Research Article

Secure Lightweight IoT Integrated RFID Mobile Healthcare System

Vankamamidi S. Naresh,1, Sivaranjani Reddi,2 and Nistala V. E. S. Murthy3

1Department of Computer Science and Engineering, Sri Vasavi Engineering College, Tadepalligudem, 534101 Andhra Pradesh, India
2Department of Computer Science and Engineering, Anil Neerukonda Institute of Technology & Science, Visakhapatnam, 530003 Andhra Pradesh, India
3Department of Mathematics, Andhra University, Visakhapatnam, 530003 Andhra Pradesh, India

Correspondence should be addressed to Vankamamidi S. Naresh; vsnaresh111@gmail.com

Received 18 August 2019; Revised 4 October 2019; Accepted 7 November 2019; Published 3 March 2020

Copyright © 2020 Vankamamidi S. Naresh et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Patient safety is a global public health concern nowadays, especially in elderly people who need physiological health monitoring systems integrated with a technology which will help to oversee and manage the medical needs. In this direction, we propose a lightweight effective healthcare monitoring system designed by using the Internet of Things (IoT) and Radio Frequency Identification (RFID) tags. In this technique, we use dual-band RFID protocols which are the one working at a high frequency of 13.56 MHz and useful to figure out the individuals, and 2.45 GHz microwave bands are used to monitor corporal information. Sensors are used to monitor and collect patient physiological data; RFID tag is used to recognize the patient. This IoT-based RFID healthcare monitoring system provides acquisition of physiological information of elderly people and patients in hospital. Further, it is aiming to secure patient’s health recordings using hyper elliptic curve- (HEC-) based signcryption algorithm while allowing the doctor to access patient health information. Privacy is provided to variable length patient medical records using different genus curves, and the evaluation shows that the proposed algorithm is optimal with respect to healthcare.

1. Introduction

Mobile healthcare (M-health) system is a system intended to preserve patient health records remotely, allowing doctors to access them from their location to give medical guidance according to need. This arrangement improves accessibility and efficiency, because both patients and doctors need not meet each other. Therefore, patients from their residence can acquire the medical diagnostic suggestions from doctors directly. In this process, RFID technology plays a vital role in patient personal information identification and medical record access ([16, 17]). RFID tag, reader, and middleware are the components present in the RFID system. Tag is used to store a unique identification number, reader is used to read the number present on tag, and middleware is responsible to store and process the data from readers. The technological advancements in this field, in particular development of chip, are very fast, have low activation power (μW), and even able to integrate diverse sensing capabilities. This development opens a challenge of investigating sophisticated applications in IoT paradigm. RFID seems to be the next disruptive modernization in healthcare, which offered several openings for improved safety, functioning effectiveness and economical savings. Even though it promises several benefits in healthcare, the adoption of this technology in healthcare has not been as striking as anticipated and still lags behind compared to other applications due to apprehensions related to security and privacy, radio frequency interference, and inadequacy of industry benchmarks. Hence, security is the major concern in RFID-based healthcare systems. In order to ensure a secured communication, authentication check should happen in tag and reader, encrypting their identification and the patient data to attain confidentiality. Many cryptographic algorithms [2] were suggested to provide security and privacy to message in communication, encryption, and decryption. Table 1 shows the comparative analysis of various cryptographic
algorithms which includes Rivest–Shamir–Adleman (RSA), Diffie Hellman Algorithm (DHA), elliptic curve (EC) ([13, 8–10]), and hyper elliptic curve (HEC) key ([11–13]); from it, we can observe that in HEC, group operations are fast over finite field than EC. For genus, \(g \geq 2\) curves ([14, 15]) can perform operations at a superior level, which made the study of HECC a need of the hour.

1.1. Contributions. The contributions of the proposed work include the following:

(i) Patient registration (RFID tag) and health reading acquisition through sensors

(ii) Transmission of health recordings along with patient RFID tag using a mobile to patient information database through the Wireless Public Network (WPN).

(iii) Secured transmission of patient health records between RPS and authorized entities (doctors and ambulance service) using HEC algorithm

(iv) Comprehensive implementation and security analysis of proposed protocol for genus 2 curve

Section 2 covers literature and mathematical background. The proposed architecture and security algorithms are in Section 3. Section 4 discusses about security analysis. Comparative analysis with existing methods is in Section 5. Finally, summary is in Section 6.

2. Background Work

Patient medical data privacy, maintenance, and security are essential considerations in healthcare. Even though RFID technology guaranteed security and the privacy up to some extent, still it is the most challenging issue ([5–7, 23–25, 27]). The privacy-related challenges mainly arise from counterfeiting the original data in RFID tags, unauthorized data accessing information in transmission [26]. In legal perspective, according to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 in USA, allegedly access of patient data stored in RFID tag is a violation of government regulations. As most of the RFID tags rely on wireless interface, a health monitoring system may also be subject to physical attacks. Eavesdropping is the concern, when patient data is in transmission to the hospital, so authentication is required between them. Research has been going on addressing these issues; [18, 19, 21, 22] have proposed frameworks, which preserve the patients privacy and data security while trying to access the health records. Another study on data secrecy concerns ([28–33]) in healthcare suggests abidance of data captured through RFID, the awareness on existing security policy to medical staffs, and usage of RFID in hospitals [20]. The IoT-based integrated healthcare service structure model [31] that can quickly receive information on patients’ conditions using in-hospital IoT equipment that uses wireless personal area networks such as RFID and Wireless Sensor Networks (WSN) among those low power wireless protocols that are provided by different healthcare service systems to provide healthcare services (e.g., diagnosis and treatment) to patients. An effective healthcare monitoring system used IoT and RFID tags without considering the security perspective [32]. Hu et al. [33] have proposed an intelligent and secure health monitoring scheme using an IoT sensor based on cloud computing and cryptography.

2.1. Mathematical Background of Hyper Elliptic Curves. A HEC \(C\) of genus \(g\) is defined over a field \(\mathbb{GF}(p)\) as

\[
y^2 + h(x) \cdot y = f(x),
\]

where \(\mathbb{C}\) is a nonsingular curve, \(h(x)\) is a polynomial with degree \(h(x) \leq g\), and \(f(x)\) is also a polynomial having degree \(f(x) - 1 = 2\). If \(p > 2\) and \(h(x) = 0\), then \(f(x)\) should be a square-free polynomial. In most situations, no \(x\) and \(y\) in algebraic closure of \(\mathbb{F}_p\), which satisfies HEC \(C\) and the two partial derivatives, i.e., \(2y + h(x) = 0\) and \(h'(x)y - f'(x) = 0\). A divisor \(D\) is a formal sum of points \(P \in \mathbb{C}: D = \sum_{P \in \mathbb{C}} m_P P\) with \(m_P \in \mathbb{Z}\) and for all but finitely many \(m_P = 0\).

The degree and order of \(D\) is \(\sum_{P \in \mathbb{C}} m_P\) and \(m_P\), respectively.

A semireduced divisor of \(D\) is \(\sum m_P Pi - (\sum m_i) \infty\), where each \(m_i \geq 0\) and all the \(P_i\)'s are finite points.

The Principal Divisor (Jacobian) [1] of the curve \(\mathbb{C}\) is expressed as

\[
J = J(\mathbb{C}) = \frac{\text{Div}(\mathbb{C})}{P}.
\]

Let \(D_1, D_2 \in \text{Div}(\mathbb{C})\). We have the following equivalence relation on \(\text{Div}(\mathbb{C})\):

\[
D_1 \sim D_2 \iff D_1 - D_2 \in P
\]

or equivalently:

\[
D_1 \sim D_2 \iff \exists R \in K(\mathbb{C}): D_1 = D_2 + \text{Div}(R).
\]

Each element of Jacobian (\(\text{Jac}(\mathbb{C})\)) is uniquely represented by \(D = P_1 + P_2 + \cdots + P_r - r \cdot \infty\), where \(r \leq g\) and \(P_i\) is asymmetric of \(P_j\).

Let \(D = \sum m_i Pi - (\sum m_i) \infty\) a semireduced divisor, which can be characterized by two polynomials as follows:

(1) \(U(x) = \prod (x - xi)^{m_i}\), a monic polynomial having root, which has the same x-coordinate points in the support of the divisor. The multiplicities of the roots are equal to order of the corresponding \(P\) on it.
infrastructure to increase its effectiveness by relying on the following components: RFID tag, Wireless Body Area Network (WBAN) Sensors, and patient information server.

(1) **RFID tag.** This is a unique identification given to the patient at the time of registration, which will be used in the future by doctors to access patient physiological data. It is the gateway to permit the grant to access the corresponding facilities needed. At first time of admission into the hospital, the patient’s personal details along with the mobile number is transformed onto the patient information server in the back-end along with the RFID tag assigned. It is also used for patient location finding. A mobile RFID reader is a mobile device having a reader embedded in it, developed in Korea and tested on various application services for service confirmation. A mobile RFID phone present in the architecture requests patient identification information by reading the tag attached to the patient through a mobile reader, then transmits this patient’s unique identification number to the back-end information server via middleware.

(2) **WBAN sensors.** Wearable sensor devices on patient body allow monitoring closely the changes in them and in the environment and provide the feedback in order to maintain the finest and instantaneous status. To monitor patient health condition periodically, various sensors like electrocardiogram (ECG), blood pressure sensor, and electroencephalogram (EEG) are placed around the patient body, along with other sensors which can be used to measure the distance, temperature, movement, etc. WBAN is a network that offers continuous monitoring over or inside the human body for a long period and can send real-time traffic such as data, voice, video of patient organism functionalities through the mobile. The mobile used is responsible to transmit the RFID tag onto the back-end patient information server. As WBAN is a short range wireless network, there are different types of wireless protocols such as Bluetooth, ZigBee, WiFi, and IEEE 802.15.6 for communication.

(3) **Patient information server.** It is used to return the requested patient physiological data to the doctor and raise an alarming message to the family members and ambulance service when there is a need. As the communication among the end users and patient information server is in open environment, privacy in the RFID health system is the concern, which permits only authorized users to access the data available on the server. This paper is aimed at providing the privacy protection by adapting the HECC in RPS in the RFID health service network. As and when the patient is connected to the server through the mobile terminal, the patient’s privacy policy can be set up and stored in RPS. Initially, patient RFID tag authentication is inquired by checking the patient tag against the database present; the received patient physiological data update will take place only when there is successful tag verification. While updating the patient’s medical records, it is responsible to check the abnormalities in current readings by comparing them against the clinically approved and established ones.

An alert message will be initiated to the doctor and the family members; based on the severity, an alert message may be sent to ambulance. Notice that in order to define the severity of alert message, we would take the corresponding inputs from the concerned medical experts and use them in RPS. Now, the doctor logs in to the patient’s account which is facilitated by an authentication, after successful verification of the doctors’ authentication. Mutual authentication is achieved via signature generation/verification.

3. Proposed Architecture

The arrangement of the RFID technology-based health monitoring system is aimed at monitoring the medical conditions of the patient by collecting the readings from the sensors attached to the patient and subsequently updated in the back-end database through mobile and the WPN connection subject to patient location. For any minor health hazards, which does not require immediate medical attention, the doctor may be logged into the database using RFID tag and observe the patient current situation for the future reference. Even the doctors or other care providers can access the patient database directly from remote and can communicate directly with the patient through video conference through the internet. In fact, this arrangement facilitates the doctor to diagnose the patient from remote based on the physiological data extracted from the patient database, which is hosted by the middleware. Sometimes, the patient may be suggested to visit the doctor if necessary. Also, the doctor is allowed to write the diagnosis information, medical treatment, and prescription information onto the patient’s information database using the patient’s RFID tag, which will improve the patient quality by eliminating the human errors and the ambiguity in patient-doctor and doctor-doctor interaction while giving the treatment to the patient.

Figure 1 shows the architecture of the proposed arrangement of the healthcare system using RFID technology. This architecture employs the existing wireless communication infrastructure to increase its effectiveness by relying on the following components: RFID tag, Wireless Body Area Network (WBAN) Sensors, and patient information server.

(i) If all $P_i$’s are distinct, $V(x) = \sum_{i} y_i / (\prod_{j \neq i} (x - x_j))$, the unique polynomial such that $\deg(V) \leq \deg(U) - 1$ and $V(x_i) = y_i$ for all $x_i$.

(ii) If all $P_i$’s are equal, we need to compute $V(x)$, the unique polynomial with degree $\leq \sum m_j - 1$ that fulfills the following condition along with the $V(x_j) = y_j$ condition and if multiplicity of $P_i = m_i$ such that $(d/dx)^j [V(x) + V(x)h(x) - f(x)]_{x=x_i} = 0$; for $0 \leq j \leq m_i - 1$, i.e., there exists a unique $V(x)$ such that $(x - x_i)m_i [V(x)2 + V(x)h(x) - f(x)]$.
between the intended parties in the communication. This is achieved by encryption and decryption operations by both the doctor and the server. In our signcryption approach, three phases were present including the following:

(i) Setup: in this phase, system/global parameters is finalized, generating the public/private keys of both doctor and server

(ii) Mutual authentication of the doctor and the server: this phase is aimed at the identification of authorized doctor by checking the mutual authentication between them. In this process, the doctor will generate the signature and send to the server; after checking the signature validity, the server concludes the correctness of the doctor’s identity

(iii) Encryption/decryption

3.1. Global Parameters and Key Generation (Setup). The signature production/verification and encryption/decryption require global parameters, which are available publicly used in the rest of the phases. HECC is used in the proposed work because solving 80-bit HEC is difficult than 160-bit elliptic curve. This makes us to finalize HEC is more appropriate for the applications using RFID. Global parameters (param) chosen for \( \mathbb{C} \) over \( \mathbb{F}_p \) having a unique reduced divisor \( D \), a large random number \( p \), and a large prime divisor \( n \) of \( p - 1 \). \( D \) is represented in the Mumford form as \(<u,v>\). After finalization of the param, the user (tag/reader) chooses a random number \( a \) \(< n \) which is treated as the private key \( PR_a \) and calculates the public key \( PU_a \) using private key as \( PU_a = (PR_a) \times D \); Figure 1 shows the steps in this phase.

3.2. Public Parameters. The parameters publicly available to the doctor and server are as follows:

(i) Select \( p \), find \( n \)

(ii) Select HEC over finite field \( F_p \) be \( G(F_p) \) and let the Jacobian of \( G(F_p) \) be \( JC(F_p) \).

(iii) Pick an element \( D \) \( \in \) \( JC(F_p) \) as a reduced divisor

(iv) \( \text{param} = (p, F_p, G(F_p), D, n) \)

3.3. Signature Generation. This phase uses param, doctor ID as nonce \( (m) \) as the input generate the signature pair \( (r, s) \). Afterwards, the signature pair is attached to an encrypted message and then transmitted onto the other side; Figure 2 shows the signature generation algorithm. A random number \( (k) \) is to be generated, used in \( r \) computation. The D-Quark Hash algorithm is used in a hash value on a given message. Although DSS states the importance of Secure Hash Algorithm (SHA-1), we have used D-Quark asSHA algorithm which is computationally intensive in hash value calculation compared to D-Quark; also, it consumes less power and storage. Figure 2 shows the comparative analysis of different Quark algorithms; it presents three families U,
D, and S Quark algorithms; and the comparative analysis is carried based on parameters no of rounds, digest length, rate, and capacity.

D-Quark was designed to provide 160-bit preimage resistance and at least bit security against all other attacks and to admit a parallelization degree of 8. Taken \( r_1 = 16; c_1 = 160; b_1 \) and \( n_1 = 176 \).

Initialize \( X \) with first \( b_1/2 \) input bits, \( Y \) to last \( b_1/2 \) input bits, and \( L \) to all \( 1s \), i.e., \( X = (s_0, s_1, \ldots, s_{(b_1/2)-1}) \) where \( s \) is the internal state.

\[
Y = (s_{(b_1/2)-1}, \ldots, s_{b_1-1})
\]

\[
L = (1, 1, \ldots, 1).
\]

(i) Function \( f_{11} \): D-Quark \( f \) uses an 88-bit register \( X \) and returns \( X0 + X11 + X18 + X27 + X36 + X42 + X47 + X58 + X64 + X67 + X71X + X71X79 + X42X47 + X11X19 + X58X67X71 + X27X36X42 + X11X36X58X79 + X42X47X67X71 + X19X27X71X79 + X47X58X67X71X79 + X11X19X27X36X42 + X27X36X42X47X58X67 \)

(ii) Function \( g_{11} \): it uses \( Y \) (88-bit) register and returns \( Y0 + Y9 + Y20 + Y25 + Y38 + Y44 + Y47 + Y54 + Y63 + Y67 + Y69 + Y69Y78 + Y44Y47 + Y9Y19 + Y54Y67Y69 + Y25Y38Y44 + Y9Y38Y54Y78 + Y44Y47Y67Y69Y78 + Y9Y19Y25Y38Y44 + Y25Y38Y44Y47Y54Y67 \)

(iii) Function \( h_{11} \): for a given registers \( X, Y \), and \( L \) (10bit), returns \( L0 + X1 + Y2 + X5 + Y12 + Y24 + X35 + X40 + X48 + Y55 + Y61 + X72 + Y79 + Y4X68 + X57X68 + X68Y79 + Y4X35X57 + Y4X57X68 + Y4X57Y79 + L0X35X57Y79 + L0X35 \)

3.4. Signature Verification. After receiving the signature pair \((m', r'', s')\), the receiver will calculate the parameters \( R, w, u_1, u_2, \) and \( V \); the user is valid when \( V \) is equal to \( r'' \). The procedure followed in signature verification is shown below. In \( u_1 \) value calculation, the receiver (server) has to decrypt the cipher text \( C' \) received from the sender (doctor) to extract A’s identity; the hash value is computed on the received ID. The signature generation and verification can be done by both the doctor and the server to establish mutual authentication before the commencement of communication.
D-Quark algorithm
Input: \( r_1, c_i, b_i, f_{i1}, g_{i1}, \) and \( h_i \), where \( r_1 \): rate; \( c_i \): capacity; \( b_i \): width; \( n_i \): digest length; and \( f_{i1}, g_{i1} \) and \( h_i \) functions
Output: message digest of \( n_i \) length
1. Initialization: message is padding by a \( 1 \) followed by \( 0 \) bits to make message length equal to multiples of \( r \)
2. Absorption: XOR \( r \) bit length of message block with state
3. Squeezing: once all blocks of the message are processed by the absorbing phase, extract \( r \) bits from the bitrate part of the internal state and then forward to permutation phase
4. Permutation: the permutation \( P \) is applied onto it to generate a fixed \( n_i \) bit hash value

**Algorithm 3**

Cantor algorithm (composition)
Input: HEC: \( y^2 + h(x) \cdot y = f(x) \), \( P = [u_p, v_p], Q = [u_q, v_q] \)
Output: semireduced divisor \( D = P + Q = [u_e, v_e] \)
1. Calculate \( d_1 = \text{GCD}(u_p, u_q) = e_1 u_1 + e_2 u_2 \)
2. Calculate \( d = \text{GCD}(d_1, v_p + v_q + h) = f_1 d_1 + f_2 (v_p + v_q + h) \)
where \( d = s_1 u_p + s_2 u_q + s_3 (v_p + v_q + h) \); \( s_1 = f_1 e_1, s_2 = f_2 s_2 s_3 = f_2 \)
3. Calculate \( u_e = u_p u_q / d^2; v_e = s_1 u_p v_q + s_2 u_q v_p + s_3 (v_p v_q + f) / d \) mod \( u_r \)

**Algorithm 4**

Signature verification algorithm
Input: param, \( r'' \), \( s' \), \( C' \)
Output: signature valid or invalid
1. User B computes \( R = \theta(r'') \mod n \)
2. Calculate \( w = (s')^{-1} \mod n \)
3. \( u_1 = H(D(C')) \mod n \) and \( u_2 = R \mod n \)
4. Calculate \( V = w \cdot [u_1 \cdot D + u_2 \cdot PU_a] \)
5. If \( V = = r'' \), then signature is valid; otherwise, invalid

**Algorithm 5**

HEC RFID decryption algorithm
Input: param, \( PU_a \), \( PR_b \), \( C \)
Output: \( m \)
1: compute \( X = PR_b \ast PU_a \)
2: return \( m = \{ C - X \} \)

**Algorithm 7**

3.6. Decryption Algorithm. After the receiver receives the cipher text, the doctor/server ID is extracted by subtracting \( X \), which is the product of the receiver’s private key and the senders public key; the detailed decryption algorithm is given below.

**4. Security Analysis**

The proposed protocol can be able to provide the security services like confidentiality, unforgeability, authentication, forward secrecy, and availability.

4.1. Confidentiality. To facilitate confidentiality, information should be only intangible to unauthorized access to an eavesdropper or interceptor. If an adversary is interested in session key \( k \) acquisition, he/she needs to estimate \( b \) from \( Y \) and \( k \) from \( X = aD \) and \( r = k \) which is corresponding to solving HCDLP.

4.2. Integrity. Integrity check insures no alteration in data in transmission and is the same as the one sent by the sender. Due to the property of the random oracle model, “it is not practicable that two different messages have identical digest/hash value.” In our scheme, the doctor/server verifies the
The proposed HECC algorithm on di
signature based on hash of the patient message to check

### 4.3. Authenticity

The property is aiming to confirm from where the message came and checks the ownership of user on the issued message called authenticity. In our proposed scheme, authenticity is based on signature generation and verification.

### 4.4. Unforgeability

It means it is infeasible for an intruder to construct valid signature without a secret key. The proposed technique is unforgeable as it is based on unforgeable hyper elliptic curve digital signature algorithm (HECDSA).

### 4.5. Nonrepudiation

Nonrepudiation restricts server from denying the signed/encrypted text it sent. Unforgeability insures nonrepudiation. If the server denies, the doctor sends signed/encrypted text to middleware; by using a verification technique, middleware can decide that the message is sent by the server.

### 4.6. Forward Secrecy

It infers that session key used in communication would not be compromised although a long-term private key revealed. In the proposed system, if an adversary obtains $d_s$ for computing session key, “$k$” needs “$r$.” Computing “$r$” is equivalent to solving a computational hard problem Hyper Elliptic Curve Discrete Logarithm Problem (HECDLP).

## 5. Experimentation and Results

The proposed HECC algorithm on different genus values was developed using a SAGE software package designed for working out in algebraic geometry and combinatorics on intel® core™ i5-6500 CPU@3.20 GHz,4 GB RAM with a 64 bit windows 10 operating system. Table 2 shows the hyper elliptic curves over $GF(p)$.

<table>
<thead>
<tr>
<th>Genus</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$x^5 + f_1 x^2 + f_2 x + f_0$</td>
</tr>
<tr>
<td>3</td>
<td>$x^7 + f_1 x^5 + f_2 x^4 + f_3 x^3 + f_0$</td>
</tr>
<tr>
<td>4</td>
<td>$x^9 + f_1 x^7 + f_2 x^6 + f_3 x^5 + f_0$</td>
</tr>
<tr>
<td>5</td>
<td>$x^{11} + f_1 x^{10} + f_2 x^9 + f_3 x^8 + f_0$</td>
</tr>
<tr>
<td>6</td>
<td>$x^{13} + f_1 x^{11} + f_0$</td>
</tr>
</tbody>
</table>

### Table 2: HECs over the finite field $GF(p)$.

<table>
<thead>
<tr>
<th>Genus</th>
<th>Group order $p$</th>
<th>Point addition $3.92$</th>
<th>Point doubling $1.55$</th>
<th>Scalar multiplication $8.87$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$2^{191}$</td>
<td>$815$</td>
<td>$877$</td>
<td>$3.54$</td>
</tr>
<tr>
<td></td>
<td>$2^{185}$</td>
<td>$538$</td>
<td>$633$</td>
<td>$2.9$</td>
</tr>
<tr>
<td>3</td>
<td>$2^{175}$</td>
<td>$783$</td>
<td>$730$</td>
<td>$3.54$</td>
</tr>
<tr>
<td></td>
<td>$2^{161}$</td>
<td>$752$</td>
<td>$671$</td>
<td>$3.38$</td>
</tr>
<tr>
<td></td>
<td>$2^{150}$</td>
<td>$559$</td>
<td>$613$</td>
<td>$3.42$</td>
</tr>
<tr>
<td>4</td>
<td>$2^{189}$</td>
<td>$579$</td>
<td>$518$</td>
<td>$2.35$</td>
</tr>
<tr>
<td></td>
<td>$2^{184}$</td>
<td>$563$</td>
<td>$508$</td>
<td>$3.6$</td>
</tr>
<tr>
<td>5</td>
<td>$2^{174}$</td>
<td>$738$</td>
<td>$672$</td>
<td>$3.11$</td>
</tr>
<tr>
<td></td>
<td>$2^{160}$</td>
<td>$767$</td>
<td>$698$</td>
<td>$3.24$</td>
</tr>
</tbody>
</table>

### Table 3: Computation time of group operations.

### Table 4: Generation of RFID tag hash code using D-Quark algorithm.

<table>
<thead>
<tr>
<th>Tag number</th>
<th>D-Quark parameters $c_i = [20, 3, 2, 20], n_1 = 22$</th>
</tr>
</thead>
<tbody>
<tr>
<td>01000000000000000000053d0444657f000010000000000000</td>
<td>$c_1 = 20, r_1 = 2, b_1 = 22, n_1 = 22$</td>
</tr>
<tr>
<td>Initialization $cc6c4ab7f11f9bdf8de03d887eb91a79b6906e9$</td>
<td>$d01314a3679f3e7a2b6e45849f6ed5d4c8914f8030$</td>
</tr>
<tr>
<td>Permutation $82c7f380e231578e2f4c2a402e18f37aea8477298d$</td>
<td>$7f8662217372833782356085717342356916$</td>
</tr>
</tbody>
</table>

$$f_4 = 172713717276878635965125059444256197781;$$
$$f_3 = 1327161209345333507125059444256188021;$$
$$f_2 = 172713717209345335965125059444256188021;$$
$$f_2 = 909765590170000006083734366502844276758;$$
$$f_0 = 666798662217372833782356085717342356916. \quad (5)$$

After the discussion of the proposed algorithm, the basic operations recognized in this are point addition, doubling, and scalar multiplication; the time required for completing these operations with respect to various field lengths is shown in Table 3. In the experimentation, firstly, the comparative analysis was done for different time estimations.
on different genus for operations of Jacobian, divisor recognition, key and signature generation, verification, and message encryption/decryption by varying field length $p$ such as $2^{10}$, $2^{128}$, $2^{256}$, and $2^{512}$. Further, the proposed protocol is compared with respect to HEC over a finite field by changing sizes.
Table 4 described the hash code value computation on the given tag using D-Quack algorithm discussed in Section 3. The computation time for Jacobian, divisor, key, signature generation/verification, and encryption/decryption is shown in Figures 3–9, respectively. From the figures, it is observed that as accumulative of genus along with field sizes, the time is increasing. Since HEC with an operand size is only a fractional amount, the proposed protocol is suitable for devices which require less storage requirements. The RFID reader has good computational capacity since it is connected.
to the server directly. But RFID tag is having less computational capacity, so it has less computational amount of time. The proposed method is compared with existing methods shown in Table 5; we can observe that better performance is achieved through Moosavi et al. [9] and the proposed protocol than [1, 3, 4] and [33] protocols.
6. Conclusion

In this paper, we proposed an architecture, which is suitable for several hospitals or to elder people and is responsible to monitor the health condition continuously and store patient medical records in the back-end database through middleware. Further, we proposed a hyper elliptic curve-based secure lightweight IoT integrated RFID mobile health care system to ensure security and privacy to the health records which are shared between the server/doctor. Security services mutual authentication and confidentiality are attained. Experimentation shows that the proposed protocol has better efficiency than other existing methods.

Data Availability

The Experimental information used to help the discoveries of this investigation are accessible from the corresponding author upon request, with this perusers can get to the information supporting the concluding remarks. Author’s contributions: The principal inventor Dr. V.S. Naresh thought about the introduced thought and built up the hypothesis and played out the calculations. The subsequent author confirmed the scientific strategies and security investigation. The principal creator Dr. V. S. Naresh urged the third creator to execute and managed the discoveries of this work. All creators examined the outcomes and added to the last composition.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

I would like to dedicate this work to my great father V. Bala Surya Narayana and thank my family members and the management of Sri Vasavi Engineering College, Tadepalligudem, who encouraged and supported me to do this work.

References


