compared against AES and the original SIMON block-encrypting techniques. On an encryption algorithm, the vertices of vital importance to ensure are two-dimensional. Let K be a field with feature p that is faultless (i.e. K p = K), a definite mathematical enclosure of K, and let n be a number that is positive definite to p. In arithmetic, a Tate pairing is anyone of numerous highly associated encoded information predicated on Tate duality connections that include mathematical techniques or abelian morphologies and are often across localised or limited areas. Imaginative techniques for activities like one-round three-party key exchange, identity-based cryptography, as well as aggregated authentication have been created using bilinear pairings. The Tate pairing may be used to create appropriate bilinear pairings for a selection of elliptic curves.

Other than CP-ABE, pairing-based cryptography involves many more applications, e.g. signature techniques, key establishment algorithms with ABE methods, privacy-enhancing schemes using anonymous credentials, etc. Pairing-based Identity-based encryption (IBE), which enables a sender to encrypt a communication without having a receiver's public key to have been authenticated and transmitted earlier, has been established using cryptography. IBE creates a public key using some type of identification for a person (or business). In (Li et al., 2022), authors proposed the control, ciphertext-policy weighted attribute-based encryption (CP-WABE) for IoT environments. The use of a projective homogenous co-ordinate system has been proposed by cryptographers to reduce the inversion cost due to arithmetic operations like point addition and points doubling on elliptic and elliptic type curves. In (Zeng et al., 2021), the authors established a trilinear pairing map of rank 3 on restricted free R-modules (R is a commutative ring) based policy-hiding attribute-based keyword search and data sharing scheme (PH-ABKS-DS) environment. The multiple key establishment approach was used for hashing purposes. Besides, it does not require

a digital signature algorithm for user confirmation. But these methods are suffering from the same policy preserving problems and token generation issues. In (Ge et al., 2022), authors suggested a Diffie-Hellman problem-based key setup mechanism using Revocable Attribute-Based Encryption with Data Integrity (RABE-DI). A revocable attribute-based encryption with data integrity (RABE-DI) system maintains data integrity of 329 the original ciphertext and the cancelled ciphertext if an adversary A has the advantage. A RABE-DI system consists of the original data owner, a cloud server, an authoritative party, and the receivers. In addition, after compiling the key setup scheme, this plan illustrates that the two users can share different keys for communication. But this method suffers from the white box traceability problems. In (Xiong et al., 2021), the authors demonstrate a competent authenticated key formation strategy that recompiles in less time than Harn's protocol using Unbounded and Efficient Revocable based ABE (UER-ABE). Because the accompanying protocol relies on self-linear maps, the available shared keys (in numbers) in the following scheme are greater than those in conventional ABE.

In, Hassan and Gutub (2021) the original image will be scaled up using the already-existing enhanced neighbour mean interpolation (ENMI) and modified neighbour mean interpolation (MNMI) techniques. The critical bits are then masked by effectively utilising the embedding approach. To assess the effectiveness of the suggested system, experiments were conducted on eight common images. One of the important areas of e-security study and application is user authentication. In order to maintain a suitable level of security while accessing computers, this study suggests developing an authentication method that combines a graphical CAPTCHA with an AES encrypted hash password. To minimise the responsibility of having to enter a password several times, (Kheshaifaty & Gutub, 2021) provide a three-layered security system that combines very effective protection methods.

Further, revocable multi-authority-based ABE (RMA-ABE) (Ming et al., 2021) has been developed to overcome the expressiveness problems presented in the conventional RABE-DI and UER-ABE methods. This method introduces two lightweight cryptographic schemes, of which one is independent of hash functions. In addition, revocable CP-ABE (Guo et al., 2021b) has been developed to reduce the computational complexity problems presented in conventional revocable methods. This method effectively reduces repayable chosen-ciphertext attacks. This method later takes the advantage of being more lightweight than the previous one because it uses self-pairing together with ABE. Further, data access control methods (Lu et al., 2021) have been developed for the IoT networks by combining the ABE and blockchain methods. Here, blockchain technology is used to reduce the number of bottleneck attacks. In addition, dual membership-based ABE (DM-ABE) (Lu et al., 2022a) is developed by using secure decision of membership (SDM) protocols. We create the Secure Decision of Membership (SDM) encryption method to safely decide things for double members, that is, PM and NM. The analytical method, which may construct compressed cryptography encapsulation of collections, is the main component of the method. Once pairings have been generated properly, they can form fields of finite order that are sufficiently large to build discrete logarithmic problems computationally but sufficiently small for making efficient computations. The Searchable ABE (Lu et al., 2022b) is widely used in lightweight web apps that interact with data storage and transmission using wireless communication applications, which are vulnerable to hackers. These functions assign pairs of elliptic curve points into the elements of the field with finite order. In (Hu et al., 2022), the authors developed the flexible and complex data access policy-based ABE. However, this

method suffers from a variety of attacks (El Hadj Youssef et al., 2022), which include modification attacks, perfect forward secrecy attacks, and known key security attacks. Faster computations and memory, power, and bandwidth savings result, which are especially relevant in restricted contexts. More importantly, when security requirements grow, LWC-ABE gains a competitive advantage over its competitors.

3. Proposed methodology

An LWC is a technique by which any information or message is exchanged securely between two or more remote parties through a communication network under the surveillance of an eavesdropper. Every cryptographic scheme consists of two processes, namely encryption and decryption. In the encryption process, a text message is encrypted (encoded) into a cipher text message, while during the decryption process, the encoded cipher text message is again decrypted (decoded) into the original text message. Moreover, every cryptographic scheme is either based on a pair of keys (public and private) or a single (shared) key which is/are used to convert the text message into cipher text and vice-versa. The proposed LWC-ABE method supports high expressiveness, access policy updates, large attribute domains, and white box traceability properties. White-box traceability is the process by which the system may identify the malicious user if a user in the system intentionally leaks their decryption key to an unauthorised user using the information included in the key. The features of the proposed LWC-ABE method are illustrated as follows:

- Large attribute domain: the number of authorised institutions influences the size of public parameters, which does not rise in a linear manner with respect to attributes. There is no need to update the system attributes if the system is formed.
- Policy modification: The data owners continuously change the policy access specifications and generate the different ciphertexts to meet the higher security standards. Further, according to policy modification, the data owners also fine tune the data access properties in a flexible manner.
- The system has the potential capability to monitor malevolent users who unlawfully distribute private keys. The white box traceability creates a list of users with their access permissions, which helps to identify unauthorised users with low computational cost.
- Many authorised authorities: The data integrity problems are solved by introducing the multiple authority system, which also solves the issue of the single authority's insufficient credibility. Human inaccuracy, whether intentionally or inadvertent, may undermine data integrity. Transfer errors, such as unintentional alterations or data compromise when moving information between devices. vulnerabilities, malware/viruses, hacking, and other online dangers are the main causes of data integrity.
- It allows for any monotonous access structure and any customisable access control access approach.

Figure 1 depicts the proposed LWC-ABE framework with trusted party, system party, data users, data owners, attribute authorities, and cloud storage providers (CSP) as fundamental operational blocks. A communications service provider (CSP) provides telecommunications services or a combination of information and media services, content, entertainment,

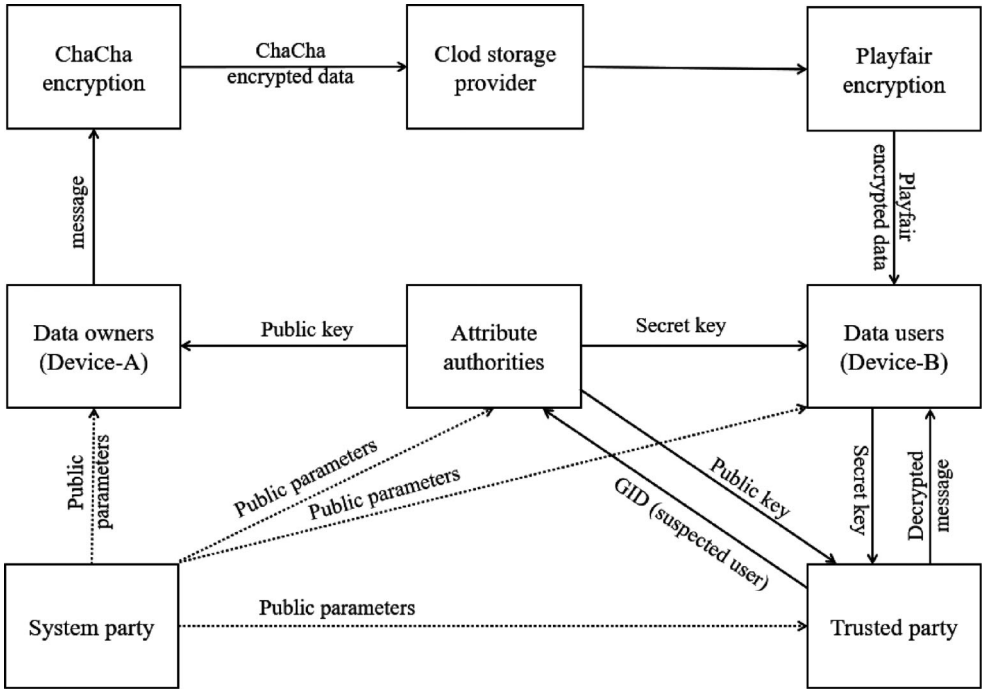

Figure 1. Proposed LWC-ABE system model.

and application services across networks, utilising network infrastructure as a rich, operational platform. Initially, the public parameters are generated by invoking the system setup. Further, some of the public parameters are delivered to trusted parties, data users, data owners, and attribution authorities in the first instance. In addition, constants, counter values, nonces, and seed keys are some of the PPs generated for the ChaCha encryption algorithm. The attribute authorities then utilise the authority establishment procedure to produce public keys and deliver them to trusted parties, data users, and data owners. Furthermore, if the data users have appropriate authorisation, the attribute authorities-based characteristics will be assigned to them based on their request. The data owner produces ciphertext using ChaCha encryption for the encrypted communication and transfers it to the CSP. Further, the data out from CSP is again encrypted by using the Playfair algorithm. Further, the policy update key is generated by the data owner and transferred to the CSP during the access policy change scenario. According to policy access change property, data owners can implement either ChaCha encryption or Playfair encryption, and both encryptions can be implemented parallelly. The ciphertext will then be updated in the cloud storage based on the chosen encryption method. Following that, if the data user's characteristics match the ciphertext access policy, they transfer the secret key to a trusted party, which produces the accurate secret key. Finally, the trusted party performs the decryption procedure and generates the final decrypted message. During this process, finally, if there is a disagreement or suspicion, the trusted party uses the tracing algorithm and transmits the suspicious user's ID (GID) to the attributed authorities.

3.1. Chacha encryption

The ChaCha algorithm is a kind of stream encryption. It is a development of Salsa20 and served as the foundation for BLAKE, a finalist for the SHA-3 competition. ChaCha with 20 rounds and a 256-bit key, often known as ChaCha20, is the variation of the game that is utilised in this text. The ChaCha encryption is widely used in many application areas, such as mobile networks and wireless communications. The ChaCha encryption is used in LWC-ABE in order to create a new keystream generator for manufacturing keys while boosting security standards and reducing difficult phases. The keys generated will be used to encrypt IoT data. These scopes need a lot of resources and have more restrictions on processor power, energy, and bandwidth utilisation. ChaCha typically employs counter mode to meet symmetric encryption standards. One key is used for both encryption and decryption in symmetric encryption. Symmetric encryption is used when a zip file is encrypted and subsequently decrypted employing the same key. Since the key must be maintained a secret from outsiders, stream cipher is sometimes known as secret key cryptography. Cryptographic primitives like ChaCha are stream cyphers, which are arranged into "rounds", with each round enhancing our security confidence at the expense of speed. Here, an XOR operation is performed between the original data and the keystream to generate the encrypted data. Furthermore, the ChaCha process implements the three light-weight procedures such as addition, XOR, and rotation of 32-bit data for gendering the ciphertext. Two input bits are compared via XOR, which produces one output bit. The reasoning is clear. If the bits match, the outcome is 0. When the bits vary, the outcome is 1. Comparable to shifting, bit rotation involves moving the bits that have fallen off at one end back to another. The pieces that come off towards the left end during left revolution are replaced at the short edge. The pieces that come off at the corresponding point during the right revolution are reattached to the left side. Here, the rotation operation is performed based on a constant integer. In addition, the dual function is developed by combining addition, XOR, and rotation-based lightweight procedures by using Quarter Round Function (QRF). The Quarter Round Function (QRF) is the backbone of the dual function, and it was developed to modify the state matrix in each round. The state matrix's diagonals are applied after the QRF has been applied to its columns. The QRF inputs are four 32-bit numbers, and the outputs are modified since 32-bit depending on the three lightweight processes. Moreover, the QRF is used to update the state matrix in each round. Finally, the proposed ChaCha-based LWC performs the 10 rounds of operations.

Table 1 presents the proposed ChaCha keystream generation process for each round. The input matrix (I) contains 512 bits with 16 seeds, and each seed contains 32 bits. The input matrix contains the different keys (k1 … k8) with a size of 256 bits, a block message counter (b1, b2) size of 64 bits, and constants [c1 … c4] with a nonce (n1, n2) size of 192 bits, respectively.

Furthermore, Table 2 presents the QRF algorithm, which is used to generate the keystream. Here, it will generate the keystream by using addition, XOR, and rotation operations. The dangers and negative effects of traditional methods of contraception include ones that are often utilised or that have been around for a long time. This revolutionary flash drive has double the storage capacity of an ordinary storage device. Generate the rotation constants from the first four bits of input I_a, I_b, I_c, and I_d, whereas conventional methods use the 16, 12, 8, and 7 as the rotation integers. Then, apply the input seeds in zigzag form as

Table 1. ChaCha keystream generation algorithm.

Input: Consider 512 bits of input I with 16 seeds $I = [I_o, I_1, \ldots.., I_{15}]$.
Output: keystream with 512 bits.
Step 1: initialise the round for keystream generation
Step 2: Apply the 4 byes of input to QRF algorithm as presented in Table 2.
Step 3: Apply 32-bit input seeds in Zigzag form as shown in Figure 2 (a).
$[K_0, K_1, K_4, K_8] = QRF(I_O, I_1, I_4, I_8)$
$[K_5, K_2, K_3, K_6] = QRF(I_5, I_2, I_3, I_6)$
$[K_9, K_{12}, K_{13}, K_{10}] = QRF(I_9, I_{12}, I_{13}, I_{10})$
$[K_7, K_{11}, K_{14}, K_{15}] = QRF(I_7, I_{11}, I_{14}, I_{15})$
Step 4: Apply 32-bit input seeds in Alternate form as shown in Figure 2 (b)
$[K_0, K_4, K_1, K_5] = QRF(I_0, I_4, I_1, I_5)$
$[K_8, K_{12}, K_9, K_{13}] = QRF(I_8, I_{12}, I_9, I_{13})$
$[K_2, K_6, K_3, K_7] = QRF(I_2, I_6, I_3, I_7)$
$[K_{10}, K_{14}, K_{11}, K_{15}] = QRF(I_{10}, I_{14}, I_{11}, I_{15})$
Step 5: Increment the round.
Step 6: Repeat the steps 2–5 until the 10 rounds are completed.
Step 7: The data presented in the $[K_o, K_1, \ldots.., K_{15}]$ vectors are the final keystream.

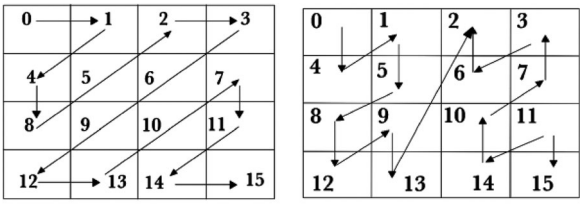

Figure 2. Input forms. (a) Zigzag form. (b) Alternate form.

Table 2. QRF algorithm.

Input: Input seeds I_a, I_b, I_c, I_d
Output: keystream seed K_a, K_b, K_c, K_d
Step 1: The rotation constants ($I_{aR}, I_{bR}, I_{cR}, I_{dR}$)are developed as follows:
$I_{aR} = I_a[3:0], I_{bR} = I_b[3:0], I_{cR} = I_c[3:0], I_{dR} = I_d[3:0]$
Step2: Generate the keystream seeds using dual function.
$K_a = I_a + I_b; K_d = (I_d \oplus I_a) <<< I_{aR});$
$K_c = I_c + I_d; K_b = (I_b \oplus I_c) <<< I_{bR})$
$K_a = I_a + I_b; K_b = (I_d \oplus I_a) <<< I_{cR})$
$K_c = I_c + I_d; K_b = (I_b \oplus I_c) <<< I_{dR})$

shown in Figure 2 (a) to QRF, instead of applying the input seeds in a column wise manner. Further, apply input seeds in an alternate form as shown in Figure 2(b), instead of applying the input seeds in a row-wise manner. This new sequence of updates leads to greater input dispersion, which increases the difficulty of critical attacks. Finally, the XOR operation is performed between the IoT sensor data and the keystream, which generates the ciphertext.

3.2. Playfair encryption

The Playfair cypher is a multi-alphabet letter encryption cypher that treats plaintext letters as separate units and converts them to ciphertext letters. The Playfair cipher was the

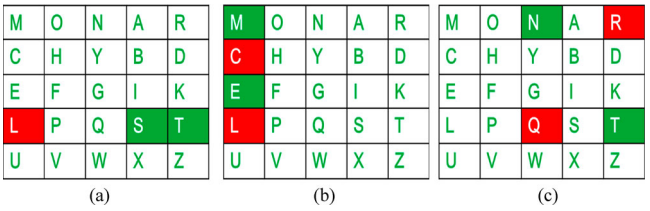

Figure 3. Polybius Square, (a) row based ciphertext generation, (b) column based ciphertext generation, (c) horizontal opposite corner based ciphertext generation.

first effective digraph substitution cipher. A cipher that uses a digraphic substitution from a single alphabet square that starts with the letters of a keyword and continues with the letters of the remaining alphabet, excluding J. In contrast to standard ciphers, we encrypt a pair of alphabets (digraphs) rather than a single alphabet in playfair cipher. The Playfair cypher utilises Polybius Square for performing the encryption operation, which acts as a key. Alphabet characters are placed in a square matrix for the Polybius square cypher. The row x column concept is used to protect the message by replacing every character with a two-digit integer (every of varies from 1 to 5 owing to the alphanumeric characters being put in a 5×5 grid). In the polybius square, the alphabets should not be repeated and the matrix size is 5×5 with 25 elements. Further, the polybius square does not contain the letter J, which causes overlapping of bits in plain text. Therefore, if the letter "J" is present in the keystream, then it is replaced with the letter "I". In addition, the letters in the polybius square should not be repeated. Then, the encryption process is performed as follows:

Step 1: The plaintext is divided into a multiple number of diagraphs, which are generated by combing the two letters in the plaintext. Further, the letter "Z" was also introduced, when the diagraph contains only one odd letter. For example, consider "INSTRUMENTS" as plaintext, which contains 11 letters. So, the bogus letter "Z" is added at the LSB end of the plaintext, which results in the outcome "INSTRUMENTSZ".

Step 2: If the diagraph contains repeated letters or the same letters twice, side by side, then assign the unknown letter "X" in the LSB position of the diagraph. For example, consider "COMMUNICATE" as plaintext, then it is divided into digraphs as CO, OM, MM, MU, UN, NI, IC, CA, AT, TE. Here, the "MM" digraph contains the same letters, so it is converted as "MX".

Step 3: For example, consider "MONARCH" as a polybius square as shown in Figure 3 (a), which acts as a key text. The empty slots in the square are replaced with non-repeated alphabets in alphabetical order. Here, write the letters of the supplied keyword in the first row (from left to right). If there are any duplicate letters in the keyword, avoid them. This indicates that a letter will only be examined once. Fill in the remaining letters in alphabetical sequence after that.

Step 4: If the plaintext digraph is present in the same row of polybius square, then the ciphertext is generated by considering the immediate right-side letters of the digraph. If the letters are not presented on the right side, then consider the initial letter of the same row. Consider the plaintext "INSTRUMENTSZ", which contains the "ST" diagraph in the fourth row of squares, as shown in Figure 3(a). So, for the plaintext letter "S", ciphertext is generated as "T" and for the plaintext letter "T", ciphertext is generated as "L".

Table 3. Performance comparison of encryption and decryption times.

Method	Encryption time (seconds)	Decryption time (seconds)
CP-WABE [20]	0.09651	0.09585
DM-ABE [24]	0.04104	0.03624
DM-ABE [21]	0.06252	0.01845
DM-ABE [27]	0.02686	0.007186
CP-ABE [25]	0.002000	0.0025
Proposed LWC-ABE	0.000835	0.000310

Step 5: If the plaintext digraph is in the same column of the polybius square, the ciphertext is generated by considering the digraph's immediate below letters. If the letters are not presented on the right side, then consider the initial letter of the same column. Consider the plaintext "INSTRUMENTSZ", which contains the "ME" diagraph in the first column of the square, as shown in Figure 3(b). So, for the plaintext letter "M", ciphertext is generated as "C" and for the plaintext letter "E", ciphertext is generated as "L".
Step 6: If the step 5 and step 6 situations do not occur and digraph letters are presented in different columns and rows, then consider the M∗N sub matrix. Furthermore, the digraph letters should be present inside the M∗N matrix. Finally, the ciphertext is generated for that ciphertext by considering the horizontal opposite corner letters of plain text. Consider the plaintext "INSTRUMENTSZ", where the "NT" diagraph is not present in a single row or column of squares, as shown in Figure 3(c). So, the 4∗3 submatrix is created with N and T as elements. Finally, for the plaintext letter "N", ciphertext is generated by considering the horizontal opposite corner letter as "R" and for the plaintext letter "T", ciphertext is generated by considering the horizontal opposite corner letter as "Q".
Step 7: Repeat the process for other digraphs and generate the ciphertext.
Step 8: The decryption technique follows the same procedures as encryption, but in reverse order. The cypher is symmetric for decryption (move up along columns and left along rows). The plain text recipient has the same.

4. Results and discussion

This section gives the detailed analysis, simulation results, and performance comparison of the proposed LWC-ABE with state-of-art approaches. The performance metrics used are attack detection time, security strength by calculating the attack detection accuracy, and encryption time and decryption time with respect to key size and message size.

4.1. Impact on encryption and decryption time

The encryption and decryption times are the times consumed by performing the encryption and decryption operations. Furthermore, the encryption and decryption times are measured for ten users with different message sizes. Table 3 shows that the proposed LWC-ABE consumes less encryption time and decryption time as compared to conventional ABE methods like CP-WABE [20], DM-ABE [24], DM-ABE [21], DM-ABE [27], and CP-ABE [25].

Because the proposed method utilises the hybrid Playfair and ChaCha encryption methods, which generate the key in a high-speed manner. It functions just like conventional encryption. The sole distinction is that it encrypts a combination of initial options, or

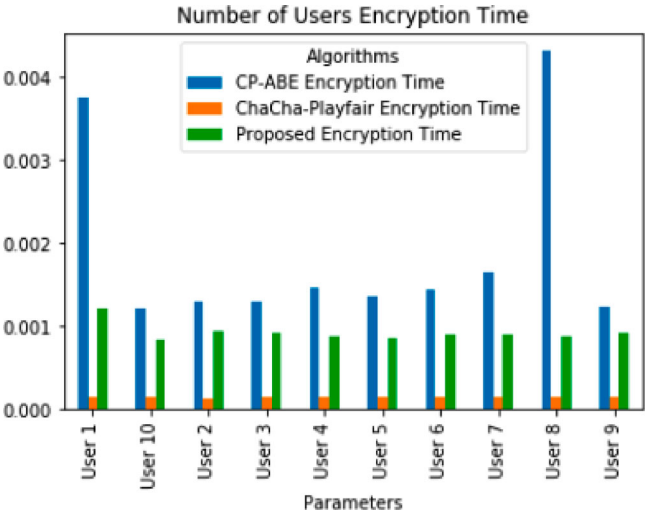

Figure 4. Encryption time analysis for ten users.

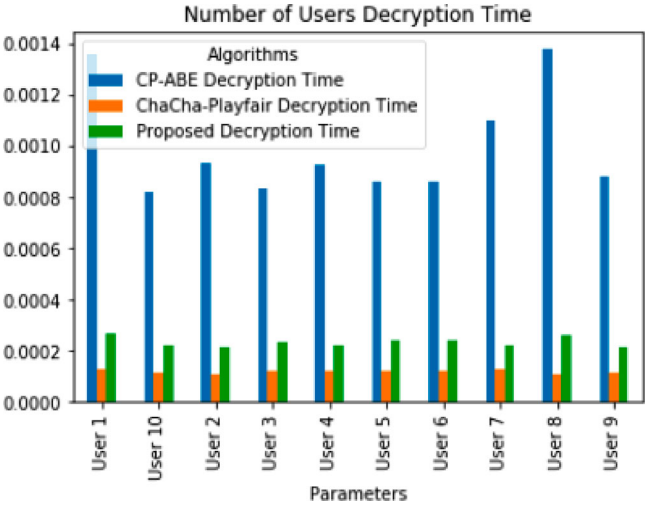

Figure 5. Decryption time analysis for ten users.

a digraph, rather than an individual character. It first generates a 5∗5 vector reference table. Letters in the grid serve as the encrypted message for information. Further, Figure 4 presents the encryption time estimation of 10 random users in an IoT environment. Similarly, Figure 5 presents the decryption time estimation of 10 random users in the same IoT network. The proposed LWC-ABE method resulted in reduced encryption and decryption times in the multiuser with multi-authority scenario. The conventional DM-ABE [27] and CP-ABE [25] methods are facing issues in access policy, which result in abnormal increments of key generation time across each user and cause increased cryptographic times Tables 4 and 5.

Table 4. Performance of encryption time analysis for ten users.

Users	CP-ABE encryption time	ChaCha – playfair encryption time	Proposed encryption time
User 1	0.0033	0.00015	0.0011
User 10	0.0010	0.00016	0.00076
User 2	0.0011	0.00014	0.00085
User 3	0.0011	0.00016	0.00082
User 4	0.0013	0.00016	0.00080
User 5	0.0012	0.00016	0.00078
User 6	0.0013	0.00016	0.00082
User 7	0.0014	0.00016	0.00018
User 8	0.0038	0.00016	0.00080
User 9	0.0011	0.00016	0.00083

Table 5. Performance of decryption time analysis for ten users.

Users	CP-ABE decryption time	ChaCha – playfair decryption time	Proposed decryption time
User 1	0.0013	0.00012	0.00026
User 10	0.00079	0.00011	0.00021
User 2	0.00090	0.00010	0.00020
User 3	0.00081	0.00011	0.00022
User 4	0.00090	0.00011	0.00021
User 5	0.00083	0.00011	0.00023
User 6	0.00083	0.00011	0.00023
User 7	0.00106	0.00012	0.00021
User 8	0.00133	0.00010	0.00025
User 9	0.00085	0.00011	0.00020

Table 6. Performance comparison of encryption and decryption times based on message size.

	Encryption time (seconds)		Decryption time (seconds)	
Message size	100 bytes	200 bytes	100 bytes	200 bytes
CP-WABE [20]	0.09259	0.06851	0.0766	0.09399
DM-ABE [24]	0.07253	0.05963	0.0667	0.07916
DM-ABE [21]	0.06855	0.04818	0.0487	0.06019
DM-ABE [27]	0.05701	0.05049	0.0150	0.04051
CP-ABE [25]	0.0020	0.00125	0.000867	0.000892
Proposed LWC-ABE	0.000123	0.000102	0.000134	0.000142

Table 6 illustrates that the proposed LWC-ABE requires less encryption and decryption time than CP-WABE [20], DM-ABE [24], DM-ABE [21], DM-ABE [27], and CP-ABE [25] for various message sizes. The proposed method generates the public key and private keys in a parallel manner, and key sizes are also automatically changed by attribute authorities based on message size, which results in reduced encryption and decryption times.

5. Conclusion

This article implements the flexible and useful LWC-ABE method for eliminating the unusual attacks generated in the IoT environment. Furthermore, by using the ChaCha and Playfair encryptions, LWC-ABE reduces hardware resources such as power consumption and implements higher security standards in the IoT network. The proposed scheme supports

simultaneous policy updating, attribute revocation, and outsourcing decryption properties. So, the data owners continuously change the policy access specifications and generate different ciphertexts to meet the higher security standards. Further, according to policy modification, the data owners also fine tune the data access properties in a flexible manner. In addition, multiple trusted authority environments are also introduced in the IoT network, which is a bottleneck in IoT servers and IoT devices, and they have the flexibility to change their access policies. The simulation results showed that the proposed LWC-ABE resulted in reduced encryption and decryption times for multiple users and different message sizes as compared to conventional approaches. The proposed LWC-ABE consumes less encryption time (0.000835) and decryption time (0.000310) as compared to conventional ABE. This work can be extended to incorporate hybrid encryption methods for improving security. In future, we will try to reduce less encryption time and decryption time than the proposed LWC-ABE method for most secured IoT environment i.e. without any threats.

Data availability statement

The data used to support the findings of this work is included within this article.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

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

Alassaf, N., Alkazemi, B., & Gutub, A. (2017). Applicable light-weight cryptography to secure medical data in IoT systems. *Journal of Research in Engineering and Applied Sciences (JREAS)*, *2*(2), 50–58. https://doi.org/10.46565/jreas.2017.v02i02.002

Alassaf, N., & Gutub, A. (2019). Simulating light-weight-cryptography implementation for IoT healthcare data security applications. *International Journal of E-Health and Medical Communications (IJEHMC)*, *10*(4), 1–15. https://doi.org/10.4018/IJEHMC.2019100101.

Alassaf, N., Gutub, A., Parah, S. A., & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications*, *78*(23), 32633–32657. https://doi.org/10.1007/s11042-018-6801-z

Alkhudaydi, M. G., & Gutub, A. A. (2020). Integrating light-weight cryptography with diacritics arabic text steganography improved for practical security applications. *Journal of Information Security and Cybercrimes Research*, *3*(1), 13–30. https://doi.org/10.26735/FMIT1649

Chinnasamy, P., Deepalakshmi, P., Dutta, A. K., You, J., & Joshi, G. P. (2022). Ciphertext-Policy attribute-based encryption for cloud storage: Toward data privacy and authentication in AI-enabled IoT system. *Mathematics*, *10*(1), 68. https://doi.org/10.3390/math10010068

El Hadj Youssef, W., Abdelli, A., Dridi, F., Brahim, R., & Machhout, M. (2022). An efficient lightweight cryptographic instructions set extension for IoT device security. *Security and Communication Networks*, *2022*, 1–17. https://doi.org/10.1155/2022/9709601

Fu, X., Ding, Y., Li, H., Ning, J., Wu, T., & Li, F. (2022). A survey of lattice based expressive attribute-based encryption. *Computer Science Review*, *43*, 100438. https://doi.org/10.1016/j.cosrev.2021.100438

Ge, C., Susilo, W., Baek, J., Liu, Z., Xia, J., & Fang, L. (2022). Revocable attribute-based encryption with data integrity in clouds. *IEEE Transactions on Dependable and Secure Computing*, *9*(5), 2864–2872. https://doi.org/10.1109/TDSC.2021.3065999

Guo, L., Yang, X., & Yau, W. C. (2021a). TABE-DAC: Efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain. *IEEE Access*, *9*, 8479–8490. https://doi.org/10.1109/ACCESS.2021.3049549

Guo, R., Yang, G., Shi, H., Zhang, Y., & Zheng, D. (2021b). O 3-R-CP-ABE: An efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT system. *IEEE Internet of Things Journal*, *8*(11), 8949–8963. https://doi.org/10.1109/JIOT.2021.3055541

Hassan, F. S., & Gutub, A. (2021). Efficient image reversible data hiding technique based on interpolation optimization. *Arabian Journal for Science and Engineering*, *46*(9), 8441–8456. https://doi.org/10.1007/s13369-021-05529-3

Hu, S., Wang, X., He, H., & Zhong, T. (2022). Complex and flexible data access policy in attribute-based encryption. *The Journal of Supercomputing*, *78*(1), 1010–1029. https://doi.org/10.1007/s11227-021-03867-5

Jammula, M., Vakamulla, V. M., & Kondoju, S. K. (2022). Performance evaluation of lightweight cryptographic algorithms for heterogeneous IoT environment. *Journal of Interconnection Networks*, *2141031*. https://doi.org/10.1142/S0219265921410310.

Kheshaifaty, N., & Gutub, A. (2021). Engineering graphical captcha and AES crypto hash functions for secure online authentication. *Journal of Engineering Research*. https://doi.org/10.36909/jer.13761

Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022a). Securing the future internet of things with post-quantum cryptography. *Security and Privacy*, *5*(2), e200. https://doi.org/10.1002/spy2.200

Kumar, V., Kumar, R., Khan, A. A., Kumar, V., Chen, Y. C., & Chang, C. C. (2022b). RAFI: Robust authentication framework for IoT-based RFID infrastructure. *Sensors*, *22*(9), 3110. https://doi.org/10.3390/s22093110

La Manna, M., Treccozzi, L., Perazzo, P., Saponara, S., & Dini, G. (2021). Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update. *Sensors*, *21*(2), 515. https://doi.org/10.3390/s21020515

Li, H., et al. (2022). "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things.". *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1949–1960. https://doi.org/10.1109/JBHI.2021.3075995

Lu, H., Yu, R., Zhu, Y., He, X., Liang, K., & Chu, W. C. C. (2022a). Policy-driven data sharing over attribute-based encryption supporting dual membership. *Journal of Systems and Software*, *188*, 111271. https://doi.org/10.1016/j.jss.2022.111271

Lu, X., Fu, S., Jiang, C., & Lio, P. (2021). âĂIJA fine-grained IoT data access control scheme combining attribute-based encryption and blockchain.". *Security and Communication Networks*, *2021, 5308206*. https://doi.org/10.1155/2021/5308206

Lu, Z., Guo, Y., Li, J., Jia, W., Lv, L., & Shen, J. (2022b). Novel searchable attribute-based encryption for the internet of things. *Wireless Communications and Mobile Computing, 2022, 8350006. https://doi.org/10.1155/2022/8350006*.

Ming, Y., He, B., & Wang, C. (2021). Efficient revocable multi-authority attribute-based encryption for cloud storage. *IEEE Access*, *9*, 42593–42603. https://doi.org/10.1109/ACCESS.2021.3066212

Nayak, M. K., & Swain, P. K. (2022). ESIT: An enhanced lightweight algorithm for secure internet of things. In *Iot and analytics for sensor networks* (pp. 107–116). Nayak, P., Pal, S., Peng, SL. (eds), Springer, https://doi.org/10.1007/978-981-16-2919-8_10

Oberko, P. S. K., Obeng, V.-H. K. S., & Xiong, H. (2022). A survey on multi-authority and decentralized attribute-based encryption. *Journal of Ambient Intelligence and Humanized Computing*, *13*(1), 515–533. https://doi.org/10.1007/s12652-021-02915-5

Perazzo, P., Righetti, F., La Manna, M., & Vallati, C. (2021). Performance evaluation of attribute-based encryption on constrained IoT devices. *Computer Communications*, *170*, 151–163. https://doi.org/10.1016/j.comcom.2021.02.012

Prakasam, P., Madheswaran, M., Sujith, K. P., & Sayeed, M. S. (2022). Low latency, area and optimal power hybrid lightweight cryptography authentication scheme for internet of things applications. *Wireless Personal Communications*, 126, 351–365. https://doi.org/10.1007/s11277-022-09748-1

Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77–89. https://doi.org/10.1016/j.future.2021.11.011

Rasori, M., La Manna, M., Perazzo, P., & Dini, G. (2022). A survey on attribute-based encryption schemes suitable for the internet of things. *IEEE Internet of Things Journal*, *9*(11), 8269–8290. https://doi.org/10.1109/JIOT.2022.315403

Tu, S., Waqas, M., Huang, F., Abbas, G., & Abbas, Z. H. (2021). A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing. *Computer Networks*, *195*, 108196. https://doi.org/10.1016/j.comnet.2021.108196

Wang, H., Meng, J., Du, X., Cao, T., & Xie, Y. (2022). Lightweight and anonymous mutual authentication protocol for edge IoT nodes with physical unclonable function. *Security and Communication Networks. Jan*, *4*, 2022. https://doi.org/10.1155/2022/1203691.

Xiang, X., & Zhao, X. (2022). Blockchain-assisted searchable attribute-based encryption for e-health systems. *Journal of Systems Architecture*, *124*, 102417. https://doi.org/10.1016/j.sysarc.2022.102417

Xiong, H., et al. (2021). Unbounded and efficient revocable attribute-based encryption with adaptive security for cloud-assisted internet of things. *IEEE Internet of Things Journal*, *9*(4), 3097–3111. https://doi.org/10.1109/JIOT.2021.3094323

Zeng, P., Zhang, Z., Lu, R., & Choo, K. K. R. (2021). Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things. *IEEE Internet of Things Journal*, *8*(13), 10963–10972. https://doi.org/10.1109/JIOT.2021.3051362

Zhang, Y., Luo, Y., Chen, X., Tong, F., Xu, Y., Tao, J., & Cheng, G. (2022). A lightweight authentication scheme based on consortium blockchain for cross-domain IoT. *Security and Communication Networks*, *2022*(6), 1–15. https://doi.org/10.1155/2022/9686049

Zitouni, N., Sedrati, M., & Behaz, A. (2022). Comparing lightweight algorithms to secure constrained objects in internet of things. In *Interactive mobile communication, technologies and learning* (pp. 1040–1051). In: Auer, M. E., Tsiatsos, T. (eds.) New Realities, Mobile Systems and Applications. Springer.