IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 29, 2020, accepted March 10, 2020, date of publication March 13, 2020, date of current version March 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2980739

A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data

MOHAMMAD AYOUB KHAN[1], (Senior Member, IEEE), MOHAMMAD TABREZ QUASIM[1], (Senior Member, IEEE), NORAH SALEH ALGHAMDI[2], AND MOHAMMAD YAHIYA KHAN[3]

[1]College of Computing and Information Technology, University of Bisha, Bisha 67714, Saudi Arabia
[2]College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[3]College of Sciences, Vice Deanship of Development and Quality, King Saud University, Riyadh 11451, Saudi Arabia

Corresponding author: Mohammad Ayoub Khan (ayoub.khan@ieee.org)

This work was supported by the Deanship of Scientific Research, Princess Nourah Bint Abdulrahman University, through the Fast-Track Research Funding Program.

ABSTRACT Mobile users are increasing exponentially to adopt ubiquitous services offered by various sectors. This has attracted attention for a secure communication framework to access e-health data on mobile devices. The wearable sensor device is attached to the patient's body which monitors the blood pressure, body temperature, serum cholesterol, glucose level, etc. In the proposed secure framework, first, the task starts with the patient authentication, after that the sensors device linked to the patient is activated and the sensor values of the patient are transmitted to the cloud server. The patient's biometrics information has been added as a parameter in addition to the user name and password. The authentication scheme is coined with the SHA-512 algorithm that ensures integrity. To securely send the sensor information, the method follows two kinds of encryption: Substitution-Ceaser cipher and improved Elliptical Curve Cryptography (IECC). Whereas in improved ECC, an additional key (secret key) is generated to enhance the system's security. In this way, the intricacy of the two phases is augmented. The computational cost of the scheme in the proposed framework is $4H + Ec + Dc$ which is less than the existing schemes. The average correlation coefficient value is about 0.045 which is close to zero shows the strength of the algorithm. The obtained encryption and decryption time are 1.032 μs and 1.004μs respectively. The overall performance is analyzed by comparing the proposed improved ECC with existing Rivest–Shamir–Adleman (RSA)and ECC algorithms.

INDEX TERMS Internet of Things, wearable sensors, cloud wireless sensors, encryption, ECC, RSA.

I. INTRODUCTION

In addition to wearable monitoring systems, the Internet of things (IoT), is a fast-growing technology that is expected to bring a broad range of healthcare applications [1]. The healthcare industry has adopted IoT very quickly [2], [3], which has increased the quality of service as well as productivity by incorporating IoT facets into medical devices, which gave tremendous benefits to the aged, diabetic patients and people with secure management [4]. The services to the patients located in remote places in both normal and emergencies situations can be provided with cloud-based services.

The associate editor coordinating the review of this manuscript and approving it for publication was Ding Xu.

The mobile communication technologies like 5G has made possible for patients and healthcare providers to provide service with Internet of things and sensors to send blood sugar level, ECG (Electrocardiogram), thyroid level, blood pressure, cholesterol level. IoT based healthcare applications can be used to capture critical health data in real-time within a regular interval of time and IoT sensors can continuously process large volumes of health data. The IoT is recognized by healthcare industries as the most important technology in the future [5]. In fact, centralized health monitoring services focused on IoT can help the safety and ease of elderly people who can't access to healthcare services [6].

The introduction of IoT in the healthcare industry has led researchers around the globe to build smart applications such

as virtual doctors, mobile healthcare, patient recommender, etc. [7]. Advanced monitoring devices can be used to collect information from people regarding their health conditions, e.g. blood pressure, glucose levels, heart rate, etc. [20], [21]. The data can be monitored and transmitted to smartphones constantly through wearable devices sensors [8]. The sensor nodes of ECG [9] are linked to the IoT network and backed up by plug-and-play functionality [10]. The cloud server can be used to store and access the historical as well as real-time patient data [11], [12]. Any system based on sensors and IoT pose concerns about privacy and security because mobile devices can be targeted for malicious attack [18]. Therefore, more research on security and privacy measures are required. For a trustworthy IoT, the framework shall be developed based on some light weight cryptography algorithm [19].

Security Issues-The security of the patient data should be the top priority. The patient data must be secured by complete protection, data encryption, user verification and application security by deploying current security requirements and validation algorithms. For cloud computing in general, these security problems were thoroughly explored [13]–[15], [17]. The security threats including manipulation of sensitive cloud data of patients, patient data privacy breach and the unauthorized use of the data are a major challenge to the cloud-based healthcare systems. Therefore, IoT and cloud-based healthcare systems must meet a number of security requirement. Following are the core criteria for security and privacy of cloud-based healthcare system [13], [14], [16].

A) Authentication: The identification of the user such as patients, healthcare staff, and partners must be verified using some strong mechanism of cryptographic routine.
B) Authorization: This is the second requirement after authentication which ensures permission, resource grants, and access priorities for users of the system. Based on the privilege users are granted different access levels.
C) Non-repudiation: This is a cryptographic mechanism to ensure that the sender has really sent this message. A digital signature, encryption and timestamps may be used to determine authenticity of patient and non-repudiation to ensure the patient in a healthcare system.
D) Integrity and Confidentiality: The integrity ensures the intactness of the received message. In healthcare system, we can say that patient data has not be altered. This can be achieved using one-way hash functions and message digests like SHA256, SHA512, and MD5 etc. While confidentiality ensures that only intended receiver can read the sent message. This can be achieved using encryption algorithms.

The structure of the paper is as follows: The related studies to the proposed technique is discussed in section 2. The proposed methodology and scheme are presented in section 3. The obtained experimental results are analyzed in section 4. Section 5, finally concludes the paper along with future direction.

II. RELATED WORK

Gupta *et al.* [18] put forward an IoT-based cloud architecture. The presented system utilized the embedded sensors of the equipment instead of smartphone sensors or wearable sensors for storing the basic attributes value of health-associated parameters. A cloud-based system comprises of cloud data center (CDC), private cloud, the and public cloud. This architecture utilized XMLWeb services for the fast and secure communication of data. The total response from CDC to the local database server almost corresponds to the increased number of users.

Rathee *et al.* [19] have presented a secure healthcare framework that is based on blockchain methodology. Authors, have utilized blockchain for assuring the transparency and security of document accessibility, patient records, and the shipment process among providers and customers. The experiential analysis of the framework was gauged on the illegal actions or communications by malicious IoT objects.

Zouka and Hosni [22] put forward a secure and computationally lightweight authentication structure which shields health data and assures security of the communications. The suggested structure enables doctors to monitor patients' real-time biosignals and was fitted with an emergency rescue approach utilizing a machine-to-machine (M2M) patient monitoring screen and remote health app. The findings supported the high-level results of the proposed system, since the average access times were decreased. The structure has the highest key generation time when the verification time and transfer time are considered.

Tyagi *et al.* [23] have developed an IoT health framework for healthcare system to assist patients in finding the best treatment for the best costs by ensuring that the health information can be securely stored and shared among the organization. However, in the proposed framework no specific algorithms for authentication or privacy has been discussed.

Wen *et al.* [24] proposed a mechanism to access real-time multimedia data by authorized users in wireless multimedia sensor network. Authors have used Chinese Remainder Theorem (CRT) for the proposed authentication system.

Li *et al.* [25] have raised numerous practical problems necessary to satisfy security and privacy requirements in wireless networks. The authors have analyzed the applicable security solutions in the sensor networks and the wireless body area network. Also, author have presented analysis on these implementations. To achieve fine-grained access control, they introduced an attribute-based encryption.

Al-Mahmud and Morogan [26] suggested an identity-based digital signature scheme for access control and user authentication. To sign and validate a message, they implemented the ECC-based digital signature algorithm. The users and sensors are registered at the base station (BS) at the time of activation, and the group identities and access privileges are also granted by the base station. The account deletion is done at the point of login by expiry of the user's access time allocated by the base station. The authenticated

user may not receive the access requested without the right of access. To some extent this scheme prevents denial-of-service attacks (DoS) but registration and password change processes is not supported for all users. The base station has to broadcast the parameters of the application settings such as the userid, groupid, and device timestamp for a new user additive that is an additional communication overhead.

Wang *et al.* [27] suggested an ECC access control scheme allowing the Key Distribution Centre (KDC) to be introduced before authentication. A user registry database of priority rights for the specific individual is created by KDC. Such privilege is composed of the privilege mask for server, groupid and account control. The same access privilege should be open to multiple users in the same group. The ECC generates a user's private and public key and a certificate for the user access list, according to the user request. Although a sensor node is authenticated, but user is not authenticated. Consequently, mutual authentication between user and sensor are not supported in proposed framework.

Le *et al.* [28] proposed an ECC-based, energy-efficient access control system. The core idea of the work is motivated by the scheme suggested by Wang *et al.* [27].

Kavitha *et al.* [29] have presented an improved authentication scheme using elliptic curve cryptography for healthcare application. Authors have discussed the problems and the failures in conventional cryptographic algorithms when applied to IoT applications. To overcome this issue authors have purposed hyper elliptic curve based public key technique that combines Digital Signature and Elgamal encryption algorithms.

Khemissa and Tandjaoui [30] have discussed many deployment issues in e-health application, particularly in IoT environment. However, the main focus of the paper is authentication of interconnected devices. Authors have suggested hash message authentication and nonce for authentication of base station and sensors. Author have claimed about the presented scheme to be more secure against attacked and energy efficient.

Wazid *et al.* [31] have presented exhaustive survey of various authentication schemes for IoT sensors, devices, gateways and users. Many challenges in the IoT environment due to limited computational capability, memory, heterogeneity, and mobility were discussed. Authors have also discussed various aspect of authentication in context to cloud and big data environment.

III. PROPOSED METHODOLOGY

In this work we have proposed a layered framework of the cloud-based healthcare system shown as figure 1. The framework has four layers connected to each other. The description of each layer is presented as follows:

People Layer – The people layer contains the actual consumers and producer of the data such as patients, doctors, technicians, and administrators.

Device Layer – This layer contains various devices that facilitate to access the information such as personal digital assistant (PDSs), mobile phones, Laptops and notebooks.

Cloud Layer – This layer contains the communication infrastructure to connect the device layer and facility layers.

Facility Layer – This layer contains the facility establishment like hospitals, community health service centers and administrators.

To provide a secure communication between people layer and cloud layer an authentication and encryption scheme is proposed. The proposed authentication and encryption scheme for IoT-based medical sensor data comprises of three stages: (a) authentication, (b) encryption, and (c) decryption. Authentication is the first stage of the proposed system.

This stage encompasses three steps: registration, login, and verification. First, the patient registers his or her details on the hospital website or app. After registration, the patient logs into the hospital's website by utilizing a username and password. The registered patient details are maintained in the cloud server and the hospital database. When each patient is registered on the website, a hash code is routinely created utilizing the SHA-512 algorithm for confirming the identity of the patient. During verification, the server confirms whether the patient utilizing the hash function is an authenticated user or not. When the patient is authenticated, the wearable sensor device linked to the patient is activated, and the information from the sensor device is continuously received by the cloud server. The sensor system information is encrypted and transmitted to the cloud server to protect the data from the attackers. Initially, the sensor data from the IoT sensor device is ciphered utilizing substitution Caesar cipher. The substitution cipher is basically an encryption technique by which plain text is swapped with ciphertext in cryptography. After that, the ciphered data is encrypted by the improved elliptical curve cryptography algorithm. The cloud server obtains the encrypted sensor data concurrently and decrypts prior it before sending to hospital system. Subsequently, cloud server sends decrypted data to the hospital management. The figure 2 shows the sequence diagram of proposed authentication scheme.

A. AUTHENTICATION

The initial phase of the proposed scheme is patient authentication. It is an important step in giving access to approved patients. This phase comprises of three steps: (i) registration, (ii) login, and (iii) verification.

1) REGISTRATION

Here, the patients register demographic and biometrics information like patient's name, date of birth, address, medical history and biometrics template in the hospital website or app. In the simulation of the framework, patient's fingerprint has been considered as B_i. After registration, the hash code is generated based on the patients' details utilizing the SHA-512 algorithm.

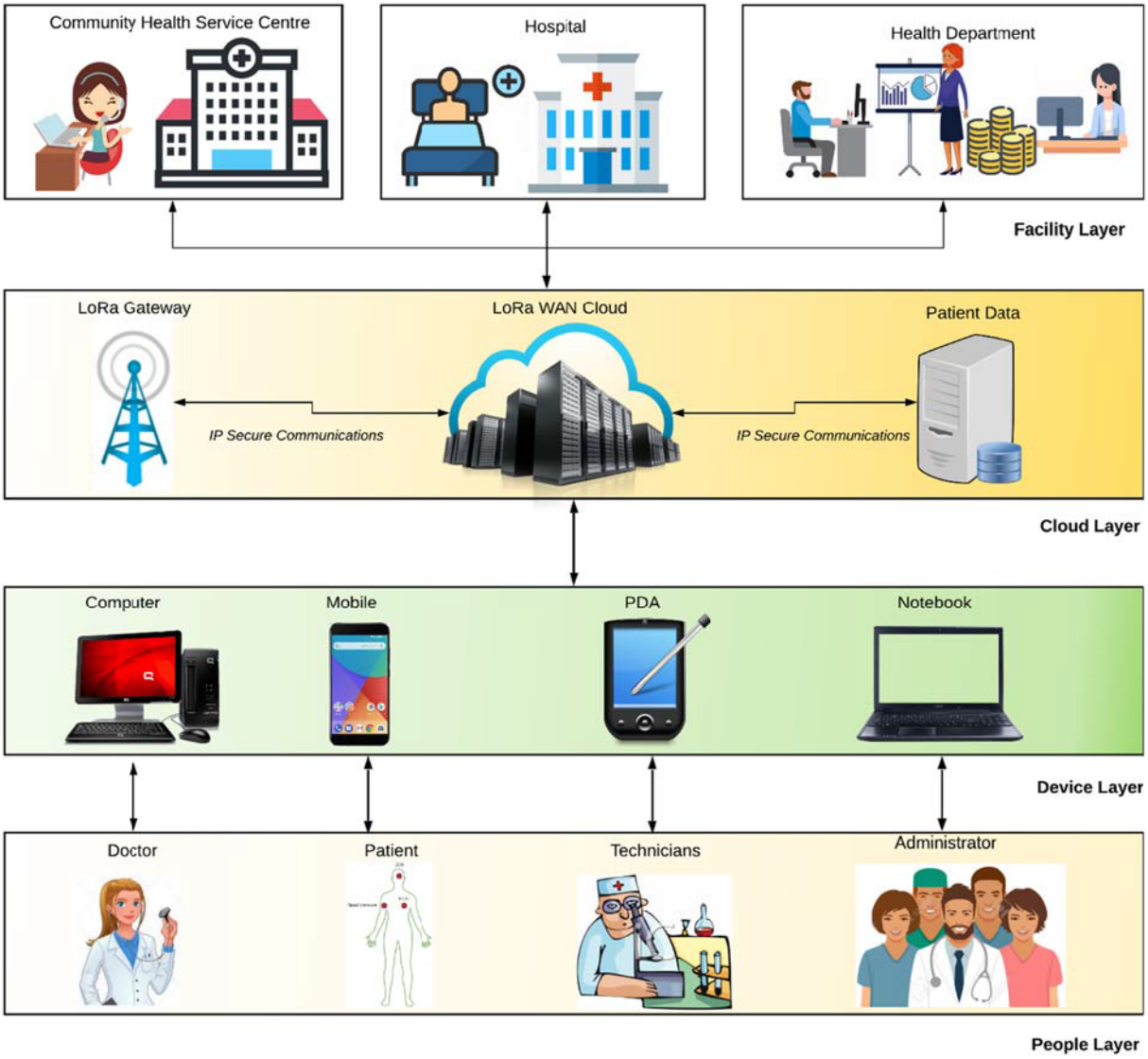

FIGURE 1. Proposed secure framework for IoT-based medical data.

Consider a patient P with identification Id_i along with a password Pw_i. Let a trusted patient be denoted as Tp. During registration, a Tp creates the private key Pr_k. The hash code created by SHA-512 is shown as equation (1):

$$Hc = hf(Id_i \parallel Pw_i \| B_i) \tag{1}$$

where Hc is the hash code that is generated and hf is a hash function.

2) LOGIN

The patients must provide the authentication data given by the hospital superintendent for authentication when they log into the system. The $Id_1, Pw_1,$ *and* B_1^* are joined to create a hash code Hs_1 in the login step utilizing the SHA-512 algorithm as shown in equation (2).

$$Hs_1 = hf(Id_1 \parallel Pw_1 \parallel B_1^*) \tag{2}$$

In the SHA-512 algorithm, few additional bits may be added to make the block size multiple of 1024 bits. The padding can be simply performed by putting '0' bits with leading zeros. The first block is united with the initial vector (IV), and the hash code is created [34]. Subsequently, following blocks are united with hash code that was previously created [34].

Hash code, Hc is joined with the private key Pr_k utilizing XOR operation, and it is encrypted to give E as shown in equation (3):

$$E_c = H_c \oplus Pr_k \tag{3}$$

3) VERIFICATION

In this step, the encrypted value is decrypted to obtain a value D_c. This is carried out by the following mathematical operation as shown in equation (4):

$$D_c = E \oplus Pr_k \tag{4}$$

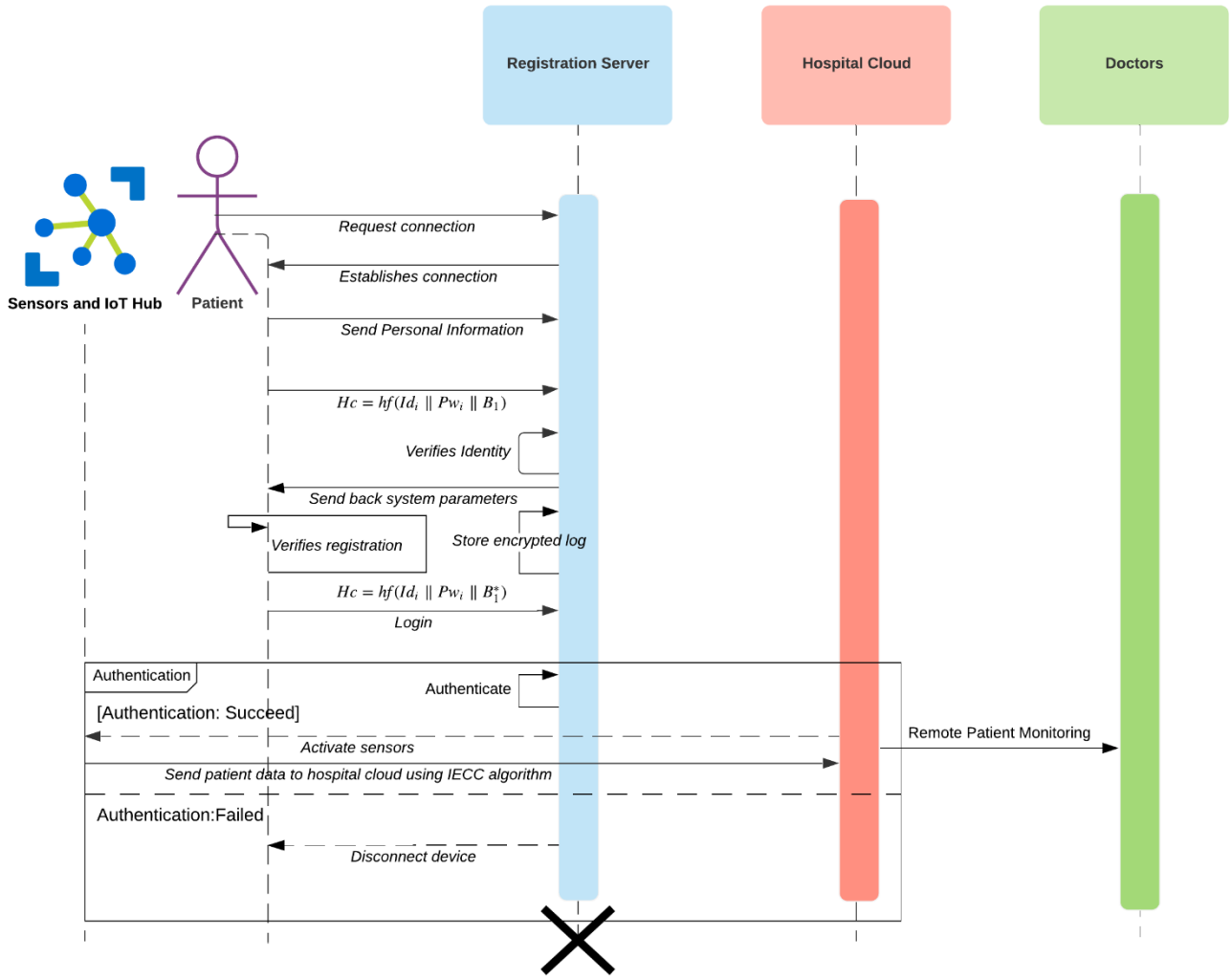

FIGURE 2. Sequence diagram of the proposed authentication and encryption scheme.

TABLE 1. Notation.

Symbol	Description
P_i	Patient i
Id_i	Identification of Patient i
Pw_i	Password of patient i
Tp	Trusted patient
B_i	P_i 's biometric information at the time of user registration phase
B_i^*	P_i 's biometric information at the time of user login phase
Pr_k	Patient's private key
Pu_k	Patient's public key
S_k	Additional key of patient
Hc	Hash code
hf	Has function
$\oplus$	XOR function
E_c	Encrypted code
D_c	Decrypted code
B_s	Base point on curve
$\parallel$	Concatenation
+,-,*	Addition, subtraction and multiplication on elliptic curve

The hash code for the ID_i, PW_i *and* B_2 *and* of the patient is computed again by utilizing the SHA-512 algorithm. This value is shown as equation (5).

$$HS_2 = h(ID_2 \parallel PW_2 \parallel B_2) \tag{5}$$

If the values of Hs_2 and Hs_1 are the same, then the patient is an authorized user, and the sensor device linked to that patient is activated. This should be noted that ID_2, PW_2 *and* B_2 is the data which is already stored at registration server. This is the same data which was created during the registration phase. If these values are not the same, then the patient is an unauthorized user, and his or her access to the system is refused.

B. DATA SECURITY

Following the activation of the IoT sensor devices, the sensor information from the device is directed to the cloud server. Security is required to move the information obtained from the IoT sensor devices. To make sure that privacy is guaranteed in transferring this sensor information, initially the sensor values from the patient are ciphered utilizing

TABLE 2. Comparable strengths of RSA and ECC [33].

Bits of Security	Key size (RSA)	Key size (ECC)	Size Ratio
80	k=1024	f= 160-223	6:1
112	k=2048	f= 224-255	8:1
128	k=3072	f= 256-383	11:1
192	k=7680	f= 384-511	20:1
256	k=15360	f= 512+	30:1

substitution Caesar cipher. After that, the ciphered text is encrypted by the IECC algorithm.

The FIPS 186-2 and ANSI X9.62 both standard presents comparable strength of RSA and ECC algorithms in table 2 [32]–[34] which shows that RSA key size 1024 bits and 160 bits for ECC are equal when compare to their strength.

1) SUBSTITUTION CAESAR CIPHER

First, the sensor values from the IoT sensor device are ciphered utilizing simple substitution cipher. The substitution cipher is basically an encryption technique by which plain text is swapped with ciphertext in cryptography. In the proposed technique, plain substitution cipher is utilized. The substitution of single letters is carried out independently. Simple substitution can be demonstrated by writing the alphabet in a certain order to signify the substitution. This is labeled as a substitution alphabet. The cipher alphabet might be reversed or shifted or else scrambled in a very intricate fashion and is then called a mixed or deranged alphabet. After substitution cipher is performed, the ciphered text is once more ciphered utilizing Caesar cipher. The outcome of substitution cipher is provided to Caesar cipher. It is a sort of substitution cipher in which every letter in the plain text is shifted to a certain place in the alphabet. For instance, with a shift of one, A would be swapped with B, B would become C, and so on. In Caesar cipher, a key is used to shift the message. Here, the key is nothing more than the number of characters by which the cipher alphabet is shifted as shown in equation (6). After performing substitution and Caesar cipher, the ciphered information is encrypted utilizing the improved ECC algorithm and sent to the cloud server.

$$e\,(x) \equiv (x + k)\,(mod 26) \tag{6}$$

where k is the key for shifting each letter and x is the plaintext. The decryption function can be written as shown in equation (7).

$$d\,(x) \equiv (x - k)\,(mod 26) \tag{7}$$

2) IMPROVED ECC ENCRYPTION

The data is encrypted by utilizing the improved ECC(IECC) encryption technique. The improved ECC is curve based that has specific base point derived from functions of prime number as shown in figure 3. Additionally, the ECC algorithm is more intricate and harder to implement, which increases the probability of implementation errors, thus reducing the algorithm's security. Therefore, to enhance security, improved ECC is proposed. In normal ECC, only two sorts of keys are created (public and private key), whereas in improved ECC, an additional key (secret key) is generated to enhance the system's security. The generated secret key is added to the formula of encryption and subtracted from the formula of decryption. In this way, the intricacy of the two phases is augmented. If the intricacy of encryption and decryption is elevated, then it is very hard to detect the original data. It automatically enhances the security level of the data. The mathematical illustration of the improved ECC is shown through equation (8) to (14):

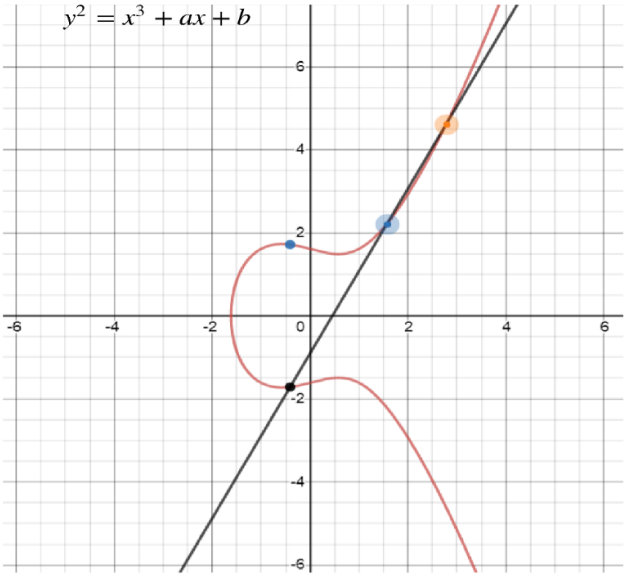

FIGURE 3. Elliptic curve.

$$y^2 = x^3 + ax + b \tag{8}$$

where a and b are integers. The reliability of the encryption is based on the method employed for key generation in a cryptographic process.

Three kinds of keys need to be generated in the proposed system. First, a public key is generated for the encryption of data. The second step is to make a private key for decrypting the data. Initially, the public key is generated for data encryption. Thereafter a private key for decrypting the data is generated. At last, secret key from the private key, public key, and the points on elliptic curve is generated.

Consider point B_s to be a base point on the curve. Choose a random number between 0 and n-1 to make a private key Pr_k. The public key Pu_k is produced as shown in equation (9) and (10):

$$Pu_k = Pr_k * B_s \tag{9}$$

Consider the equation as below:

$$Pu_k = \prod (Pr_k, B_s) \tag{10}$$

where:

Pu_k - public key
Pr_k - private key
B_s - point on elliptic curve

The secret key is generated by summing Pu_k, Pr_k, and B_s, which is written as equation (11):

$$S_k = \sum (Pu_k, Pr_k, B_s) \tag{11}$$

Here, S_k denotes the secret key.

After the generation of the key, the values that are obtained from the IoT devices are encrypted. The encrypted information contains two ciphertext that are mathematically written as equation (12) and (13).

$$C_1 = (S_1 * B_s) + S_k \tag{12}$$
$$C_2 = M + (S_1 * Pu_k) + S_k \tag{13}$$

where C_1 and C_2 are ciphertext 1 and ciphertext 2; S_1 is a random number, which is between 1 and n-1; and M indicates the original message. The original information can be obtained from the decryption procedure.

The inverse of encryption is decryption, therefore, the secret key generated during the decryption phase is subtracted from the normal equation for decryption as shown in equation (14).

$$M = ((C_2 - Pr_k) * C_1) - S_k \tag{14}$$

IV. RESULTS AND DISCUSSIONS

The simulation of proposed authentication and encryption scheme for IoT-based medical sensor data is developed using the Java platform and NS3. For simulation of proposed system Hungarian data set has been used for patient data, which is freely available in public domain [48].

A. PERFORMANCE ANALYSIS(SIMULATION)

First, the performance of the improved ECC security algorithm has been compared to algorithms like ECC and RSA with respect to encryption/decryption time, and security analysis.

1) ENCRYPTION TIME

This indicates the time utilized by the encryption algorithm to create a ciphertext from a plain text. It is the difference between the encryption ending and starting times and is expressed as shown in equation (15).

$$i_{(t)} = i_{end(t)} - i_{start(t)} \tag{15}$$

where:

$i_{(t)}$ - Encryption time
$i_{end(t)}$ - Encryption ending time
$i_{start(t)}$ - Encryption starting time

2) DECRYPTION TIME

This is evaluated by taking the difference between the decryption ending and starting times and is expressed as shown in equation (16).

$$o_{(t)} = o_{end(t)} - o_{start(t)} \tag{16}$$

where:

$o_{(t)}$ - Decryption time
$o_{end(t)}$ - Decryption ending time
$o_{start(t)}$ - Decryption starting time

3) CORRELATION COEFFICIENT ANALYSIS

Statistical analysis such as correlation coefficient factor between plaintext and ciphertext is mostly deployed to ascertain the relationship between the variables [44]. This coefficient indicates the degree of extent the encryption algorithm strongly secures statistical attacks. A strong encryption algorithm should have entirely different ciphertext from plain text [45], [46]. The correlation coefficient shall be calculated by the following equation [43]–[47]:

$$Corr\ Coef\ (x, y) = \frac{\sum_{i=1}^{n} (x_i - \mu(x))(y_i - \mu(y))}{\sigma\ (x)\, \sigma(y)} \tag{17}$$

where:

$\mu(x)$ - mean of x
$\mu(y)$ - mean of y
(x) - plaintext
(y) - ciphertext

$$\mu\ (x) = \frac{1}{n} \sum_{i=1}^{n} x_i \quad \text{and } \mu\ (y) = \frac{1}{n} \sum_{i=1}^{n} y_i \tag{18}$$

The standard deviations of x and y can be expressed as below:

$$\sigma\ (x) = \sqrt{\sum_{i=1}^{N} (x_i - \mu(x))^2}, \quad \text{and}$$
$$\sigma\ (y) = \sqrt{\sum_{i=1}^{N} (y_i - \mu(y))^2} \tag{19}$$

The coefficient = 1, represent identical plaintext and ciphertext while as correlation coefficient = 0, represents that the ciphertext and plaintext are completely different. Thus, strength of the encryption algorithm is indicated by smaller values of the correlation coefficient.

B. PERFORMANCE ANALYSIS (FORMAL)

The cost of authentication phase can be expressed as T_a that consist of hash function and comparison. The encryption cost of substitution Ceaser cipher and IECC is represented by E_c. Importantly, T_{hash} is examined using SHA-512. In order to authenticate the user, it takes $2T_{hash}$ and some negligible t_δ for comparing the received Hs_1 and Hs_2.

The simulation defines 160-bits for all the authentication schemes including time stamps, random numbers, one-way hash functions, wireless access and a medical-sensor node. The computational cost which includes one-way hash function, symmetric encryption/decryption and elliptical curve

TABLE 3. Comparison of hash functions.

Scheme	User	Gateway	Sensors
Shipra et al. [35]	10H	8H	6H
Gope et al. [36]	7H	9H	3H
Wu et al. [37]	11H	17H	6H
Deebak et al. [38]	9H	7H	3H
Proposed	2H	1H	1H

TABLE 4. Performance of authentication and encryption schemes.

Scheme	Computational Cost (μs)			Comm. cost (bits)
	Total	Gateway	sensors	
Shipra et al. [35]	0.328	0.2624	0.1968	3040
Gope et al. [36]	0.2296	0.2952	0.984	2400
Wu et al. [37]	0.3608	0.5576	0.1968	2720
Deebak et al. [38]	0.2908	0.2296	0.984	1216
Proposed	0.1455	0.0722	0.072	1440

point multiplication were assumed to be 0.0005, 0.0087 and 0.063075 micro seconds, respectively [39]–[42]. The proposed authentication and improved ECC applies one-way hash function hf, xor $\oplus$ and concatenation $||$ operations, substitution cipher $e(x)$ and ECC point operation to keep authentication and encryption secure. The cost of $\oplus$ and $||$ is negligible, therefore, the cost of hf, symmetric encryption and IECC is considered. The total computational cost can be computed at user as a registration/login phase hashing cost which is $2H$ while as at sensor it can be computed by adding hashing and encryption cost, i.e. $1H+Ec$. The cost at gateway can be computed by adding the verification and decryption cost i.e. $1H + Dc$. Total computation cost can be expressed as follows:

$$\begin{aligned} &= 2H + (1H + Ec) + (1H + Dc) \\ &= 4H + Ec + Dc \\ &= 0.14555\mu s \end{aligned}$$

The cost in terms of bits can be computed as a function of message structure. The first message which is the registration can be expressed as combination of $(Id_i \| Pw_i \| B_i, H_c)$, the login $(Id_i \| Pw_i \| B_i^*, H_c)$, and message transmission as (C_1, C_2) that takes place between user(patient), gateway, and medical sensor. The message communication overhead of the proposed authentication and encryption scheme can be computed as $(32+32+32+512)+(32+32+32+512)+(32+16+16+160) = 1440$ bits. The table 3 shows that the proposed scheme has a smaller number of hash computation as compared to existing schemes.

C. COMPARATIVE ANALYSIS

Table 5 compares the secure data transfer of IECC with existing ECC and RSA based on encryption time and decryption time. The performance is assessed based on the number of IoT nodes, ranging from 5 to 25. For 25 IoT nodes, the proposed IECC takes 0.35 μs as encryption time, but the existing ECC and RSA take 0.56 μs and 0.84 μs for encryption respectively. Similarly, for the remaining IoT nodes, the proposed IECC takes less encryption time. Likewise, for 25 IoT nodes, the proposed IECC takes 1.55 μs decryption time, but the existing security algorithms take more decryption time. Hence, it is concluded that IECC's encryption and decryption time is faster than other methods. This analysis is graphically illustrated in Figure 4 and 5.

TABLE 5. The comparison of encryption and decryption time (μs).

Number of IoT nodes	Proposed IECC		Existing ECC		Existing RSA	
	$i_{(t)}$	$o_{(t)}$	$i_{(t)}$	$o_{(t)}$	$i_{(t)}$	$o_{(t)}$
5	0.35	0.37	0.56	0.56	0.84	0.87
10	0.87	0.83	1.09	1.13	1.34	1.30
15	1.02	0.98	1.53	1.57	1.72	1.78
20	1.34	1.29	1.86	1.84	2.01	2.07
25	1.58	1.55	2.04	2.03	2.48	2.51
Average Time	1.032	1.004	1.416	1.426	1.678	1.706

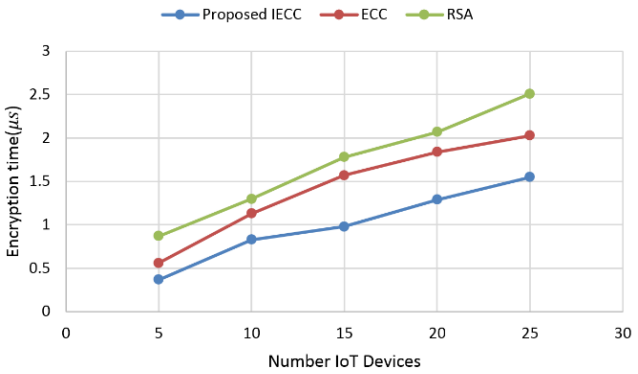

FIGURE 4. Comparative analysis of encryption time.

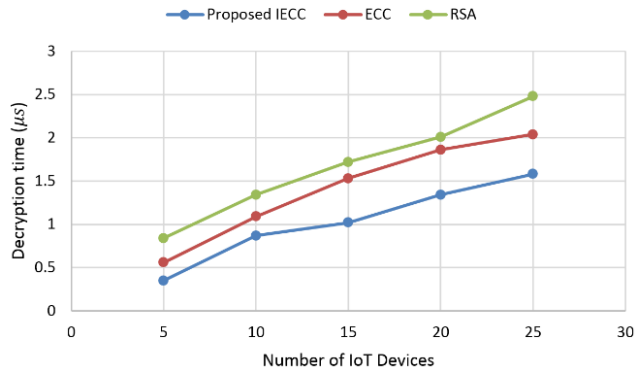

FIGURE 5. Comparative analysis of decryption time.

TABLE 6. Correlation coefficient values of proposed IECC.

Message	Description	Values
M_1	Connection establishment data	0.023
M_2	User registration data	0.014
M_3	User login data	0.053
M_4	Patient data	0.073
M_5	Control messages	0.065
Average		0.045

Table 6 shows the correlation coefficient computed using different type of message set. The results show that the proposed IECC's coefficient of correlation is around 0.045 which is close to zero.

V. CONCLUSION

In this research, a secure framework for authentication and encryption using improved ECC in IoT-based medical sensor data is proposed. The proposed authentication scheme combines biometric parameters in addition to user credentials. To improve the security of ECC, an additional key (secret key) is generated to enhance the system's security. In normal ECC, only two sorts of keys are created (public and private key), whereas in improved ECC, an additional key (secret key) is generated to make the system more secure. Therefore, the intricacy of the two phases is augmented. The scheme achieves security requirements such as low encryption, decryption time and communication overhead. The strength of the proposed framework is proven through formal security analysis and simulation. The evaluation of the proposed scheme compares with existing RSA and ECC. The average encryption and decryption time 1.032 and 1.004 μs respectively, which is lower than the ECC and RSA. A statistical analysis is performed to measure the relationship between plaintext and ciphertext. The average correlation coefficient 0.045 which is demonstrate the strength of the proposed scheme.

As a part of future work, we would like to extend this work for implementation of proposed framework which involve interface with the people layer, device layer, cloud layer and facility layer such as capturing the data from the wearable sensors and performing real-time analysis.

REFERENCES

[1] G. Manogaran, D. Lopez, C. Thota, M. Kaja Abbas, S. Pyne, and R. Sundarasekar, "Big data analytics in healthcare Internet of Things," in *Innovative Healthcare Systems for the 21st Century*. Cham, Switzerland: Springer, 2017, pp. 263–284.

[2] L. M. Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on Internet of Things and cloud computing for healthcare," *Electronics*, vol. 8, no. 7, p. 768, 2019.

[3] F. Ahmed, "An Internet of Things (IoT) application for predicting the quantity of future heart attack patients," *Int. J. Comput. Appl.*, vol. 164, no. 6, pp. 36–40, 2017.

[4] N. Scarpato, A. Pieroni, L. D. Nunzio, and F. Fallucchi, "E-health-IoT universe: A review," *Management*, vol. 21, no. 44, p. 46, 2017.

[5] N. Manh Khoi, S. Saguna, K. Mitra, and C. Ahlund, "IReHMo: An efficient IoT-based remote health monitoring system for smart regions," in *Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom)*, Oct. 2015, pp. 563–568.

[6] L. A. Durán-Vega, P. C. Santana-Mancilla, R. Buenrostro-Mariscal, J. Contreras-Castillo, L. E. Anido-Rifón, M. A. García-Ruiz, O. A. Montesinos-López, and F. Estrada-González, "An IoT system for remote health monitoring in elderly adults through a wearable device and mobile application," *Geriatrics*, vol. 4, no. 2, p. 34, 2019, doi: 10.3390/geriatrics4020034.

[7] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for smart healthcare: Technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26521–26544, 2017.

[8] K.-H. Yeh, "A secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, 2016, doi: 10.1109/ACCESS.2016.2638038.

[9] S. Chandurkar, S. Arote, S. Chaudhari, and V. Kakade, "The system for early detection of heart-attack," *Int. J. Comput. Appl.*, vol. 182, no. 27, pp. 30–33, 2018.

[10] B. David Chung Hu, H. Fahmi, L. Yuhao, C. C. Kiong, and A. Harun, "Internet of Things (IOT) monitoring system for elderly," in *Proc. Int. Conf. Intell. Adv. Syst. (ICIAS)*, Kuala Lumpur, Malaysia, Aug. 2018, pp. 1–6.

[11] A. Youssef and M. Alageel, "Security issues in cloud computing," *GSTF Int. J. Comput.*, vol. 1, no. 3, pp. 36–45, 2011.

[12] E. Ahmed Youssef and M. Alageel, "A framework for secure cloud computing," in *Proc. Int. J. Comput. Sci. Issues (IJCSI)*, vol. 9, no. 4, No 3, pp. 478–500, Jul. 2012.

[13] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of Things in healthcare: Interoperatibility and security issues," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 6121–6125.

[14] M. Abdel-Basset, A. Gamal, G. Manogaran, L. H. Son, and H. V. Long, "A novel group decision making model based on neutrosophic sets for heart disease diagnosis," *Multimedia Tools Appl.*, 2019, doi: 10.1007/s11042-019-07742-7.

[15] K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," in *Proc. 33rd Int. Conv. MIPRO*, Opatija, Croatia, 2010, pp. 344–349.

[16] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *Proc. IEEE 3rd Int. Conf. Cloud Comput.*, Miami, FL, USA, Jul. 2010, pp. 268–275, doi: 10.1109/CLOUD.2010.62.

[17] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9, doi: 10.1109/INFCOM.2010.5462174.

[18] P. K. Gupta, B. T. Maharaj, and R. Malekian, "A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres," *Multimedia Tools Appl.*, vol. 76, no. 18, pp. 18489–18512, Sep. 2017.

[19] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools Appl.*, 2019, doi: 10.1007/s11042-019-07835-3.

[20] J. Vijayashree and S. H. Parveen, "A machine learning framework for feature selection in heart disease classification using improved particle swarm optimization with support vector machine classifier," *Program. Comput. Softw.*, vol. 44, no. 6, pp. 388–397, 2018.

[21] A. A. Mutlag, M. K. Abd Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Gener. Comput. Syst.*, vol. 90, pp. 62–78, Jan. 2019.

[22] A. H. El Zouka and M. M. Hosni, "Secure IoT communications for smart healthcare monitoring system," in *Internet of Things*. Amsterdam, The Netherlands: Elsevier, 2019.

[23] S. Tyagi, A. Agarwal, and P. Maheshwari, "A conceptual framework for IoT-based healthcare system using cloud computing," in *Proc. 6th Int. Conf.-Cloud Syst. Big Data Eng. (Confluence)*, Noida, India, Jan. 2016, pp. 503–507, doi: 10.1109/CONFLUENCE.2016.7508172.

[24] M. Wen, J. Lei, J. Li, Y. Wang, and K. Chen, "Efficient user access control mechanism for wireless multimedia sensor networks," *J. Comput. Inf. Syst.*, vol. 7, no. 9, pp. 3325–3332, 2011.

[25] Li M, Lou W, Ren K, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.

[26] A. Al-Mahmud and M. C. Morogan, "Identity-based authentication and access control in wireless sensor networks," *Int. J. Comput. Appl.*, vol. 41, no. 13, pp. 18–24, 2012.

[27] H. Wang, B. Sheng, and Q. Li, "Elliptic curve cryptography-based access control in sensor networks," *Int. J. Secur. Netw.*, vol. 1, nos. 3–4, pp. 127–137, 2006.

[28] X. H. Le, S. Lee, I. Butun, M. Khalid, R. Sankar, M. Kim, M. Han, Y.-K. Lee, and H. Lee, "An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography," *J. Commun. Netw.*, vol. 11, no. 6, pp. 599–606, 2009.

[29] S. Kavitha, P. J. A. Alphonse, and Y. V. Reddy, "An improved authentication and security on efficient generalized group key agreement using hyper elliptic curve based public key cryptography for IoT health care system," *J. Med. Syst.*, vol. 43, Jul. 2019, Art. no. 260, doi: 10.1007/s10916-019-1378-2.

[30] H. Khemissa and D. Tandjaoui, "A lightweight authentication scheme for E-Health applications in the context of Internet of Things," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Cambridge, U.K., Sep. 2015, pp. 90–95, doi: 10.1109/NGMAST.2015.31.

[31] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019, doi: 10.1016/j.sysarc.2018.12.005.

[32] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer-Verlag, 2004, doi: 10.1007/b97644.

[33] E. B. Barker and Q. H. Dang, "Recommendation for key management Part 3: Application-specific key management guidance," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-57, 2015, doi: 10.6028/NIST.SP.800-57pt1r4.

[34] B. Schneier, *Applied Cryptography*. Hoboken, NJ, USA: Wiley, 1996.

[35] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Comput. Netw.*, vol. 104, pp. 137–154, Jul. 2016, doi: 10.1016/j.comnet.2016.05.007.

[36] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016, doi: 10.1109/TIE.2016.2585081.

[37] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 727–737, May 2018.

[38] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-Healthcare systems in IoT," *IEEE Access*, vol. 7, pp. 135632–135649, 2019, doi: 10.1109/ACCESS.2019.2941575.

[39] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.

[40] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, Jul. 2008, doi: 10.1016/j.comcom.2007.12.005.

[41] W. Li, Q. Wen, Q. Su, and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Comput. Commun.*, vol. 35, no. 2, pp. 188–195, Jan. 2012.

[42] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, and R. Baliyan, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3527–3542, Nov. 2016, doi: 10.1002/sec.1558.

[43] M. Ahmad and M. S. Alam, "A new algorithm of encryption and decryption of images using chaotic mapping," *Int. J. Comput. Sci. Eng.*, vol. 2, no. 1, pp. 46–50, 2009.

[44] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 3156, M. Joye and J. J. Quisquater, Eds. Berlin, Germany: Springer, 2004, pp. 16–29.

[45] I. F. Elashry, O. S. F. Allah, A. M. Abbas, S. El-Rabaie, and F. E. A. El-Samie, "Homomorphic image encryption," *J. Electron. Imag.*, vol. 18, no. 3, 2009, Art. no. 033002.

[46] N. El-Fishawy and O. M. A. Zaid, "Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms," *Int. J. Netw. Secur.*, vol. 5, no. 3, pp. 241–251, Nov. 2007.

[47] A. I. Sallam, O. S. Faragallah, and E.-S.-M. El-Rabaie, "HEVC selective encryption using RC6 block cipher technique," *IEEE Trans. Multimedia*, vol. 20, no. 7, pp. 1636–1644, Jul. 2018.

[48] D. Dua and C. Graff. (2019). *UCI Machine Learning Repository*. University of California, School of Information and Computer Science, Irvine, CA, USA. [Online]. Available: http://archive.ics.uci.edu/ml

MOHAMMAD AYOUB KHAN (Senior Member, IEEE) received the Master of Technology degree in computer science and engineering from Guru Gobind Singh Indraprastha, New Delhi, India, and the Ph.D. degree in computer engineering from Jamia Millia Islamia, New Delhi. He is currently working as an Associate Professor with the University of Bisha, Saudi Arabia. His research interests include the Internet of Things, RFID, wireless sensors networks, ad hoc networks, smart cities, industrial IoT, signal processing, NFC, routing in network-on-chip, and real time and embedded systems. He has more than 14 years of experience in his research area. He has published many research papers and books in the reputed journals and international IEEE conferences. He is contributing to the research community by various volunteer activities in the capacity of an Editor for many journals and the Conference Chair.

MOHAMMAD TABREZ QUASIM (Senior Member, IEEE) received the Ph.D. degree in computer science from Tilkamanjhi University, India. He is currently working as an Assistant Professor with the University of Bisha, Saudi Arabia. His research interests include but are not limited to: the IoT, big data, cloud computing, and blockchain bioinformatics. He has more than seven years of experience in his research area. He has published many journal articles, and edited book, book chapters, and conference papers in various internationally recognized academic databases. He is contributing to the research community by various volunteer activities. He has served as the Conference Chair in various reputed IEEE/Springer.

NORAH SALEH ALGHAMDI received the Bachelor of Computer Science degree from Taif University, Taif, Saudi Arabia, in 2004, and the Master of Computer Science and Ph.D. degrees from the Department of Computer Science, La Trobe University, Melbourne, Australia, in 2015. She has worked as an Assistant Professor with Taif University, from 2016 to 2017. She is currently an Assistant Professor with the Department of Computer Science, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. Her research interests include data mining, machine learning, the IoT, security, and databases.

MOHAMMAD YAHIYA KHAN received the M.Sc. degree in computer science from M. D. University, Rohtak, India. He has more than 15 years of experience in e-learning technologies, networking, the IoT, cybersecurity, and administration. He is currently working as a Supervisor of IT with the College of Sciences, Vice Deanship of Development and Quality, King Saud University, Riyadh, Saudi Arabia.