Journal of Engineering Research

Volume 8
Issue 3 *issue 3*

Article 22

2024

Securing Body Area Networks with Fingerprint Cryptography and Authentication in MANET

Alaa M. Elbanaa
Tanta University, Faculty of Engineering, alaa138772@f-eng.tanta.edu.eg

Roayat Ismail Abdelfatah
Faculty of Engineering, Tanta University, royat_esmaeel@f-eng.tanta.edu.eg

Mohamed E. Nasr
Faculty of Engineering, Tanta University, mohamed.nasr@f-eng.tanta.edu.eg

Follow this and additional works at: https://digitalcommons.aaru.edu.jo/erjeng

 Part of the Applied Mathematics Commons, Architecture Commons, Biomedical Informatics Commons, Engineering Commons, Health Information Technology Commons, and the Nanotechnology Commons

Recommended Citation

Elbanaa, Alaa M.; Abdelfatah, Roayat Ismail; and Nasr, Mohamed E. (2024) "Securing Body Area Networks with Fingerprint Cryptography and Authentication in MANET," *Journal of Engineering Research*: Vol. 8: Iss. 3, Article 22.
Available at: https://digitalcommons.aaru.edu.jo/erjeng/vol8/iss3/22

This Article is brought to you for free and open access by Arab Journals Platform. It has been accepted for inclusion in Journal of Engineering Research by an authorized editor. The journal is hosted on Digital Commons, an Elsevier platform. For more information, please contact rakan@aaru.edu.jo, marah@aaru.edu.jo, u.murad@aaru.edu.jo.

Securing Body Area Networks with Fingerprint Cryptography and Authentication in MANET

Cover Page Footnote

I would like to thank both editor and reviewer for their promising comments.

This article is available in Journal of Engineering Research: https://digitalcommons.aaru.edu.jo/erjeng/vol8/iss3/22

I. INTRODUCTION

Wireless Body Area Networks (BANs) are instrumental for real-time healthcare monitoring through various multimedia formats such as text, audio, image, and video [1]. This approach offers a nonintrusive and mobile solution for monitoring vital signs and environmental parameters, thus presenting a cost-effective alternative to traditional healthcare systems [2]. BANs consist of interconnected sensors, wearable or implantable, that monitor vital signs and environmental factors [3]. However, there are significant research challenges to address before widespread deployment. These challenges include the limited resources of sensors, necessitating lightweight communication solutions, and ensuring the security and privacy of medical data [4]. Safe sensor networks are crucial to maintain medical data privacy, confidentiality, authentication, and integrity. The lack of security in resource-constrained medical sensor nodes within BANs has impeded the advancement of this technology [5]. Figure 1 illustrates the broad dissemination of Body Area Networks (BANs) and their interaction with the surrounding environment. Patients serve as the source of biomedical data input, which is then transmitted to the internet via a Wireless BAN gateway, which could take the form of a mobile device, laptop, Personal Digital Assistant (PDA), or similar tools [6]. To enhance data security during transmission, robust encryption methods are employed, safeguarding the data's integrity throughout its wireless journey. Additionally, biometric authentication, whether unimodal or multimodal, is utilized to verify and authenticate patients accurately. These biometric identifiers serve as keys in the cryptography stage, fortifying the authentication security process [7].

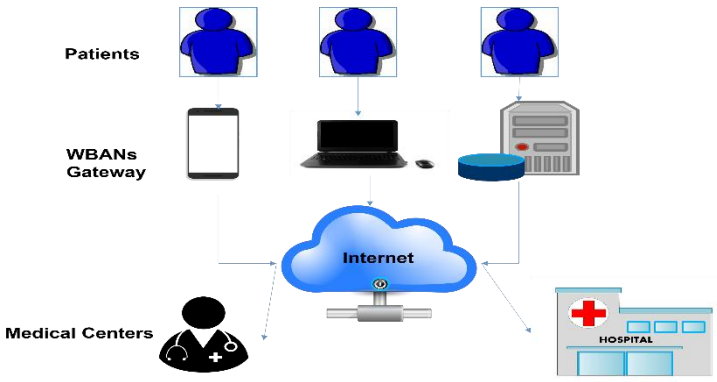

Figure 1. The structure of wireless BAN

Cryptography and authentication play vital roles in securing multimedia healthcare services transmitted wirelessly within Body Area Networks (BANs) [8]. Sensors within BANs typically utilize cryptographic keys to ensure the security of multimedia data communication. While various key management and distribution schemes exist for general wireless sensor networks, they often cannot be directly applied to BANs due to the unique scale and characteristics of biomedical sensors. Consequently, designing an efficient key management and agreement scheme tailored specifically to BANs remains a significant challenge [9].

Mobile Ad-hoc network is a dynamic network composed of mobile wireless nodes that interact with one another without the usage of a centralized authority (device). Devices that connect to the network must be capable not just on data transmission and reception, but on the disorganized administration of all network functions such as packet routing, security, and QOS (Quality of Service). For a variety of security threats, including black holes, wormholes, and fast assaults. MANET characteristics, applications, routing protocols, security objectives, and multiple threats [10].

Securing communication between nodes in a network necessitates reliable key management systems for key generation and distribution, coupled with a secure routing protocol defining the communication path. However, in Mobile Ad hoc Networks (MANETs), the absence of a central server poses a significant challenge for key management due to dynamic changes in network topology and a lack of trust among nodes [11]. MANETs involve mobile nodes functioning as both end terminals and intermediate routers [12].

We operate under the assumption that MANETs are structured into groups, each led by a group leader responsible for key management [13]. Our proposed decentralized key management approach eliminates the need for a Trusted Third Party (TTP). Before joining the network, mutual verification occurs between a new node and the group leader within the suggested key management system. Simultaneously, our secure routing protocol enables authentication of communication parties and intermediary nodes while preserving message integrity [14].

The appeal of Mobile Ad hoc Networks (MANETs) in military applications has grown with advancements in mobile computing and wireless communications [15]. However, their susceptibility to security threats, stemming from open communication channels, node mobility, absence of centralized security services, and lack of prior security associations, makes supporting security-sensitive applications in hostile environments a crucial area of study for MANETs [16, 17]. In high-security MANETs, continuous and

frequent user authentication is vital to prevent unauthorized access or alterations to network resources, especially in environments where device seizure is likely [18, 19].

User authentication in MANETs can be achieved through knowledge factors (e.g., passwords), possession factors (e.g., tokens), and biometric factors. While knowledge and possession factors are straightforward to implement, they may pose challenges in distinguishing genuine users from impostors without a direct link between individuals and their passwords or tokens [20]. Biometric technologies, encompassing fingerprint recognition, iris recognition, face recognition, retina recognition, etc., present potential solutions to address the authentication dilemma [21]. This technology enables the automated and continuous verification or recognition of individuals based on their physiological and behavioral characteristics, eliminating the need for human involvement. Additionally, in MANETs, the presence of Intrusion Detection Systems (IDSs) is crucial for effectively identifying malicious activities and enabling the MANET to respond accordingly [22]. IDSs are categorized as follows: 1) network-based intrusion detection, positioned at the network's gateway to scrutinize all incoming packets; 2) router-based intrusion detection, installed on routers to prevent unauthorized access to the network; and 3) host-based intrusion detection, which receives audit data from the host's operating system and scrutinizes the generated events to maintain the security of the local node [23].

Human recognition using biometric traits is a new occurrence in modern culture. It has garnered increasing attention in recent years due to the necessity for security in a wide range of applications [24]. The fingerprint is often regarded as one of the most practical biometric traits. Fingerprint recognition involves little effort from the user, captures only the necessary information for the recognition process, and performs rather well [25]. Another reason for fingerprints' appeal is their low cost, which allows for easy incorporation into PC keyboards, smart cards, and wireless devices. In the Biometric Authentication System for MANET Encryption based on Elgamel encryption is utilized in this work [26, 27]. The authentication process involves capturing multiple biometric traits from the user, such as fingerprints and are then processed, fused, and compared against pre-registered templates to authenticate the user's identity.

Once the user is authenticated, the system establishes a secure communication channel between the authenticated nodes in the MANET. This channel is protected using a combination of Fingerprint and Elgamal encryption. Fingerprint is used to securely exchange the symmetric key required for

MANET encryption. The symmetric key is then used by Elgamal to encrypt the actual data transmitted between the authenticated nodes, ensuring confidentiality and integrity.

In order to overcome the black hole problem, we presented a solution [28]. To fool the black hole, a bluff packet with a virtual destination address was produced. This innovative solution employs a novel mechanism for detecting numerous black hole assaults with minimal impact on network performance. Because perfection is unachievable, the suggested system must discover a protection mechanism to safeguard the network from any intruder attack during data transmission. A digital signature may be employed as an authentication tool to improve network security against any intruder assault.

In MANET, the authentication procedure is seen as a challenge. The authentication procedure was safeguarded in a variety of methods, including the use of passwords or encrypted passwords, as well as (tokens) and private cards. Password security is ineffective since passwords may be stolen and cards can be lost. Another reason is that there is no direct link between the user and his card with passwords, tokens, and private cards. Passwords are simple and quick to use, but it is difficult to differentiate a genuine user from impostors since there is no direct connection between the user and his card [29].

Because biometrics cannot be stolen and have a strong relationship with the user, they are frequently utilized in security operations. Biometrics is a technology that is typically defined as the automatic identification or verification of an individual based on physiological or behavioral features. Fingerprints, iris, and face photographs are examples of common physiological biometric features.

The suggested solution is adaptable to any routing protocol, such as AODV. Each node in this routing protocol has its own routing information, and the discovery process begins only when it is required. When RREQ is received by any node in the network, the source is broadcasting route request messages (RREQ). If this node is the destination or has a route to the destination, route reply will be generated (RREP). This route reply message is used by the source to determine the path to the destination before delivering the data packet. The source can obtain the path to the destination when RREP moves hop by hop, which means that the source node obtains the path from the returned RREP [13].

Asymmetric-key cryptography is another name for it. Each user has two keys: one public and one private. The public key is used for encryption, and everyone has access to it. The private key is only known to the owner and is used for decryption. Public key cryptography was created to address two major issues: key distribution and digital signatures. It has three types of applications: first,

encryption/decryption (provide secrecy), second, electronic signatures (provide authentication), third, key exchange (of session keys). Because public-key cryptosystems are slower than symmetric-key systems, they are primarily employed for digital signatures and key exchange.

The major contribution of the paper are listed as follows:

1- Applying a Body Area Network scheme to capture the body sensors including ECG, EEG, and so on and send the data across MANET.
2- Encryption of the biomedical data using hybrid Elgamal algorithm.
3- Boosting the encryption process with the fingerprint as a key to the cryptographic process.
4- Comparing the results with different key size and key generation.
5- Calculating of the FAR, FRR, ERR with different threshold values for the patients.
6- Evaluation the GAR with the FAR for the genuine patients in the scheme.

The rest of the paper are organized as follows. Section 2 includes the related work. Section 3 illustrates the proposed work. Section 4 demonstrates the experimental results and discussion. Section 5 discuss the conclusion and future directions.

II. RELATED WORK

Body Sensor Network (BSN) or Body Area Network (BAN) composed of biosensors and a Personal Wireless Hub (PWH) for collecting and transmitting Personal Health Information (PHI) to a remote healthcare canter. Emphasis is placed on admitting only authorized biosensors and PWHs into the network and ensuring secure transmission to protect PHI privacy. The paper presented by He et al., 2012 [30] presented a secure network admission and transmission subsystem using a polynomial-based authentication scheme. This subsystem efficiently establishes keys for biosensors while considering communication and energy constraints. Additionally, it proposes utilizing channel errors to dynamically update keys and enhance key secrecy against adversaries. Furthermore, they includes theoretical analysis and experimental results demonstrating the security and efficiency of the proposed protocol on resource-limited sensor platforms.

The BSN is extensively employed in the Internet of Medical Things (IoMT) to enable remote access to patient data at low cost by connecting various biosensors. However, security threats, particularly hacking issues, pose significant risks to BSNs. To address this, a secured fuzzy extractor combined with a fuzzy vault is developed by Mahendran and Velusamy, 2020 [31] to enhance security using a biometric key authentication scheme. Initially, preprocessing is conducted to eliminate noise in ECG signals through adaptive

filtering. The Secured Fuzzy Extractor is tailored to extract features such as QRS, PR, and QT intervals, forming the basis for generating private keys for authentication. Due to the unique features of each ECG, private keys are resistant to hacking. Random chaff points, generated using polynomial construction principles, are stored with a checksum vector in a separate fuzzy vault set. During authentication, the data in the fuzzy set is cross-checked with checksum values to detect communication errors. The device's IP address serves as the public key for estimating sensor bit rates during decoding. The system's security heavily relies on the hash function, with the proposed method ensuring the hash variable's independence to enhance network security without affecting latency or delay. Compared to previous encoding techniques, the proposed fuzzy extractor-based biometric key authentication scheme demonstrates improved outcomes, including a 40% reduction in data loss, 20% decrease in energy consumption, and reduced delay.

The advancement in wireless technology and miniaturized, battery-powered microelectronics has led to the emergence of smart computing, where spatially distributed autonomous devices form wireless sensor networks (WSNs) to monitor physical or environmental conditions. WSNs find applications in diverse areas such as healthcare, utilities, smart cities, and smart homes, enhancing quality of life. Wireless body area networks (WBANs), formed over the human body, serve various purposes including eldercare, disease detection, sports, and military applications. Both WSNs and WBANs handle sensitive data, necessitating robust security and privacy measures. This chapter provides an overview of WSNs and WBANs, highlighting their characteristics and the importance of security and privacy. It discusses potential threats to security and privacy in these networks and existing defense mechanisms. Additionally, it identifies open research challenges to encourage further investigation in this field [32].

Integrating ubiquitous computing with mobile health technology using wireless sensors and smartphones is crucial for monitoring the well-being of chronic patients, such as those with cardiac, Parkinson's, or epilepsy conditions. Due to the sensitivity of patient physiological data, maintaining confidentiality is paramount, particularly for patients with embarrassing illnesses. Sahoo, 2012 [33] proposed a three-tier security architecture for mobile health (mHealth) applications, focusing on lightweight data confidentiality and authentication protocols to safeguard patient privacy. The proposed schemes address the energy and hardware constraints of wireless body sensors by designing low-complexity data confidentiality and authentication mechanisms. Performance evaluation demonstrates that the proposed architecture can meet the energy and

hardware limitations of sensors while maintaining network security. Additionally, the proposed schemes outperform standard key establishment security schemes in terms of energy consumption, memory usage, and computation time.

The survey presented by Gravina et al., 2017 [34] delves into the motivations and benefits of multi-sensor data fusion, with a specific emphasis on its application in physical activity recognition. It aims to offer a systematic classification and comparison framework of existing literature by identifying key properties and parameters that influence data fusion design choices across various levels: data, feature, and decision. Additionally, the survey explores the application of data fusion in other domains such as emotion recognition and general health monitoring. It introduces relevant directions and challenges for future research in multi-sensor fusion within the Body Sensor Network (BSN) domain.

However, ensuring the integrity and privacy of medical data over wireless channels presents a significant challenge. Zhang et al., 2012 [35] introduces a key agreement scheme for BANs, leveraging electrocardiogram (ECG) signals to enable neighboring nodes to share a common key. The Improved Jules Sudan (IJS) algorithm is proposed for establishing key agreements for message authentication, offering plug-and-play security without key distribution overheads. Simulation and experimental results demonstrate that the ECG-IJS scheme outperforms existing approaches in terms of metrics such as false acceptance rate (FAR) and false rejection rate (FRR), while also exhibiting energy efficiency suitable for BANs, as indicated by power consumption analysis.

Since MANET operates without a fixed infrastructure and is crucial for efficient data transfer in complex network environments. The recent advancements in communication networks, including routing algorithms and security measures, distinguish MANET from traditional infrastructure-based networks. However, there remains a need for new routing methods and algorithms to enhance data transfer efficiency and security. Many algorithms focus on parameters such as security, authentication, reachability, and mobility, which are akin to human senses. Just as human senses gather information from the external world and the body, gateway nodes in MANET serve as intermediaries between different sub-networks. Kumar and Sandeep, 2012 [36] draws parallels between human senses and network behaviors, particularly from the perspective of gateway nodes.

Lightweight and resource-efficient biometrics-based security solutions have been proposed for BSN. These solutions utilize physiological characteristics

captured by individual sensors in the BSN to generate entity identifiers (EIs) for securing keying materials through a biometric approach. The study presented by Miao et al., 2013 [37] focuses on an enhanced key distribution solution using energy distribution information from physiological signals (EDPSs)-based EIs. Various EDPS-based EI generation schemes are explored, including a modified multi-windows Fourier transform scheme and a method based on the discrete cosine transform of autocorrelation sequences.

Authentication in wireless networks, particularly in Wireless Body Area Networks (WBANs) containing sensitive e-healthcare data, demands stringent privacy and security measures. While numerous anonymous WBAN authentication systems exist in literature, Wang et al. 2024 [7] presents a comprehensive review, categorization, and comparison of these schemes. Through a detailed taxonomy and survey, it delineates security services, vulnerabilities, and the attributes of an ideal anonymous authentication scheme. Schemes are classified by their encryption algorithms, including bilinear pairings-based, elliptic curve cryptography-based, lattice-based, and XOR-based approaches. Further, they specifies and discusses authentication capabilities, cryptographic features, security advantages, evaluation metrics, and shortcomings of each scheme. A thorough comparison reveals their resilience against various security threats, highlighting areas needing further exploration, such as group authentication, multi-factor authentication, and protection against DDoS attacks. Only a small fraction of schemes addresses group authentication and utilize multi-factor authentication, while few tackle DDoS attacks. The study concludes with recommendations for future research based on identified literature gaps.

User authentication is crucial for upholding integrity and confidentiality, especially in Mobile Ad Hoc Networks (MANETs), which face challenges like decentralized coordination and resource constraints. In high-security MANETs, continuous authentication is particularly valuable for monitoring sessions and mitigating vulnerabilities. Biometrics, directly tied to user identity, present promising solutions to authentication challenges in MANETs.

Richard Yu et al., 2008 [38] introduced biometric technologies and their relevance to MANET authentication, highlighting the benefits of multimodal biometrics in compensating for inaccuracies. It proposes an optimal continuous authentication scheme based on multimodal biometrics for MANETs and presents numerical evidence of its effectiveness.

Deny et al. [39] offered a technique for enhancing the security model in MANET by combining multimodal biometric confirmation and interruption identification. The suggested plan's conclusions included multi-model biometric

verification plans and interruption recognition for MANET based on the manner of an armed force situation. Verification was a mission without a focal power in strategic operations that required secure MANET. It provided MANET verification methodologies based on the behaviour of a military site. Their proposed strategy tried to enhance the general execution of security in a MANET. Narayanan et al. worked on intrusion detection and authentication in MANET in Ref. [18]. They employed a combination of biometric methods across multiple modes alongside an intrusion detection system. Their proposed method enhanced network security, and simulations indicated that integrating diverse sensor data in a distributed manner aligns effectively with the concept of cross-layer security, an increasingly important aspect in the realm of MANET security. Authors in [23] Authentication system based on Multimodal Biometrics. For authentication, face biometrics were employed, while fingerprint biometrics were used for security. To increase security, the data and the sender's eigenface were encrypted using the key retrieved from the receiver's fingerprint biometric. The suggested security solution provided authentication, security, and revocability to mobile ad hoc networks for high security applications. Many security issues persist in ad hoc networks, and they will be addressed in future work.

Zafar et al. [40] created an algorithm and presented biometric perception as a technique that combines iris characteristics collected from iris image acquisition with a perception system. The genetic algorithm clarifies MANET QOS concerns. The value of the research solution is demonstrated by improved findings when compared to other traditional approaches. Their study proposes employing a metaheuristic method to improve biometric-based authentication for secure MANET. The solution used a metaheuristic algorithm to mitigate the security and privacy problems that present in biometric technology, which resulted in a greater level of security. The requirement of this strategy was to overcome different data threats such as wormholes, etc., in order to obtain a secure MANET [40–42].

III. PROPOSED WORK

The proposed work, as depicted in Figure 2, entails a comprehensive examination of an authentication system for Mobile Ad-hoc Networks (MANETs), leveraging fingerprint-based keys and hybrid Elgamal encryption for enhanced security during authentication. Initially, patients serve as the primary input for the proposed scheme, with their biomedical data utilized within the system. Biomedical data, acquired from various sensors embedded in the patient's body such as ECG, EEG, blood pressure, EMG, and motion sensors,

is transmitted through Body Area Network (BAN) sensors. Following extraction from each enrolled patient, the biomedical data undergoes processing within the cryptography stage. To reinforce security measures, fingerprint biometrics are employed as keys within this cryptographic process. The fingerprint undergoes pre-processing stages, including region of interest (RoI) identification, minutiae and core definition, and data normalization, culminating in the extraction of features from fingerprint images and minutiae components [43]. Feature vectors of lengths 256, 512, and 1024 are obtained, followed by encryption using the Elgamal encryption scheme. This scheme comprises three stages. Key Generation: Involves the generation of public key (PK) and secret key (SK) from prime numbers (P). A cyclic group generator (Cg) of size (S) is selected, with a random element (ζ) chosen from {1, 2, ..., S-1}. The computation of $\chi = Cg^{\zeta}$ (mod P) is then conducted. Encryption: Utilizes the PK and the extracted feature vector message key (m) from the fingerprint. A random element (β) from {1, 2, ..., S-1} is chosen, followed by the computation of $c1 = Cg^{\beta}$ (mod P) and $c2 = Cg^{m}$ (mod P) × Γ, where Γ represents the secret key of m and $\Gamma = \chi^{\beta}$. The resulting encrypted message is denoted as $\varepsilon(x) = [c1, c2]$. Decryption: Involves obtaining the decrypted message using SK and the encrypted message. Through this process, the authentication system ensures robust security measures within MANETs, utilizing fingerprint biometrics and hybrid Elgamal encryption for secure authentication.

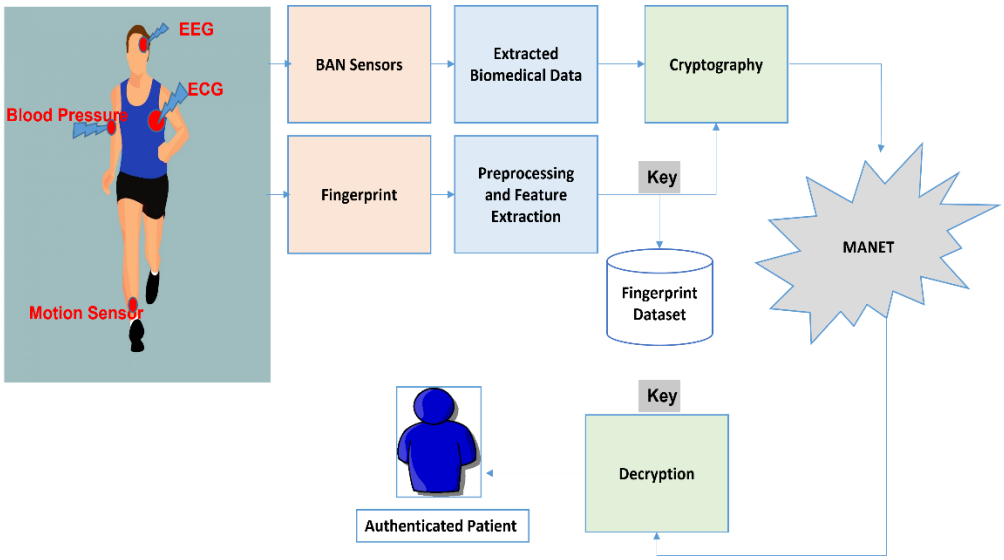

Figure 2. The general structure of the proposed scheme

Figure 3. depicts a block diagram of a fingerprint authentication system that incorporates Elgamal encryption and decryption. In the first stage, the user's fingerprint is captured by a sensor and then undergoes preprocessing to

eliminate noise and enhance the clarity of the fingerprint ridges. Then, feature extraction techniques are applied to extract a unique mathematical representation of the fingerprint's identifying characteristics. This block represents a database that stores templates of enrolled users' fingerprints. Each template consists of the extracted features from a user's fingerprint. A key generation phase is included where a secret key (SK) is created. When a user attempts to authenticate themselves, their fingerprint is captured and preprocessed as described earlier. The extracted features, denoted by "x" are then subjected to Elgamal encryption using the public key (PK) retrieved from the database. The Elgamal encryption process transforms the fingerprint data (x) into a ciphertext (ε(x)) that conceals the original data. The encrypted fingerprint data (ε(x)) is then transmitted across a network (represented by MANET in the diagram) to the authentication server [44]. MANET stands for Mobile Ad Hoc Network, which refers to a temporary network of devices that communicate without a central infrastructure as shown on Figure 3.

The procedure of transmitted data through MANET from source to destination undergoes different steps shown in Figure 4, which depicts a typical MANET presentation. When node Source (S) wishes to send a message to node Destination (D) through the path, but before the message is sent through the path, the fingerprint properties of node S will secure data and encrypted with the public key. When the message was delivered, Node D may decode the encrypted data using its private key text [45].

Upon receiving the encrypted data (ε(x)), the authentication server utilizes the user's secret key (SK) to decrypt the ciphertext (ε(x)) using Elgamal decryption. This decryption process recovers the original fingerprint data (x). The decrypted fingerprint data (x) is then compared to the user's template stored in the fingerprint dataset. A distance metric, such as the Euclidean distance, is employed to calculate the similarity between the two sets of data. The Euclidean distance is a common way to measure the distance between two points in space. In the context of fingerprint recognition, it's used to measure how similar two fingerprint templates are. A predefined threshold value, denoted by matching score (MS), is established. If the calculated distance between the decrypted fingerprint data (x) and the stored template falls above the threshold, a successful match is concluded, and the user is granted access (Accept). Conversely, the authentication fails, and access is denied (Reject) [46]. In essence, this system leverages Elgamal encryption to safeguard the confidentiality of the user's fingerprint data during transmission over a network. The decryption process solely occurs on the authentication server using the

user's specific secret key, ensuring that the raw fingerprint information remains protected.

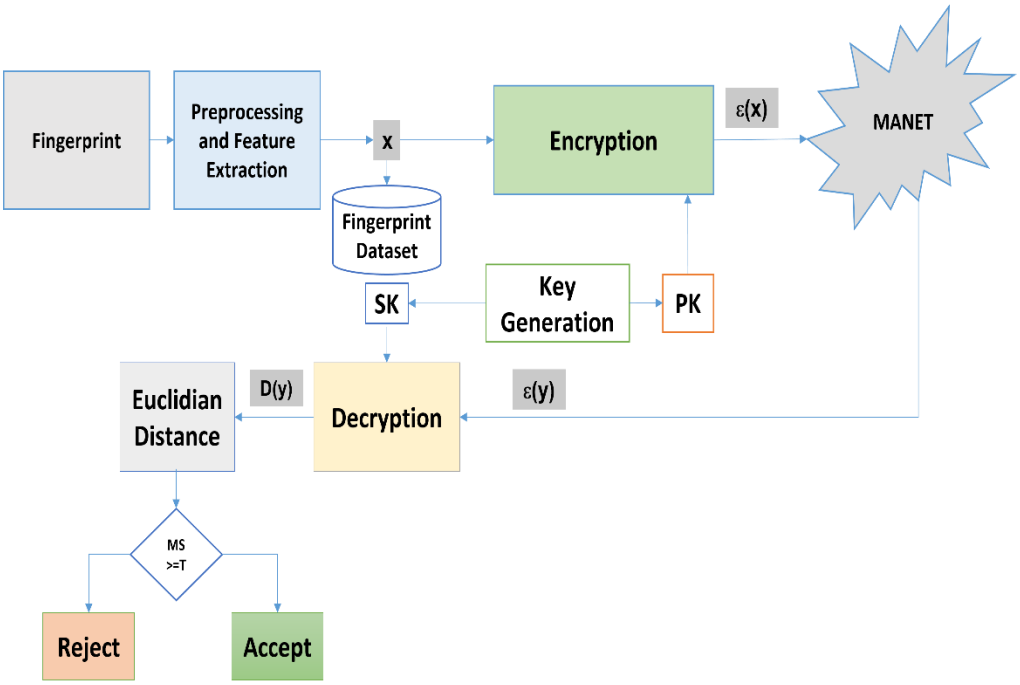

Figure 3. Authentication process of the proposed scheme.

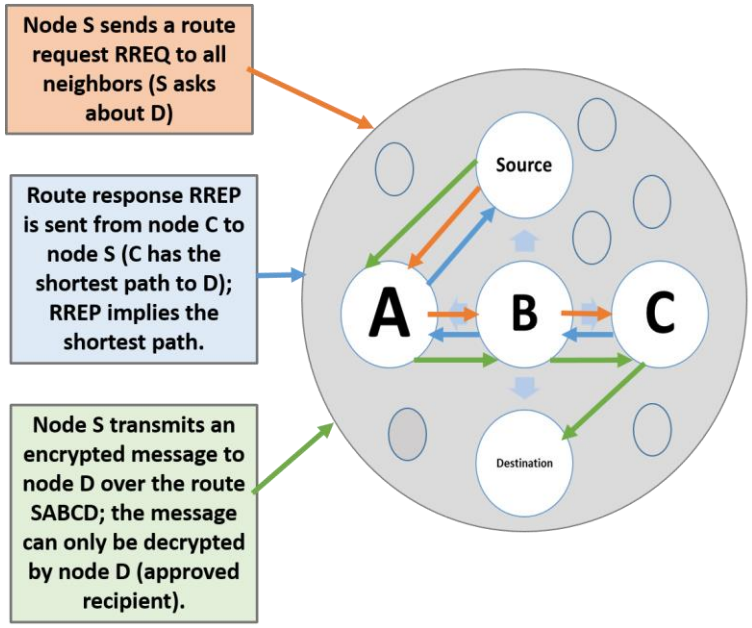

Figure 4. The transmission of data in MANET from source to destination

IV. EVALUATION RESULTS

The suggested system's empirical results are based on using FVC2000 datasets [47] for fingerprint. The FVC2000 datasets comprised 880 fingerprints from 110 separate fingers. Figure 5 shows a sample image of DB1-FVC200 dataset. The minutiae feature extraction procedure is used to extract the characteristics of each enrolled fingerprint as shown in Figure 6, which are subsequently, encoded using the Elgamal algorithm. The grey scale fingerprint picture may be categorised into endpoints and bifurcation that extracted the major points in minutiae portions during minutiae feature extraction. Despite the low quality of the initial picture, feature extraction based on minutiae can promote ridge-valley patterns, allowing for more accurate minutiae extraction. Many criteria may be used to evaluate system performance, however in the MANET context, time spent on key creation, encryption, and decryption is utilised.

Figure 5. Samples of fingerprint images from DB1-FVC2000 dataset

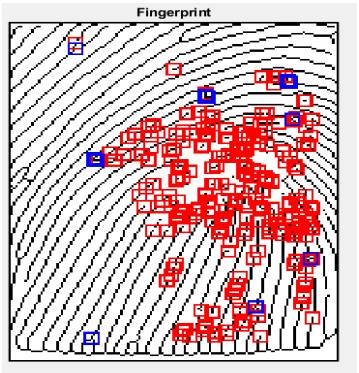

Figure 6. Extracted features from fingerprint-based minutia parts.

The dataset comprises 880 fingerprint images sourced from 4 databases. We partitioned this data into a training set consisting of 80% (704 images) and a testing set comprising the remaining 20% (176 images). Specifically, 704 images were allocated for training, while the remaining 176 were reserved for

testing. Within the training set, we further categorized the 704 images into 352 genuine and 352 impostor samples to facilitate the authentication process. Similarly, within the testing set, we designated 88 images as genuine and 88 images as impostors for evaluation purposes.

In our authentication process, we utilized the Euclidean Distance (ED) to gauge the similarity between the decrypted template and the pre-stored templates in the fingerprint database. This procedure generates a matching score, where acceptance of the patient's data occurs if the score is greater than or equal to the set threshold. Conversely, if the score falls below the threshold, the data is rejected, as illustrated in Figure 3. To comprehensively assess system performance, we conducted an analysis across various threshold values, focusing on the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (ERR), as depicted in Figure 7. This detailed examination allowed us to understand how the system behaves under different thresholds, providing insights into its performance across a spectrum of acceptance criteria. By systematically adjusting threshold values, we observed fluctuations in the rates of false acceptance and false rejection, identifying the Equal Error Rate (ERR) at the point of intersection. This analysis offers valuable insights into system reliability and aids in optimizing performance to achieve the desired balance between security and usability. Specifically, we found that the ERR stands at 0.375 with a threshold of 0.24, indicating an optimal balance between false acceptance and false rejection rates.

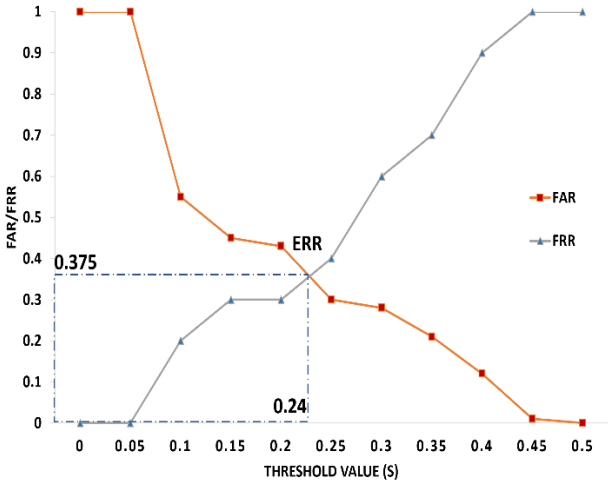

Figure 7. Comparative Analysis of FAR, FRR, and ERR Across Threshold Values.

We assessed the system's performance through Receiver Operating Characteristic (ROC) analysis, illustrating the interplay between the Genuine Acceptance Rate (GAR) and the False Acceptance Rate (FAR), as presented in

Figure 8. This analytical approach provides a thorough evaluation of the system's accuracy and efficiency in differentiating genuine users from impostors across a range of thresholds. We determined a Genuine Acceptance Rate (GAR) of 96.3%, indicating the system's high authentication rate. These findings underscore the system's effectiveness in accurately verifying users based on concatenated face and fingerprint data. The results obtained in the Table 1 show that the proposed scheme for elapsed time for key generation, encryption and decryption. The length of the cryptographic key used in Elgamal encryption, typically measured in bits. A larger key size translates to stronger encryption but also incurs more computational overhead. Encryption and decryption times increase as the key size grows (from 256 to 1024 bits). This is because larger keys necessitate more complex mathematical operations during both encryption and decryption processes.

Table 2 compares the proposed scheme to Ref [23], Ref [15], and [48] in terms of key generation, encryption, and decryption delay times (ms). Table 2, shows that the proposed scheme achieves comparatively good performance when compared to Shanthini et al. [23], in terms of overhead and security level. When compared to Shanthini et al. [23], the suggested system's key size was 64, and the delay time achieved a superior value than that reported in Ref. [23]. This is due to the fact that we utilised a tiny key size and a unimodal fingerprint.

The length of the cryptographic key in Elgamal encryption, typically measured in bits, is a crucial determinant of encryption strength, with larger key sizes offering greater security but also imposing higher computational overhead. Key generation time, measured in milliseconds, indicates the average duration required to generate a new Elgamal key pair, including both public and private keys. Similarly, encryption and decryption times, also measured in milliseconds, reflect the average duration for encrypting and decrypting messages using the Elgamal algorithm with specific key sizes. Analysis of the provided table reveals that both encryption and decryption times increase as key size expands, ranging from 256 to 1024 bits, due to the heightened complexity of mathematical operations involved. These performance metrics are pivotal considerations when selecting an appropriate key size for an Elgamal encryption system, as larger keys offer heightened security but may not be viable for resource-constrained devices or real-time applications where speed is paramount. Thus, striking a balance between security and performance is essential in key size selection, ensuring optimal functionality across diverse use cases and environments.

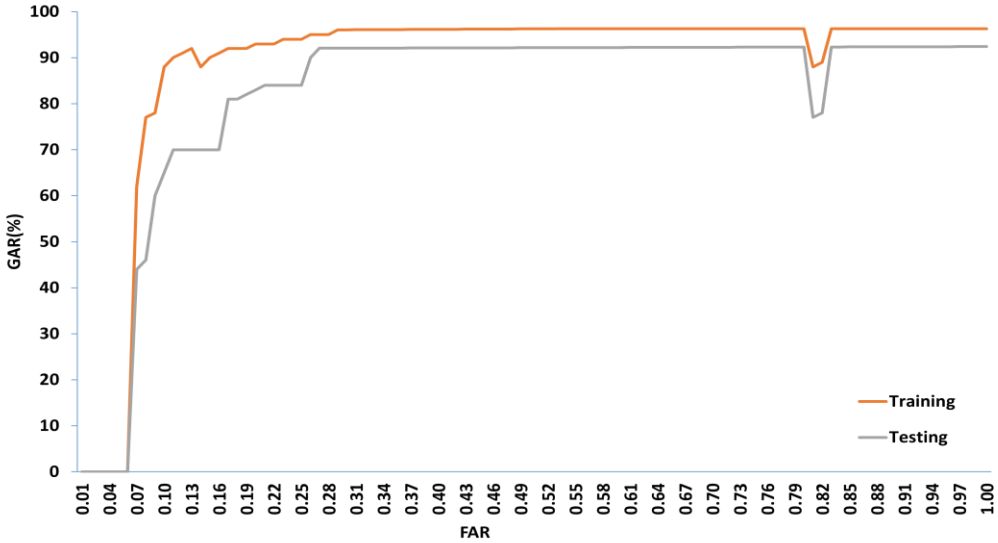

Figure 8. The Receive Operating Characteristics for the proposed scheme.

Table 1. The key size via the key generation, encryption, and decryption of the proposed authenticatin scheme.

Key Size	Key generation (ms)	Encryption (ms)	Decryption (ms)
256	0.022	0.011	0.017
512	0.036	0.014	0.020
1024	0.041	0.017	0.029

Table 2. The comparative study between the proposed method and the recent MANET authentication systems

Methods	Key Size	Key generation (ms)	Encryption (ms)	Decryption (ms)
Shanthini et al. [23]	64	0.06	0.04	0.03
	128	0.13	0.10	0.10
	192	0.08	0.08	0.07
	256	0.13	0.12	0.11
Saada et al. [15]	64	0.06	0.02	0.03
Elbanaa et al. [48]	1024	0.042	0.019	0.032
Proposed Scheme	**1024**	**0.041**	**0.017**	**0.029**

V. CONCLUSION AND FUTURE WORK

The vulnerabilities inherent in standard Mobile Ad hoc Networks (MANETs), such as incorrect transmission and susceptibility to unauthorized node access, highlight the pressing need for enhanced security measures, particularly in authentication procedures. This paper has presented a novel approach to address these challenges by integrating a Body Area Network (BAN) scheme to capture biomedical data from sensors like ECG and EEG, facilitating secure data transmission across MANETs. Furthermore, we have utilized a hybrid Elgamal algorithm for encrypting biomedical data, strengthened by fingerprint biometrics, to fortify the cryptographic process and bolster network security. Moreover, through comparative analyses encompassing different key sizes and generation techniques, we have evaluated the system's performance by calculating key metrics like the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (ERR) across various threshold values for patient authentication.

Additionally, we have assessed the Genuine Acceptance Rate (GAR) alongside the FAR, specifically focusing on genuine patients within the scheme, thereby providing insights into the system's authentication efficacy. Our findings have revealed an optimal ERR of 0.375 at a threshold of 0.24, striking a balance between false acceptance and rejection rates. Furthermore, the GAR, indicative of the authentication rate, has been determined to be 96.3%, underscoring the effectiveness of our proposed secure system. Through practical testing and analysis, our study has demonstrated the resilience and robustness of the proposed multimodal biometric authentication system, offering a promising solution for secure communication in dynamic and resource-constrained MANET environments. In our future endeavors, we envision leveraging Body Area Network (BAN) signals such as ECG or EEG for encryption over wireless networks. This innovative approach holds promise for enhancing the security of data transmission while ensuring the privacy and integrity of sensitive biomedical information. Moreover, our focus will extend to optimizing the energy efficiency and processing capabilities required for handling various cryptographic keys within the network model. We aim to explore efficient algorithms and methodologies that strike a balance between security requirements and resource constraints, including memory usage, computation time, and energy consumption. By conducting comprehensive analyses and experiments, we seek to identify key parameters and configurations that not only bolster network security but also minimize resource utilization, thereby enhancing the overall performance and scalability of the system. This holistic approach will contribute to the development of robust and

energy-efficient solutions for secure communication in dynamic wireless environments, paving the way for broader applications in healthcare [49], IoT, and beyond.

Funding: No financial support was provided for this study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Tobón DP, Falk TH, Maier M (2013) Context awareness in WBANs: a survey on medical and non-medical applications. IEEE Wireless Communications 20:30–37

2. Nissar G, Khan RA, Mushtaq S, et al (2024) IoT in healthcare: a review of services, applications, key technologies, security concerns, and emerging trends. Multimedia Tools and Applications 1–62

3. Rao TVN, Mothukuri L, Bhavana S (2024) IoT Networks for Real-Time Healthcare Monitoring Systems. In: Analyzing Current Digital Healthcare Trends Using Social Networks. IGI Global, pp 143–158

4. Wajgi DW, Tembhurne JV (2024) Localization in wireless sensor networks and wireless multimedia sensor networks using clustering techniques. Multimedia Tools and Applications 83:6829–6879

5. Ahmed SF, Alam MSB, Afrin S, et al (2024) Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. Information Fusion 102:102060

6. Abdelfatah RI, Saqr HM, Nasr ME (2023) An efficient medical image encryption scheme for (WBAN) based on adaptive DNA and modern multi chaotic map. Multimed Tools Appl 82:22213–22227. https://doi.org/10.1007/s11042-022-13343-8

7. Wang D, Zhou J, Masdari M, et al (2023) Security in Wireless Body Area Networks via Anonymous Authentication: Comprehensive Literature Review, Scheme Classification, and Future Challenges. Ad Hoc Networks 103332

8. Rabie OBJ, Selvarajan S, Hasanin T, et al (2024) A full privacy-preserving distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless medical sensor networks (HWMSNs). International Journal of Information Security 23:51–80

9. Szymoniak S (2024) Key Distribution and Authentication Protocols in Wireless Sensor Networks: A Survey. ACM Computing Surveys 56:1–31

10. Hoebeke J, Moerman I, Dhoedt B, Demeester P (2004) An overview of mobile ad hoc networks: applications and challenges. Journal-Communications Network 3:60–66

11. Jawandhiya PM, Ghonge D, Ali MS, Deshpande JS (2010) A survey of mobile ad hoc network attacks. Pradip M Jawandhiya et al/International Journal of Engineering Science and Technology 2:4063–4071

12. Macker JP, Corson MS (1998) Mobile ad hoc networking and the IETF. ACM SIGMOBILE Mobile Computing and Communications Review 2:9–14

13. Abdelfatah RI, Abdal-Ghafour NM, Nasr ME (2021) Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions. IEEE Access 10:1096–1115

14. Sesay S, Yang Z, He J (2004) A survey on mobile ad hoc wireless network. Information Technology Journal 3:168–175

15. Saada II, Sakr RH, Rashad MZ (2018) Authentication Using Fingerprint and Rivest-Shamir-Adleman Encryption in Mobile Ad Hoc Network. Journal of Computational and Theoretical Nanoscience 15:2510–2514

16. Glynos D, Kotzanikolaou P, Douligeris C (2005) Preventing impersonation attacks in MANET with multi-factor authentication. In: Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05). IEEE, pp 59–64

17. Hamouid K, Adi K (2015) Efficient certificateless web-of-trust model for public-key authentication in MANET. Computer Communications 63:24–39

18. Narayanan KL, Castro AF (2012) High Security for Manet Using Authentication and Intrusion Detection with Data Fusion. International Journal of Scientific & Engineering Research 3:1

19. Shams MY, Tolba AS, Sarhan SH (2017) A vision system for multi-view face recognition. arXiv preprint arXiv:170600510

20. Shanmugham EK, Dhatchnamurthy S, Pakkiri PS, Garg N (2024) Adaptive activation Functions with Deep Kronecker Neural Network optimized with Bear Smell Search Algorithm for preventing MANET Cyber security attacks. Network: Computation in Neural Systems 1–25

21. Shams MY, Tolba AS, Sarhan SH (2016) Face, iris, and fingerprint multimodal identification system based on local binary pattern with variance histogram and combined learning vector quantization. Journal of Theoretical and Applied Information Technology 89:53

22. Alzubaidi M, Shah U, Agus M, Househ M (2024) FetSAM: Advanced Segmentation Techniques for Fetal Head Biometrics in Ultrasound Imagery. IEEE Open Journal of Engineering in Medicine and Biology

23. Shanthini B, Swamynathan S (2011) A secure authentication system using multimodal biometrics for high security MANETs. In: International Conference on Advances in Computing and Information Technology. Springer, pp 290–307

24. Sarhan S, Nasr AA, Shams MY (2020) Multipose Face Recognition-Based Combined Adaptive Deep Learning Vector Quantization. Computational Intelligence and Neuroscience 2020:

25. Shams MY, Tolba AS, Sarhan SH (2016) Face, iris, and fingerprint multimodal identification system based on local binary pattern with variance histogram and combined learning vector quantization. Journal of Theoretical and Applied Information Technology 89:53

26. Tsiounis Y, Yung M (1998) On the security of ElGamal based encryption. In: International Workshop on Public Key Cryptography. Springer, pp 117–134

27. Luo Y, Ouyang X, Liu J, Cao L (2019) An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access 7:38507–38522

28. Varshney I, Ali S (2017) Study on MANET: concepts, features and applications. ELK's Int J Comput Sci 2:2394–0441

29. Tu J, Tian D, Wang Y (2021) An active-routing authentication scheme in MANET. IEEE Access 9:34276–34286

30. He D, Chen C, Chan S, et al (2012) Secure and lightweight network admission and transmission protocol for body sensor networks. IEEE journal of biomedical and health informatics 17:664–674

31. Mahendran RK, Velusamy P (2020) A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. Computer Communications 153:545–552

32. Roy M, Chowdhury C, Aslam N (2020) Security and privacy issues in wireless sensor and body area networks. Handbook of Computer Networks and Cyber Security: Principles and Paradigms 173–200

33. Sahoo PK (2012) Efficient security mechanisms for mHealth applications using wireless body sensor networks. Sensors 12:12606–12633

34. Gravina R, Alinia P, Ghasemzadeh H, Fortino G (2017) Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges. Information Fusion 35:68–80

35. Zhang Z, Wang H, Vasilakos AV, Fang H (2012) ECG-cryptography and authentication in body area networks. IEEE Transactions on Information Technology in Biomedicine 16:1070–1078

36. Kumar JS, Sandeep J (2012) Does MANET Have Senses? – An Intellectual Approach. Procedia Engineering 38:1415–1431. https://doi.org/10.1016/j.proeng.2012.06.176

37. Miao F, Bao S-D, Li Y (2013) Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security. IET Information Security 7:87–96

38. Richard Yu F, Tang H, Leung VC, et al (2008) Biometric-based user authentication in mobile ad hoc networks. Security and Communication networks 1:5–16

39. Deny J, Sundhararajan M (2016) Multi modal biometric security for mobile ad-hoc networks and its applications. Indian Journal of Science and Technology 9:1–6

40. Zafar S, Soni MK, Beg MS (2015) An optimized genetic stowed biometric approach to potent QOS in MANET. Procedia computer science 62:410–418

41. Gagandeep A, Kumar P (2012) Analysis of different security attacks in MANETs on protocol stack A-review. International Journal of Engineering and Advanced Technology (IJEAT) 1:269–75

42. Von Mulert J, Welch I, Seah WK (2012) Security threats and solutions in MANETs: A case study using AODV and SAODV. Journal of network and computer applications 35:1249–1259

43. Gadallah OG, Nasr ME, Elkhobby HA (2024) Comparative Study between Various Algorithms of Image Compression Techniques using MODIS Image. In: 2024 Fourth International Conference on Advances in Electrical,

Computing, Communication and Sustainable Technologies (ICAECT). pp 1–6

44. Abdelfatah RI, Baka EA, Nasr ME (2021) Keyed Parallel Hash Algorithm Based on Multiple Chaotic Maps (KPHA-MCM). IEEE Access 9:130399–130409. https://doi.org/10.1109/ACCESS.2021.3113855

45. Hikal NA, Shams MY, Salem H, Eid MM (2021) Detection of black-hole attacks in MANET using adaboost support vector machine. Journal of Intelligent & Fuzzy Systems 41:669–682. https://doi.org/10.3233/JIFS-202471

46. Shams MY, Sarhan SH, Tolba AS (2017) Adaptive Deep Learning Vector Quantisation for Multimodal Authentication. Journal of Information Hiding and Multimedia Signal Processing 8:702–722

47. Maio D, Maltoni D, Cappelli R, et al (2002) FVC2000: Fingerprint verification competition. IEEE transactions on pattern analysis and machine intelligence 24:402–412

48. M. Elbanaa A, Y. Shams M, I. Abdelfatah R, E. Nasr M (2024) Empowering Manets with Advanced Multimodal Biometric Authentication and Encryption. IJNSA 16:17–27. https://doi.org/10.5121/ijnsa.2024.16202

49. Eltabakh MA, Abdelrahman E, Nasr, M. E, Abdelfatah RI (2023) Blockchain for Healthcare Systems: Concepts, Applications, Challenges, and Future Trends. Journal of Engineering Research 7:132–143