International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

LIGHT ACTKR: LIGHTWEIGHT ADVANCED ENCRYPTION CURVE CRYPTOGRAPHY AND ADAPTIVE TRUNCATED KARATSUBA RING-BASED SECURITY FRAMEWORK FOR POWER-CONSTRAINED SMART DEVICES

[1]Neha Purohit, [2]Shubhalaxmi Joshi

[1]School of Computer Science, Dr. Vishwanath Karad, MIT World Peace University, Pune, India.

[2]Associate Dean, Faculty of Science, Dr. Vishwanath Karad, MIT World Peace University, Pune, India.

purohitneha04@gmail.com, shubhalaxmi.joshi@mitwpu.edu.in

Abstract

In the current era, the world is increasingly connected to the internet, influencing high-level security as well as minimal complexity among power-constrained devices. Owing to the constrained nature of smart devices, existing security frameworks have faced certain challenges, including instability, lack of robustness, and inefficiency due to their complex structures. Consequently, the research proposes lightweight advanced encryption curve cryptography and an adaptive truncated Karatsuba ring-based (Light ACTKR) security framework to alleviate the aforementioned limitations among power-constrained smart devices. The proposed secure framework is composed of lightweight advanced encryption curve cryptography (LightAEnC)-based signature algorithm and Lightweight adaptive N-th degree truncated Karatsuba ring (Light ANTKR)-based data encryption algorithms to improve security within the power-constrained smart devices. Moreover, the research adopts a lightweight concept in both algorithms to reduce computational complexity within the power-constrained smart devices and ensure minimal storage capacity. In addition to that, the research introduced advanced secure parameters within the LightAEnC signature algorithm, which possibly enhance security and make it resilient to security threats. According to the merits of the Light ACTKR secure framework, gains 2s of encryption time, 2.060s of decryption time, and 352KB of memory usage at a number of 200 devices in comparison with the current results of the existing literature.

Keywords- Power-constrained smart devices, security framework, Karatsuba algorithm, cloud computing, Interplanetary File System.

1. Introduction

The technological advancements with the integration of wearable devices, namely the Internet of Things (IoT), have transformed into the most promising area for changing the mode of communication [1]. The implementation of IoT in various applications has led to the exploitation of power-constrained devices [2][3]. The devices are limited in computational capabilities and energy resources, which reduces the quality of services [4]. The energy

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

constraints affect the confidentiality of the data, which opens the need for improved security networks for maintaining data integrity. The smart devices, namely the IoT devices as well as the sensors, have critical limitations including storage, battery expectancy, and processing power [5]. The development of effective and lightweight mechanisms is crucial for higher security since the conventional cryptographic algorithms exhibit a potential overhead on these devices [6]. In addition, the existing issues with the lack of security measures in the design of embedded systems also require consideration [7]. The maintenance cost is higher as well, and the operational lifespans are reduced in the devices with power restrictions [8][9].

The encryption was performed using a public key, which made it easier to share securely among the users. With the increasing number of security threats, the utilization of symmetric encryption became highly challenging in maintaining security [10]. The majority of communications were performed through public key cryptography due to the secure transactions as well, and there were no requirements for prior communication between the users before the encryption [8][11]. However, existing methods have limited capabilities in communication between the nodes, which presents a challenge to maintaining data integrity [7][12]. In symmetric cryptography, information leakage at each time was probably caused by the utilization of a key, which cannot be reconstructed by the attackers [13]. In addition, for large-scale organizations, the distribution of keys to all users was highly complex, and the loss or compromise of keys led to the risk of all encrypted data [13]. Asymmetric cryptography offered more security than symmetric cryptography because of the utilization of different keys for encryption and decryption [15][35]. The method eliminates the requirement for secure key exchange, which was considered the major challenge in symmetric key-sharing methods [16] [17].

The development of Elliptical cryptography (ECC) has a higher capability in providing data security with smaller key sizes, making it ideal for implementing efficient security measures [14]. The ECC-based security systems improve the overall safety of IoT systems with the potential to provide robust protection against cryptographic attacks [13]. The approach maintains the balance between the computational efficacy and cryptographic strength of the sensitive networks [16]. The symmetric methods necessitate more storage when the edge devices are integrated with the IoT network protocols, whereas ECC requires less storage [18][8]. The ECC protocol offered more effectiveness than the conventional approaches, yet had limitations that needed to be addressed to improve security [19] [20]. In addition to that, the computation time is longer for decryption and encryption, as well as has potential vulnerabilities such as side-channel attacks that result in the leakage of information [21]. In line with this, the selection of elliptical curve parameters was significant, where the poor selection weakened the strength of encryption [22]. Moreover, the implementation of ECC was time-consuming and complex to understand [23]. In addition, the size of the encrypted key is larger, and the processing of binary curves is highly expensive [24].

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Motivated by the existing researchers' summary of the unsuitability of using conventional cryptographic methods for power-constrained smart devices, the research proposes a LightACTKR secure framework to solve the aforementioned challenges of this experiment and ensure foremost security. Here, the proposed framework is designed based on the lightweight structure, thus eliminating complications and memory constrain are evacuated. Additionally, integrating the lightAEnC-based signature algorithm and lightANTKR-based device data encryption mechanisms offers a high degree of security. The context below reflects the contribution of the proposed framework.

Lightweight advanced encryption curve cryptography-based signature algorithm for authentication: The LightAEnC signature algorithm encrypts registered device credentials and introduces advanced secure parameters to define security while communicating. Additionally, constructing the LightAEnC algorithm excludes irrational operations to facilitate a lightweight structure that minimizes computational complexities within the power-constrained smart devices.

Lightweight adaptive N-th degree truncated Karatsuba ring for device data encryption: In the LightANTKR algorithm, device data are encrypted by utilizing the Karatsuba algorithm rather than regular polynomial multiplications, which indeed reduces overheads while computation and also makes it efficient for power-constrained smart devices.

The subsequent sections of this research are organized as follows: Section 2 provides a literature review, a system model is presented in Section 3, the proposed methodology is described in Section 4, and results and conclusions are explained in Sections 5 and 6. The list of notations are depicted in the Table 1.

Table 1. List of Nomenclature

Symbol	Description	Symbol	Description
D_X	Device data	s_1	Integer
D_I	Device index	v, k	Signature
D_{df}	Distance factor	$h(A_i')$	Hash of secure parameter
D_{nm}	Device name	R	Integer ring
h_{id}	Host ID	R_e	Residual class ring
Rq_c	Request message	T_e	Truncated polynomial ring
I_i	Name	p_i, q_i	Polynomial coefficient
nm_i	Index	e	Large prime number
$D_{dt(i)}$	i^{th} device data	Nm	Bit polynomial
A_i'	Secure parameter	p_0, p_1, q_0, q_1	Primary polynomial

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A_i	Device parameter	a	Public key
Z	Elliptic curve	p, p_f	Private keys
B_x	Finite field	Q	Encrypted device data
x, y	Parameters of the curve	d	Randomly selected integer
r, s	Coordinates of the curve	f	Coprime factor
m	Private key	G	Data transfer intimation
x	Prime number	v	Authenticity of S_i
W	Public key	K_{rq}	Key request
S_i	Controller	w	Decryption
u	Pseudo random integer	ver_{int}	Verification intimation message

2. Literature Review

In this section, the existing security framework for resource-constrained smart devices is described with its pros and cons that deliberately help understand the problems faced in traditional approaches and regulate this research for effective security outcomes. S. Baccouri et al. [1] presented a mutual lightweight authentication-based Elliptic curve ElGamal (ECEG) scheme for secure resource-constrained smart devices. Authentication of endpoints and the encoding parameters were performed at the same time, nevertheless, had gained lower efficiency during authentication. S. Loredana Nita and M. Iulian Mihailescu [7] developed an ECC-based query authentication protocol, which offered a high-security level by providing user anonymity against selective identity threats for secure resource-constrained smart devices, however, the computational cost and time were quite high. Z.Ul Islam Adil et al. [15] introduced a lightweight sensor node authentication (Light AUTH) scheme, centered on multiple standard encryption techniques and mathematical algorithms, integrated to minimize block sequence issues. In contrast, Light AUTH offered lower throughput and ledger scalability. A. Maarouf et al. [11] utilized elliptic curve cryptography (ECC), an offline direct authentication scheme for resource-constrained internet of medical things (IoMT) provided a stronger security realm and robustness with minimal cost, but failed to produce higher scalability within large-scale networks.

Popoola et al. [25] created a secure smart home healthcare system based on an optimized hybrid encryption framework that relied solely on both ECC-256r1 with AES-128 algorithms, which affirmed resistance to common cyber threats. Nonetheless, the established system is still anticipated to address efficiency challenges and quantum threats. X.. Jin et al. [26] employed a physical unclonable function (PUF) and Chebyshev chaotic map (CCM)-based authentication scheme for secure resource-constrained smart devices. Both mechanisms played a crucial role in maintaining two-way authentication and protection against insecure channels, however solely relied on computational power. V.Tanksale [27] presented a substantial key exchange

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

protocol using the Elliptic curve Diffie–Hellman (ECDH), tailored for resource-constrained smart devices that evaded power, energy, and memory constraints and offered a balance between security as well as resource efficiency. Despite that, it cannot be guaranteed for side channel and quantum attacks. I. Keshta, et al. [28] incorporated Cyclic Redundancy Check (CRC) and ECC techniques for both information authentication and message authentication over resource-constrained smart devices, which offered security and robustness, yet didn't succeed in real-time application and further effectiveness.

2.1 Challenges

Substantial challenges of the existing literature are listed below.

- The ECEG method exhibited lower efficiency, and the computationally intensive nature leads to potential overheads during the authentication process. Moreover, the larger key size led to slower processing of larger ciphertext values [1].
- The lightweight authentication (Light AUTH) was not effective in managing the security of smart healthcare data. Furthermore, the scalability of the ledger and overall throughput were lower [15].
- The resistance of the Offline Direct Authentication Scheme to advanced node attacks was not evaluated, and the feasibility was reduced in large-scale environments [11].
- The ECDH algorithm did not provide a guarantee for side channel attacks and quantum attacks due to insufficient security paradigms [27].

The previous research works faced difficulties with potential overheads in the authentication process, limited scalability, low throughput took place in lightweight authentication, less feasibility with offline authentication schemes, and insufficient security paradigms during the authentication process. Moreover, the above-mentioned limitations are overcome in the proposed Light ACTKR technique by incorporating a Lightweight adaptive N-th degree truncated Karatsuba ring for device data encryption and a Lightweight advanced encryption cryptography-based signature algorithm for authentication for Power-Constrained Smart Devices.

2.2 Problem statement

The power-constrained smart devices are designed to perform tasks with minimal consumption of energy, especially for wireless environments where access to a constant power source is not feasible. However, the algorithms designed for improving the data security exhibited higher computational overhead, longer key size, as well as higher complexities, which significantly limit over power-constrained smart devices [12] [29]. Additionally, to simplify the authentication process on smart devices, limited resources, including power, memory, and energy, were paramount but not considered in existing techniques [10] [15]. The main motivation of this research is to address the aforementioned limitations by proposing a LightACTKR secure framework in power-constrained smart devices using lightweight encryption and signature verification schemes to store and access secure data from the smart device within the network. Let the number of smart devices (S) in the network be denoted as,

Received: July 20, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$S = \{S_1, S_2, .., S_i, .., S_N\}$$

(1)

where, S_i denotes i^{th} smart device and S_N belongs to the total number of devices in the network. Each device has a specific power consumption factor, where the overall power consumption with respect to time $\rho(t)$ is evaluated by the given formula.

$$\rho(t) = -\sum_{i=1}^{N} K_{S_i} U_{S_i}(t)$$

(2)

here, K_i is the constant for the relative impact of a i^{th} smart device, U_S represents the total usage of smart devices, and t denotes the time interval, respectively. Incorporation of the lightweight scenario of the proposed security framework potentially reduces the requirement of high computational power as well as time and shows effectiveness towards power-constrained smart devices.

3. System model

Smart devices are the entity that makes data transfer from the current device to the Interplanetary File System (IPFS) storage system in the cloud. Here, the internet-connected devices including, smart monitors, smart radar, smart cars, smart refrigerators, smart meters, and wearable devices such as smartwatches, lenses, and so on are direction connected to the controller responsible for transferring device data to secure manner, also includes verification process to identify the authenticity of the smart devices. Moreover, the controller connects to the IPFS of the cloud storage system, which mainly focuses on securely storing the device data and transferring it when a smart device is needed. As seen in Figure 1, the signature algorithm and encryption scheme were crucial in a cloud storage system that enhances the security of sensitive data and offers certain merits, including data integrity, compliance, and confidentiality. In the era of ubiquitous connectivity, secure communication remains challenging, especially for power-constrained smart devices, therefore, investigating powerful mechanisms to ensure robust security is indeed necessary.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

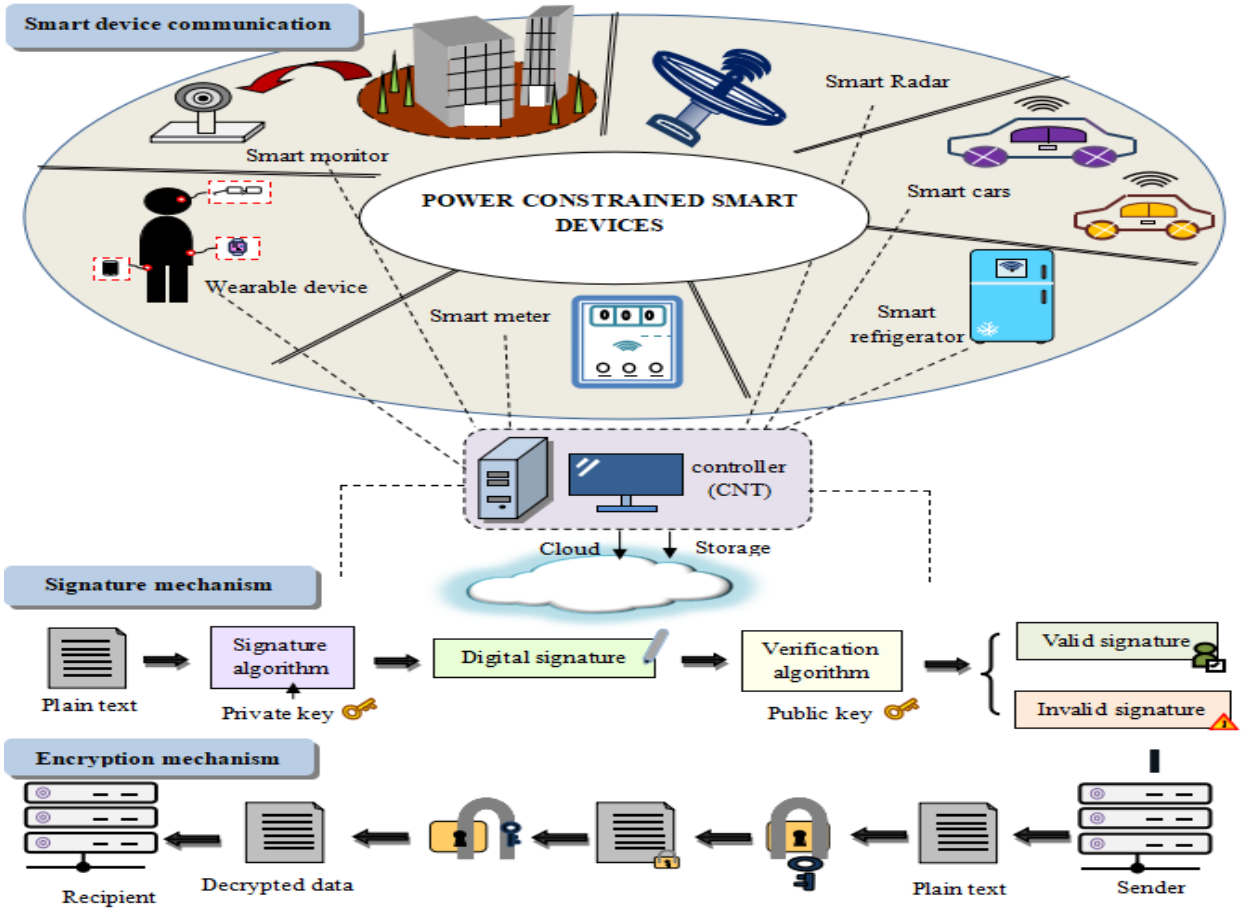


Figure 1. System model for Secure framework over power-constrained smart device

4. Lightweight advanced encryption curve cryptography and adaptive truncated polynomial ring-based security framework for power-constrained smart devices

The research aims to address the limitations of developing a cryptography-based security framework by proposing the LightACTKR framework. In the proposed system, the process involves storage and access, where initially the power-constrained smart device undergoes registration for creating an identity in a single server. Then the device identity and the data are secured using the LightAEnC-based signature algorithm. The process enables the creation of keys and the generation of signatures, thereby verifying them for authentication. In line with this, the device data is further encrypted using the LightANTKR encryption algorithm that enables adaptive keys to prevent data breaches. After the encryption, the encrypted data is securely stored in the IPFS storage system in the cloud for further access. During the data access, the user sends a data request to retrieve the encrypted data from the IPFS storage. Then, the data decryption is performed where the user identity is verified using the proposed signature-based verification to ensure the authenticity of the users. Moreover, the requested data can be transmitted by verifying the user identity, which significantly prevents attackers from accessing the sensitive information. At the same time, implementing a lightweight

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

paradigm opens up power-constrained smart devices. The block diagram of the LightACTKR secure framework is presented in Figure 2.

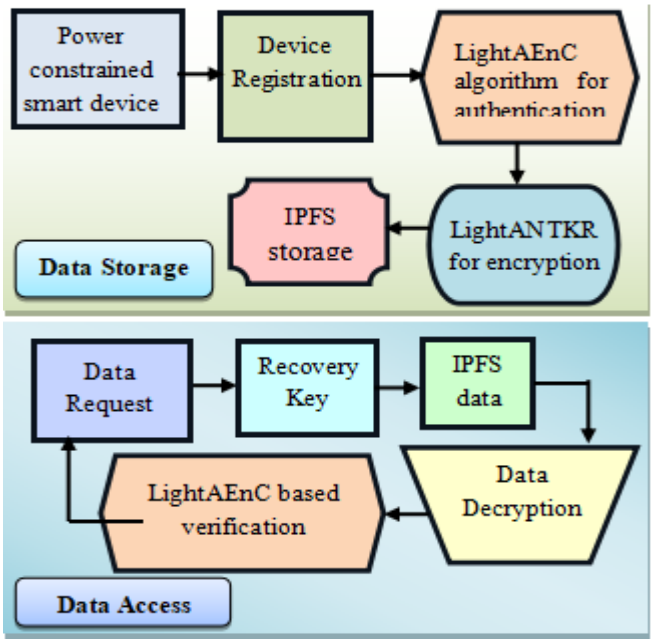


Figure 2: Block diagram of the proposed Light ACTKR secure framework

4.1 Initialization of devices

Initially, the smart devices are considered with the base parameters, which include device data $D_X = \{X_1, X_2, .., X_i, .., X_n\}$, device index $D_I = \{I_1, I_2, .., I_i, .., I_n\}$, distance factor $D_{df} = \{df_1, df_2, .., df_i, .., df_n\}$ and device name $D_{nm} = \{nm_1, nm_2, .., nm_i, .., nm_n\}$.

All initialized parameters are linked within the controller (CNT), which originally stores device parameters when a smart device interconnects with the controller. During the communication, requests Rq_c from smart devices are forwarded to the controller, and the host ID (h_{id}) for the corresponding smart devices is sent as acknowledgment, once it is verified. Here, the request message contains the device name and index $Rq_c = \{I_i, nm_i\}$ After acknowledgment is sent, the controller receives i^{th} device data $D_{dt(i)}$ of S_i and stores it in the cloud server with its shared parameters and IP address, respectively.

The stored parameters are represented as,

$$D'_{nm} = \{nm'_1, nm'_2, .., nm'_i, .., nm'_n\}$$

(3)

$$D'_I = \{I'_1, I'_2, .., I'_i, .., I'_n\}$$

(4)

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$D'_{Ip} = \{Ip'_1, Ip'_2, .., Ip'_i, .., Ip'_n\} \quad (5)$$

Moreover, each smart device holds a trust score of 1, which increases or decreases depending on the transaction. The illustration of the initialization phase is shown in Figure 3.

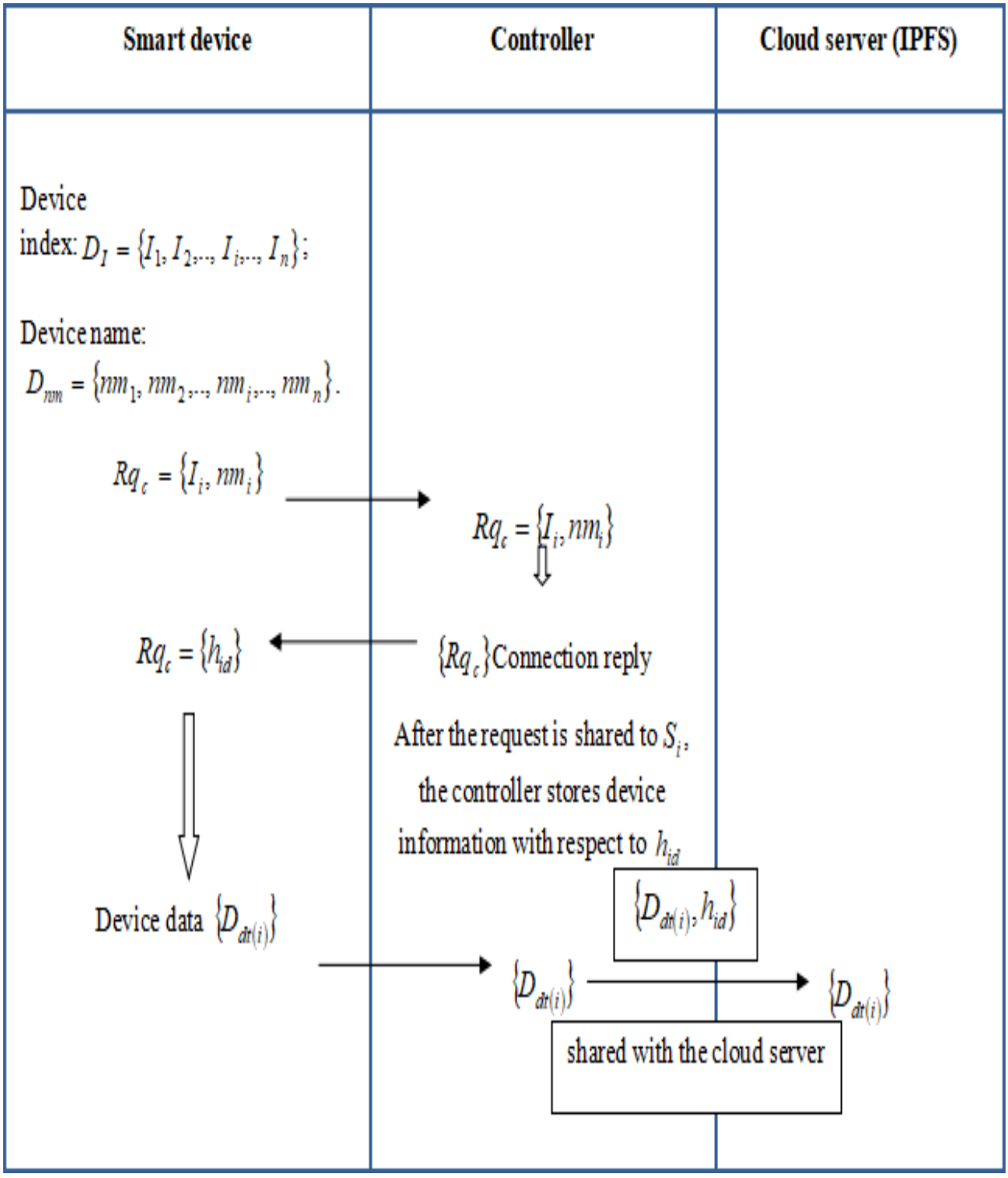


Figure 3: Illustration of the initialization phase

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.2 Device Registration

Device registration is one of the crucial tasks to ensure that only authorized devices can access the system while preventing unauthorized access, also encrypting data for secure storage. Therefore, the research develops a LightACTKR secure framework for power-constrained smart devices, which combines a LightAEnC-based signature algorithm and LightANTKR for both authentication and data encryption, respectively. The LightAEnC algorithm prerequisite to generate appropriate keys and digital signatures that authenticate corresponding smart devices and bolster compliance with industry regulations. Moreover, the data encryption-based LightANTKR algorithm facilitates confidentiality towards sensitive information, and the lightweight concept certainly reduces computational constraints. The context below reflects the contribution of the proposed framework.

4.2.1 Lightweight advanced encryption curve cryptography-based signature algorithm for authentication

For the past decades, traditional algorithms, including AES [30] and ECC [31], have shown valuable results, but in the case of computation, it offered several constraints. Considering the AES algorithm, only operating on bytes rather than bits of input data at a time offered more time as well as power while computing. Owing to the complex structure of the ECC algorithm possesses potential vulnerabilities, especially in power-constrained smart devices. Therefore, the research utilizes a LightAEnC-based signature algorithm for authentication, which initially creates an advanced secure parameter regarding the smart device parameters, including the combination of device name and ID, that is accomplished with limited power constraints and securely saved by the controller for further generation of key and digital signatures. The concept of developing an advanced secure parameter enables high-level security and feasible authentication for power-constrained devices.

The LightAEnC algorithm insists on security by encrypting registered smart device parameters and facilitating trust while communicating. Initially, the encryption of registered smart device parameters takes place with 10 rounds that comprise three transformation processes, such as substitute byte, shift rows, and add round key, which is shown in Figure 3. Each phase undergoes a further operation to encrypt a 128-bit block and offers a secure parameter. Here, the substitute byte depends on a nonlinear S-box that substitutes a byte in the state with another byte, the shift rows perform cyclical shifting of bytes to the left in each row, and remain the same in size. Now, taking the output byte from the previous transformer block that shifts rows to the Add round key, primarily distributing the input bytes to matrices, which offers more security during encryption. Excluding the mix column operation from the traditional AES algorithm offers minimal time consumption and facilitates lightweight operation over power-constrained devices. Finally, generating the secure parameter as,

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$A_i' = AESencrypt(A_i) \tag{6}$$

$$A_i = (nm \| h_{id}) \tag{7}$$

Where A_i' denotes the advanced secure parameter, and A_i be the device parameter, a combination of device name as well as host ID respectively. For instance, let us consider $h_{id} = Dev\_frid\_1$ and $Ip = 184.19.243.3$ then $A_i = Dev\_frid\_1184.19.243.3$. Here, the 16-byte key is used to encrypt each device and is stored along with each value of within the encrypted form over the controller, since the symmetric key is used for encryption and decryption. The cryptographic implications help in cyber security for data protection, Financial Transactions, confrontation against various attacks and quantum threats. The cryptographic techniques safeguarding data integrity, preventing modification, and only authorized individuals can access sensitive information. Further, the key entropy is utilized for measuring confidentiality of the key information. The security of the cryptographic key is protected by bit-security. With high bit security and high entropy, the cryptography is protected against attacks. Figure 4 depicts the architecture of the LightAEnC algorithm.

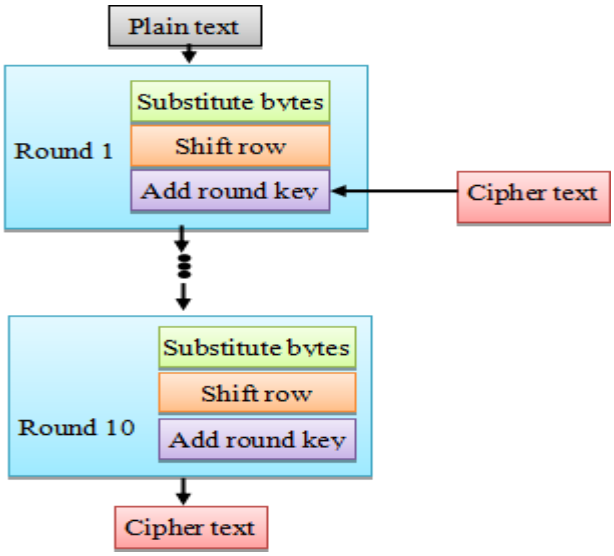


Figure 4: Architecture of the LightAEnC algorithm

On the contrary, the lightweight scenario can limit the security and privacy of authorized devices. To leverage security constraints, the research integrates lightweight key generation as well as digital signatures, where the controller identifies whether unauthorized devices are making access within the network or not. Once the secure factor is generated, it is sent to the corresponding smart devices, additionally, it is also used for generating digital signatures within the controller phase. To do so, the research takes an elliptic curve Z over a finite field B_x and the curve equation is defined as

Received: July 20, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$r^2 = s^3 + xs + y$$
(8)

where, x, y are the parameters of the curve, here x is a prime number, and r, s are the coordinates of the curve. In Encryption process domains are defined as the specific data that is protected by encryption, and the number of bits used to create an encryption key is called bit-lengths or key size. The limiting condition of the encryption is called the encryption bounds. Further, in encryption, ring dimension refers to the degree of the polynomials used in the ring, and its impact on the security and performance of the encryption scheme. Larger ring dimensions generally offer increased security. During the key generation, a random integer (m) within the time interval $[1, t-1]$ is initially selected. Integrating m with a prime number x thereby generating a public key, which is computed as,

$$W = mx$$
(9)

Now, W specifies the public key of S_i and m refers to the private key of S_i respectively. So far, random acquisition of private key enables stronger security, especially when the device gains access to the cloud server. On the other hand, generating a digital signature for A_i' of S_i includes the selection of a pseudorandom integer u, that belongs to $[1 \le u \le t-1]$ interval of time and evaluating u as,

$$ux = s_1, r_1 \text{ and } v = s_1 \bmod t \,.$$
(10)

here, s_1 represents an integer between 0 and $y-1$. While computing them, if the value of $v = 0$, then pull back to the initial step, otherwise compute k by inversing a pseudorandom integer multiplying with the hash of an advanced secure parameter $h(A_i')$ obtained by the Secure Hash Algorithm-1 (SHA-1) algorithm and v respectively, which is given in equation (11),

$$k = u^{-1}\{h(A_i') \cdot v\} \bmod t$$
(11)

Once the signature (v, k) is created for A_i', securely stored within the controller for further verification purposes. In line with this, using the LightAEnC-based signature algorithm reduces computational complexity, influencing minimal power and time constraints, at the same time increasing secure authentication of the digital signatures and keys respectively. In addition to that, the signature for the ecure parameter generated is transferred to the smart device, significantly reducing the usage of raw device attacks, which are susceptible to data theft or misuse. Furthermore, careful tuning is required to consider the parameters and

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

implementation done through selecting the optimal configuration. Figure 5 depicts the illustration of the LightAEnC-based signature algorithm for secure authentication.

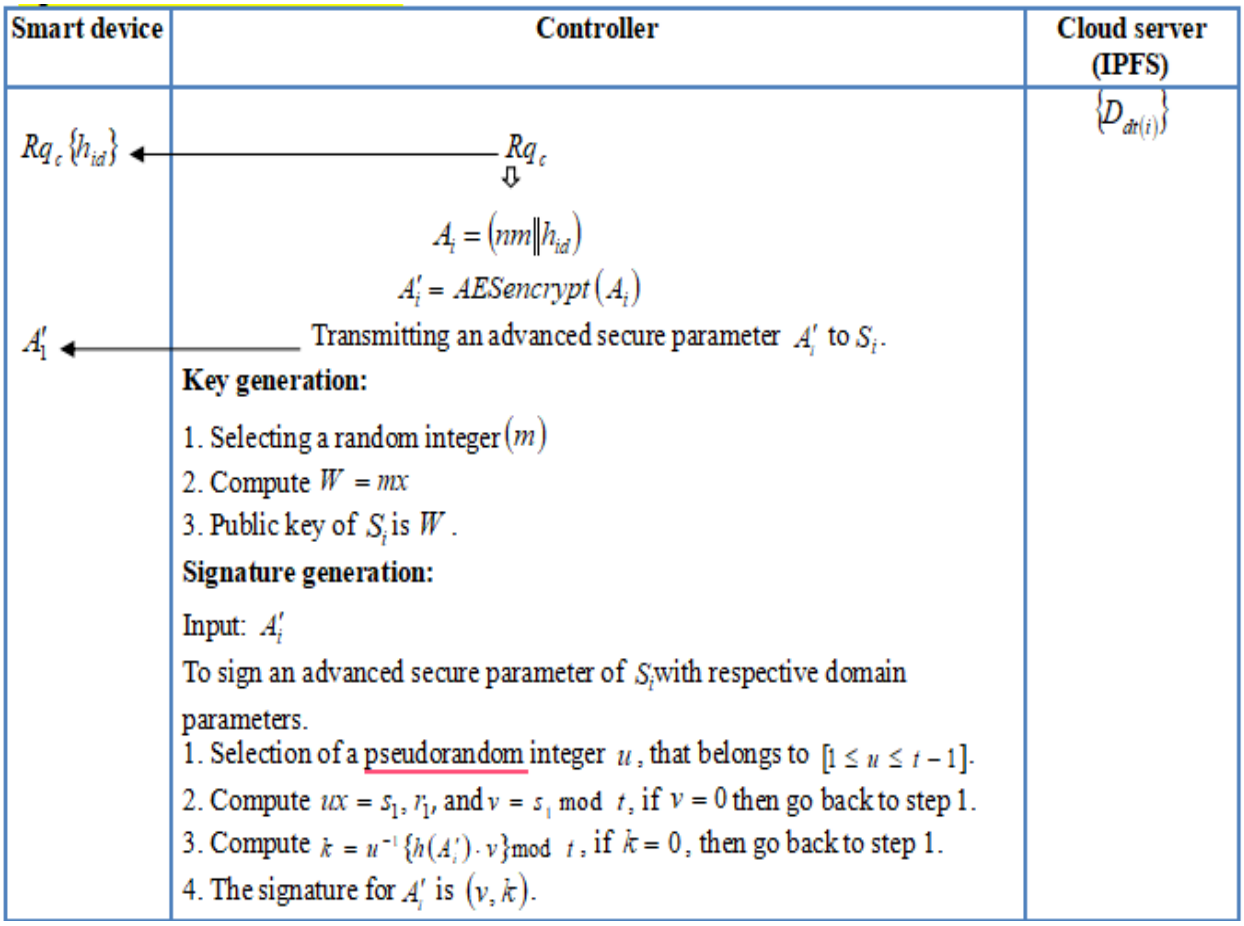


Figure 5: Illustration of a lightAEnC-based signature algorithm for secure authentication

4.2.2 Lightweight adaptive N-th degree truncated Karatsuba ring for data encryption

To enhance data security, the research adopts the LightANTKR encryption algorithm to convert original device data into an unreadable format and ensure less complexity for power-constrained smart devices. Besides, the traditional NTRU mechanism [30] was quite vulnerable and consumed a lot of time for execution due to the integration of the polynomial multiplication concept within encryption as well as decryption, which minimized the significance of power-constrained smart devices. As a consequence of this scenario, the research has utilized the Karatsuba algorithm instead of polynomial multiplication, which reduces the number of multiplications needed and makes it more efficient than traditional methods, especially for large numbers. Initially, the collected data $D_{dt(i)}$ from the corresponding S_i is encrypted using the LightANTKR algorithm within the cloud server. To do so, consider an integer ring R and residual class ring R_e, R/R_e where the truncated polynomial ring as $T_e = R_e[J]/(J^{Nm}-1)$ contains polynomials with degrees less than Nm and coefficients in R_e respectively. Here, considering

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

two polynomials, $p,q \in T$ and splitting them into $2^{\theta} - parts$, also imposing one more condition, that is $\left.\frac{Nm}{2^{\theta-1}}\right| e-1$, now the $Nm-bit$ polynomial is represented as,

$$p=\sum_{i=0}\left(J^{\frac{iNm}{2^{\theta}}}\cdot p_i\right) \quad \text{and} \quad q=\sum_{j=0}^{2^{\theta-1}}\left(J^{\frac{jnm}{2^{\theta}}}\cdot q_j\right) \tag{12}$$

From the above equations, e indicated that large prime numbers used as a modulus for the polynomial coefficient, $p_i \, and \, q_i, \ \forall i,j=0$, $2^{\theta-1}$ are the primary polynomial. For the case of $\theta=1$, the Karatsuba algorithm separated into $2-part$ as,

$$p=p_0+J^{\frac{Nm}{2}}\cdot p_1 \quad \text{and} \quad q=q_0+J^{\frac{Nm}{2}}\cdot q_1 \tag{13}$$

Where, $\frac{Nm}{2}$ indicates the midpoint of the polynomial, p_0, p_1, q_0, q_1 are denoted as a primary polynomial. From this polynomial, the public key is computed as,

$$a=p_0q_0-p_1q_1+J^{Nm/2}\left((p_0+p_1)(q_0-q_1)-p_0q_0-p_1q_1\right) \tag{14}$$

To reduce the computational constraints, the above formula is designed in a lightweight form as,

$$a=p_0(q_0-q_1)+J^{Nm/2}\left((p_0+p_1)(q_0+q_1)-p_1(q_0+q_1)\right) \tag{15}$$

Here, the public key is represented as a , and the private keys are $p, p_f \in T_e$ satisfying $p_f \square p \equiv 1 (\mathrm{mod}\, f)$.After generating the keys, the given device data $D_{dt(i)}$ is encrypted as

$$Q \equiv fd \square a + D_{dt(i)} (\mathrm{mod}\, e) \tag{16}$$

where, Q denotes the encrypted device data, d is a randomly selected integer, and f pecifies a coprime factor. In line with this, the modified steps within the LightANTKR algorithm minimize the overall power needed for encryption. Additionally, the proposed encryption algorithm does not rely on computational time and high memory resources, thus proving minimal power requirements for public key generation over power-constrained devices. Finally, the encrypted data is stored in the IPFS storage system, and the decryption key parameters are transferred to the corresponding smart devices $K_T\{(p_f, p), h_{id}\}$, where K_T represent the key transfer setup. The illustration of device data encryption using the LightANTKR algorithm is depicted in Figure 6.

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

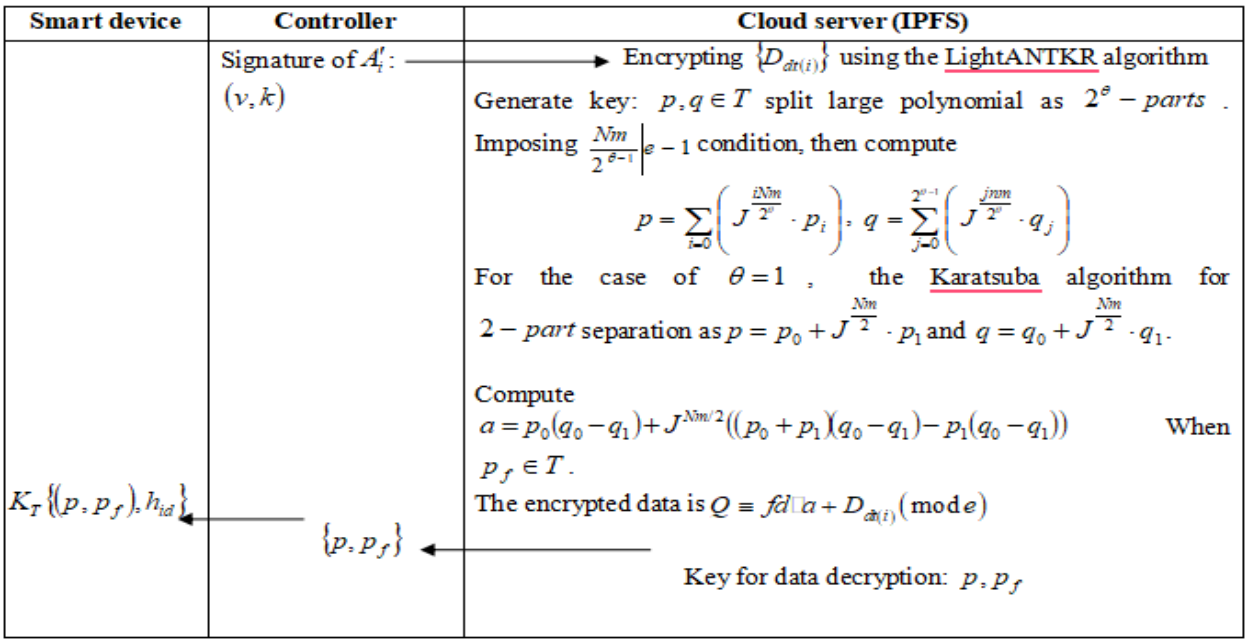


Figure 6: Lightweight adaptive N-th degree truncated Karatsuba ring for data encryption

4.3 Device authentication and data transfer phase

Consider the scenario, if the smart device requests Rq_c for its own data from the controller as $S_i : Rq_c\{G(A_j')\} \rightarrow CNT$,authentication of the device must be verified. Therefore, this phase proclaimed secure data transfer with significant authentication on power-constrained devices over the cloud server. When the controller receives a request from S_i containing the host ID and advanced secure parameter (A_j') along with data transfer intimation (G), it acquires a signature based on the given parameters using the LightAEnC-based signature algorithm and verifies whether the signature is valid or not, $CNT : check\ A_i' \in \{A_j'; j \rightarrow 0\ to\ n\}$. The verification can be computed as follows.

$$U = k^{-1} \bmod t \text{ and } h(A_i') \tag{17}$$

$$b_1 = h(A_j')U \bmod t \text{ and } b_2 = vU \bmod t \tag{18}$$

$$b_1 x + b_2 y = (r_0, s_0) \text{ and } E = r_0 \bmod t \tag{19}$$

Presuming that the received and stored secure parameters are similar $E = v$, the authenticity of S_i is successful and hence requesting Q over the cloud IPFS storage system. Once the data request $Rq_c\{G(A_i'), h_{id}\}$ is received within the IPFS, proceeding to the decryption process,

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

which involves sending a key request (K_{rq}) directly to the smart device and receiving a valid key for decryption. While decryption, computing $w = p \square Q (\mathrm{mod} e)$, and $w = fd \square q + p \square D_{dt(i)} (\mathrm{mod} e)$ with the acknowledged keys (p_f, p). Moreover, the absolute value of the coefficient in $fd \square q + p \square D_{dt(i)}$ is smaller and the corresponding e is chosen to be larger, then w is derived as

$$w = fd \square q + p \square D_{dt(i)} \tag{20}$$

Finally recovering the original device data as,

$$D_{dt(i)} = p_f \square w (\mathrm{mod} f) \tag{21}$$

Owing to the lightweight nature of the proposed scheme, it offers speed computation, and post-quantum security, and is mainly suitable for power-constrained devices. On the other hand, the verification is considered as unsuccessful if the secure parameters are dissimilar so then sending verification intimation message ver_{int} to the smart device and terminating the access for the retrieval of device data, thus enhancing the security.

$$ver_{\text{int}} = \begin{cases} 1, & if\ verification\ successful \\ 0, & if\ verification\ unsuccessful \end{cases} \tag{22}$$

The illustration of the device authentication and data transfer phase is shown in Figure 7.

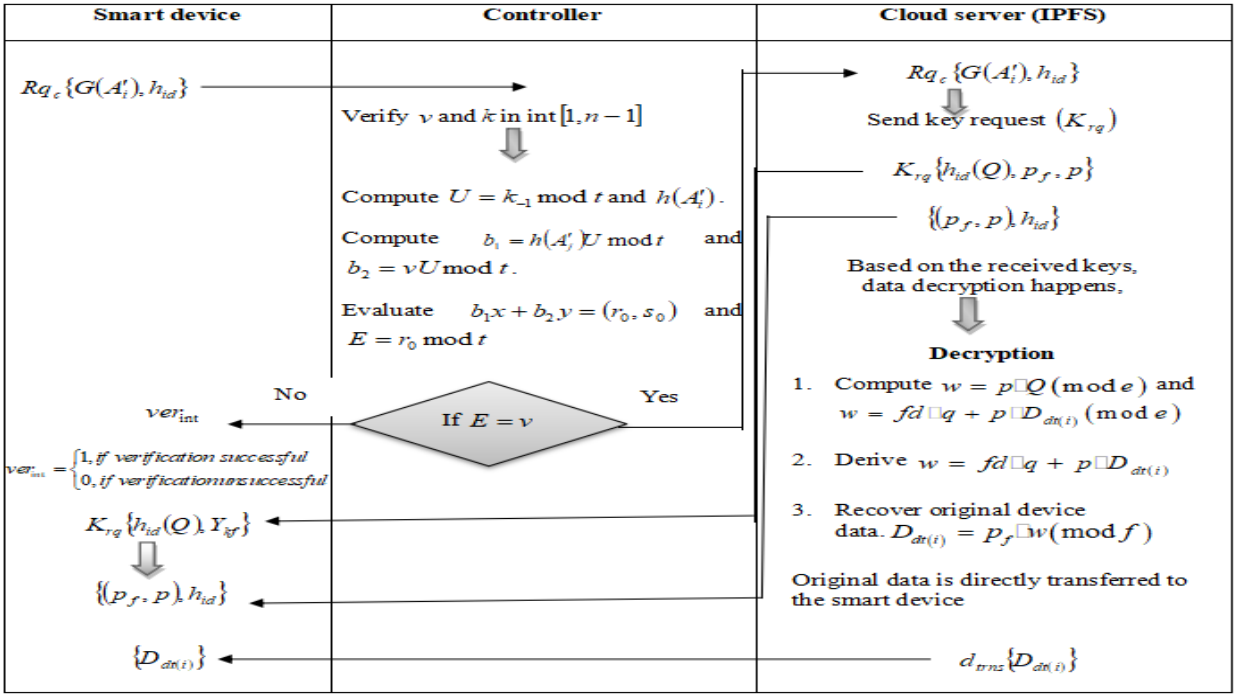


Figure 7: Device authentication and data transfer phase

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5. Results and discussion

The section presents implementation details of the proposed model and reveals the performance of the LightACTKR secure framework for power-constrained smart devices, also compared with other current algorithms to exhibit its robustness.

5.1 Experimental setup

The experiment of the LightACTKR secure framework for power-constrained smart devices is implemented on PyCharm software equipped with the Python tool running on the Windows 11 operating system. In order to facilitate this experiment, the research utilized 16GB of RAM and more than 100GB of ROM memory, thus encouraging minimal storage capacity for the execution.

5.2 Simulation parameters

In this experiment, parameters including smart device ID, unique host ID, Power, Distance, Trust 1, Name, position, and random device data are utilized to construct the LightACTKR secure framework. Here, the research induces initial power as 1, the distance is calculated from the controller, also known as a base station, and trust 1 varies depending on the transactions. The parameters involve the bit length of 64, the size of the prime is 4, and the ring dimension of 3 used in encryption.

5.3 Performance metrics

Standard performance metrics involved in assessing the proposed LightACTKR secure framework are encryption time, encryption rate, decryption time, memory usage, power loss, responsiveness, and throughput ratio, respectively. Here, the encryption time and decryption time metrics merely focus on measuring the time taken to encipher and decipher the device data, meanwhile, the encryption rate evaluates the speed at which the proposed algorithm encrypts device data. Moreover, the memory usage metric quantifies the amount of memory consumed for executing the LightACTKR secure framework, the power loss metric measures the total energy loss while encryption, responsiveness metric evaluates how quickly the message is passed over the cloud server and the smart device while encryption and the throughput metric measure the number of successful encryptions per second. Each metric symbolizes the corresponding time and energy consumed during encryption and decryption of the LightACTKR secure framework, also specifies memory as well as power consumption specifically for power-constrained smart devices, and proves its robustness.

5.4 Comparative analysis

The comparative investigation validates the effectiveness of the proposed LightACTKR secure framework by stacking up against Elliptic Curve ElGamal (ECEG) [1], Lightweight Sensor Nodes Authentication (LightAuth) [15], Physical Unclonable Function and Chebyshev chaotic map (PUF-CCM) [26], Elliptic curve Diffie–Hellman (ECDH) key exchange [27], Cyclic

Received: July 20, 2025

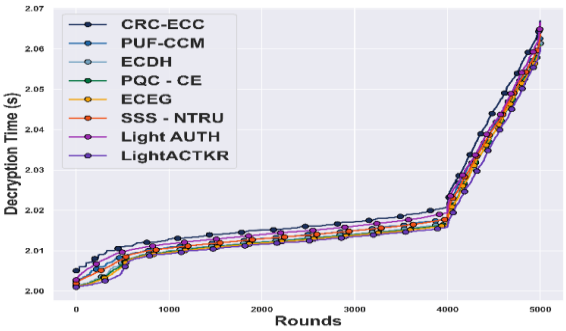
Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

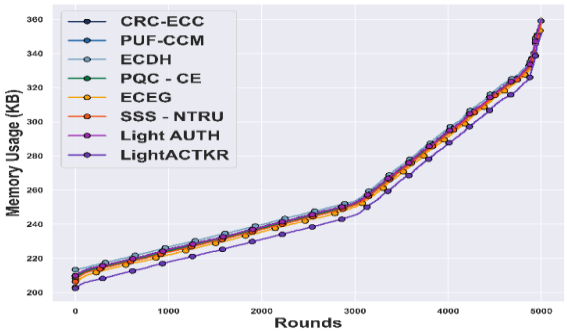
Redundancy Check with Elliptic Curve Cryptographic based model (CRC-ECC) [28], and Post-Quantum Cryptography for Consumer Electronics (PQC-CE) [33], and Shamir's Secret Sharing based Nth Degree Truncated Polynomial Ring encryption (SSS-NTRU) [34] methods over power-constrained smart devices. The validation takes place employing a number of devices, such as 50, 100, 150, and 200, and analysing with a number of rounds, which is described in the sections below.

5.4.1 Comparative analysis using 200 devices

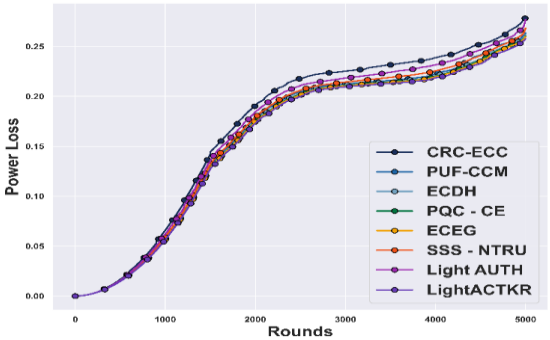
Figure 8 presents the comparative analysis with 200 devices and reveals that the LightACTKR secure framework is way better than the CRC-ECC, PUF-CCM, ECDH, ECEG, PQC-CE, Light AUTH, and SSS-NTRU approaches for power-constrained smart devices. In this comparison, the proposed LightACTKR secure framework shows 0.007s improvement with the CRC-ECC approach in decryption time, 8KB improvements in memory usage compared with CRC-ECC, 0.021 improvements in power loss, and 0.007ms improvements in responsiveness seen in round 5000 against CRC-ECC mechanisms. On round 5000, the LightACTKR secure framework gains 0.02 improvements while analyzing with the throughput ratio metric, thus making it an ideal choice for real-time applications.



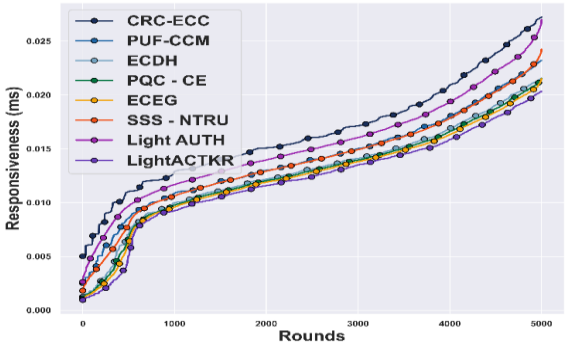
Decryption time



Memory usage



Power loss

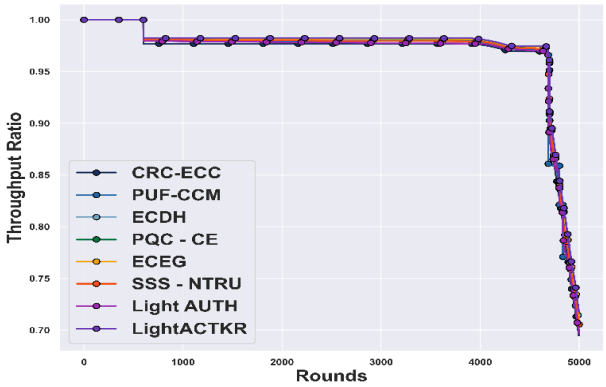


Responsiveness

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

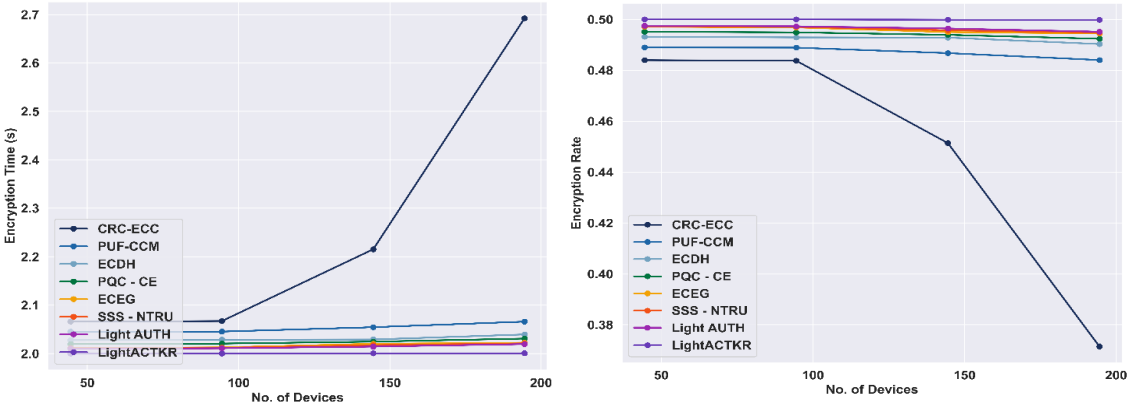


Throughput ratio

Figure 8: Comparative Analysis of 200 devices

5.4.2 Comparative analysis in terms of encryption rate and encryption time

From the Figure 9 observation, the encryption time and rate of the proposed LightACTKR secure framework are analyzed based on a number of devices 50, 100, 150, and 200, also compared with existing mechanisms such as CRC-EC, PUF-CCM, ECDH, ECEG, Light AUTH, PQC-CE and SSS-NTRU in order to reveal the robustness. While comparing with CRC-EC, PUF-CCM, and ECDH methods, LightACTKR secure framework showed maximum improvements of encryption rates as 0.016, 0.011, 0.007,0.005, and 0.003 rates using 50 devices and 0.129, 0.016, 0.01, 0.008, 0.006, 0.005 using 200 devices respectively. In addition to that, the proposed system shows a similar encryption time of 0.5s for all 200 devices, meanwhile, other existing systems offered maximum time. Based on the performances, the LightACTKR security framework can lead to faster communication and potentially reduce overall complexities while computation within the power-constrained devices.



Encryption rate Encryption Time

Figure 9: Comparative evaluation in terms of encryption rate and encryption time

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.5 Comparative Discussion

The section discusses the obtained results of the proposed LightACTKR secure framework against CRC-ECC, PUF-CCM, ECDH, PQC-CE, ECEG, SSS- NTRU, and Light AUTH mechanisms and ensures that the proposed framework is highly significant for power-constrained smart devices. On the contrary, some of the existing techniques, ECDH, PQC-CE, and ECEG, exhibited poor efficiency and showed a computationally intensive nature throughout execution. Furthermore, some of the algorithms do not guarantee against side-channel attacks and quantum attacks due to insufficient security paradigms. These limitations are possibly eliminated by the proposed LightACTKR secure framework because of the incorporation of a lightweight structure into the power-constrained smart devices. Moreover, the security also expands by incorporating a LightAEnC authentication scheme while considering advanced secure parameters, thus highlighting the inherent trade-off between reliability and dependability. The proposed framework appears to be more efficient in terms of processing time while maintaining a lower proportion of memory usage and computational complexities. So, the proposed framework requires a minimal 2.00s encryption time, 2.060s decryption time, 352KB memory usage, 0.258 power loss, and 0.020ms for responsiveness, also gains an increased throughput ratio of 0.718 and an encryption rate of 0.500 analyzed based on 200 devices, respectively, presented in Tables 2 and 3. Owing to the robustness and secure implementation, the proposed framework can be preferred for real-time applications. Overall, the LightACTKR secure framework ensures sensitive information remains private and cannot be intercepted by unauthorized access. The existing techniques faced difficulties with overheads, less scalability, and low throughput took place in lightweight authentication, and insufficient security paradigms during the authentication process. The utilization of the LightAEnC signature algorithm encrypts registered smart device credentials and introduces advanced secure parameters to define security while communicating. Additionally, constructing the lightAEnC algorithm enables a lightweight structure that minimizes computational complexities within the power-constrained smart devices. In the LightANTKR algorithm, device data is encrypted by the Karatsuba algorithm, which reduces overheads during computation. Specifically, the cryptographic implications in the research support in cyber security for data protection, confrontation against various attacks and quantum threats. Also, preserving data integrity, stopping modification, allow sensitive information after authentication and verification process. More specifically, the proposed technique is efficient for power-constrained smart devices with a lightweight structure and secures device data against various attacks, which enhances the robustness of the proposed LightACTKR framework.

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 2**.** Comparative discussion with 200 devices and 5000 rounds

	200 devices and 5000 rounds				
Methods vs metrics	**Decryption time (s)**	**Memory usage (KB)**	**Power loss**	**Responsiveness (ms)**	**Throughput ratio**
CRC-ECC [28]	2.067	360	0.279	0.027	0.695
PUF-CCM [26]	2.063	360	0.264	0.023	0.700
ECDH [27]	2.061	361	0.261	0.022	0.708
PQC-CE [33]	2.061	361	0.261	0.022	0.708
ECEG [1]	2.061	361	0.260	0.022	0.709
Light Auth [15]	2.064	360	0.268	0.024	0.703
SSS-NTRU [34]	2.067	360	0.277	0.027	0.696
LightACTKR	2.060	352	0.258	0.020	0.718

Table 3: Comparative discussion in terms of Encryption time and rate

	Encryption time (s)				**Encryption rate**			
Methods vs. devices	**Device 50**	**Device 100**	**Device 150**	**Device 200**	**Device 50**	**Device 100**	**Device 150**	**Device 200**
CRC-ECC [28]	2.066	2.067	2.215	2.692	0.484	0.484	0.451	0.371
PUF-CCM [26]	2.045	2.045	2.054	2.066	0.489	0.489	0.487	0.484
ECDH [27]	2.028	2.029	2.029	2.039	0.493	0.493	0.493	0.490
PQC-CE [33]	2.020	2.021	2.025	2.031	0.495	0.495	0.494	0.492
ECEG [1]	2.012	2.013	2.020	2.022	0.497	0.497	0.495	0.494
Light Auth [15]	2.011	2.012	2.017	2.021	0.497	0.497	0.496	0.495
SSS-NTRU [34]	2.010	2.011	2.014	2.019	0.497	0.497	0.496	0.495
LightACTKR	2.000	2.000	2.001	2.001	0.500	0.500	0.500	0.500

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.6 Statistical Analysis

Statistical analysis is utilized to evaluate the robustness of the reported results and concluding those variations might help to explain the reason for the trial results from one experiment to the next. Furthermore, several statistical measures such as best, mean, and variance are computed for the various evaluation metrics such as Decryption time (s), Memory usage (KB), Power loss, Responsiveness (ms), and Throughput ratio. The proposed LightACTKR technique achieved a high best value in comparison to other existing models, demonstrating the effectiveness of the suggested technique. Tables 4 depict the statistical analysis of the proposed LightACTKR technique using the metrics based on best, mean, and variance, respectively, for 5000 rounds.

Table 4: Statistical Analysis

5000 rounds									
Performance metrics	**Methods**	**CRC-ECC**	**PUF-CCM**	**ECDH**	**PQC-CE**	**ECEG**	**LightAuth**	**SSS-NTRU**	**LightACTKR**
Decryption time (s)	Best	2.21	2.16	2.17	2.15	2.14	2.16	2.19	2.15
	Standard Deviation	2.03	2.03	2.02	2.02	2.02	2.02	2.03	2.01
	Variance	0.00024	0.00022	0.00018	0.00018	0.00017	0.00020	0.00023	0.00015
Memory usage (KB)	Best	353	352	348	347	347	350	353	344
	Standard Deviation	251	249	245	244	244	247	250	242
	Variance	1328	1329	1326	1327	1329	1328	1328	1326
Power loss	Best	0.324	0.319	0.313	0.313	0.313	0.318	0.324	0.310
	Standard Deviation	0.188	0.178	0.167	0.165	0.164	0.173	0.183	0.160
	Variance	0.011	0.010	0.009	0.008	0.008	0.009	0.010	0.008
Responsiveness (ms)	Best	0.174	0.136	0.128	0.127	0.127	0.146	0.164	0.114
	Standard	0.025	0.023	0.015	0.014	0.013	0.019	0.024	0.011

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Deviation								
	Variance	0.00006	0.00005	0.00003	0.00003	0.00003	0.00004	0.00005	0.00002
Throughput ratio	Best	1	1	1	1	1	1	1	1
	Standard Deviation	0.956	0.962	0.968	0.970	0.971	0.965	0.959	0.974
	Variance	0.005	0.004	0.003	0.003	0.002	0.003	0.004	0.002

5.7 Security Analysis

The security analysis is conducted to evaluate the security of the proposed LightACTKR technique by analyzing the model with potential attacks, including the side-channel, quantum threats, and fault injection in the process of decryption. The security analysis for the proposed approach is depicted in Figure 10. The decryption with various attacks is evaluated. The proposed approach achieved 2.66 with no attack for decryption operations, 2.14 with side-channel, 2.15 with quantum threats, and 2.13 with fault injection, respectively. However, the proposed LightACTKR technique achieved better performance in the criteria without attack, which evaluates the integrity and security of authentication.

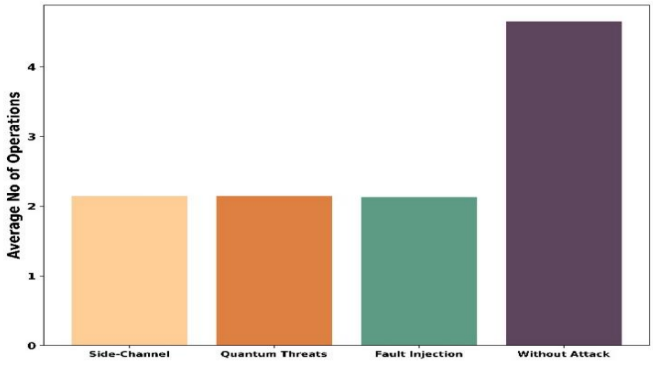


Figure 10: Security Analysis

6. Conclusion

The proposed cryptographic security framework, LightACTKR for power-constrained smart devices, hinges on a delicate balance among security, performance, memory usage, and power consumption. The choice of LightACTKR secure framework is influenced by the specific performance and security needs of the application. While incorporating lightweight concepts indeed restricts complex computation and makes an appealing choice for power-constrained smart devices. Implementing a LightAEnC-based signature algorithm verifies the authenticity of the smart device. Further, enabling standardized security. More specifically, integrating the

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

LightACTKR-based data encryption mechanism rapidly secures device data against quantum attacks, revealing robustness towards power-constrained smart devices. Owing to the advantages of stochastic mechanisms, the LightACTKR secure framework gains 2s of encryption time, 2.060s of decryption time, and 352KB of memory usage analysed based on 200 devices in comparison with the results of the other existing techniques. In the future, the present secure framework will be incorporated with other ideal encryption mechanisms to enhance security over power-constrained smart devices.

References

[1] S. Baccouri, H. Farhat, T. Azzabi, and R. Attia, "Lightweight authentication scheme based on elliptic curve El Gamal," Journal of Information and Telecommunication, Vol. 8, No. 2, pp. 231–261, 2024.

[2]B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for Internet of Things (IoT)," IEEE Systems Journal, Vol. 14, No. 3, pp. 3440–3450, 2020.

[3] A. Tidrea, A. Korodi, and I. Silea, "Elliptic curve cryptography considerations for securing automation and SCADA systems," Sensors, Vol. 23, No. 5, pp. 2686, 2023.

[4]L. Rosa, M. Freitas, S. Mazo, E. Monteiro, T. Cruz, and P. Simões, "A comprehensive security analysis of a SCADA protocol: From OSINT to mitigation," IEEE Access, Vol. 7, pp. 42156–42168, 2019.

[5] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: secure protocols, incidents, threats and tactics," IEEE Communications Surveys & Tutorials, Vol. 22, No. 3, pp. 1942–1976, 2020.

[6] Y. S. Yang, S. H. Lee, J. M. Wang, C. S. Yang, Y. M. Huang, and T. W. Hou, "Lightweight authentication mechanism for industrial IoT environment combining elliptic curve cryptography and trusted token," Sensors, Vol. 23, No. 10, pp. 4970, 2023.

[7] P. Sun, H. He, Y. Sun, R. Lu, Y. Zhang, and G. Xie, "A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions," Computers & Security, vol. 148, Art. no. 104097, 2025.

[8] E. A. Hagras, S. Aldosary, H. Khaled, and T. M. Hassan, "Authenticated public key elliptic curve based on deep convolutional neural network for cybersecurity image encryption application," Sensors, Vol. 23, No. 14, pp. 6589, 2023.

[9] S. L. Nita and M. I. Mihailescu, "Elliptic curve-based query authentication protocol for IoT devices aided by blockchain," Sensors, Vol. 23, No. 3, pp. 1371, 2023.

[10] R. A. Devi and A. R. Arunachalam, "Enhancement of IoT device security using an improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM," High-Confidence Computing, Vol. 3, No. 2, pp. 100117, 2023.

[11] A. Maarouf, R. Sakr, and S. Elmougy, "An offline direct authentication scheme for the Internet of Medical Things based on Elliptic Curve Cryptography," IEEE Access, Vol. 12, No. 1, pp. 134902–134925, 2024.

[12] E. T. Oladipupo, O. C. Abikoye, A. L. Imoize, J. B. Awotunde, T. Y. Chang, C. C. Lee,

Received: July 20, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and D. T. Do, "An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks," IEEE Access, Vol. 11, No. 1, pp. 1306–1323, 2023.

[13] S. Izza, M. Benssalah, and K. Drouiche, "An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment," Journal of Information Security and Applications, Vol. 58, No. 1, pp. 102705, 2021.

[14]Z. Bao, Y. Lin, S. Zhang, Z. Li, and S. Mao, "Threat of adversarial attacks on DL-based IoT device identification," IEEE Internet of Things Journal, Vol. 9, No. 11, pp. 9012–9024, 2021.

[15] Z. U. I. Adil, M. Iqbal Khan, K. Sanam, S. U. Malik, S. A. Moqurrab, and G. Srivastava, "LightAuth: A lightweight sensor nodes authentication framework for smart health system," Expert Systems, Vol. 42, No. 2, p. 13756, 2025.

[16] H. Kadry, A. Farouk, E. A. Zanaty, and O. Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security," Alexandria Engineering Journal, Vol. 71, pp. 491–500, 2023.

[17]Y. S. Yang, S. H. Lee, W. C. Chen, C. S. Yang, Y. M. Huang, and T. W. Hou, "TTAS: Trusted token authentication service of securing SCADA network in energy management system for industrial Internet of Things," Sensors, Vol. 21, No. 8, pp. 2685, 2021.

[18]S. Yeasmin and A. Baig, "Permissioned blockchain-based security for IIoT," in Proceedings of the 2020 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada, pp. 1–7, 2020.

[19] P. Boobalan, S. P. Ramu, Q. V. Pham, K. Dev, S. Pandya, P. K. R. Maddikunta, and T. Huynh-The, "Fusion of Federated Learning and Industrial Internet of Things: A Survey", Computer Networks, Vol. 212, No. 1, pp. 109048, 2022.

[20] N. Purohit, S. Joshi, M. Pande, and S. Lincke, "Pragmatic Analysis of ECC Based Security Models from an Empirical Perspective", Journal of Discrete Mathematical Sciences and Cryptography, Vol. 26, No. 3, pp. 739–758, 2023.

[21] C. M. Chen, S. Liu, X. Li, S. Kumari, and L. Li, "Design and Analysis of a Provable Secure Two-Factor Authentication Protocol for Internet of Things", Security and Communication Networks, Vol. 2022, No. 1, pp. 4468301, 2022.

[22] H. AlMajed and A. AlMogren, "A Secure and Efficient ECC-Based Scheme for Edge Computing and Internet of Things", Sensors, Vol. 20, No. 21, pp. 6158, 2020.

[23] N. Purohit and S. Joshi, "Comprehensive Analysis on Various Cryptographic Algorithm for Constrained Devices", In: Proc. of the 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET), pp. 1–7, 2024.

[24] A. Rizzardi, S. Sicari, and A. Coen-Porisini, "Analysis on functionalities and security features of Internet of Things related protocols", Wireless Networks, Vol. 28, No. 7, pp. 2857–2887, 2022.

[25] O. Popoola, M. A. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, "An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security", Internet of Things, Vol. 27, No. 1, pp. 101314, 2024.

[26] X. Jin, N. Lin, Z. Li, W. Jiang, Y. Jia, and Q. Li, "A lightweight authentication scheme

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

for power IoT based on PUF and Chebyshev chaotic map", IEEE Access, Vol. 12, pp. 83692–83706, 2024.

[27] V. Tanksale, "Efficient elliptic curve Diffie–Hellman key exchange for resource-constrained IoT devices", Electronics, Vol. 13, No. 18, pp. 3631, 2024.

[28]I. Keshta, "A CRC-Based Authentication Model and ECC-Based Authentication Protocol for Resource-Constrained IoT Applications", IEEE Access, Vol. 12, pp. 156765–156784, 2024.

[29]J.N. Mamvong, G.L. Goteng, B. Zhou, and Y. Gao, "Efficient security algorithm for power-constrained IoT devices", IEEE Internet of Things Journal, Vol. 8, No. 7, pp. 5498–5509, 2020.

[30] I.A. Awan, M. Shiraz, M.U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, "Secure framework enhancing AES algorithm in cloud computing", Security and Communication Networks, Vol. 2020, Article ID 8863345, pp. 1–12, 2020.

[31] T. Islam, R.A. Youki, B.R. Chowdhury, and A.T. Hasan, "An ECC based secure communication protocol for resource constraints IoT devices in smart home", In: Proceedings of the International Conference on Big Data, IoT, and Machine Learning (BIM), pp. 431–444, 2021.

[32] E. Camacho-Ruiz, M.C. Martínez-Rodríguez, S. Sánchez-Solano, and P. Brox, "Timing-attack-resistant acceleration of NTRU round 3 encryption on resource-constrained embedded systems," Cryptography, Vol. 7, No. 2, Art. no. 29, 2023.

[33] D. Commey, B. Appiah, G. S. Klogo, W. Bagyl-Bac, and J. D. Gadze, "Performance Analysis and Deployment Considerations of Post-Quantum Cryptography for Consumer Electronics," arXiv preprint, arXiv:2505.02239, 2025

[34] M. A. Hammed and M. F. Al-Gailani, "Quantum-Secure Key Distribution in a Resource-Constrained Environment," Iraqi Journal of Information and Communication Technology, vol. 8, no. 1, pp. 50–62, 2025.

[35]Nilima S, Alind, Nitin Arora,"Randamization Technique for Desiging of Substitution Box in Data Encryption Standard Algorithm", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.5, No.3, pp.27-36, 2019. DOI: 10.5815/ijmsc.2019.03.03

Received: July 20, 2025