International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Telemedicine System with Architectural Framework and Data Transfer Protocol Validation

Charul Dewan*[1], Dr. T. Ganesh Kumar[2]

Submitted:14/03/2024 **Revised**: 29/04/2024 **Accepted**: 06/05/2024

Abstract: The human race lives in a globalized world and, thereby, enabling the humanity to communicate with individuals anywhere in the world. Similarly, telemedicine connects doctors and patients worldwide. Telemedicine is used to provide technical care and support to patients in long distance communication environment. In telemedicine services, patients' data is gathered using sensors and wireless broad area networks (WBANs). Doctors can examine the data that has been sent from sensors to cloud servers. Since telemedicine systems operate on public networks, it's critical to protect the privacy of sensitive and private data that is transferred. In this paper, the architectural framework of the proposed protocol will be illustrated that would verify the authenticity of data transfers between doctors and patients along with the proposed architecture's algorithm. It preserves privacy, efficiency and security more effective than prior methods using automated validation of internet security protocols and applications (AVISPA). These results show that the proposed architectural framework may be applied in practical scenarios.

Keywords: *WBAN, AVISPA, Healthcare, Telemedicine, security*

1. Introduction

Healthcare is a significant aspect of our day-to-day life as people are becoming more aware due to rising health issues. Technology and internet are booming trends and it gave rise to many smart devices like smart watches, IoT sensors, smart phones which help a normal person to measure their heart beat, amount of sleep, blood pressure, physical steps etc. [1] This is a simple way to collect and store the data and helps in self-assessment of healthcare. The data from Internet of things (IoT) sensors or smart phones is passed onto local servers from where it is transferred to the cloud servers. Physician servers can access this data and help can be rendered to patients while sitting at home. This way more and more patients can be given healthcare services. By 2030, there will be more than 60 billion intelligent Internet of Things (IoT) devices or sensors in use. [2–4]. A hyperconnected world where people, things, information and processes are increasingly connected to the network, thereby giving big impact to the future [5,6]. The main challenge is to secure the data while transferring it from one machine to another machine or from a server to server. If the author is not able to provide data security, then confidential information of the patient can be leaked making it vulnerable to numerous attacks and, therefore, it is necessary to authenticate the data. [7,8] Though block-chain technology has the ability to help the healthcare industry get past the problems with data security, privacy, sharing, and storage. Blockchain can also provide the highest level of transparency in the security of health-related information within the healthcare system still the data is vulnerable and can be tampered by malicious users. [9- 10]. Blockchain is a shared, unchangeable ledger that makes it easier to track assets and record transactions across a network of businesses. The widespread application of blockchain in telemedicine and telehealth is still relatively new. For blockchain technology to be widely used in telehealth and telemedicine systems, a number of obstacles and research issues must be overcome. [11-13] Figure 1 illustrates a scenario in which a user from one network tries to connect with a user from another network. Figure 1 depicts the architecture of Tele medical healthcare services in which patients are monitored by IoT devices and then data from sensor devices is being stored in TMIS server, which, in turn, is accessed by the physicians in the hospital. Furthermore, the TMIS offers the convenience of storing and sharing healthcare data among healthcare professionals, enabling seamless transfer and timely access to vital medical information. In addition, the telecare medical information system allows patients to send health-related information and use portals for health monitoring and other healthcare-related services over the Internet or mobile networks, reducing the need for unnecessary travel and hospitalization time. This advancement in healthcare technology has greatly benefited patients who are disabled or unable to attend the hospital regularly, as it provides them with access to medical and healthcare services from the comfort of their homes. However, the TMIS also poses a significant challenge in terms of data security. As the TMIS database system houses a substantial amount of private data, ensuring the security and confidentiality of this information

[1] *Galgotias University, Greater Noida, Uttar Pradesh – 203201, India Corresponding Author Email id: charularora@gmail.com*
[2] *Galgotias University, Greater Noida, Uttar Pradesh – 203201, India Email id tganeshphd@yahoo.com:*

is of utmost important. Data which is being transferred from patient to physician and vice versa needs to be authenticated as doctors are giving remote treatment to the patients, thereby, making it vulnerable with threats of eavesdropping, denial of service. In an increasingly wireless environment, the security of TMISs has become a focal point. The security of TMISs must be a top priority to safeguard confidential patient information in today's interconnected world.

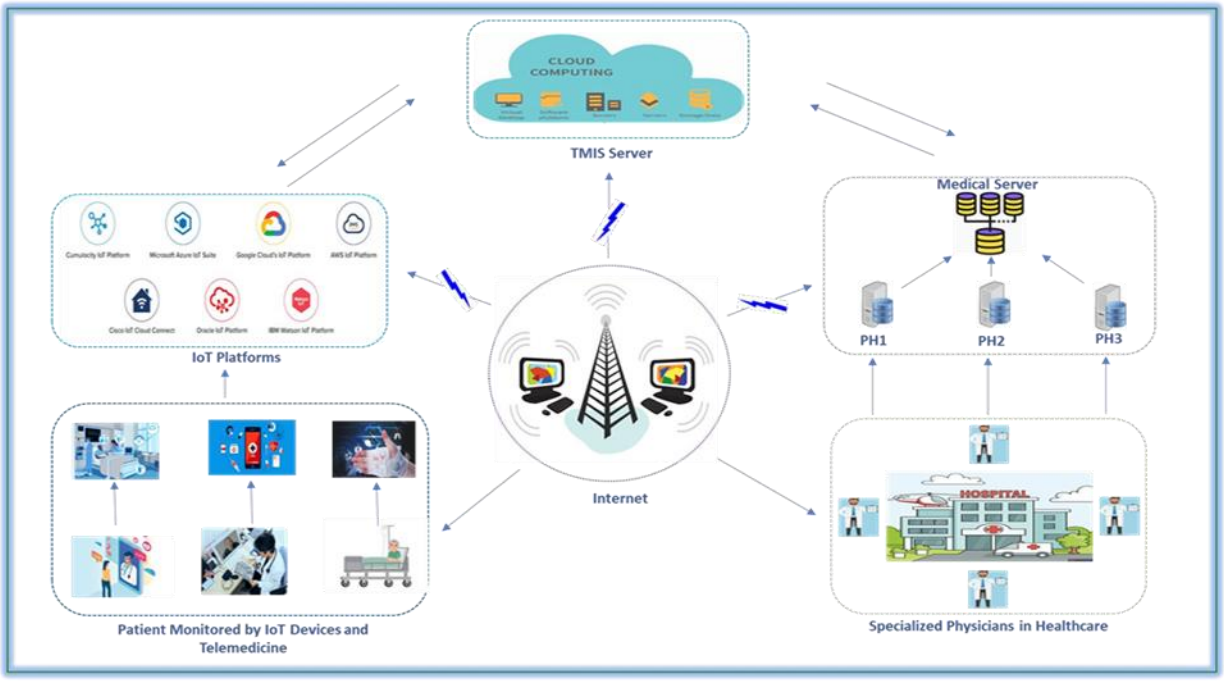


Fig 1 Architecture of Telemedical Healthcare Services

It consists of PH i.e. Physician Server and MH which means medical servers. The architecture of telemedical health care services is depicted in figure 1. On one end, it shows patients wearing Internet of Things (IoT) gadgets, and these sensors are collecting their data. On the other end, doctors are able to communicate with patients virtually and prescribe medications and testing. Medical servers are where these data are kept. The data of both physicians and patients is maintained by the telemedical information system server at the top. As a result, the information that physicians and patients communicate is vulnerable to several threats.

2. Literature Review

Multiple techniques for authentication for telemedical healthcare have been suggested and compared on the basis of computation cost and efficiency [14]. Due to the availability of sensor nodes, these protocols may potentially deal with authentication frames for electronic health monitoring. [15,16] Both symmetric and asymmetric key-based approaches are used in the related study. Multicasting and communication broadcasting rely on symmetric- based public key cryptography. For the sensor-based application, RSA and ECC (elliptic curve cryptography) are primarily employed. The authors also focused on IoT authentication, the importance of session keys, and the incorporation of IoT with blockchain- and AI-based security methods. [17-19] This article focuses on developments in the field of Internet of Medical Things, or IoMT. IoMT is an extension of IoT that provides people with timely, high-quality healthcare in real-time, powered by data analytics. With ubiquitous technologies like IoMT and IoT, security has always been a difficulty that needs to be addressed. [20-22].

In the literature, Tan et al [23] proposed the DBAKA protocol for various wireless roaming services and ensured mutual authentication by using BAN logic. The DBAKA protocol prevented the need for pre-shared keys between VLR and HLR while ensuring communication confidentiality. Their method of online and offline authentication has a communication cost of 8928 and 768 bits, respectively. Tan et al compared their protocol with delegation- based authentication protocols and told that it was vulnerable to known key attacks and communication confidentiality. Secret communication between the home location register (HLR) and visited location register (VLR) was a need for the protocol outlined by Hwang et al. and Kim et al. [24,25].

Amin et al. [26] presented an efficient and reliable user authentication technique using the cryptographic hash function for the Tele medical healthcare industry. The security and performance studies' findings demonstrated that their protocol is effective, secure against common security risks, and guarantees user anonymity and untrace ability. Amin et al compared their protocol to Das et al's [27] and showed that Das's protocol is unsafe against traceability attacks, other smartcard-related attacks, and is unable to guarantee anonymity.[28]. The protocol of Amin and Biswas [29] is not secure against multiple attacks like insider, replay attack and man-in- the-middle attack, and contains design faults in the registration, login, and authentication stages, as shown by Das et al. in their study. In a similar way, the protocols fostered by Li et al [30] and Wang et al [31] were open to smart card launch attacks.

Mehmood et al [32] rectified the shortcomings of Omid et al.'s strategy [33] and proposed a strong and effective authentication and key agreement scheme for E-Health Services that demonstrated to be provably secure against all conceivable threats, including user impersonation and user anonymity attacks. On the basis of various complexities like computational, cost, communication and moreover, security requirements, the suggested protocol has outperformed in terms of security and resilience.

Lei et al [34] proposed a 3-factor authentication and key agreement scheme for multiple servers whereas earlier proposed schemes were suitable for single server. Their strategy protects user confidentiality and anonymity in the Tele Medical Information System.

Vijaykumar et al [35] suggested an effective and safe IoT based architecture for anonymous authentication that also protects location privacy. In the suggested approach, firstly, the patient anonymously validated the physician to ensure the doctor's credentials, and the healthcare provider anonymously verified the patient. Additionally, TA (Trusted Authority) secured the patient's and doctor's location privacy, and it was disclosed to the authorized patients or physicians depending on the usage of CRT (Chinese Remainder Theorem). The security research revealed that our system might offer defense against multiple threats such as message alteration, replay, eavesdropping, and man-in-the-middle. Their scheme is more practicable for IoT-based wireless body area networks applications because of its efficiency in terms of computing cost. They have compared their scheme with Shen et al [36] and found that in Shen’s scheme there is no confidentiality for healthcare providers and geographical location privacy is also not protected whereas Vijaykumar’s scheme has used multiplicative cycles to find the computation cost.

Hameed et al [37] proposed an IoT-based cloud-based CDSS system that was utilized to predict illness and the degree of its recurrence was given. Medical sensors are also used to collect patient information and a patient's past medical history, which aids in providing the patient with better care. Data gathered from multiple sources, including as IoT sensors and previously saved patient data, are first saved in a database, after which the data are then secured using block-chain technology and retained in utility storage. 5G services are used to provide the data that is safely kept in cloud storage to healthcare providers. The specialist then consults with a team of medical experts, if the patient has a condition for which neither the expert system nor the specialist has a record of the symptoms. In order to keep up with emerging illnesses and their therapies, the expert system is updated. A group of medical professionals meets, shares knowledge about the health problem, does experiments, and compiles all pertinent data. Following the conclusion, patients are advised to seek therapy either through the hospital or online using an expert system. They compared their proposal to that of Castiglione et al. [38] and found that very few systems enable the quick and secure exchange of clinical experiences between various organizations.

A multi-functional remote medical care system that can assist patients in bed in remote environments was proposed by Lin et al. [39] The recommended plan works for both synchronous and asynchronous tele health as patients own their data, and users have control and decision-making authority over it. Lin et al divided the telemedicine in three levels- Webcam, smartphone, or wearable device users make up Level 1 (primary healthcare unit), which allows for the transmission of steady biodata using wireless technologies including RFID, NFC, Bluetooth, Wi-Fi. Without being transported to other systems, steady biological information is sent to the user's smart device. Before being sent to a larger hospital or medical facility, a patient may attend a clinic or neighborhood hospital at level 2 (city or district hospital). When treating a rare or incurable condition, Level 3 (specialist centre) uses telemedicine to cure rare or incurable disease. The security of the data is provided with the help of smartcard. A smartcard and reader must be used by a medical practitioner in order to access the measured biodata on the server. Whenever a medical practitioner inserts their smartcard, the proposed scheme's authenticated key agreement phase is enabled, allowing for the safe transmission of the session key-encrypted measured biodata. They compared their paper’s outline with Wang et al [40] and Suresh Kumar et al [42] and found that their scheme lacks user anonymity and cannot prevent server spoofing attack. Key confirmation is a feature of the Lin et al method that is absent from other schemes and guarantees that clients and servers are using the same shared key during a session. [41]

Two alternative ROM-based techniques were put out by Kumar et al. [43] to exemplify formal security analysis. They also demonstrated how RAPCHI is immune to man-in-the-middle attack and replay attack using the simulation tool AVISPA. A variety of security attributes and properties were used in this informal security analysis, comprising data non-repudiation, known-key property, replay attack, privacy of data, man-in-the-middle attack, patient unlink ability, falsification attack, session encryption security, and message authentication for physicians as well as patients. In terms of compute and transmission costs, Kumar's et al.'s work is more secure and productive. They likened their work to that of [44-45] in terms of healthcare communication systems, but these don't go far enough to address the system's basic concerns regarding confidentiality and security.

For cloud-assisted TMIS, the authors provided a more secure mutual authentication and privacy preservation approach that addresses the security flaws identified in the system developed by Mohit et al. [46] The authentication methodology proposed by the authors successfully handles cloud-assisted TMIS with more efficiency and meets the majority of functionality requirements for privacy protection. [47-49]. They compared their work with Mohit et al and found it to be insecure against patient anonymity and mobile device stolen attack.

A secure authentication mechanism based on RFID-TMIS was suggested by Chander et al [50] which successfully resists all threats including stolen, replay, DoS, MTM, spying, and de-synchronization impersonating data integrity, and privacy. They used the well-known security verification programmes AVISPA and Scyther to examine the suggested paradigm. Additionally, GNY logic based on BAN logic was employed to adhere to the generality of the protocol architecture. The simulation results of the suggested protocol show that it is secure from all attacks and incurs fewer overheads than existing protocols in terms of communication and computation costs. The author compared their work with Agrahari et al [51], Hosseinzadeh et al [52] and Qikun et al [53] and found that their system lacked indemnity, privacy with mobility, and scalability in the healthcare atmosphere.

3. Proposed Methodology

This section discusses a ground-breaking key exchange and authentication technique created for accessing data in healthcare applications within the framework of the Mutual Authentication Protocol for Remote Cloud Healthcare. In two independent processes, authentication is necessary: first, between the user and their own gateway, and second, between Gateways 1 and 2, which are located on different networks. Seven separate phases make up the proposed protocol, which are universally applicable to a variety of communication scenarios involving diverse Healthcare application users. Following is a summary of these seven phases:

Setup of the Gateway/Gateway Setup Phase

- Registration of Users
- Initial Phase of the Server
- Phase of User Login
- Phase and Key for User Authentication
- Password updation phase
- Revocation phase

The aforementioned authentication processes are implemented by IoT healthcare providers so as to ensure a secure network. The schemes’ used notations have been specified in Table 1 given below.

Table 1 Symbols and their meanings

Symbol	Meaning
Uj	User
GW	Gateway
d	Gateway's Private Key
ISi	Sensor's Identity
di	Private Key of the sensor
PKs	Public Key of the sensor
IUj	User's identity
PUj	User's password
H()	One-Way Hash function
SCj	Smart card
$\oplus$	Symbol for XOR
p,q	Prime Numbers
‖	Concatenation operator
T1,T2,T3	Time stamp

ΔT	Transmission Delay
RNG	Random number
Te	Exponentiation

The following section provides a detailed description of each of the aforementioned phases:

Gateway Setup Phase: All gateways from various networks start the configuration procedure in offline mode during this phase, following these steps:

Step 1: The 'GT' gateway is initiated by selecting two prime numbers, r and s, and then we have to computes P as the product of these primes:

P = r * s

Step 2: Subsequently, 'GT' chooses two integers, c and d, that satisfy the congruence relations:

c * d ≡ 1 (mod n)

d ≡ c ^ (-1) (mod n)

c is the public key for the initial setup, whereas the private key in the example above is d.

Registration of users: The user 'Uj' starts the registration procedure with the gateway ('GT') during the user registration phase. The following actions are part of

this phase:

Step 1: The password "PWUj", random number "Ri," and identity "IDUj" is chosen by User "Uj" in the first step. As "APWUj = H(IDUj || Ri"), "Uj" generates a random identity for itself. The gateway receives this "APWUj" after which "Uj" is registered utilizing a secure/confidential server communication link.

Step 2: In the second step, the gateway "GT" calculates a message "Mi = H(APWUj || d)" after receiving "APWUj" from the user "Uj," and here "d" represents the gateway's private key and "H" stands for the one-way hash function.

Step 3: The gateway ‘GT’, then uses the formula "SCj = Mi, HC, a, b" to generate a smart card, which it then transmits to user "Uj". During the user registration phase, the user 'Uj' initiates the registration process with the gateway 'GT'. The following actions are part of this phase:

Step 4: Upon receiving the smart card "SCj," user "Uj" applies algorithm "APWUj = H(PWUj || Rj)" to create a new password. In addition, 'Uj' computes the following values for the three parameters 'Aj,' 'Bj,' and 'Cj':

APWUj || IDUj = Aj = Mi H (In this case, "" stands for a bitwise XOR operation) Bj = H(IDUj || APWUj)

Cj is equal to Rj H(IDUj || PWUj).

There are three parameters on the smart card "SCj": "Aj," "Bj," and "Cj."

'Uj' then removes the recorded value 'H1' from the memory of the smart card 'SCj', leaving the smart card with the information '(Aj, Bj, Cj, a, b, HC)'. This procedure makes sure that users register securely with the gateway, protecting private data.

Server Registration Phase: During the Server Registration phase, all server devices that need to communicate with the gateway are registered offline. This process unfolds as shown below:

Step 1: The gateway (referred to as "GT") chooses an identity (referred to as "IDSi") and a private key (referred to as "di") for each sensor device (referred to as "Si"). It then computes the appropriate public key (referred to as "Pks = di * p," where "p" stands for a large prime integer).

Step 2: Furthermore, the gateway 'GT' uses a one - way hash function 'h' applied to the concatenation of 'IDSi' and 'di' to calculate a pseudo-random identity 'RSi' such that RSi = h(IDSi || di)

Step 3: In the step 3, while the sensor 'Si' saves {IDSi, di, RSi} in its memory, the gateway node 'GT' keeps {IDSi, RSi, Pks} in its own database. The 'Pks' key is made available to all users and classified as public.

In this manner, server devices are registered with the gateway, ensuring secure and organized communication within the network.

User Login Phase: During the User Login Phase, the login process is initiated by the user 'Uj' along with the gateway node. This stage progresses as follows:

Step 1: The first stage involves user 'Uj' inserting a smart card with their password 'PWUj' and identification 'IDUj'.

Step 2: The 'SCj' smart card runs the following calculations:

"Rj" = "Cj H(IDUj || PWUj")," "PWUj" = "H(IDUj || Rj)," and "APWUj" = "H(PWUj || Rj)""Bj" =

"H(IDUj APWUj)"M1 is equal to Aj H(APWUj || IDUj).

The user 'Uj' is validated to move on to the next stage if 'Bj' = 'Bj' holds.

The login request is declined if "Bj" "Bj," which indicates that the criteria

is not satisfied.

Step 3: The smart card denoted by 'SCj' then computes a random number 'Rs' and a timestamp 'Ti,' then computes:

'Dj' equals 'H(APWUj" || Rs || M1" || Ti)'Ej' = 'H(PWUj' || APWUj' || M1') ⊕ Rs' 'Fj' = 'H(PWUj' || APWUj' || Rs || M1' || Ti)' ^ a mod b'

Then, using 'SCj', the message <Dj, Ej, Fj> is transmitted across a secure channel to the gateway node.

The user's identity and authorisation are confirmed during this user login phase, which grants access to the succeeding phase if the prerequisites are met or denies access if they are not.

Phase of Authentication and Key Exchange: During this phase, a shared session key is used to mutually authenticate the user and the gateway, providing access to sensor devices. During this stage, the gateway node (GT) initiates the key exchange process and verifies the user 'Uj'. This procedure is outlined in the steps shown below:

Step-1: The gateway node is termed as step one. GT receives the message from user 'Uj' and decrypts 'Fj' to obtain the data 'PWUj, APWUj, Rs, M1, T1'. GT determines via its private key "d" that:

(PWUj, APWUj, Rs, M1, T1) = d = (Fj)d mod b

To stop replay attacks, GT checks the reliability of the timestamp 'T' (i.e., |T2 - T1| T). The process ends if the timestamp requirement is not satisfied; otherwise, it moves on to the next authentication stage.

Step-2 GT must then compute "M1" = H(PWUj || d) and compare it to "M1" in the second step. If "M1"

= "M1" is true, the procedure is carried out; if not, the login request is cancelled.

Step 3: If 'M1' = 'M1,' GT determines 'Rs' = Ej H(PWUj || APUj || M1) and determines whether 'Rs' = Rs is true. If the criteria are met, it moves on to the subsequent step; if not, it ends this stage.

Step-4: In the step 4, GT computes Dj' = H(APWUj || Rs || M1' || T1) in the fourth step and compares it to Dj. If Dj' = Dj is true, then the operation continues. GT generates a timestamp ('T2') and a random number ('Rg') to build a session key:

PWUj || APWUj || Rs' || Rg || T1 || T2 Kj = H(Sk || M1' || Rg || T1 || Rs || T2) Gj = Rs' Rg

User "Uj" receives the authentication request from GT.

Step-5: User 'Uj' receives 'Gj, Kj, T2' using smart card 'SCj' at step 5. The timestamp is initially checked by 'Uj' (|T2 - T1| T). The session moves on to step 7 if the timestamp is accurate; else, it is terminated.

Step-6: User 'Uj' calculates in step 6:

Rg' = Rs ⊕ Gj Sk = H(PWUj', APWUj', Rs', Rg, T1, T2) Kj' = H(Sk, M1, Rg, T1, Rs, T2)

The user and the gateway are mutually authenticated if Kj' = Kj holds true. The session ends in such a case.

Step 7: Another timestamp, 'T3', is calculated by smart card 'SCj' and yields the following results: Sk' equals H(Sk || M1' || PWUj || T2 || T3

Through a secure communication channel, SCj' sends Sk', T3> to gateway node 'GT'.

Step 8: The message Sk', T3> is received by Gateway Node 'GT'. GT checks the timestamp first (|T3 - T2| T). If this is true, Sk' is calculated as H(Sk' || M1 || PWUj || T2 || T3), and Sk' is then compared against Sk. If the prerequisite is met, communication between the user and the gateway is carried out using encrypted communications that employ the secret key Sk. If not, contact is cut off.

In order to ensure secure and verified connection between the user and the gateway, this summarizes the user login and authentication process.

Password Change Phase: During the password change phase, the user 'Uj' performs the following internal process:

Step 1: User 'Uj' uses a smart card at a dedicated sensor terminal 'Si' to input their identification, 'IDuj,' and password, 'PWuj'.

Step 2: The 'SCj' smart card runs the following computations:

"Rj" = "Ci H(IDuj || PWuj"), "PWuj" = "H(IDuj || Rj")," "APWuj" = "H(PWuj || Rj"")," "Bj" = "H(IDuj APWuj"")," and "M1" = "Aj H(APWuj || IDuj)."

It confirms and compares "Bj" with the stored version on the smart card "SCj." When 'Bj' = 'Bj' is valid, it verifies the user's identity and requests a new password, 'NPWuj.' If not, the session is terminated.

Step 3: The gateway "GT" is given the freshly created password " NPWuj" by the user "Uj".

Step 4: The 'SCj' smart card performs the following calculations:

'NAj' = 'M1' H(ANPWuj || IDuj) 'ANPWuj' = 'H(NPWuj || Rj')'"NBj" = "H(PWuj ANPWuj")" "NCj" =

"Rj" H(IDuj || NPWuj)"'

All of the values of 'Aj' are replaced by the new 'A1' (NAj), 'Bj' by the new 'B1' (NBj), and 'Cj' by the new 'Cj' (NCj) on the smart card.

The user can safely update their password during this password change phase, which also protects data integrity and authentication.

Phase of Revocation: In the case that the authorized user 'Uj's+' smart card 'SCj' is misplaced or taken, 'Uj' can regain access by performing the following actions:

Step 1: First, a new request with a new password is initiated by 'Uj' with help from the gateway node 'GT'. Protection against impersonation attacks on "Uj" is no longer provided by the use of the previous password and random number values.

Step 2: In the second step, "Uj" asks "GT" to cancel the lost or stolen smart card. 'GT' validates 'Uj' by utilizing previously established identity or values given by 'Uj.'

Step 3: "GT" requests a new password from "Uj" following a successful verification. "Uj" creates a brand- new password:

IDuj || Rj' = PWUj

'Uj' sends 'GT' a secure communication channel request for a new password.

Step 4: 'GT' determines 'M1' = H(PWuj' || d), where 'd' denotes 'GT's private key. 'GT' uses a secure communication channel to transfer the data (M1', a, b, and HC) to 'Uj'.

Step 5: 'Uj,' using smart card 'SCj,' executes the computations listed below:

H(PWuj' || Rj') = APWuj'

Aj = H(APWuj' || IDuj) M1"

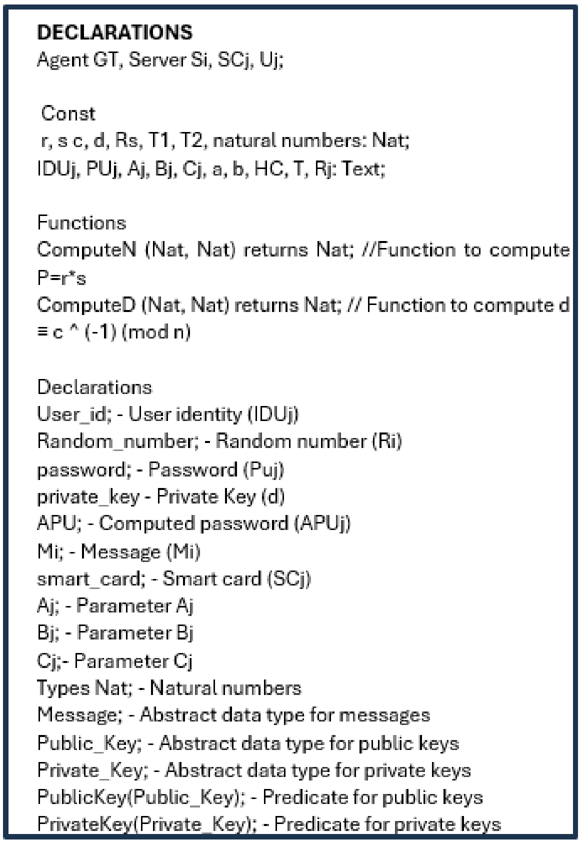
The formulas Bj' = H(IDuj APWuj') and Cj' = Rj' H(IDuj || Puj') are used to store all three parameters (Aj', Bj', and Cj') onto the new smart card. On the new smart card, there are now ((Aj', Bj', Cj', a, b, HC)).

After their smart card is lost or stolen, "Uj" can use this revocation phase to securely regain access to the system with improved security against unauthorized access.

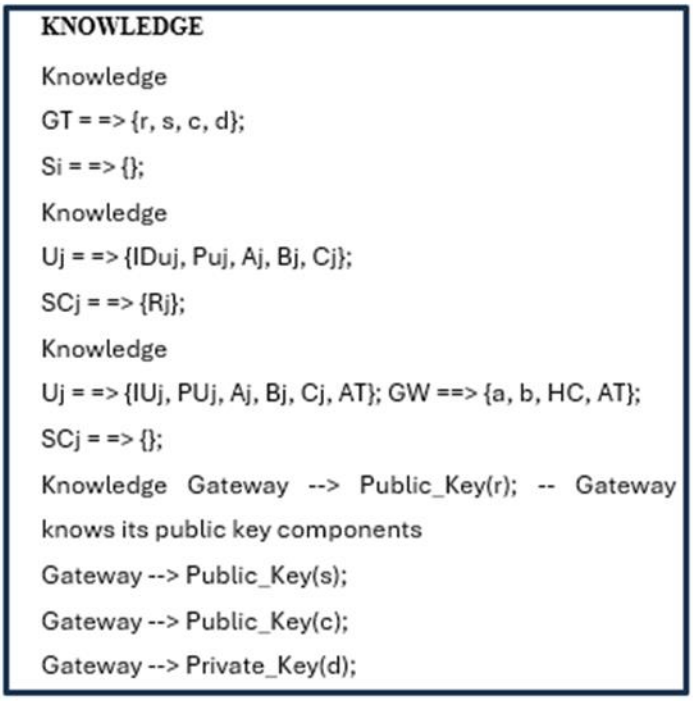
4. Formal Security Validation using AVISPA Tool

We simulate the authentication and key exchange protocols using automated validation of internet security protocol and application (AVISPA) in this part. The High-Level Protocol Specification Language (HLPSL) is used to code AVISPA. The authentication process's phrasing is effective. Our protocol is resistant to every form of known attack, according to the simulation. The HLPSL code with all entities ("user Uj and the gateway GW") for the suggested protocol is shown in Figures 2 and 3. The High-Level Protocol Specification Language code is shown in Figures 4, 5, and 6 for the user login and password change phases. These figures demonstrate that the proposed work is resilient to all existing threats. Our protocol is SAFE in both the OFMC and the CI-Atse model simulation settings. This section demonstrates how the protocol defends against active and passive attacks, reply attacks, MITM attacks and other threats.

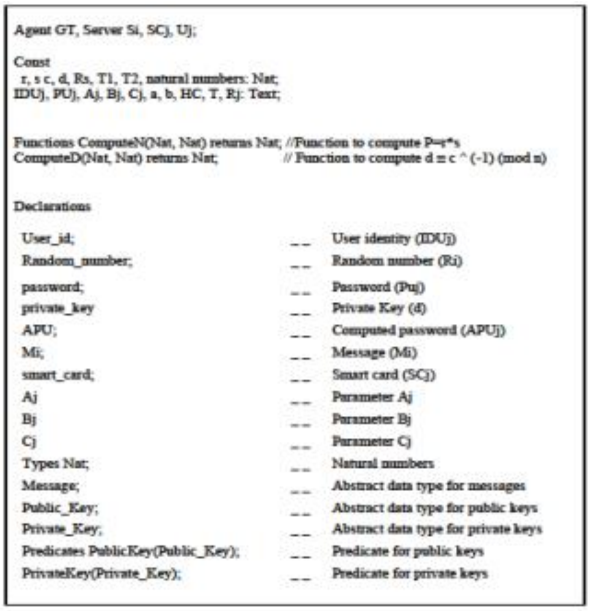
The algorithm for the above mentioned has been shown below along with declarations and knowledge:



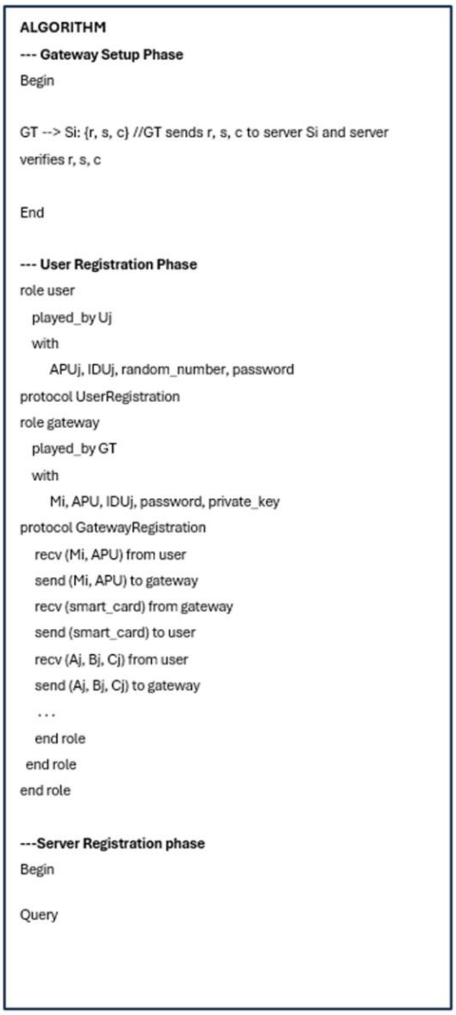
```
DECLARATIONS
Agent GT, Server Si, SCj, Uj;

 Const
 r, s c, d, Rs, T1, T2, natural numbers: Nat;
IDUj, PUj, Aj, Bj, Cj, a, b, HC, T, Rj: Text;

Functions
ComputeN (Nat, Nat) returns Nat; //Function to compute
P=r*s
ComputeD (Nat, Nat) returns Nat; // Function to compute d
≡ c ^ (-1) (mod n)

Declarations
User_id; - User identity (IDUj)
Random_number; - Random number (Ri)
password; - Password (Puj)
private_key - Private Key (d)
APU; - Computed password (APUj)
Mi; - Message (Mi)
smart_card; - Smart card (SCj)
Aj; - Parameter Aj
Bj; - Parameter Bj
Cj;- Parameter Cj
Types Nat; - Natural numbers
Message; - Abstract data type for messages
Public_Key; - Abstract data type for public keys
Private_Key; - Abstract data type for private keys
PublicKey(Public_Key); - Predicate for public keys
PrivateKey(Private_Key); - Predicate for private keys
```



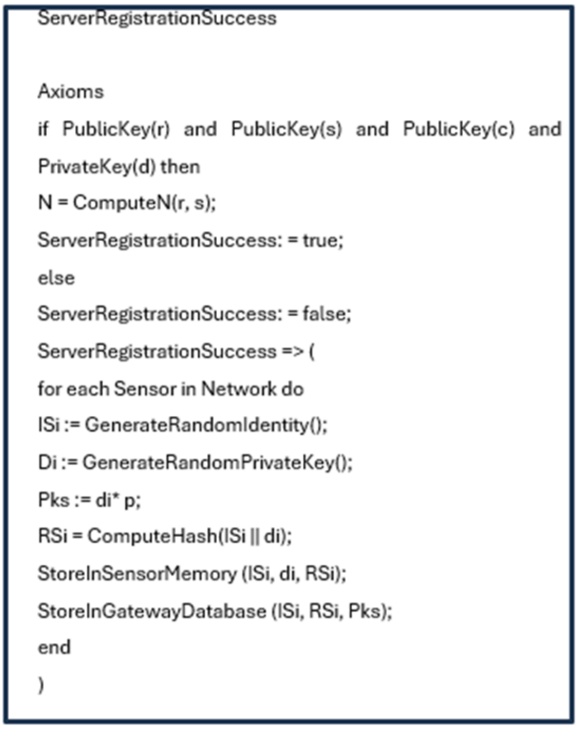
```
KNOWLEDGE
Knowledge
GT = => {r, s, c, d};
Si = => {};
Knowledge
Uj = => {IDuj, Puj, Aj, Bj, Cj};
SCj = => {Rj};
Knowledge
Uj = => {IUj, PUj, Aj, Bj, Cj, AT}; GW ==> {a, b, HC, AT};
SCj = => {};
Knowledge Gateway --> Public_Key(r); -- Gateway
knows its public key components
Gateway --> Public_Key(s);
Gateway --> Public_Key(c);
Gateway --> Private_Key(d);
```



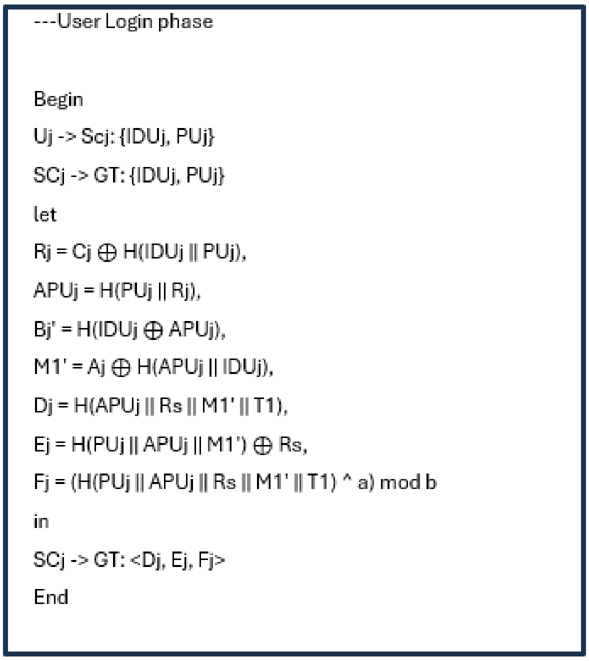
```
Agent GT, Server Si, SCj, Uj;

Const
 r, s c, d, Rs, T1, T2, natural numbers: Nat;
IDUj, PUj, Aj, Bj, Cj, a, b, HC, T, Rj: Text;


Functions ComputeN(Nat, Nat) returns Nat; //Function to compute P=r*s
ComputeD(Nat, Nat) returns Nat;           // Function to compute d ≡ c ^ (-1) (mod n)


Declarations

 User_id;                                  __   User identity (IDUj)
 Random_number;                            __   Random number (Ri)
 password;                                 __   Password (Puj)
 private_key                               __   Private Key (d)
 APU;                                      __   Computed password (APUj)
 Mi;                                       __   Message (Mi)
 smart_card;                               __   Smart card (SCj)
 Aj                                        __   Parameter Aj
 Bj                                        __   Parameter Bj
 Cj                                        __   Parameter Cj
 Types Nat;                                __   Natural numbers
 Message;                                  __   Abstract data type for messages
 Public_Key;                               __   Abstract data type for public keys
 Private_Key;                              __   Abstract data type for private keys
 Predicates PublicKey(Public_Key);         __   Predicate for public keys
 PrivateKey(Private_Key);                  __   Predicate for private keys
```



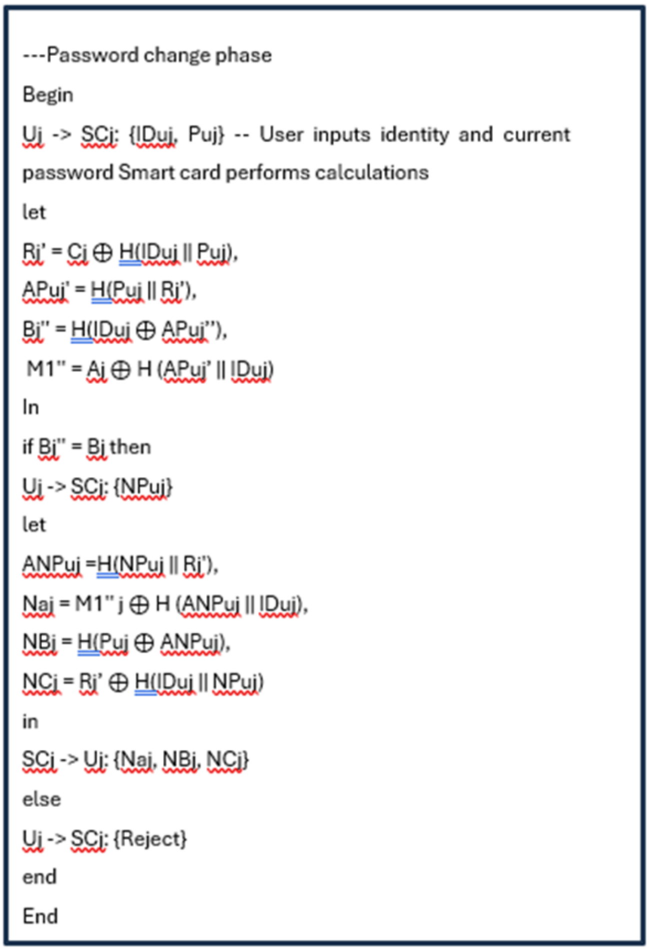
```
ALGORITHM
--- Gateway Setup Phase
Begin

GT --> Si: {r, s, c} //GT sends r, s, c to server Si and server
verifies r, s, c

End

--- User Registration Phase
role user
  played_by Uj
  with
     APUj, IDUj, random_number, password
protocol UserRegistration
role gateway
  played_by GT
  with
    Mi, APU, IDUj, password, private_key
protocol GatewayRegistration
   recv (Mi, APU) from user
   send (Mi, APU) to gateway
   recv (smart_card) from gateway
   send (smart_card) to user
   recv (Aj, Bj, Cj) from user
   send (Aj, Bj, Cj) to gateway
    . . .
   end role
 end role
end role

---Server Registration phase
Begin

Query
```



```
ServerRegistrationSuccess


Axioms
if PublicKey(r) and PublicKey(s) and PublicKey(c) and
PrivateKey(d) then
N = ComputeN(r, s);
ServerRegistrationSuccess: = true;
else
ServerRegistrationSuccess: = false;
ServerRegistrationSuccess => (
for each Sensor in Network do
ISi := GenerateRandomIdentity();
Di := GenerateRandomPrivateKey();
Pks := di* p;
RSi = ComputeHash(ISi || di);
StoreInSensorMemory (ISi, di, RSi);
StoreInGatewayDatabase (ISi, RSi, Pks);
end
)
```



```
---User Login phase

Begin
Uj -> Scj: {IDUj, PUj}
SCj -> GT: {IDUj, PUj}
let
Rj = Cj ⊕ H(IDUj || PUj),
APUj = H(PUj || Rj),
Bj' = H(IDUj ⊕ APUj),
M1' = Aj ⊕ H(APUj || IDUj),
Dj = H(APUj || Rs || M1' || T1),
Ej = H(PUj || APUj || M1') ⊕ Rs,
Fj = (H(PUj || APUj || Rs || M1' || T1) ^ a) mod b
in
SCj -> GT: <Dj, Ej, Fj>
End
```



```
---Password change phase
Begin
Uj -> SCj: {IDuj, Puj} -- User inputs identity and current
password Smart card performs calculations
let
Rj' = Cj ⊕ H(IDuj || Puj),
APuj' = H(Puj || Rj'),
Bj'' = H(IDuj ⊕ APuj''),
 M1'' = Aj ⊕ H (APuj' || IDuj)
In
if Bj'' = Bj then
Uj -> SCj: {NPuj}
let
ANPuj =H(NPuj || Rj'),
Naj = M1''j ⊕ H (ANPuj || IDuj),
NBj = H(Puj ⊕ ANPuj),
NCj = Rj' ⊕ H(IDuj || NPuj)
in
SCj -> Uj: {Naj, NBj, NCj}
else
Uj -> SCj: {Reject}
end
End
```

5. Comparative Analysis

The security characteristic and computational cost of the suggested schemes are defined by the performance analysis. Table 4 displays the associated work's computing costs for cryptographic procedures. Execution time for the hash function Th is 0.02 milliseconds, while the XOR operation takes 0.04 milliseconds, according to the statistics in Xu and Wu (2015). These numbers were computed using the C/C++ library in MI RACL: TXOR is 0.13 seconds, Te is 0.16 seconds, Tadd is 0.0045 milliseconds, Tmul is 0.0041 seconds, and Taes is 0.978 seconds. For determining the energy consumption for the mica motes with values of U = 3.0 V and I = 8 mA in active mode, we use the formula E = U *I * t. The comparison of different attributes and security attacks by proposed protocols have been shown in Table 3. The overall execution time and energy usage of the various authentication techniques have been displayed through Table 4. Figures 7 and 8 illustrates, respectively, the overall execution time and energy usage of the various authentication techniques

Table 2 Comparison of different security attacks by proposed protocol [✓: Safe; ✗: Not Safe]

Protocol Attacks/Attributes	Mehmood et al [33]	Lei et al [35]	Vijaykumar et al [36]	Lin et al [40]	Kumar et al [45]	Bhanu et al [53]	Our paper
Impersonation Attack	✓	✗	✗	✓	✓	✓	✓
Denial Of Service Attack	✗	✗	✗	✓	✓	✓	✓
Insider Attack	✓	✗	✗	✗	✓	✓	✓
Replay Attack	✓	✗	✗	✗	✓	✓	✓

Password Guessing Attack	✕	✕	✕	✕	✓	✓	✓
Stolen Verifier Attack	✕	✕	✕	✓	✓	✓	✓
Session Key Security	✕	✕	✕	✕	✓	✓	✓
Perfect Forward Secrecy	✕	✕	✕	✕	✓	✓	✓
Impersonation Attack	✓	✕	✕	✓	✓	✓	✓
Man In Middle Attack	✕	✕	✕	✕	✓	✓	✓
User Privacy	✕	✓	✓	✓	✓	✓	✓
False Login Attack	✕	✕	✕	✕	✓	✓	✓
Mutual Authentication	✓	✕	✓	✕	✓	✓	✓
Low Communication Cost	✕	✕	✕	✕	✕	✕	✓
Secure Protocol	✕	✕	✕	✕	✕	✕	✓

Table 3 Computation Cost, energy consumption and time taken by different proposed scheme

Schemes	**Computation cost**	**Total Time Taken(ms)**	**Energy consumption(mj)**
Amin et al	$21T_h$ + 4 RNG + 22xor	7.28	174.2
Mehmood et al	$19T_{oh}$ + $3T_{Es}$ + 14 xor + 4RNG	9.134	255.52
Lei et al	$5TG_{mul}$ + T_{mul} + $11T_h$+2RNG	7.23	202.44
Vijaykumar et al	$4T_P$ + $2T_h$ + 4Tm	8	192
Lin et al	$9T_h$ + $4T_{ch}$ +$2T_{sym}$	14.38	345.12

Kumar et al	$4T_{Sign} + 6T_S + 2T_M +$ 24Th	7	168
Bhanu et al	18TH+ 3RNG + 31xor	7.39	177.36
Our paper	10xor + 10Th + 4RNG + 2Te	5.82	139.68

6. Conclusion

In long-distance communication settings, telemedicine systems, a multifunctional remote healthcare service, may help patients in need. It is crucial to protect the privacy of sensitive and private data as the data is communicated on a public network. In an IoT network, the recommended protocol offers efficient user-to-gateway authentication. Through the key exchange, the user is offered a portal for effective information communication. The proposed research provides a secure tele medical health system with architectural framework and data transfer protocol validation for patient-doctor communication. The suggested protocol is proven to be excellent and secure against various active and passive threats. The proposed work is secure against impersonation attack and privacy. Regarding computing costs, execution time, energy economy, and security aspects, the the proposed protocol is effective. With excellent security characteristics, the AVISPA study demonstrates the practical application and viability in the telemedical healthcare context. We would build on this research in subsequent work by incorporating certain metaverse concepts.

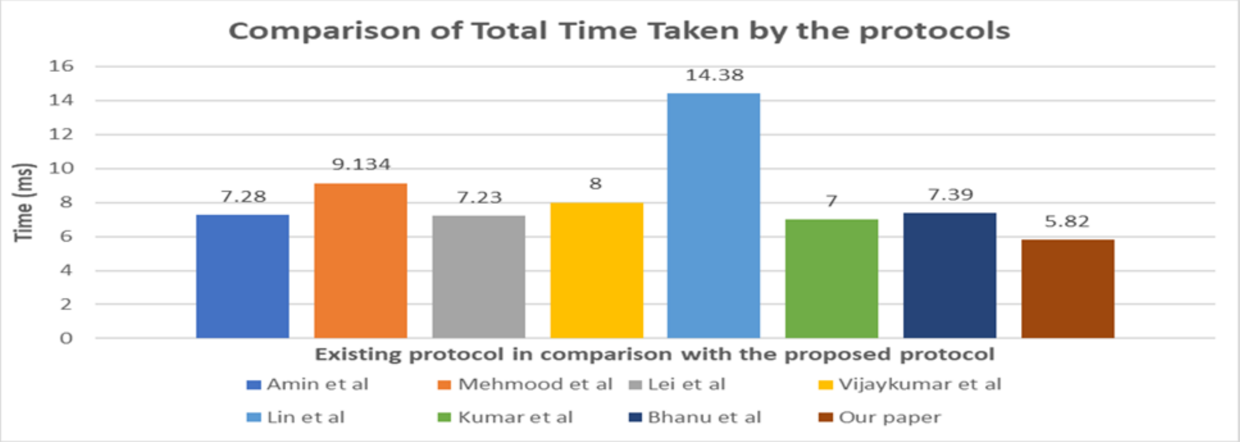


Fig 2 Execution time as represented by different proposed schemes

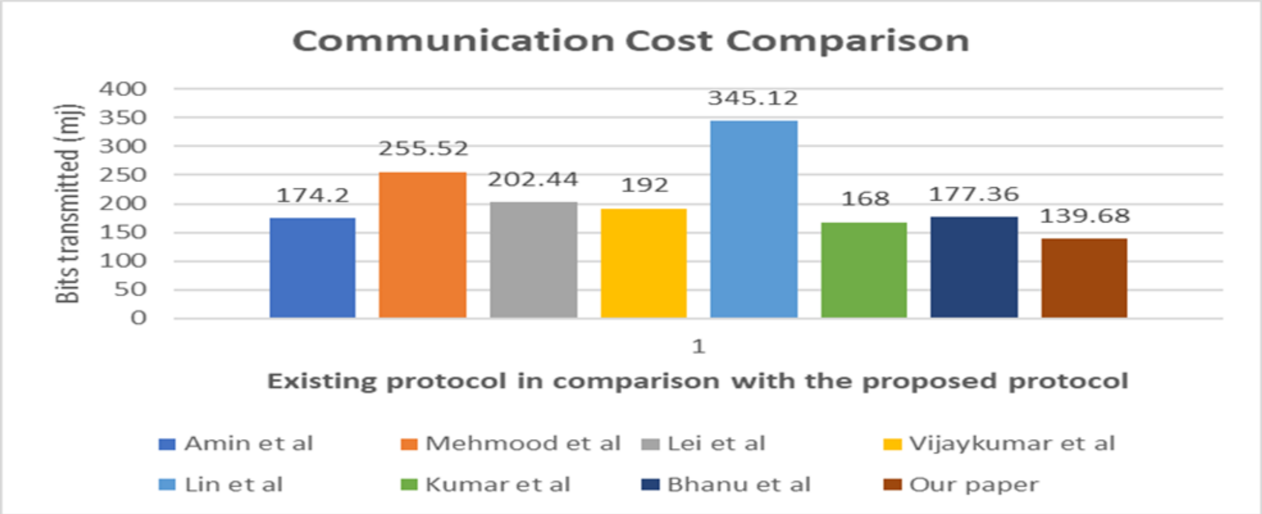


Fig 3 Energy Consumption by different proposed Protocols

References

[1] P. Alexander, R. Baashirah, A. Abuzneid, Comparison and feasibility of various RFID authentication methods using ECC, Sensors 18 (9) (2018) 2902.

[2] Lijun Xiao, Songyou Xie, Dezhi Han, Wei Liang, Jun Guo, Wen-Kuang Chou, A lightweight authentication scheme for telecare medical information system, Connect. Sci. 33 (3) (2021)769–785,

[3] M. Samani, A. Khademzadeh, Integration of WSN and RFID networks, and redundant data filtering, J. Commun. Eng. (2021).

[4] A.K. Singh, A. Anand, Z. Lv, H. Ko, A. Mohan, A survey on healthcare data: a security perspective, ACM Trans. Multimedia Comput. Commun. Appl. 17 (2s)

[5] S. Shukla, S.J. Patel, A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing, Computing (2022)

[6] Gupta, S. (2023). 17 System for secure edge healthcare. Edge-AI in Healthcare: Trends and Future Perspectives, 245.

[7] Dewan, C., Kumar, T. G., & Gupta, S. (2022). A comparative analysis on remote user authentication schemes in telemedical healthcare systems. International Journal of System of Systems Engineering, 12(2), 134-149

[8] Dewan, C., Ganesh Kumar, T., & Gupta, S. (2022). Comparative Study of Various Authentication Schemes in Tele Medical Information System. In Applications of Computational Methods in Manufacturing and Product Design: Select Proceedings of IPDIMS 2020 (pp. 557-564). Singapore: Springer Nature Singapore

[9] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Methodologies for Improving the Quality of Service and Safety of Smart Healthcare System. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham.

[10] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Internet of Medical Things (IoMedT) vs Internet of Things (IoT). In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_3

[11] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Digital Medical Records (DMR) Security and Privacy Challenges in Smart Healthcare System. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_6.

[12] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Authentication Methods for Internet of Medical Things. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_10

[13] Gupta, S., Sharma, H. K., & Kapoor, M. (2022). Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer. ISBN: 978-3-031-18895-4

[14] Gupta, S. (2023). Fog-based smart building IoT model: development and energy cost estimation. International Journal of Critical Infrastructures, 19(4),354-366.

https://doi.org/10.1504/IJCIS.2023.132209

[15] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Application and Challenges of Blockchain in IoMT in Smart Healthcare System. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_4

[16] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Emerging and Digital Technology in Telemedicine System. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_12.

[17] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Introduction to Internet of Medical Things (IoMT) and Its Application in Smart Healthcare System. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_2

[18] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Introduction to Smart Healthcare and Telemedicine Systems. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_1.

[19] Vyas, S., & Gupta, S. (2023). WBAN-based remote monitoring system utilizing machine learning for healthcare services. International Journal of System of Systems Engineering, 13(1), 100-108.

[20] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Integration of IoMT and Blockchain in Smart Healthcare System. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_7

[21] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Smart Healthcare and Telemedicine Systems: Present and Future Applications. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-

18896-1_15

[22] Gupta, S., Sharma, H.K., Kapoor, M. (2023). Introduction to Blockchain and Its Application in Smart Healthcare System. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_5

[23] V. Tan, "Secure Delegation-Based Authentication for Telecare Medicine Information Systems," in IEEE Access, vol. 6, pp. 26091-26110, 2018, doi: 10.1109/ACCESS.2018.2832077.

[24] Hwang and C.-H. You, ‘‘A delegation-based unlinkable authentication protocol for portable communication systems with non-repudiation,’’ in Advanced Technologies, Embedded and Multimedia for Human Centric Computing (Lecture Notes in Electrical Engineering), vol. 260. Heidelberg, Germany: Springer, 2014, pp. 923–932.

[25] M. Kim, N. Park, and D. Won, ‘‘Security analysis of a delegation-based authentication protocol for wireless roaming service,’’ in Multimedia and Ubiquitous Engineering (Lecture Notes in Electrical Engineering), vol. 308. Heidelberg, Germany: Springer, 2014, pp. 445–450.

[26] R. Amin, S. H. Islam, P. Gope, K. -K. R. Choo and N. Tapas, "Anonymity Preserving and Lightweight Multimedical Server Authentication Protocol for Telecare Medical Information System," in IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 4, pp. 1749-1759, July 2019, doi: 10.1109/JBHI.2018.2870319

[27] A.K. Das, V. Odelu, and A. Goswami, “A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS,” J. Med. Syst., vol. 39, no. 9, 2015, Art. no. 92.

[28] T. Maitra and D. Giri, “An efficient biometric and password based remote user authentication using smart card for telecare medical information systems in multi-server environment,” J. Med. Syst., vol. 38, no. 12, 2014, Art. no. 142. doi: 10.1007/s10916-014-0142-x.

[29] R.Amin and G. P. Biswas, “A novel user authentication and key agreement protocol for accessing multimedical server usable in TMIS,” J. Med. Syst., vol. 39, no. 3, 2015, Art. no. 33

[30] X. Li, Y. P. Xiong, J. Ma, and W. D. Wang, “An efficient and security dynamic identity-based authentication protocol for multi-server architecture using smartcards,” J. Netw. Comput. Appl., vol. 35, no. 2, pp. 763–769, 2012.

[31] B. Wang and M. Ma, “A smart card based efficient and secured multi-server authentication scheme,”Wireless Pers. Commun., vol. 68, no. 2, pp. 361–378, 2013

[32] Z. Mehmood, A. Ghani, G. Chen and A. S. Alghamdi, "Authentication and Secure Key Management in E-Health Services: A Robust and Efficient Protocol Using Biometrics," in IEEE Access, vol. 7, pp. 113385-113397, 2019, doi: 10.1109/ACCESS.2019.2935313.

[33] O. Mir and M. Nikooghadam, ‘‘A secure biometrics-based authentication with key agreement scheme in telemedicine networks for e-health services,’’ Wireless Pers. Commun., vol. 83, no. 4, pp. 2439–2461, 2015

[34] C -L. Lei and Y. -H. Chuang, "Privacy Protection for Telecare Medicine Information systems with Multiple Servers Using a Biometric-based Authenticated Key Agreement Scheme," in

[35] IEEE Access, vol. 7, pp. 186480-186490, 2019, doi: 10.1109/ACCESS.2019.2958830.

[36] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam and N. Kumar, "Efficient and Secure Anonymous Authentication with Location Privacy for IoT-Based WBANs," in IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2603-2611, April 2020, doi: 10.1109/TII.2019.2925071.

[37] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, “Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks,” J. Netw. Comput. Appl., vol. 106, no. 6, pp. 117–123, 2018.

[38] Kashif Hameed, Imran Sarwar Bajwa, Nadeem Sarwar, Waheed Anwar, Zaigham Mushtaq, Tayyaba Rashid, "Integration of 5G and Block-Chain Technologies in Smart Telemedicine Using IoT", Journal of Healthcare Engineering, vol. 2021, Article ID 8814364, 18 pages, 2021. https://doi.org/10.1155/2021/8814364

[39] Lin, T.-W.; Hsu, C.-L.; Le, T.-V.; Lu, C.-F.; Huang, B.-Y. A Smartcard-Based User-Controlled Single Sign-On for Privacy Preservation in 5G-IoT Telemedicine Systems. Sensors 2021, 21, 2880. doi:10.3390/s21082880

[40] Wang, X.; Zhao, J. An Improved Key Agreement Protocol Based on Chaos. Commun. Nonlinear Sci. Numer. Simul. 2010, 15, 4052–4057

[41] Lin, H.Y. Improved Chaotic Maps-Based Password-Authenticated Key Agreement Using Smart Cards. Commun. Nonlinear Sci. Numer. Simul. 2015, 20, 482–488

[42] Sureshkumar, V.; Amin, R.; Obaidat, M.S.;

Karthikeyan, I. An Enhanced Mutual Authentication and Key Establishment Protocol for TMIS Using Chaotic Map. J. Inf. Secur. Appl. 2020, 53, 102539.

[43] Kumar, V., Mahmoud, M.S., Alkhayyat, A. et al. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. J Supercomput 78, 16167–16196 (2022).

[44] Chen C-L, Yang T-T, Chiang M-L, Shih T-F (2014) A privacy authentication scheme based on cloud for medical environment. J Med Syst 38(11):143

[45] Chiou S-Y, Ying Z, Liu J (2016) Improvement of a privacy authentication scheme based on cloud for medical environment. J Med Syst 40(4):101

[46] Li C-T, Shih D-H, Wang C-C (2018) Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Comput Methods Prog Biomed 157:191–203

[47] Mohit P, Amin R, Karati A, Biswas G, Khan MK (2017) A standard mutual authentication protocol for cloud computing-based health care system. J Med Syst 41(4):50

[48] Chandrakar P, Sinha S, Ali R (2019) Cloud-based authenticated protocol for healthcare monitoring system. J Ambient Intell Human Comput, 1–17

[49] Deebak BD, Al-Turjman F (2020) Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. IEEE J Sel Areas Commun 39(2):346–360

[50] Bhanu Chander, Kumaravelan Gopalakrishnan,A secured and lightweight RFID-tag based authentication protocol with privacy-preserving in Telecare medicine information system,Computer Communications, Volume 191,2022,pages 425-437,ISSN 0140-3664,https://doi.org/10.1016/j.comcom.2022.05.002

[51] A A.K. Agrahari, S. Varma, A provably secure RFID authentication protocol based on ECQV for the medical internet of things, Peer-To-Peer Netw. Appl. 14 (3) (2021) 1277–1289.

[52] B M. Hosseinzadeh, J. Lansky, A.M. Rahmani, C. Trinh, M. Safkhani, N. Bagheri, B.Huynh, A new strong adversary model for RFID authentication protocols, IEEE Access 8 (2020) 125029-125045.

[53] CZ. Qikun, G. Yong, Z. Quanxin, W. Ruifang, T. Yu-An, A dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application, IEEE Access 6 (2018) 24064–24074.