Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 1468281, 13 pages
https://doi.org/10.1155/2020/1468281

Research Article

Secure Lightweight IoT Integrated RFID Mobile Healthcare System

Vankamamidi S. Naresh,[1] **Sivaranjani Reddi**,[2] **and Nistala V. E. S. Murthy**[3]

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

Guest Editor: Zahia Guessoum

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

Table 1: Comparison of key sizes (bits).

Field	RSA and DH	EC	HEC
$F(2^{80})$	1024	160	50-80
$F(2^{112})$	2048	224	112
$F(2^{128})$	3072	256	128
$F(2^{192})$	7680	384	192
$F(2^{256})$	15360	512	256

algorithms which includes Rivest–Shamir–Adleman (RSA), Diffie Hellman Algorithm (DHA), elliptic curve (EC) ([3, 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 $''\mathbb{C}''$ of genus g is defined over a field $G(Fp)$ as

$$y^2 + h(x) \cdot y = f(x), \tag{1}$$

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 $h(x)$ is 0, then $f(x)$ should be a square-free polynomial. In most situations, no x and y in algebraic closure of $\mathcal{F}_q$, which satisfies HEC $''\mathbb{C}''$ 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 $P \in C : D = \sum_{P \in \mathbb{C}} m_P P$ with $m_p \in Z$ 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 $D = \sum_i m_i Pi - (\sum_i m_i)\infty$, where each $m_i \geq 0$ and all the $Pi's$ are finite points.

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

$$J = J(\mathbb{C}) = \frac{\mathrm{Div0}(C)}{P}. \tag{2}$$

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

$$D1 \sim D2 \Longleftrightarrow D1 - D2 \in P \tag{3}$$

or equivalently: $D1 \sim D2 \Longrightarrow \exists R \in K(C)$: $D1 = D2 + \mathrm{Div}(R)$.

Each element of Jacobian $(\mathrm{Jac}(\mathbb{C}))$ is uniquely represented by $D = P1 + P2 + \cdots + Pr - r \cdot \infty$, where $r \leq g$ and P_i is asymmetric of P_j.

Let $D = \sum_i m_i Pi - (\sum_i m_i)\infty$ 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

(2) At this juncture, there are two scenarios as follows:

(i) If all $Pi^{'}s$ are distinct, $V(x) = \sum_i y_i((\prod_{j\neq i}(x - xj))/(\prod_{j\neq i}(xi - xj)))$, the unique polynomial such that $\deg\ (V) \leq \deg\ (U) - 1$ and $V(xi) = y_i$ for all x_i

(ii) If all $Pi^{'}s$ are equal, we need to compute $V(x)$, the unique polynomial with degree $\leq \sum_i m_i - 1$ that fulfills the following condition along with the $V(x_i) = y_i$ 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 $(x - xi)m_i|\,(V(x)2 + V(x)h(x) - f(x))$

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.

(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

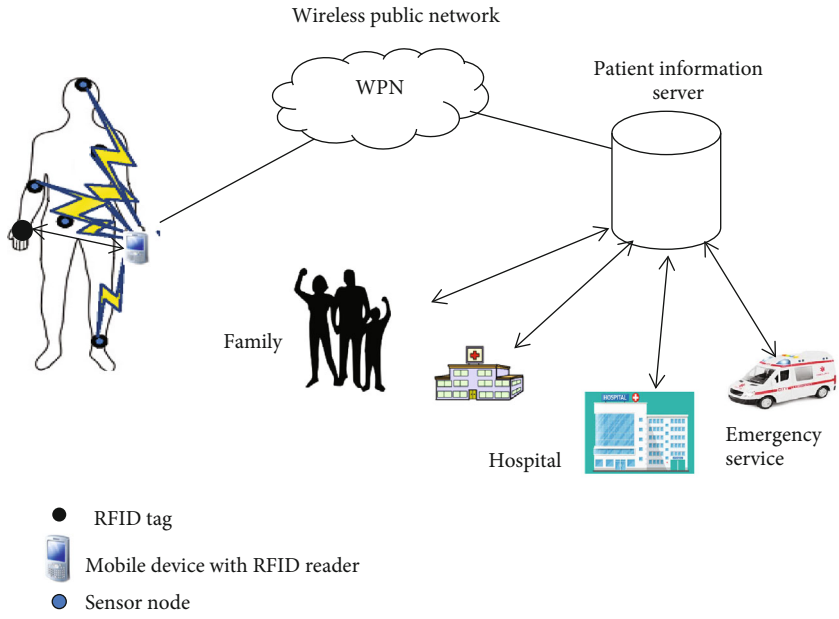

Figure 1: RFID mobile healthcare system architecture.

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 sever; 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 Fp, 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 $(PU_a) = (PR_a) * D$; Figure 1 shows the steps in this phase.

Public and private key generation algorithm
Input: public parameters param
Output: public key (PU_a) and private key (PR_a)
1. Choose $a \in [1, n-1]$, assign to PR_a
2. Compute $PU_a = a * D$

Algorithm 1: Algorithm to generate public and private keys.

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 $D \in JC(Fp)$ as a reduced divisor

(iv) 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,

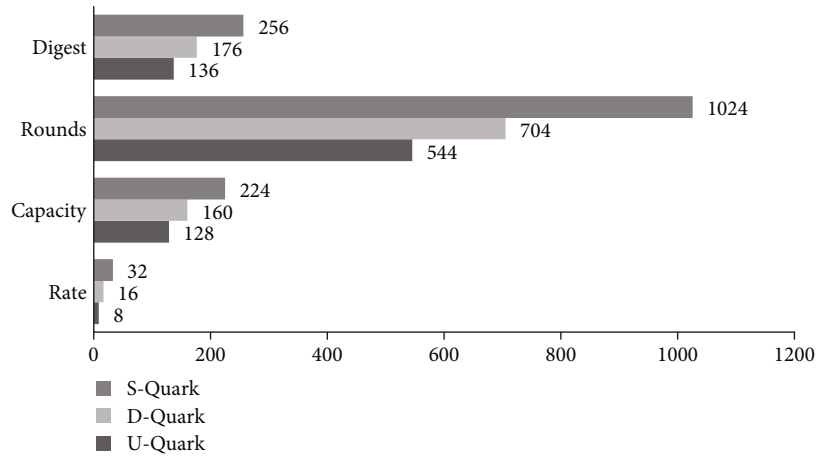

Figure 2: Comparison of Quark algorithms.

Signature generation algorithm
Input: param, m
Output: signature pair (C, r, s)
1. Choose $k \in [1, n-1]$ and calculate $r = k\,D$
2. The function $\theta : J(Fp) \rightarrow Fp \ni \theta(r) = r'$, i.e., map r to r' using Mumford's representation of the points of $J(F_q)$, θ is defined by

$$\theta(r) = \begin{cases} u_1, & u_1,\ if\ D = [\mathbf{x}^2 + u_1\mathbf{x} + u_0, v(\mathbf{x})], \\ u_0, & if\ D = [\mathbf{x} + u_0, v(\mathbf{x})], \\ 0, & if\ D = [1, 0] \end{cases}$$

3. Calculate $r' = \theta(r) \bmod n$, $C = E(m)$
4. Calculate $s = k^{-1}(H(m) + PR_a r') \bmod n$
5. Send user public key and the signature pair (C, r, s) onto other side user B.

Algorithm 2

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 b1/2 input bits, Y to last b1/2 input bits, and L to all 1s, i.e., $X = (s_0, s_1, ---, s_{(b1/2)-1})$ where s is the internal state.

$$Y == \left(s_{(b1/2)}, ---, s_{b1-1}\right),$$
$$L = (1, 1, \cdots.., 1). \tag{4}$$

(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 $Y0 + Y9 + Y20 + Y25 + Y38 + Y44 + Y47 + Y54 + Y63 + Y67 + Y69 + Y69Y78 + Y44Y47 + Y9Y19 + Y54Y67Y69 + Y25Y38Y44 + Y9Y38Y54Y78 + Y44Y47Y67Y69 + Y19Y25Y69Y78 + Y47Y54Y67Y69Y78 + Y9Y19Y25Y38Y44 + Y25Y38Y44Y47Y54Y67$

(iii) Function h_1: 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_1, b_1, f_{11}, g_{11}, and h_1, where r_1: rate; c_1: capacity; b_1: width; n_1: digest length; and f_{11}, g_1, and h_1: functions
Output: message digest of n_1 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_1 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 $D = P + Q = = [u_r, v_r]$
1. Calculate $d_1 = \mathrm{GCD}\,(u_p, u_q) = e_1 u_1 + e_2 u_2$
2. Calculate $d = \mathrm{GCD}(d_1, v_p + v_q + h) = f_1 d_1 + f_2(v_p + v_q + h)$,
where $\mathrm{d} = s_1 u_p + s_2 u_q + s_3(v_p + v_q + h)$; $s_1 = f_1 e_1$, $s_2 = f_1 e_2$;$s_3 = f_2$
3. Calculate $u_r = u_p u_q / d^2$; $v_r = s_1 u_p v_q + s_2 u_q v_p + s_3(v_p v_q + f)/d \bmod u_r$

Algorithm 4

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

Algorithm 5

HEC RFID encryption algorithm
Input: param, PR_a, m, PU_b
Output: C
1: compute $Y = PR_a.PU_b$
2: return $C = \{m + Y\}$

Algorithm 6

3.5. Encryption Algorithm. In signature generation process, individual doctor/server ID is encrypted and then transferred to the other end. The encryption process is shown below. Once the message willing to be communicated is finalized, then the sender (doctor/server) computes the Y by multiplying the sender's private key with the receiver's public key that is added to the message in order to produce the cipher text. This algorithm is intended to secure either their ID or message intended to communicate to the other end.

HEC RFID decryption algorithm
Input: param, PU_a, PR_b, C
Output: m
1: compute $X = PR_b * PU_a$
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

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

Genus	$f(x)$
2	$x^5 + f_3x^3 + f_2x^2 + f_1x + f_0$
3	$x^7 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$
4	$x^9 + f_7x^7 + f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$
5	$x^{11} + f_9x^9 + f_8x^8 + f_7x^7 + f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$
6	$x^{13} + f_{11}x^{11} + f_{10}x^{10} + f_9x^9 + f_8x^8 + f_7x^7 + f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$

signature based on hash of the patient message to check the integrity.

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 signcrypted text it sent. Unforgeability insures nonrepudiation. If the server denies, the doctor sends signcrypted 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_a 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 $GF(p)$.

$$f_{11} = 1325136172093450000751250594442561670 21;$$

$$f_{10} = 1727137172093453359651250594442561977 81;$$

$$f_9 = 3474423475824521858939032977073425614 9;$$

$$f_8 = 1325136172034250000751250594477761670 28;$$

$$f_7 = 1727137172093453359651996744425619778 1;$$

$$f_6 = 3474456775824521858939032977070420714 9;$$

$$f_5 = 1327136758934533507512505944425618802 1;$$

Table 3: Computation time of group operations.

Genus	Group order	Point addition	Point doubling	Scalar multiplication
1	2^{191}	3.92	1.55	8.87
2	2^{190}	815	877	3.54
	2^{185}	538	633	2.9 ms
	2^{175}	783	730	3.54
	2^{161}	752	671	3.38
	2^{150}	559	613	3.42
3	2^{189}	579	518	2.35 ms
	2^{184}	563	508	3.67 ms
	2^{174}	738	672	3.11
	2^{160}	767	698	3.24

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

Tag number	0100000000000000853d0444657f0000010000000000
D-Quark parameters	$c_1 = 20$, $r_1 = 2$, $b_1 = 22$, $n_1 = 22$
Initialization	cc6c4ab7d11fa9bdf6eede03d87b68f91baa706c20e9
Permutation	d013143e679faec7a2b6eb458498fed5dc498145f380
Hashcode	82c7f380e231578e2ff4c2a402e18bf37aea8477298d

$$f_4 = 1727137172768786359651250594442561977 81;$$

$$f_3 = 1327136172093453350751250594442561880 21;$$

$$f_2 = 1727137172093453359651250594442561880 21;$$

$$f_1 = 9090765590170000060837343605284423767 58;$$

$$f_0 = 6667986622173728337823560857173423569 16. \quad (5)$$

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

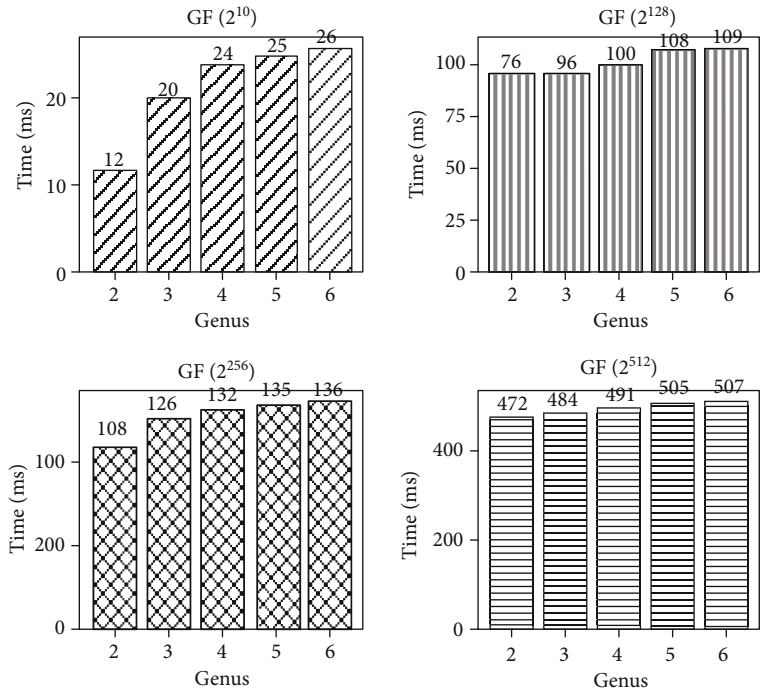

Figure 3: Jacobian computation time.

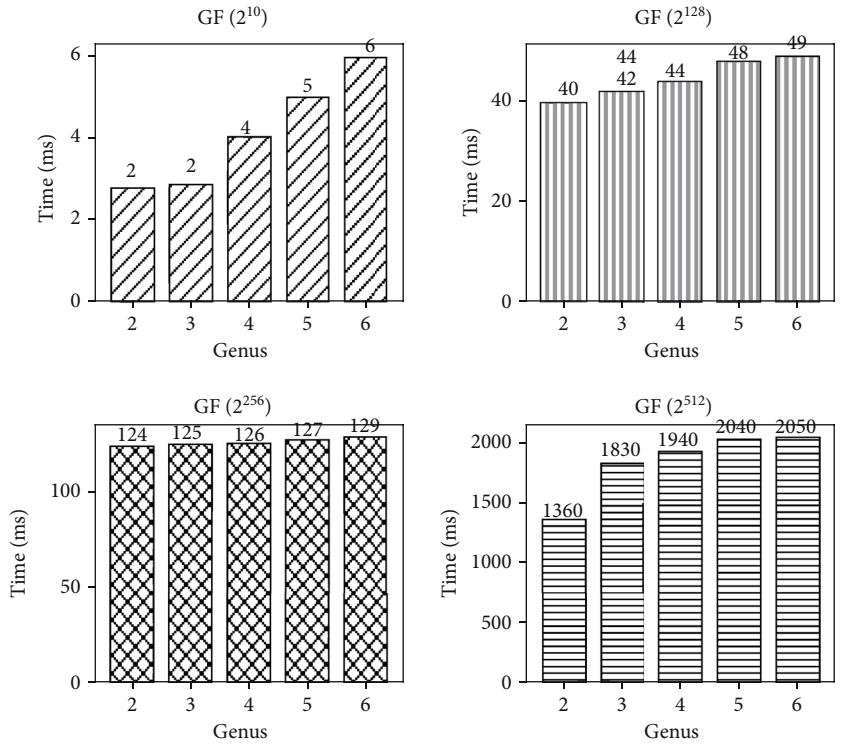

Figure 4: Divisor computation time.

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.

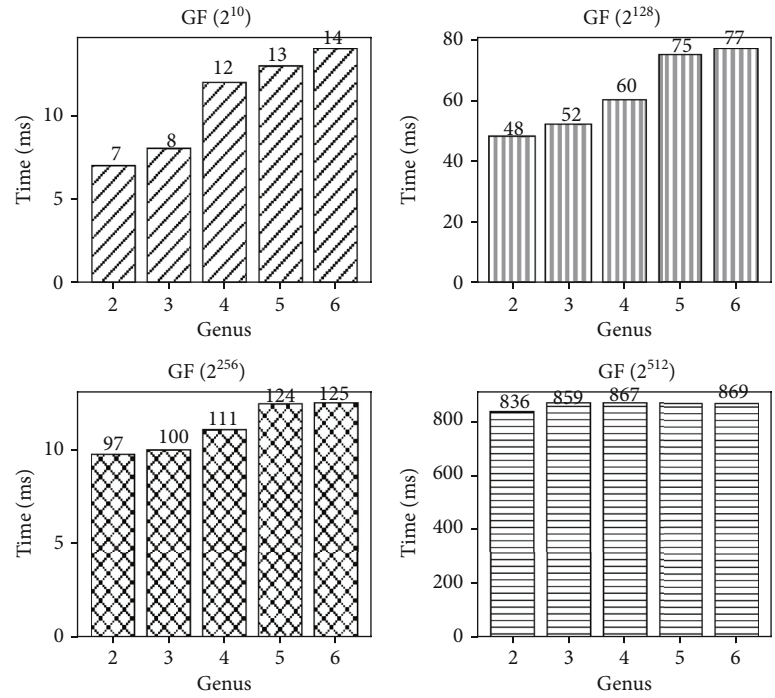

Figure 5: Key agreement time.

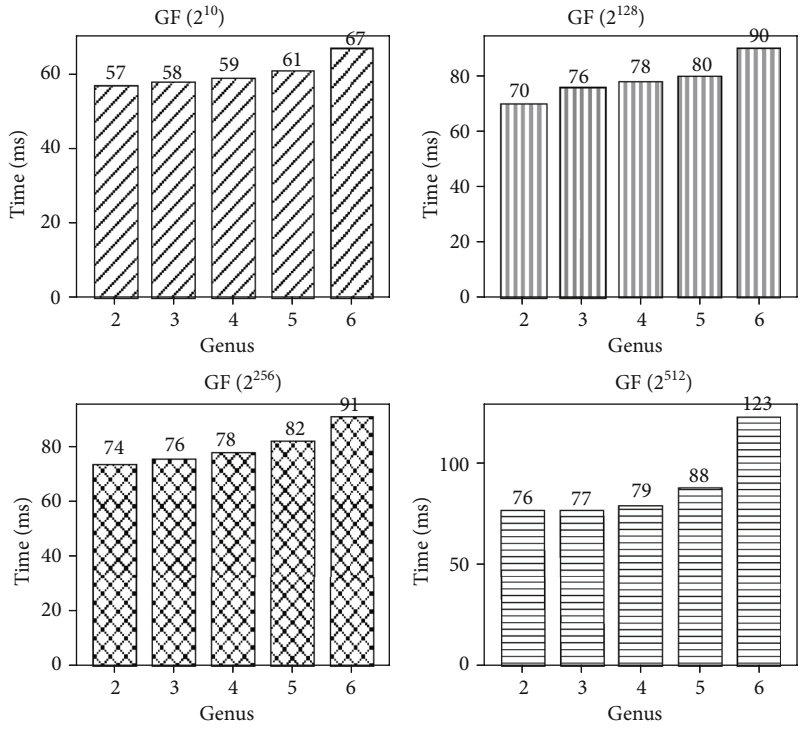

Figure 6: Signature generation time.

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

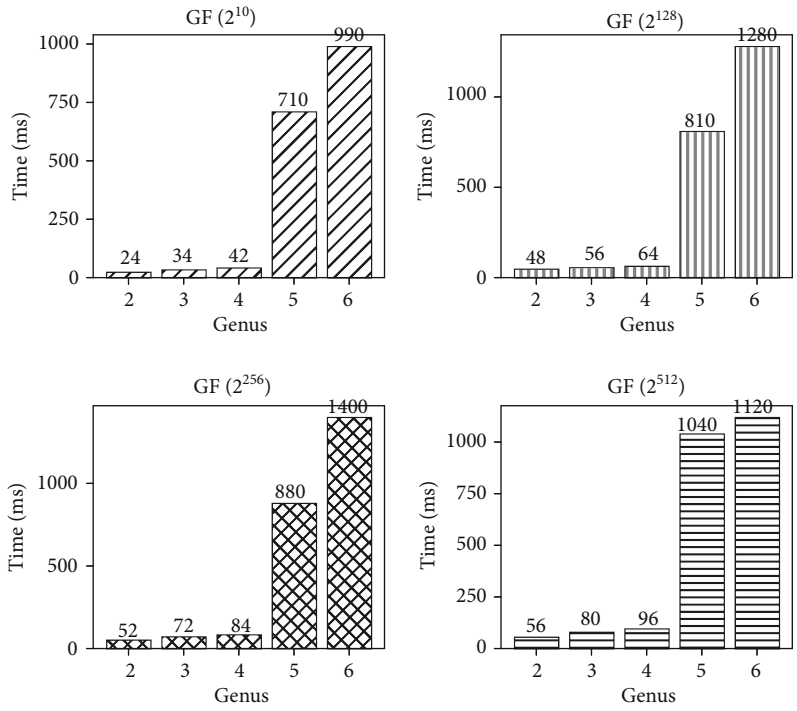

Figure 7: Signature verification time.

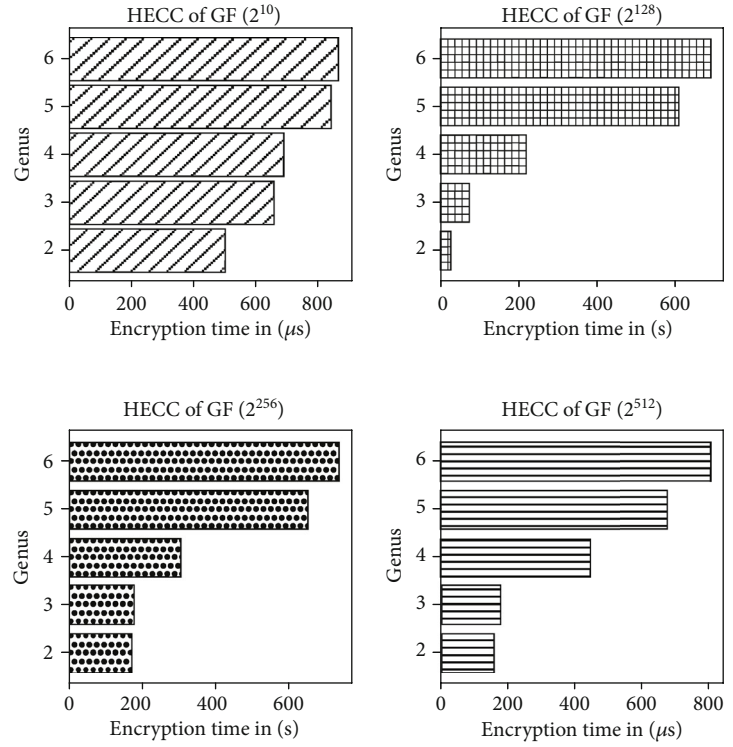

Figure 8: Encryption time.

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.

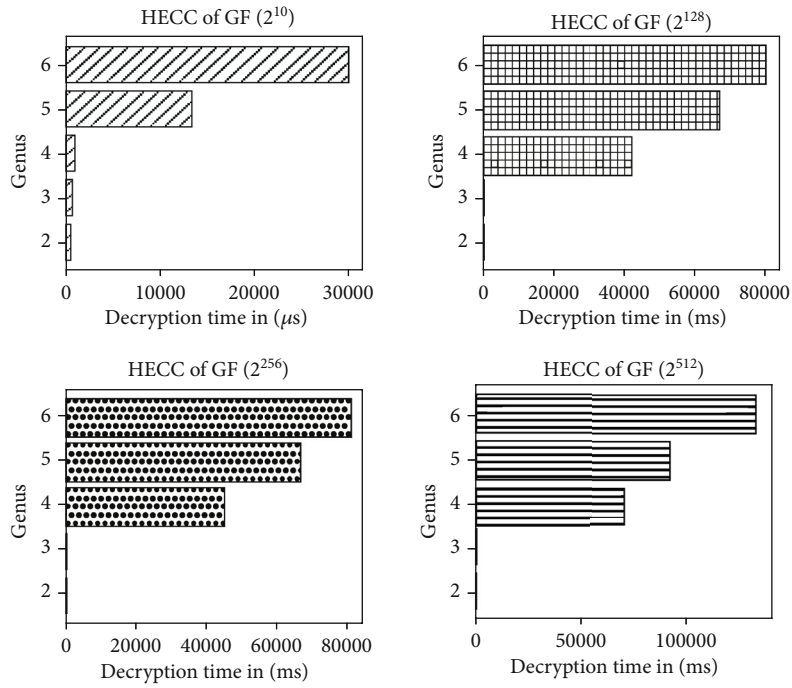

Figure 9: Decryption time.

Table 5: Comparison of existing mechanisms.

Parameter→ Method↓	Ev	Im	Ra	Fs	Ma	Pe
Batina et al. [1]	√	×	√	×	×	Lo
Zhang et al. [3]	√	√	√	√	×	Lo
Lee et al. [4]	√	√	√	√	√	Lo
Hu et al. [33]	√	√	√	√	√	Lo
Moosavi et al. [9]	√	√	√	√	√	Be
Proposed	√	√	√	√	√	Be

Ev: eavesdropping; Im: impersonation; Ra: replay attack; Fs: forward security; Ma: mutual authentication; Pe: performance; Lo: less; Be: better.

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

[1] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*, pp. 217–222, White Plains, NY, USA, 2007.

[2] Y. K. Lee, L. Batina, D. Singelee, B. Preneel, and I. Verbauwhede, "Anti-counterfeiting, untraceability and other security challenges for RFID systems: public-key-based protocols and hardware," in *Towards Hardware-Intrinsic Security*, Information Security and Cryptography, A.-R.

Sadeghi and D. Naccache, Eds., pp. 237–257, Springer, Berlin, Heidelberg, 2010.

[3] X. Zhang, J. Li, Y. Wu, and Q. Zhang, "An ECDLP-based randomized key RFID authentication protocol," in *2011 International Conference on Network Computing and Information Security*, vol. 2, pp. 146–149, Guilin, China, 2011.

[4] Y. K. Lee, L. Batina, D. Singelée, and I. Verbauwhede, "Wide–weak privacy–preserving RFID authentication protocols," in *Mobile Lightweight Wireless Systems*, P. Chatzimisios, C. Verikoukis, I. Santamaría, M. Laddomada, and O. Hoffmann, Eds., vol. 45 of Mobilight 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 254–267, Springer, Berlin, Heidelberg, 2010.

[5] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks," in *Proceedings of the 2nd International Workshop on RFID Technology - Concepts, Applications, Challenges - Volume 1: IWRT*, pp. 73–86, Porto, Portugal, 2008.

[6] "Radio frequency identification," April 2017, https://en.wikipedia.org/wiki/Radio-frequency_identification.

[7] K. Finkenzeller, *RFID Handbook*, John Wiley & Sons, 1999.

[8] M. T. Wankhede Barsgade and S. A. Meshram, "Comparative study of elliptic and hyper elliptic curve cryptography in discrete logarithmic problem," *IOSR Journal of Mathematics*, vol. 10, no. 2, pp. 61–63, 2014.

[9] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "An elliptic curve-based mutual authentication scheme for RFID implant systems," *Procedia Computer Science*, vol. 32, pp. 198–206, 2014.

[10] J.-S. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 75–94, 2014.

[11] Nizamuddin, S. Ashraf Ch, and N. Amin, "Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem," in *8th International Conference on High-capacity Optical Networks and Emerging Technologies*, Riyadh, Saudi Arabia, 2011.

[12] N. Koblitz, "*Hyperelliptic cryptosystems*," *Journal of Cryptology*, vol. 1, no. 3, pp. 139–150, 1989.

[13] O. Diao and M. Joye, "Unified addition formulæ for hyperelliptic curve cryptosystems," in *Proceedings of the 3rd Workshop on Mathematical Cryptology (WMC 2012) and 3rd International Conference on Symbolic Computation and Cryptography (SCC 2012)*, pp. 45–50, Castro Urdiales, Spain, 2012.

[14] H. Hisil and C. Costello, "Jacobian coordinates on genus 2 curves," in *Advances in Cryptology – ASIACRYPT 2014. ASIACRYPT 2014*, P. Sarkar and T. Iwata, Eds., vol. 8874 of Lecture Notes in Computer Science, pp. 338–357, Springer, Berlin, Heidelberg, 2014.

[15] J. W. Bos, C. Costello, H. Hisil, and K. Lauter, "Fast cryptography in genus 2," in *Advances in Cryptology – EUROCRYPT 2013. EUROCRYPT 2013*, T. Johansson and P. Q. Nguyen, Eds., vol. 7881 of Lecture Notes in Computer Science, pp. 194–210, Springer, Berlin, Heidelberg, 2013.

[16] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, "User privacy in transport systems based on RFID e-tickets," in *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications*, pp. 102–122, Malaga, Spain, October 2008.

[17] Y.-C. Yen, N.-W. Lo, and T.-C. Wu, "Two RFID-based solutions for secure inpatient medication administration," *Journal of Medical Systems*, vol. 36, no. 5, pp. 2769–2778, 2012.

[18] F. Rahman, M. Z. A. Bhuiyan, and S. I. Ahamed, "A privacy preserving framework for RFID based healthcare systems10.1016/j.future.2016.06.001," *Future Generation Computer Systems*, vol. 72, pp. 339–352, 2017.

[19] J. T. Kim, "Privacy and security issues for healthcare system with embedded rfid system on internet of things," *Advanced Science and Technology Letters*, vol. 72, pp. 109–112, 2014.

[20] T. G. Winston, S. Paul, and L. Iyer, "A study of privacy and security concerns on doctors' and nurses' behavioral intentions to use RFID in hospitals," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, 2016.

[21] F. Rahman, D. Williams, S. I. Ahamed, J.-J. Yang, and Q. Wang, "PriDaC: Privacy preserving data collection in sensor enabled RFID based healthcare services," in *2014 IEEE 15th International Symposium on High-Assurance Systems Engineering*, Miami Beach, FL, USA, 2014.

[22] A. Aguilar, W. Van Der Putten, and F. Kirrane, "Positive patient identification using RFID and wireless networks," in *HISI 11th Annual Conference and Scientific Symposium*, Dublin, Ireland, 2006.

[23] L. Hu, D. M. Ong, X. Zhu, Q. Liu, and E. Song, "Enabling RFID technology for healthcare: application, architecture, and challenges," *Telecommunication Systems*, vol. 58, no. 3, pp. 259–271, 2015.

[24] A. Coustasse, B. Cunningham, S. Deslich, E. Wilson, and P. Meadows, *Management of RFID systems in hospital transfusion services*, 2015.

[25] M. Martínez Pérez, G. Vázquez González, and C. Dafonte, "Evaluation of a tracking system for patients and mixed intravenous medication based on rfid technology," *Sensors*, vol. 16, no. 12, p. 2031, 2016.

[26] W. Yao, C.-H. Chu, and Z. Li, "The adoption and implementation of RFID technologies in healthcare: a literature review," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3507–3525, 2012.

[27] B. P. Rosenbaum, "Radio frequency identification (RFID) in health care: privacy and security concerns limiting adoption," *Journal of Medical Systems*, vol. 38, no. 3, p. 19, 2014.

[28] B. Lee and H. Kim, "Privacy management for medical service application using mobile phone collaborated with RFID reader," in *2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System*, pp. 1053–1057, Shanghai, China, 2007.

[29] D. S. Kim, T.-H. Shin, and J. S. Park, "A security framework in RFID multi-domain system," in *The Second International Conference on Availability, Reliability and Security (ARES'07)*, Vienna, Austria, 2007.

[30] A. Grover and H. Berghel, "A survey of RFID deployment and security issues," *Journal of Information Processing Systems*, vol. 7, no. 4, pp. 561–580, 2011.

[31] Y.-S. Jeong and S.-S. Shin, "An efficient healthcare service model using IoT device and RFID technique in the hospital environment," *Journal of Advanced Research in Dynamical and Control systems*, vol. 10, 2017.

[32] S. Khan, "Health care monitoring system in internet of things (IoT) by using RFID," in *2017 6th International Conference on Industrial Technology and Management (ICITM)*, Cambridge, UK, 2017.

[33] J.-X. Hu, C.-L. Chen, C.-L. Fan, and K.-h. Wang, "An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing," *Journal of Sensors*, vol. 2017, Article ID 3734764, 11 pages, 2017.