International Journal of Safety and Security Engineering
Vol. 15, No. 12, December, 2025, pp. 2613-2624
Journal homepage: http://iieta.org/journals/ijsse

Attribute-Based Lightweight Encryption Framework for Securing a Voter Database

Safa A. Ahmed[1,2*], Ali M. Sagheer[3]

[1] Informatics Institute for Postgraduate Studies, University of Information Technology and Communications, Baghdad 10001, Iraq
[2] Department of Chemical Engineering and Petroleum Pollution, College of Chemical Engineering, University of Technology, Baghdad 10066, Iraq
[3] Department of Computer Networks Systems, College of Computer Science and Information Technology, University of Anbar, Ramadi 31001, Iraq

Corresponding Author Email: safa.a.ahmed@uotechnology.edu.iq

https://doi.org/10.18280/ijsse.151217

Received: 16 October 2025
Revised: 15 December 2025
Accepted: 23 December 2025
Available online: 31 December 2025

Keywords:
attribute-based encryption, lightweight cryptography, fingerprint minutiae, Rivest Shamir Adelman key exchange, dynamic key session, election security, voter database protection, hybrid cryptography

ABSTRACT

The emergence of digital governance raises concerns about the security of election data if elections are conducted online. Election information has been moved to the internet, courtesy of advances in digital technology, and is therefore prone to hacking and misuse. The proposed framework in this paper employs lightweight encryption algorithms that emphasize both attributes and novel key exchange to secure the voter registration database, as well as attribute-based encryption (ABE) and biometric authentication. This provides data confidentiality, authenticity, fine-grained access control, efficient computations, and applicability in digital elections. The presence of an essential key generation mechanism at multiple levels that incorporates the user's attributes and biometric data, which changes dynamically in each session, makes the process more secure. The encryption of the voter registration database is ensured using fast, lightweight symmetric algorithms. The framework is tested using a real database of Iraqi voters and fingerprint images from 60 users. The output demonstrates that the key values generated have high entropy and high scores on the standard statistical randomness tests, with accepted p-values, indicating excellent statistical representation and a high degree of randomness. These results prove the fact that the proposed framework develops and exchanges key within a rapid fashion with the effective throughput, resilient to brute-force and impersonation attacks, which adds to its adaptability to real-life and large-scale elections.

1. INTRODUCTION

The rapid growth in digital data, driven by the rise of cloud technologies and the Internet of Things (IoT), requires finding secure and effective encryption systems. Traditional cryptography algorithms, though very strong, might not provide a balance among security, scalability, and computational efficiency in contemporary distributed systems [1-3]. Users, companies, and governmental organizations need security solutions to store their sensitive documents and data in cloud platforms [4]. Thus, the researchers have already thought of the existence of hybrid and lightweight cryptography schemes, the combination of symmetric and asymmetric approaches to the establishment of the confidentiality and performance levels [5-7]. Meanwhile, chaotic maps and pseudorandom generators are also proposed as an effective method for key generation that is both secure and reliable, owing to their high sensitivity to initial conditions and unpredictability [8]. The properties of the chaotic maps, such as the logistic map, piecewise linear chaotic maps, and higher-dimensional chaotic systems, are appropriate for generating complex keystreams [9]. Biometric methods have reduced user-centric authentication compared to chaotic systems, thereby increasing predictability. Biometric techniques, in particular, fingerprint minutiae extraction, have been more useful for identity verification, thereby providing value to cryptographic keys [10-12]. Multi-biometric fusion has been analyzed to enhance higher accuracy in authentication [2, 13]. At the same time, the mechanism of ABE has been developed as a paramount control of access rights when considering attributes (e.g., name, email, organizational role) of users directly inside the encryption methodology [14]. This paradigm ensures that the decryption process does not purely depend on cryptographic keys but also on attribute policies, which makes it particularly successful with cloud and FinTech applications, where multi-user access is a characteristic feature [15-17]. Despite these improvements, the existing knowledge tends to discuss biometric authentication and ABE separately. Some studies combine the use of passwords with biometrics in the generation of keys based on Rivest Shamir Adelman (RSA) [18, 19] or utilize hybrid cryptography for cloud storage [20, 21]. Nevertheless, an active combination of user attributes, biometrics, and chaos-based key generation is not studied properly. Furthermore, lightweight frameworks are needed to support resource-constrained devices [1, 2]. It rarely deals with the dynamic properties of the session-specific secret keys that change with each transaction. The current literature in election data security tends to focus on ABE, biometric authentication, chaos-based or hash-based generation of keys as individual tools, but does not offer a cohesive framework of how cryptographic keys are tied to the identity of the user and to the attributes of the session. Specifically, the joint operation of fine-grained access control and dynamically generated biometric-based session keys is even under-investigated, particularly in the lightweight and large-scale database models. In a bid to fill this gap, this paper proposes a hybrid security model that incorporates ABE with fingerprint biometrics and hash-based key derivation involving the use of the SHA-512 hash algorithm to generate dynamic and secure keys. The suggested scheme binds the secret keys to user features and biometric minutiae, hence, session-related and identity-related encryption. A suggested mechanism based on RSA is used to perform safe key exchange, whereas lightweight ciphers are used to ensure efficient data encryption. The integrated design offers a scalable and viable solution to the security of sensitive voter data on cloud- and IoT-assisted elections. The remainder of this paper is organized as follows. Section 2 summarizes related work. Section 3 explains the proposed method for the framework and its primary elements. Section 4 will present the experimental results. Lastly, Section 5 presented the conclusion of the paper.

2. RELATED WORK

Recent studies on the generation of secure keys and encryption have looked at different methods, such as chaos-based, biometric, ABE, hybrid cryptographic models, and integration of the methods into incorporation systems. The objectives of these have been to produce random cryptographic keys and pseudorandom sequences, offer special capabilities in authentication and key derivation, and trade off performance and security in resource-constrained environments. Nevertheless, there is difficulty in integrating these methods into a unified lightweight model of dynamic, session-dependent, and fine-grained protection of data. Literature classifies the existing technologies into five major categories: Chaos-Based Key Generation, Biometric-Based Key Generation, ABE, Hybrid Approaches, which is a combination of biometrics, chaos, ABE, and hybrid cryptography, and lightweight encryption. Chaotic systems are good at generating cryptographic keys and pseudorandom numbers due to their randomness and high sensitivity. Akif et al. [22] designed a 2D chaotic system to generate bit pseudorandom systems. Yu et al. [23] investigated the use of hyperchaotic maps for randomness and unpredictability. Mahdi and Hoobi [8] suggested approaches to integrate chaotic maps with the reinforcement of learning algorithms (A2C) to produce strong and efficient cryptographic keys. The methods of fingerprint enhancement and minutiae extraction were discussed by Sochat and Wang [10] and Situmorang and Andrea [11]. Whereas Siddiqui et al. [12] provided powerful algorithms to tackle contactless fingerprinting matching. Multi-biometric fusion has been reported to enhance better authentication and anti-spoofing attack resistance [13, 24]. Suresh et al. [18] combined fingerprint authentication with passwords to obtain RSA keys, which demonstrates the possibility of generating cryptography keys biometrically supported to ensure secure communication. ABE enables access control of fine-grained access control of attributes of the users directly linked to the cryptographic keys or the ciphertexts. Kaliyaperumal and Sammy [14] demonstrated ABE to share patient health records securely, whereas Naregal and Kalmani [25] investigated lightweight ABE to share information over mobile IoT. Jammula et al. [26] suggested hybrid lightweight cryptography and ABE to have scaled IoT security. ABE with cloud environments integration has been highlighted in literature on hybrid encryption methods and in the protection of big data [15-17, 20]. Anitha Kumari et al. [27] examined key derivation based on passwords and biometrics in the environment of two servers or edge computing. Mohanraj and Santhosh [7] suggested a hybrid encryption framework to secure big data in Hadoop systems. Ashraf et al. [5] presented a strong and lightweight symmetric key exchange algorithm in next-generation IoE devices. Salah et al. [6] used the combination of the RSA and Diffie-Hellman to improve the security of network transmission. Besides, the literature on resource-constrained IoT devices has proposed lightweight cryptosystems, like DNA-RC4, and efficient encryption algorithms to be used in smart cities [1, 2]. As Koppaka and Lakshmi [20] and Veerabadrappa et al. [21] underlined, the hybrid methods of cloud data security are significant, whereas the combination of asymmetric key exchange and symmetric data encryption can be used to ensure performance and reliability. Based on such a review, it is noticeable that a general pattern observed among the current methods is to have isolated means of data protection, be it biometric authentication, ABE, or chaos-based key generation, but nothing in between, providing an integrated and lightweight system. Most studies use static derivation of keys or do not have fine-grained access control, whereas others have strong randomness properties without linking cryptographic keys to user identity or session-specific attributes. Conversely, the suggested framework presents a combination of ABE with a biometric-based dynamic session key and lightweight encryption functions in a single structure. The design can overcome these limitations because it allows handling access control at fine-grains, security on a session basis, and computational efficiency that is appropriate in voter databases of considerable scale. The solution given is, therefore, more comprehensive and practical than the current approaches.

3. PROPOSED METHOD

The proposed method aims at developing a secure and light hybrid cryptographic architecture that integrates biometric authentication and multi-level encryption. The system combines user identifications and characteristics based on fingerprinting to dynamically create distinct encryption keys every session. This combination ensures the balance between computability and cryptographic capability. The model uses the RC5 block cipher and a ChaCha-based stream cipher to protect biometric information and uses an RSA-based approach that is enhanced with a six-dimensional hyperchaotic system to exchange keys safely, as shown in Figure 1. It is a multi-tiered architecture that enhances confidentiality, integrity, and resistance to brute-force and replay assaults, which makes it suitable in current IoT and cloud-assisted environments where security and efficiency are the most crucial factors.

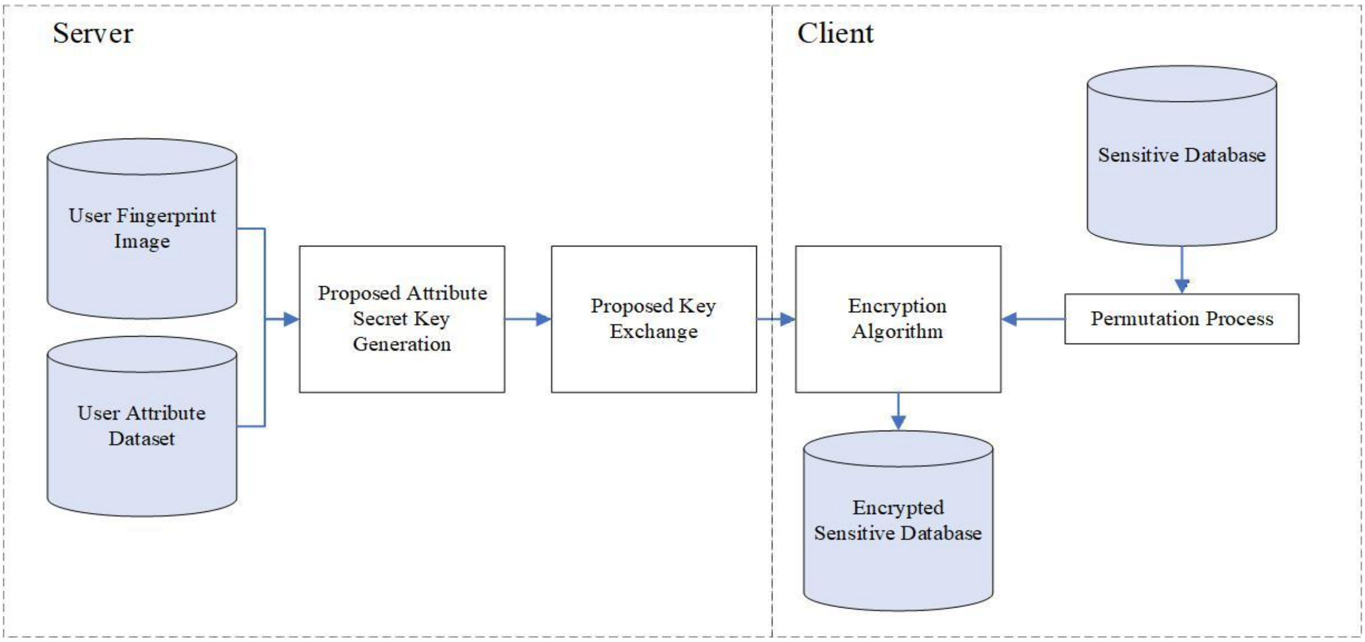


Figure 1. General framework for the proposed method

The formal key-policy attribute-based encryption (KP-ABE) component is used in the proposed system, which includes a set of universal attributes $\mathcal{U}$, a finite set of attributes $\mathcal{A}$, which are attributes describing user-related and system-related values, user role, affiliation to an organization, identity parameter, and biometric-derived credentials, where $\mathcal{A} \subseteq \mathcal{U}$. The policy access $\mathcal{P}$ is established over the attribute set space using a Boolean structure with only those attribute sets satisfying the policy implemented within the secret key of the user to be decrypted. The KP-ABE scheme used in this work is composed of the following 4 polynomial-time algorithms:

- Setup (λ): The setup algorithm takes a security parameter λ and constructs the system by creating the public parameters PK and a master secret key MSK.
- Key Generation (MSK, $\mathcal{P}$): The key generation algorithm generates an attribute secret key SK with the help of master secret key MSK and access policy $\mathcal{P}$. This key is safely authorized to a certified user.
- Encrypt (PK, M, $\mathcal{A}$): With the public parameters PK, message M (in this case represented as a dynamically generated session key) is encrypted with respect to attribute set $\mathcal{A}$, then the ciphertext CT is obtained.
- Decrypt (SK, CT): The decryption algorithm can successfully extract the message M out of CT only when the attribute set satisfies the access policy that comes with the secret key SK.

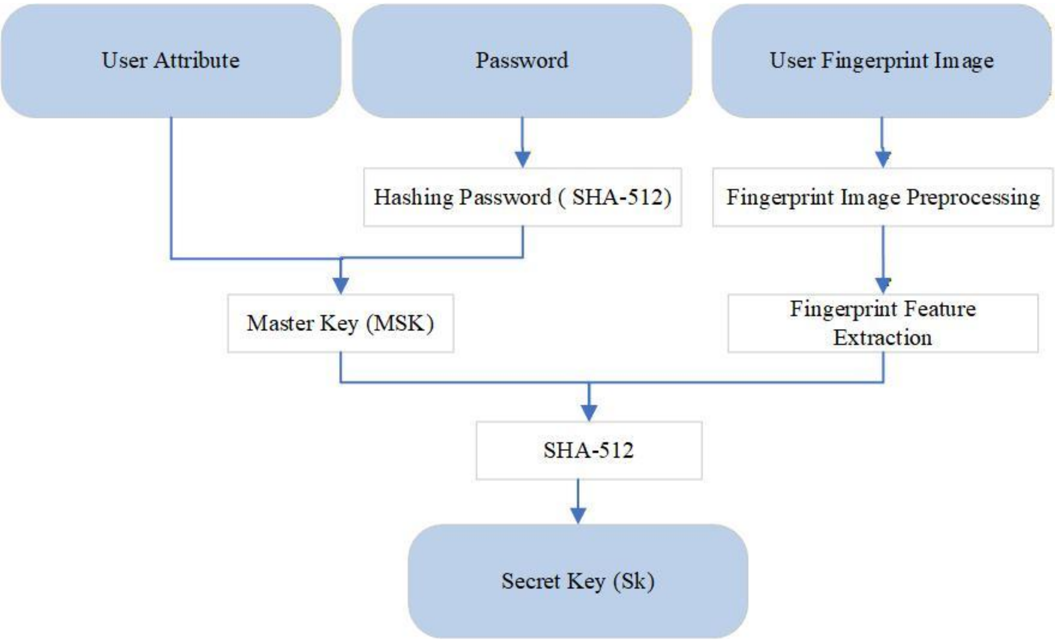
In comparison to traditional KP-ABE systems, where it is often assumed that big data objects are simply encrypted, the framework proposed modifies KP-ABE to secure dynamically generated session keys. where user attributes such as the hashed credentials and a secured biometric template are calculated to produce the session key. These session keys are then employed together with the lightweight symmetric encryption algorithms to encrypt the voter registration database. The design option maintains computational efficiency and allows fine-grained, attribute-based access control, where the policy of access is outlined as a conjunctive attribute rule, where the session key will be created only in the case of all the requirements being met. The KP-ABE component security is taken to be in the standard model of indistinguishability under chosen-plaintext attack (IND-CPA) model. Informally, an adversary who lacks a secret key with an access policy that meets the corresponding attribute set is unable to differentiate between encryptions of two randomly chosen session keys with non-negligible advantage. Because the session keys are calculated based on biometric measurements and cryptographic hash message-digest algorithms, and the underlying construction of the KP-ABE is based on time-tested IND-CPA secure designs, the framework of the proposed construction inherits its confidentiality properties. Any attack on the ABE-protected session keys would hence connote the violation of the underlying KP-ABE security assumption.

A combination of multi-tiered encryption algorithms, including the RC5 method, which is inspired by ChaCha, and RSA with chaotic key generation, generates a strong hybrid framework. Such a framework aimed to ensure significant entropy in key generation, instant modification, and enhanced resistance to both the differential and statistical attacks.

3.1 Proposed attribute secret key generation scheme

The suggested key-generating scheme incorporates user attributes with biometrics to generate dynamic and secure session keys. The password is first hashed with SHA-512, and then it is combined with the hexadecimal form of the username. This combination is rehashed to create a given length Master Key. Simultaneously, fingerprint minutiae are extracted, such as x-y coordinates, the type of ends of the ridges, as well as their bifurcation, and their angle. All features are normalized and transformed into a hexadecimal value. Minutiae features with a pseudo-random selection are sampled.

Each communication session has a seeding value of the Master Key and the session identifier, making it unpredictable and varying as illustrated in Figure 2. The chosen features are then combined with the Master Key and digested with the SHA-512 to obtain the final Session Key. Such dynamic keys are subsequently used in a hybrid cryptographic architecture, a mixture of RC5 and ChaCha, to obtain both a lightweight property and resistance to cryptographic attacks.



User Attribute
Password
User Fingerprint Image
Hashing Password (SHA-512)
Fingerprint Image Preprocessing
Master Key (MSK)
Fingerprint Feature Extraction
SHA-512
Secret Key (Sk)

Figure 2. Proposed attribute secret key generation scheme

3.1.1 Fingerprint feature extraction (minutia)

The extraction of fingerprint features is a crucial step in biometric-based security systems, which aim to produce stable and reliable data for further processing. Images of raw fingerprints are initially processed in several stages, which include noise elimination, histogram equalization, image scaling, binarization, and thinning to promote clarity of ridges and valleys and to increase uniformity of the images. Figure 3 indicates the block diagram of the preprocessing step.

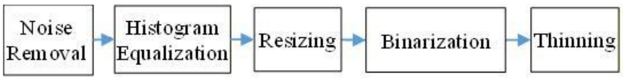


Figure 3. Fingerprint preprocessing stages

Noise reduction will reduce the artifact added in the acquisition phase, but histogram equalization will redistribute pixel values to increase contrast and show ridge lines. The scaling process normalizes image ratios in an appropriate way, whereas the thinning process removes ridges to a single pixel line without reducing their structural integrity, hence allowing accurate minutiae recognition. After the preprocessing, the crossing number (CN) method is used to detect the unique fingerprint features, which include ridge ends and bifurcations expressed via x and y coordinates, orientation angles, and types. The method of CN is grounded on the analysis of pixel distribution of the fingerprint and assists in categorizing the minutiae as shown in Eq. (1).

$$CN = \frac{1}{2}\sum_{i=1}^{8}|P_i - P_{i-1}| \tag{1}$$

where, P_i is the current pixel, while P_{i-1} is the neighboring pixel. Each feature extracted is then translated into a hexadecimal and joined together into one string. To achieve diversity in security, a dynamically chosen set of these minutiae features is used during each session to produce a session-specific secret key, thus increasing the system's resistance to replay and key-compromise attacks. Figure 4 shows the outcome of the preprocessing and extraction of features of the fingerprint image.

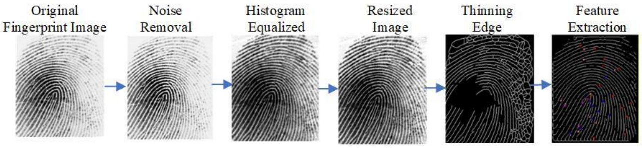


Figure 4. Preprocessing and feature extraction result

3.1.2 Master key generation

The integration of the user attributes and a password generates the master key. The user-provided password is first fetched from the input field and converted to a hexadecimal form. This string is hashed with SHA-512. Simultaneously, the user attributes typed by the user are also converted to their hexadecimal value in the same way. The user attributes string is finally concatenated with the hashed password to create a unique master key used to securely perform cryptographic operations.

3.1.3 Secret key generation

The last step involves the generation of the secret key by the proposed system using the fingerprint feature that has been extracted, together with the master key that was obtained earlier. The two parts are then joined into a single string and fed into a modified version of the SHA-512 hashing algorithm. The product of this hashing algorithm is the final secret key, which is unique, resistant, and immutable to cryptanalytic attacks. The resulting secret key is then shown in the system interface and used as the main component in securing further cryptographic operations.

3.2 Key exchange using Rivest Shamir Adelman

To guarantee the safety of the communication process, the suggested system makes use of the RSA algorithm to exchange the keys, which is supplemented with a six-dimensional hyperchaotic system to increase the level of randomness in the parameters generation.

$$\dot{x}_1 = \alpha(1 - \beta|x_6|)x_2 - ax_1 \quad (2)$$

$$\dot{x}_2 = cx_1 + dx_2 - x_1x_3 + x_5 \quad (3)$$

$$\dot{x}_3 = -bx_1 + x_1^2 \quad (4)$$

$$\dot{x}_4 = ex_2 + fx_4 \quad (5)$$

$$\dot{x}_5 = -rx_1 - kx_5 \quad (6)$$

$$\dot{x}_6 = -x_2 \quad (7)$$

The mentioned chaotic system consists of six equations, namely, Eqs. (2)-(7), which contain state variables (x_1, x_2, x_3, x_4, x_5, and x_6) and system parameters (α, β, a, b, c, d, e, f, r, and k) [23].

Firstly, the 6D system is used to generate chaotic sequences based on the initial conditions and control parameters provided. These sequences are then normalized, rounded, and converted to integers. Next, the prime numbers among these generated numbers are identified, and RSA key components are created using these primes. Specifically, two prime pairs are selected to generate the public and private key parameters. Each pair is used to compute the Euler totient function, which helps determine the correct modular inverse. After setting the RSA parameters, the secret key from the previous step is encrypted using the public key. All parts of the secret key are converted into hexadecimal and decimal formats, and modular exponentiation is applied to secure the key exchange. The encrypted segments become the RSA ciphertext, which is stored and transmitted, while the private key parameters are securely kept at the receiver's end, as shown in Figure 5, This approach combines the predictability of chaotic systems with the strength of RSA to enhance resistance against cryptanalytic and brute-force attacks.

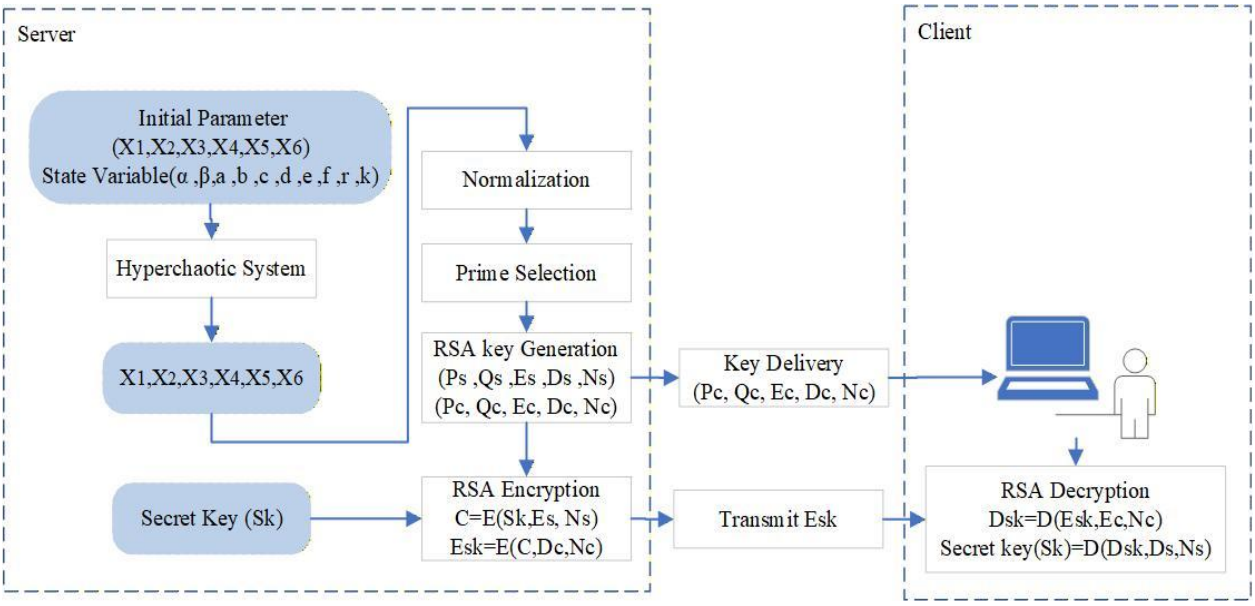


Figure 5. Proposed key exchange

3.3 Premutation step (confusion step)

At this point, the redistribution of bits is done through a 6D hyper-chaotic system, in which the rows of the database are not correlated, thus disconnecting the connection between the data, which are frequently repeated because of the repetition of the data elements (names and numbers).

3.4 Encryption algorithm

Two fundamental algorithms are used in the stream cipher as part of the encryption technique. The RC5 algorithm is used in the first technique, and the ChaCha algorithm is used in the second. With respect to cryptographic parameters, the RC5 algorithm was set at 12 rounds, a relatively standard setting in lightweight cryptography implementation that offers a realistic tradeoff between the level of security and the cost of computation. In the same fashion, the ChaCha parameters were chosen according to typical literature recommendations so that there is enough diffusion and resistance against all known cryptanalytic attacks, and low computational overhead, such that encryption of large databases is feasible.

3.4.1 RC5 stream cipher (diffusion step)

Sensitive data is encrypted, and the encrypted data is obtained by using the secret key that is supplied from the server as a seed to create a sequence of keys.

The RC5 symmetric block cipher algorithm was used to provide a secure and computationally efficient encryption layer for biometric data. The encryption process begins with initializing the RC5 parameters, where the word size (w) is defined as 32 bits, the number of rounds is 12, and the key length is 16 bytes. The constants P and Q are derived from the mathematical values of the natural logarithm base (e = 2.718281828) and the golden ratio (φ = 1.618033988), respectively, to enhance randomness during the key expansion phase. A sub-key array is generated, producing a table of 26 words that serves as the foundation for the round-based encryption process. The algorithm works on files with loaded data of 512 bits of hexadecimal type. The plaintext pair input of encryption is broken down into two 64-bit words that make up each segment. The encryption algorithm employs modular arithmetic, XOR, and circular shift bits by processing the two-word blocks in each round (twelve rounds) to guarantee a high level of diffusion and confusion. All the encryption and decryption procedures are implemented with 64-bit unsigned integer arithmetic to provide numerical accuracy and consistency. This encryption module is an RC5-based block that is used as a part of the proposed hybrid cryptographic architecture, in which features derived with the help of biometrics are used to create and dynamically manage encryption keys. The proposed framework, which integrates symmetric encryptions using RC5 with a biometric-based key generation, is lightweight and highly secure, and thus it would be ideal in secure communication and protection of data in the resource-constrained setting, including IoT and cloud-assisted systems.

3.4.2 ChaCha stream cipher (diffusion step)

The secret key dispatched by the server is used as a seed to create a sequence of keys, which is used in encrypting the existing database.

3.5 Saved encryption data

At this level, the encrypted information will be stored by assigning certain symbols, which will be the order of the record in the database. Using a 6D Hyperchaotic System, it is produced in a way that makes this data encrypted and does not have the same order as the database being original.

4. EXPERIMENTAL RESULTS

The experiment was carried out in a controlled computing environment that had an Intel Core i7 processor, 16GB of RAM, and MATLAB R2024a. The assessment was done to assess the level of security, computation speed, and scalability against traditional cryptographic models. To determine the effectiveness and efficiency of the proposed hybrid cryptographic technique, a sequence of experimental tests was carried out based on real local data of biometric images of the fingerprints of the users. The fingerprint image is scanned with 2 megapixels and 500 dpi quality with a 280 MHz CPU fingerprint scanner (ZK9500 USB Fingerprint Scanner). The dataset of fingerprints employed in the present study is based on the images of 60 authorized users who were recruited to participate in the study voluntarily. Informed consent was given by all the participants to use their fingerprint data on the basis of the research only, and the dataset was anonymized to avoid the possibility of revealing personal identities. Biometric classification and learning-based training were not applied to the fingerprint images, but they were used only in minutiae extraction and dynamic key derivation. Consequently, the experimental protocol did not have to undergo training-testing partitioning. This data is a collection of 1200 thumb fingerprints of 60 different users; each user has ten fingerprint images on the right and 10 fingerprint images on the left. Figure 6 shows the fingerprint image of the local data.

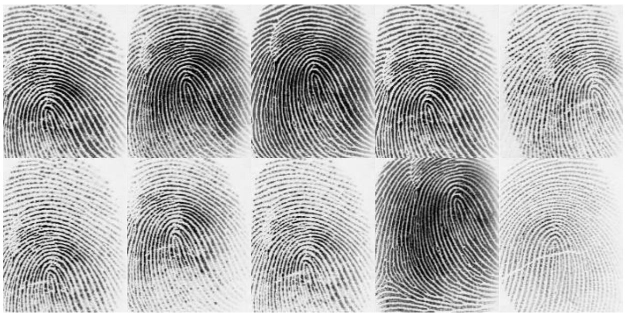
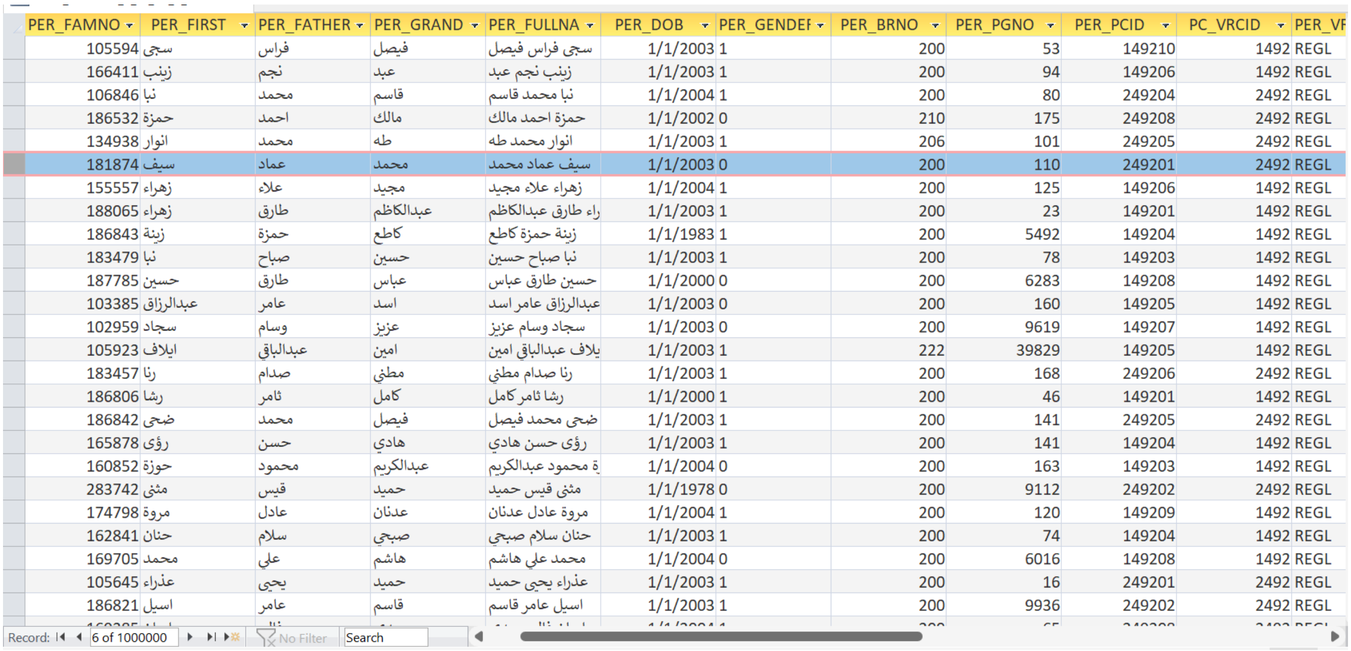


Figure 6. Fingerprint images of the local dataset for the left thumb



PER_FAMNO	PER_FIRST	PER_FATHER	PER_GRAND	PER_FULLNA	PER_DOB	PER_GENDEI	PER_BRNO	PER_PGNO	PER_PCID	PC_VRCID	PER_VI
105594	سجى	فراس	فيصل	سجى فراس فيصل	1/1/2003	1	200	53	149210	1492	REGL
166411	زينب	نجم	عبد	زينب نجم عبد	1/1/2003	1	200	94	149206	1492	REGL
106846	نبا	محمد	قاسم	نبا محمد قاسم	1/1/2004	1	200	80	249204	2492	REGL
186532	حمزة	احمد	مالك	حمزة احمد مالك	1/1/2002	0	210	175	249208	2492	REGL
134938	انوار	محمد	طه	انوار محمد طه	1/1/2003	1	206	101	249205	2492	REGL
181874	سيف	عماد	محمد	سيف عماد محمد	1/1/2003	0	200	110	249201	2492	REGL
155557	زهراء	علاء	مجيد	زهراء علاء مجيد	1/1/2004	1	200	125	149206	1492	REGL
188065	زهراء	طارق	عبدالكاظم	راء طارق عبدالكاظم	1/1/2003	1	200	23	149201	1492	REGL
186843	زينة	حمزة	كاطع	زينة حمزة كاطع	1/1/1983	1	200	5492	149204	1492	REGL
183479	نبا	صباح	حسين	نبا صباح حسين	1/1/2003	1	200	78	149203	1492	REGL
187785	حسين	طارق	عباس	حسين طارق عباس	1/1/2000	0	200	6283	149208	1492	REGL
103385	عبدالرزاق	عامر	اسد	عبدالرزاق عامر اسد	1/1/2003	0	200	160	149205	1492	REGL
102959	سجاد	وسام	عزيز	سجاد وسام عزيز	1/1/2003	0	200	9619	149207	1492	REGL
105923	ايلاف	عبدالباقي	امين	يلاف عبدالباقي امين	1/1/2003	1	222	39829	149205	1492	REGL
183457	رنا	صدام	مطني	رنا صدام مطني	1/1/2003	1	200	168	249206	2492	REGL
186806	رشا	ثامر	كامل	رشا ثامر كامل	1/1/2000	1	200	46	149201	1492	REGL
186842	ضحى	محمد	فيصل	ضحى محمد فيصل	1/1/2003	1	200	141	249205	2492	REGL
165878	رؤى	حسن	هادي	رؤى حسن هادي	1/1/2003	1	200	141	149204	1492	REGL
160852	حوزة	محمود	عبدالكريم	ة محمود عبدالكريم	1/1/2004	0	200	163	149203	1492	REGL
283742	مثنى	قيس	حميد	مثنى قيس حميد	1/1/1978	0	200	9112	249202	2492	REGL
174798	مروة	عادل	عدنان	مروة عادل عدنان	1/1/2004	1	200	120	149209	1492	REGL
162841	حنان	سلام	صبحي	حنان سلام صبحي	1/1/2003	1	200	74	149204	1492	REGL
169705	محمد	علي	هاشم	محمد علي هاشم	1/1/2004	0	200	6016	149208	1492	REGL
105645	عذراء	يحيى	حميد	عذراء يحيى حميد	1/1/2003	1	200	16	249201	2492	REGL
186821	اسيل	عامر	قاسم	اسيل عامر قاسم	1/1/2003	1	200	9936	249202	2492	REGL

Figure 7. Sample of Iraqi voter registration in the parliamentary elections database

The database of Iraqi voter registration in the parliamentary elections is used to evaluate the effectiveness and efficiency of the proposed hybrid cryptographic method. The size of this database is 128 MB of 1 million records, each record contains information about one voter (PER_ID: voter ID, PER_FAMNO: voter family number, PER_FIRST: voter first name, PER_FATHER: voter middle name, PER_GRAND: voter last name, PER_FULLNAME: voter full name, PER_DOB: voter date of birth, PER_GENDER: voter gender, PER_BRNO: voter electoral branch number, PER_PGNO:

voter electoral page number, PER_PCID: voter electoral center ID, PC_VRCID: ID of the district area to which the polling station belongs, PER_VRTYPE_2013: type of voter registration according to the 2013 register). Figure 7 shows a sample of Iraqi voter registration in the parliamentary elections database. Each record in the election database is individually processed, with all the cells of a single record concatenated into a single cell to ensure uniformity and data integrity during encryption, as shown in Table 1. Specifically, every row is retrieved and converted into its corresponding hexadecimal representation, after which appropriate padding is applied to achieve a standardized length of 512 hexadecimal digits, as shown in Table 2. Every row of the database stores data regarding a single voter, and this preprocessing step is done for all the records of the database in a systematic manner that ensures employment of a uniform and safe encryption process. To ensure the effectiveness and strength of the presented hybrid cryptographic setup, some experimental trials were performed with the focus on the key generating process, key exchange, encryption/decryption speed, and system efficiency.

Table 1. Sample of Iraqi voter registration in the parliamentary elections database after record concatenation

Record No.	Concatenated Data
1	10033921,105594,”53,1,149210,1492,"00168",200,"1",00:00:00 2003/1/1,"سجى فراس فيصل","فيصل","فراس","سجى",”REGL”
2	10033923,166411,”94,1,149206,1492,"م0627",200,"1",00:00:00 2003/1/1,"زينب نجم عبد","عبد","نجم","زينب",”REGL”
3	10033926,106846,”80,1,249204,2492,"م0278",200,"1",00:00:00 2004/1/1,"نبا محمد قاسم","قاسم","محمد","نبا",”REGL”
4	10033927,186532,”175,977168,249208,2492,"م0161",210,"0",00:00:00 2002/1/1,"حمزة احمد مالك","مالك","احمد","حمزة",”REGL”
5	10033929,134938,”101,1,249205,2492,"00635",206,"1",00:00:00 2003/1/1,"انوار محمد طه","طه","محمد","انوار ",”REGL”
6	10033933,181874,”110,1,249201,2492,"00833",200,"0",00:00:00 2003/1/1,"سيف عماد محمد","محمد","عماد","سيف",”REGL”
7	10033934,155557,”125,1,149206,1492,"00756",200,"1",00:00:00 2004/1/1,"زهراء علاء مجيد","مجيد","علاء","زهراء",”REGL”
8	10033937,188065,” 2003/1/1,"زهراء طارق عبدالكاظم","عبدالكاظم","طارق","زهراء 23,709288,149201,1492,"00186",200,"1",00:00:00,”REGL”
9	10033940,186843,”5492,44614,149204,1492,"00028",200,"1",00:00:00 1983/1/1,"زينة حمزة كاطع","كاطع","حمزة","زينة",”REGL”
10	10033942,183479,”78,1,149203,1492,"00961",200,"1",00:00:00 2003/1/1,"نبا صباح حسين","حسين","صباح","نبا",”REGL”

Table 2. Sample of Iraqi voter registration in the parliamentary elections database after processing

Record No.	Data in Hexadecimal
1	03103003003303303903203102C03103003503503903402C02263362C64902202C02264163162763302202C02264164A63 564402202C02263362C64902064163162763302064164A63564402202C03102F03102F03203003003302003003003A0300 3003A03003002C02203102202C03203003002C02203003003103603802202C03503302C03102C03103403903203103002 C03103403903202C02205204504704C022000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000
2	03103003003303303903203302C03103603603403103102C02263264A64662802202C02264662C64502202C02263962862 F02202C02263264A64662802064662C64502063962862F02202C03102F03102F03203003003302003003003A03003003A 03003002C02203102202C03203003002C02203003603203764502202C03903402C03102C03103403903203003602C03103 403903202C02205204504704C0220000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000
3	03103003003303303903203602C03103003603803403602C02264662862702202C02264562D64562F02202C02264262763 364502202C02264662862702064562D64562F02064262763364502202C03102F03102F03203003003402003003003A0300 3003A03003002C02203102202C03203003002C02203003203703864502202C03803002C03102C03203403903203003402 C03203403903202C02205204504704C022000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000
4	03103003003303303903203702C03103803603503303202C02262D64563262902202C02262762D64562F02202C02264562 764464302202C02262D64563262902062762D64562F02064562764464302202C03102F03102F03203003003202003003003 3A03003003A03003002C02203002202C03203103002C02203003103603164502202C03103703502C03903703703103603803 02C03203403”0320’003802C03203403903202C02205204504704C02200000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000
5	03103003003303303903203902C03103303403903303802C02262764664862763102202C02264562D64562F02202C02263 764702202C02262764664862763102064562D64562F02063764702202C03102F03102F03203003003302003003003A0300 3003A03003002C02203102202C03203003602C02203003003603303502202C03103003102C03102C032034039032030035 02C03203403903202C02205204504704C0220000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000
6	03103003003303303903303302C03103803103803703402C02263364A64102202C02263964562762F02202C02264562D64 562F02202C02263364A64102063964562762F02064562D64562F02202C03102F03102F03203003003302003003003A0300 3003A03003002C02203002202C03203003002C02203003003803303302202C03103103002C03102C032034039032030031 02C03203403903202C02205204504704C0220000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000
7	03103003003303303903303402C03103503503503503702C02263264763162762102202C02263964462762102202C022645 62C64A62F02202C02263264763162762102063964462762102064562C64A62F02202C03102F03102F03203003003402003 003003A03003003A03003002C02203102202C03203003002C02203003003703503602202C03103203502C03102C031034

	03903203003602C03103403903202C02205204504704C0220000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
8	03103003003303303903303702C03103803803003603502C02263264763162762102202C02263762763164202202C02263962862F62764464362763864502202C02263264763162762102063762763164202063962862F62764464362763864502202C03102F03102F03203003003302003003003A03003003A03003002C02203102202C03203003002C02203003003103803602202C03203302C03703003903203803802C03103403903203003102C03103403903202C02205204504704C022000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
9	03103003003303303903403002C03103803603803403302C02263264A64662902202C02262D64563262902202C02264362763763902202C02263264A64662902062D64563262902064362763763902202C03102F03102F03103903803302003003003A03003003A03003002C02203102202C03203003002C02203003003003203802202C03503403903202C03403403603103402C03103403903203003402C03103403903202C02205204504704C0220000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
10	03103003003303303903403202C03103803303403703902C02264662862702202C02263562862762D02202C02262D63364A64602202C02264662862702063562862762D02062D63364A64602202C03102F03102F03203003003302003003003A03003003A03003002C02203102202C03203003002C02203003003903603102202C03703802C03102C03103403903203003302C03103403903202C02205204504704C0220000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

4.1 Secret key evaluation

In order to manage and enhance the control system towards accessing the database, biometric fingerprint data of authorized personnel is added to their respective features to build a safe and sound authentication process. A one-way secret key is generated using a SHA-512 to encrypt and decrypt the data to provide confidentiality and integrity. The hash operation is irreversible, which improves the level of security of confidential information and provides brute force protection. The output secret keys were severely tested in the form of standardized statistical and cryptographic tests to ascertain their randomness, uniqueness, and unpredictability. The cryptographic strength of the proposed key gen mechanism was estimated, in particular, with the help of the statistical test suite, hamming distance analysis, and entropy measures that are offered by the National Institute of Standards and Technology (NIST). The NIST tests were used to ensure that the keys generated were statistically uniform in a number of samples, and calculated the minimum, average, and maximum results that are illustrated in Table 3. It is worth noting that the acceptance test of the NIST statistical tests is not only a consideration of the lowest p-value that is observed in all the sequences that are generated. A test is deemed to pass according to the NIST SP 800-22 guidelines when most of the sequences under examination result in a p-value exceeding the designated level of significance (0.01). Sometimes the low p-values can be because of the fluctuations of randomness, particularly when multiple sequences and multiple tests have been used. In the presented findings, a few of the minimum p-values are lower than the threshold, but the average and maximum p-values of these tests are above the 0.01 threshold, which means that the generated keys can be considered to meet the statistical randomness criteria in general. Thus, it can be stated that the offered method will pass the NIST randomness test successfully.

The Hamming distance test is applied to test the variation of bit-level between generated secret keys. The greater the Hamming distance, the greater the diffusion properties and the lesser the similarity between keys, which are critical in preventing key correlation and differential attacks. The results of Hamming distance are given in Table 4, which shows the effectiveness of the proposed key generation mechanism in generating diverse and unpredictable secret keys with respect to the key size.

Table 3. Results of the National Institute of Standards and Technology (NIST) statistical tests for the generated secret key

Test Type	The P-Value of the Proposed Method			Status
	Min	Average	Max	
Frequency	0.0352	0.1161	0.1000	pass
Block Frequency	0.0050	0.1348	0.0121	pass
Run Test	0.0008	0.0439	0.1510	pass
The Longest Run of Ones	0.0250	0.0725	0.0322	pass
Fast Fourier Transform	0.0690	0.0612	0.0556	pass
Overlapping Template Matching	0.0821	0.0258	0.2524	Pass
Approximate Entropy	0.0450	0.0153	0.1847	pass
Cumulative Sum	0.0458	0.0852	0.2216	pass
Linear Complexity	0.0266	0.0910	0.0372	pass
Random Excursions	0.0082	0.1131	0.0965	pass
Random Excursions Variant	0.0574	0.0028	0.0052	pass
Rank	0.0081	0.0645	0.2955	pass
Serial	0.0830	0.1399	0.2295	pass
Universal Statistical	0.0274	0.1068	0.1832	pass

Table 4. Hamming distance test for secret key

Test Case	Key Pairs	Hamming Distance
1	512	287
2	640	334
3	768	432
4	896	489
5	1024	549

Table 5. Entropy evaluation for generated secret keys

Key Length (bit)	Entropy Value (bit)
800	7.302384
1024	7.351416
1600	7.394566
2048	7.379827
3200	7.409832
4096	7.448632
5000	7.539021
6000	7.493419
7000	7.639823
8192	7.7089327

The entropy analysis is used to measure the randomness and unpredictability of the obtained secret keys. An increase in entropy values represents increased resistance to statistical and brute-force attacks since they represent a more uniform distribution of key bits. Table 5 gives the values of entropy of various key lengths, indicating a steady increase in the values with the increase in key size. The fact that the entropy values are close to the ideal value proves that the suggested key generation mechanism generates very random and secure secret keys, which can be used in cryptography applications.

4.2 Key exchange performance and security analysis

The effectiveness and safety of the proposed key exchange mechanism based on a 6D hyper chaotic system in RAS were thoroughly tested to determine its effectiveness and strength in practice. Computational time was also analyzed, and the results were summarized in Table 6. The offered approach demonstrated the average key exchange time of 1.711 seconds, which proves its appropriateness regarding lightweight and time-sensitive applications.

Table 6. Performance evaluation of the key exchange process

Parameter	Measured Value
Key Generation Time	1.711929898 s
RSA Encryption Time	2.853216496 s
RSA Decryption Time	3.164314111s
Average Key Exchange Time	2.576486835 s
Throughput	161.804417 KB/s

Note: RSA = Rivest Shamir Adelman.

The resistance to common attack vectors, which include interception, replay, and key-compromise attacks, was also analyzed as a major exchange. The combination of ABE and biometric-based session keys made key exchange dynamic, user-specific, and session-specific key exchange, which boosted confidentiality and scalability. Table 7 shows that Experimental results indicated that the proposed technique exhibits low computational overhead and still, a high degree of cryptographic strength and data protection.

Table 7. Security evaluation of the proposed key exchange mechanism

Attack Type	Evaluation Metric	Result
Interception Attack	Key Recovery Probability	$< 10^{-8}$
Replay Attack	Session Reuse Detection Rate	100%
Key Compromise Attack	Average Key Lifetime	Session (non-1 reusable)
Differential Attack	Key Variation Rate (Hamming %)	52.19% – 56.25% (Mean = 54.54%, SD ≈ 1.70%)

The security analysis proves that the proposed key exchange protocol is effective against interception and replay attacks. The dynamic key generation is based on the session, which means that despite the publicity of one of the session keys, further communications are safe.

4.3 Encryption and decryption performance evaluation

The effectiveness of the proposed cryptographic model using RC5 and ChaCha was discussed in detail with the help of various quantitative indicators, such as encryption and decryption time, entropy, and correlation coefficient. A combination of these parameters is the measure of the computational efficiency, randomness, and statistical resistance of the scheme. Encryption and decryption times were observed on various data sizes to establish the efficiency of processing. The proposed system, as illustrated in Table 8, has a low latency in encryption and decryption, and thus proves to be suitable in real-time and lightweight applications.

Entropy analysis was done to further study the statistical power of the ciphertexts. The entropy values were close to an ideal value of 8 bits/symbol, which proved the high level of randomness as well as unpredictability, as in Table 9.

Table 8. Encryption and decryption time evaluation

Data Size (KB)	RC5 Encryption Time (ms)	RC5 Decryption Time (ms)	RC5 Throughput (KB/s)	ChaCha Encryption Time (ms)	ChaCha Decryption Time (ms)	ChaCha Throughput (KB/s)
10	10.62805047	8.502440377	0.940906333	9.884086938	7.90726955	1.01172724
20	23.38170154	18.70536123	0.855369741	21.74498243	17.39598594	0.91975241
30	37.93412063	30.3472965	0.790844746	35.27873218	28.22298575	0.850370695

Table 9. Entropy analysis for row data and encrypted data

Data Sample	Entropy for Row Data (bit)	Entropy for Encrypted Data (bit)
10	5.650831962	7.781387894
20	5.435281298	7.455706299
30	5.386750543	7.331728525
Average	5.490954601	7.522940906

4.4 Comparative analysis

In order to measure the performance and unique merits of the proposed lightweight hybrid cryptography scheme, a comparative analysis has been done against the recent state-of-the-art encryption methods available in the literature. This comparison is based on several major points, such as the key generation techniques, the incorporation of biometric properties, supporting attribute-based access control ABE, the kind of encryption or cryptosystem implemented, and interesting insights in terms of security and performance. Table 10 provides an organized description of these studies with emphasis on the distinctive advantages of the proposed approach in the form of session-dependent dynamical generation of keys, hybrid cryptosystem execution, and increased security aspects, without compromising computational efficiency, to be applicable in the process of practical implementation of the proposed methodology into practice in the current IoT and cloud-assisted environments.

Table 10. Comparative evaluation of state-of-the-art encryption techniques and the proposed lightweight framework

Study	Key Generation Method	Biometric Integration	Attribute-Based Access	Encryption / Cryptosystem	Observations / Comparison Points
[22]	Pseudorandom generation using a 2D chaotic system	No	No	N/A	High randomness keys, not user-specific
[23]	Hyperchaotic maps for key generation	No	No	N/A	Strong entropy, not tied to biometrics or attributes
[26]	Hybrid lightweight cryptography	No	Yes, ABE	Lightweight symmetric + Asymmetric	Strong ABE support, no biometric integration
[14]	Key sharing via ABE	No	Yes	Symmetric encryption	Secure access control lacks biometric features
[18]	RSA key derived from password and fingerprint	Fingerprint + Password	No	RSA	Similar biometric-based key, lacks ABE, static key
[11]	Feature extraction from fingerprint	Minutiae extraction	No	N/A	Focus on biometric feature extraction, not encryption
[1]	Lightweight cryptosystem for IoT	No	No	Custom lightweight cipher	Focus on IoT efficiency, lacks ABE and biometric integration
[20]	Hybrid cryptography + RSA	No	No	Hybrid symmetric + Asymmetric	Cloud security-oriented, no biometrics
[12]	Contactless fingerprint key generation	Fingerprint	No	N/A	Advanced biometric extraction, not combined with attributes
[8]	Chaotic maps + A2C algorithm	No	No	N/A	Dynamic key generation, good for security, lacks biometric binding
[2]	DNA-RC4 lightweight encryption	No	No	DNA-RC4	Efficient lightweight encryption, no hybrid key derivation
Proposed Work	SHA-512 + Master key + Dynamic session key	Fingerprint minutiae	User attributes (name, email, phone, etc.)	RC5 and ChaCha	Session-dependent keys, hybrid ABE integration, dynamic and secure key generation

Note: ABE = Attribute-Based Encryption; RSA = Rivest Shamir Adelman.

In general, these results verify that the proposed encryption model using RC5 or ChaCha can guarantee a good level of data confidentiality, a high level of statistical randomness, and a low level of computation overhead, which makes it an efficient and secure cryptography implementation in the modern context.

5. DISCUSSION

These experimental findings validate the fact that user attributes combined with fingerprint-derived minutiae allow the creation of session-specific cryptographic keys that have high randomness and diversity characteristics. The results of the observed entropy and statistical randomness demonstrate that derived keys are unpredictable enough to resist brute-force attack and exploitation of key patterns. Moreover, the inconsistency of the Hamming distance of the generated keys shows successful key diversity that will mitigate key reuse and improve resistance to replay and key-compromise attacks.

System-wise, the proposed hybrid solution has a tradeoff between the level of security and the level of computational efficiency. Lightweight symmetric encryption to protect large voter records has significantly lower computational costs than the case of fully asymmetric encryption of bulk data, and the suggested key exchange protocol allows secure distribution of session keys with minimal introduction of latency overhead. These features facilitate the extension of the framework to large voter databases where responsiveness and data confidentiality are very important. As per the comparative analysis conducted in Table 10, most of the current techniques consider isolated features of data security, like biometric authentication, ABE, without providing a solution to an integrated solution, which is a combination of fine-grained access control with dynamic identity-bound key generation. The suggested framework, on the other hand, combines attribute-based policy enforcement, biometric-generated session keys, and lightweight encryption algorithms in one architecture. This combination renders it more scalable and practically applicable than other related works, especially in election database security, where access control, authentication, and useful bulk encryption have to co-exist. In spite of such positive outcomes, there are several limitations to be considered. The biometric data set was sampled locally and might not be quite representative of the variations in large public datasets. As well, the existing testing is on database protection and key management, as opposed to end-to-end deployment over a full election infrastructure. Although the empirical randomness and attack-oriented analysis support the security analysis, the theoretical basis should be enhanced in the future by offering more formal security arguments to the component of ABE and the key exchange mechanism. Regarding its practical implication, the suggested framework can be implemented as a protection layer to cloud- and IoT-assisted election settings, voter registration databases. The attribute-based policy element aids role-based management and auditing, whereas biometric binding enhances identity assurance of the privileged access. Future research can involve assessment using larger, more heterogeneous biometric data, exploration of privacy-preserving template protection schemes, and practical research in experimental election systems to further confirm the viability of deploying the systems in the real world.

6. CONCLUSIONS

The paper introduced a minimalist hybrid security framework for a voter registration database protection based on ABE, biometric authentication, and dynamic generation of session keys. The proposed solution can secure access control and make digital elections resistant to most types of security risks by linking the cryptographic keys to user attributes and features based on fingerprints. As was experimentally shown, the suggested framework offers high security properties at the expense of computational efficiency, which is appropriate when large-scale databases are considered. Lightweight encryption is integrated with secure key exchange mechanisms, and this allows the deployment of the application in practice, where performance and scalability are critical. Although these are the benefits, there are some limitations to the present study. The biometric test was performed on a dataset collected in the region, and the framework was evaluated at the database security level, mainly, and not at the entire end-to-end election infrastructure. Future work will involve the scaling of the framework to bigger and more varied biometric data, formal security proofs of the ABE and key exchange components, and testing whether the framework can be deployed in practice in actual election systems. On the whole, the proposed framework suggests a convenient and expandable way of making voter databases more secure and leads to the creation of more secure digital systems of governance.

REFERENCES

[1] Hazzaa, F., Hasan, M.M., Qashou, A., Yousef, S. (2024). A new lightweight cryptosystem for IoT in smart city environments. Mesopotamian Journal of CyberSecurity, 4(3): 46-58. https://doi.org/10.58496/MJCS/2024/015

[2] Fanfakh, A., Idrees, A.K. (2025). A new lightweight encryption method based on the DNA-RC4 substitution for resource-constrained IoT devices. Iraqi Journal for Computer Science and Mathematics, 6(3): 22. https://doi.org/10.52866/2788-7421.1287

[3] El Bourakkadi, H., Chemlal, A., Tabti, H., Kattass, M., Jarjar, A., Benazzi, A. (2024). Enhanced color image encryption utilizing a novel Vigenere method with pseudorandom affine functions. Acadlore Transactions on AI and Machine Learning, 3(1): 36-56. https://doi.org/10.56578/ataiml030104

[4] Albak, L.H., Hamdany, A.H.S. (2025). Solution evaluation to enhance cloud computing security: Challenges and solutions. International Journal of Safety and Security Engineering, 15(9): 1901-1907. https://doi.org/10.18280/ijsse.150913

[5] Ashraf, Z., Sohail, A., Yousaf, M. (2023). Robust and lightweight symmetric key exchange algorithm for next-generation IoE. Internet of Things, 22: 100703. https://doi.org/10.1016/j.iot.2023.100703

[6] Salah, O., El-Sawy, A., Taha, M. (2023). A hybrid algorithm for enhancement of the data security during network transmission based on RSA and DH. International Journal of Intelligent Engineering Systems, 16(3): 614-624. https://doi.org/10.22266/ijies2023.0630.49

[7] Mohanraj, T., Santhosh, R. (2022). Hybrid encryption algorithm for big data security in the Hadoop distributed file system. Computer-Assisted Methods in Engineering and Science, 29(1-2): 33-48. https://doi.org/10.24423/cames.375

[8] Mahdi, A.A., Hoobi, M.M. (2025). Robust and efficient methods for key generation using chaotic maps and A2C algorithm. Mesopotamian Journal of CyberSecurity, 5(1): 301-318. https://doi.org/10.58496/MJCS/2025/019

[9] Hashmi, S.S., Arif, M.A.A., Mohammad, A.K., Atheeq, C., Chinapaga, R. (2023). Advancing secure mobile cloud computing: A Chaotic Maps-based password key agreement protocol. Ingenierie des Systemes d'Information, 28(6): 1669-1678. https://doi.org/10.18280/isi.280625

[10] Socheat, S., Wang, T. (2020). Fingerprint enhancement, minutiae extraction and matching techniques. Journal of Computer and Communications, 8(5): 55-74. https://doi.org/10.4236/jcc.2020.85003

[11] Situmorang, B.H., Andrea, D. (2023). Identification of biometrics using fingerprint minutiae extraction based on crossing number method. KOMPUTASI: Jurnal Ilmiah Ilmu Komputer dan Matematika, 20(1): 71-80. https://doi.org/10.33751/komputasi.v20i1.6814

[12] Siddiqui, M., Iqbal, S., AlHaqbani, B., AlShammari, B., Khan, T., Razzak, I. (2024). A robust algorithm for contactless fingerprint enhancement and matching. In 2024 International Conference on Digital Image Computing: Techniques and Applications (DICTA), Perth, Australia, pp. 214-220. https://doi.org/10.1109/DICTA63115.2024.00041

[13] Osorio-Roig, D., González-Soler, L.J., Rathgeb, C., Busch, C. (2024). Privacy-preserving multi-biometric indexing based on frequent binary patterns. IEEE Transactions on Information Forensics and Security, 19: 4835-4850. https://doi.org/10.1109/TIFS.2024.3386310

[14] Kaliyaperumal, K., Sammy, F. (2022). An efficient key generation scheme for secure sharing of patients health records using attribute based encryption. In 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, pp. 1-6. https://doi.org/10.1109/IC3IOT53935.2022.9767726

[15] Ali, G., Mijwil, M.M., Buruga, B.A., Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech. Iraqi Journal for Computer Science and Mathematics, 5(3): 45-91. https://doi.org/10.52866/ijcsm.2024.05.03.004

[16] Li, X. (2023). Data protection of accounting information based on big data and cloud computing. Scientific Programming, 2023(1): 8387441. https://doi.org/10.1155/2023/8387441

[17] Pothireddy, S., Peddisetty, N., Yellamma, P., Botta, G., Gottipati, K.N. (2024). Data security in cloud environment by using hybrid encryption technique: A comprehensive study on enhancing confidentiality and reliability. International Journal of Intelligent Engineering Systems, 17(2): 159-170. https://doi.org/10.22266/ijies2024.0430.14

[18] Suresh, K., Pal, R., Balasundaram, S.R. (2022). Two-factor-based RSA key generation from fingerprint biometrics and password for secure communication. Complex and Intelligent Systems, 8(4): 3247-3261. https://doi.org/10.1007/s40747-022-00663-3

[19] Majeed, S.H. (2025). A cyber security model using gaussian noise for text encryption and decryption algorithm. JOIV International Journal on Informatics Visualization, 9(5): 1871-1880. https://doi.org/10.62527/joiv.9.5.2925

[20] Koppaka, A.K., Lakshmi, V.N. (2024). An efficient and secured big data storage in a cloud-based environment using hybrid cryptography algorithm and Rivest, Shamir, Adleman algorithm. International Journal of Intelligent

Engineering Systems, 17(1): 525-535. https://doi.org/10.22266/ijies2024.0229.45

[21] Veerabadrappa, K., Naikodi, C.B., Venkataswamy, S.B., Narayanaswamy, H.K. (2024). Elliptic curve cryptography and password based key derivation function with advanced encryption standard method for cloud data security. International Journal of Intelligent Engineering Systems, 17(6): 814-823. https://doi.org/10.22266/ijies2024.1231.62

[22] Akif, O.Z., Ali, S., Ali, R.S., Farhan, A.K. (2021). A new pseudorandom bits generator based on a 2D-chaotic system and diffusion property. Bulletin of Electrical Engineering and Informatics, 10(3): 1580-1588. https://doi.org/10.11591/eei.v10i3.2610

[23] Yu, F., Qian, S., Chen, X., Huang, Y., Cai, S., Jin, J., Du, S. (2021). Chaos-based engineering applications with a 6D memristive multistable hyperchaotic system and a 2D SF-SIMM hyperchaotic map. Complexity, 2021(1): 6683284. https://doi.org/10.1155/2021/6683284

[24] Vekariya, V., Joshi, M., Dikshit, S. (2024). Multi-biometric fusion for enhanced human authentication in information security. Measurement: Sensors, 31: 100973. https://doi.org/10.1016/j.measen.2023.100973

[25] Naregal, K., Kalmani, V. (2023). Cloud security with lightweight ABE on mobile IoT devices. International Journal of Intelligent Engineering Systems, 16(6): 145-157. https://doi.org/10.22266/ijies2023.1231.13

[26] Jammula, M., Vakamulla, V.M., Kondoju, S.K. (2022). Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system. Connection Science, 34(1): 2431-2447. https://doi.org/10.1080/09540091.2022.2124957

[27] Anitha Kumari, K., Kamatchi, T.P., Senthil Prabha, R., Samanthula, B.K. (2023). Hyperelliptic curve Diffie–Hellman-based two-server password-only authenticated key exchange protocol for edge computing systems. IETE Journal of Research, 69(7): 4311-4322. https://doi.org/10.1080/03772063.2021.1951371

NOMENCLATURE

Latin Symbols

CN	crossing number method for fingerprint minutiae detection
$\mathcal{U}$	universal attribute
$\mathcal{A}$	user attributes
MSK	master key generated from attributes and password
SK	session key generated dynamically per session
PK	public parameters of KP-ABE
M	message (plain text)
CT	cipher text
e	RSA public exponent / chaotic control parameter
f	chaotic system control parameter
k	chaotic system control parameter
KP-ABE	key-policy attribute-based encryption
RC5	lightweight block cipher used in the diffusion layer
SHA-512	cryptographic hash function used in key derivation
w	RC5 word size
r	chaotic system parameter
P	RC5 key schedule constant
Q	RC5 key schedule constant
x_1	state variable of the 6D hyperchaotic system
x_2	state variable of the 6D hyperchaotic system
x_3	state variable of the 6D hyperchaotic system
x_4	state variable of the 6D hyperchaotic system
x_5	state variable of the 6D hyperchaotic system
x_6	state variable of the 6D hyperchaotic system

Greek Symbols

λ	security parameters for KP-ABE
$\mathcal{P}$	access policy used to generate secret key
α	chaotic system parameter
β	chaotic system parameter
θ	fingerprint minutiae orientation angle
φ	golden ratio constant used in cryptographic functions

Subscripts

L	left block in encryption round
R	right block in encryption round
p	prime number (RSA key generation)
i	iteration index
sess	session-specific value
usr	user attribute identifiers

Superscripts

n	iteration number
T	transpose (if used in matrix notation)