On the Security Weaknesses in Password-Based Anonymous Authentication Scheme for E-Health Care

Rifaqat Ali, Preeti Chandrakar and Aashish Kumar

Abstract With rapid change of Internet technology, E-health care services are available for the patients at anytime and from anywhere. The patients access these services using a public channel. Therefore, the security of privacy maintaining is the prominent issue in E-health service. In order to authorize the patients, the authentication protocol plays a fundamental role in E-health system. Nowadays, a number of protocols based on mutual authentication and session key agreement have been brought before in the domain of security. Recently, Mishra et al. brought an authentication scheme for the remote user in telecare medical information system (TMIS). The claims made suggested that their scheme defends user anonymity and provides an efficient login along with smooth password change phase where wrong input could be quickly identified and the user is also provided with the facility to change password without the intervention of server. However, the authors have shown that the protocol is inadequate for real-world application because of several problems (1) Designing imperfection in login phase; (2) Designing imperfection in authentication phase; (3) Designing imperfection in change of password phase; (4) Lack of biometric update or change phase; (5) Strong replay attack, and (6) Clock synchronization problem. Moreover, we present the performance comparison taking cost comprising with communication, computation, smart card storage, and also with relevant security features.

R. Ali (✉)
Department of Computer Applications, Madanapalle Institute of Technology & Science, Madanapalle 517325, Andhra Pradesh, India
e-mail: rifaqatali27@gmail.com

P. Chandrakar · A. Kumar
Department of Computer Science & Engineering, National Institute of Technology (NIT), Raipur 492010, Chhattisgarh, India
e-mail: pchandrakar.cs@nitrr.ac.in

A. Kumar
e-mail: aashish2096@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_2

1 Introduction

The existence of life on this planet depends on a few factors among them are air, food, medication, etc. Medication or health care has its inception since the primitive ages and was one of the most critical elements, which have been taken care of. There implies plenty of improvements in the way medication is delivered since the time of its inception. The recent improvement and current age of modernization have revolutionized many fields ranging from defense, communication, services, etc. and each improvement setting its own benchmark. Every service which we avail has tried to make the life of human as easy as possible. Health care is also a stream, which has seen a drastic change in the way it was earlier and how it is now. Now, an attempt is made to provide each of these services available remotely and provide the same experience with many additional benefits. It comes bundled together in the name of TMIS (Telecare Medical Information System).

TMIS consists the services such as remote diagnosis, electronic medical records, etc. Remote diagnosis is the latest service, which is extremely useful for carrying out the diagnosis from a distant location. It becomes very useful in emergencies situation and providing instant medication and support. Another milestone is EMR (an electronic medical record), which supports the remote diagnosis. The only requirement for the services is the connection with the network and authorization to access the same. TMIS architecture described in Fig. 1. Generally, the user getting authorized via biometric check, if its success then it makes access the service otherwise it is denied. The subsequent medical data capture been made via the sensors embedded in the device and update with the device, which is then encrypted and propagated across the channel and finally to the central storage. The records as per request are availed at the hospital's end, and the details are accessed after decryption and then after that, the same is decrypted again and resent across the channel and the same is reflected in the central storage and the process goes on as a service.

Each of these services addressed comprises handling of sensitive data for each individual, which needs to be kept secure from that of adversary. There are numerous other reasons to keep the records secure. To address the security, there should be a proper message hiding and encryption technique, which should be used such as ECC (Elliptic Curve Cryptography), RSA (Ron Rivest, Adi Shamir, and Len Adleman), biometrics embedding, etc. to ensure that the system remains secure. Every technique have their own pros and cons, which makes it vulnerable to attacks various kinds. The new technique, which enables security for the services should be capable enough to deal with the shortcomings of various probable attacks and make the system robust enough to combat the consequences of attack if the adversary managed to intercept the channel. At the same time, the techniques should be efficient on the front of computation and communication standards to make it feasible enough to keeping other constraints into consideration (Fig. 1).

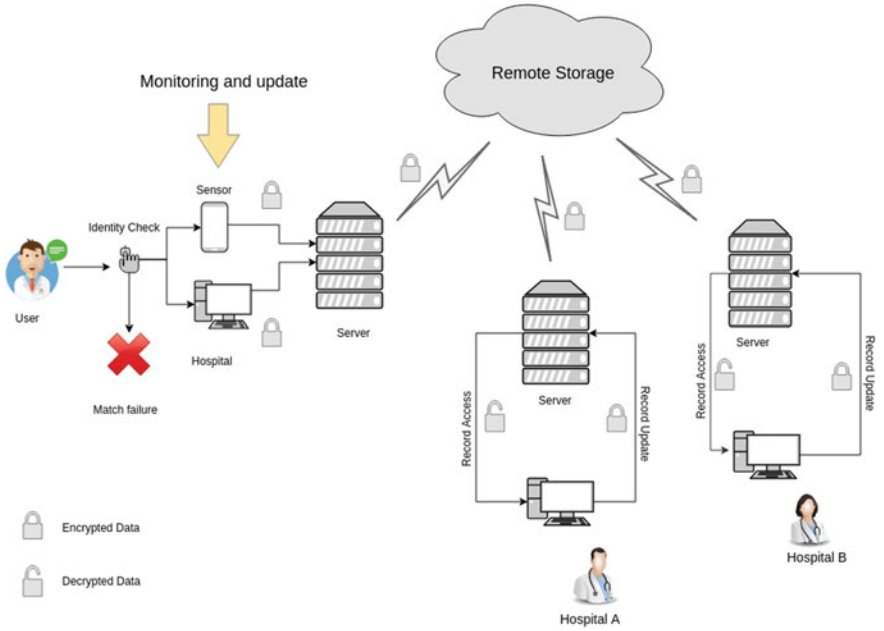

Fig. 1 TMIS workflow

1.1 Threat Model

For the sake of security, the scheme is proposed which would enable the secure transmission of information. However, the adversary always seeks an opportunity to make the attack and disrupt the smooth flow. There are few assumptions which are made before. There is no chance to seek or snoop information transmission in the reliable channel. Attempt to break one-way hash function always leads to failure. Adversary has the freedom to access monitor the data over the unreliable channel on which there would be an attempt to access transmission details. So, the protocol should be in a form that no adversary should be entertained and the transmission should be attack resistant.

1.2 Bio-hash Function

A hash function is a one-way transformation function. The hash function accepts an arbitrary length input and produces a fixed length string, which is called a hash value or a message digest.

Due to uniqueness characteristic and ability of biometric, various systems use biometric as an adopted method to solve authentication and verification problems.

However, a small change in biometric data may result in a massive change in the hash value. In other words, the result of the hash function will be changed due to the slight differences in the input and recognition errors will occur from slight biometric changes. To address this problem, a bio-function system is designed and studied [1, 2]. The bio-hash function has the following properties:

- Similar hash values are produced by the similar biometric information.
- Similar hash values are not produced by the different biometric information.
- Translation and rotation of the original biometric template should not have a substantial impact on hash values.
- Partial biometric information should be matched if sufficient detailed matters are present.

The hash function's certain class can be formulated to be everlasting to the order in which the input pattern is presented to the hash function, and such hash functions are referred to as the bio-hash function. So, the bio-hash function can solve the recognition error of general hash function and can authenticate a legitimate user even if the user's biometric information slightly change.

1.3 Contribution

In 2015, Mishra et al. [3] proposed an improved user authentication protocol for TMIS. They claimed that their scheme has the following merits: (i) efficient login phase and password change phase, (ii) Achieve user anonymity, (iii) Provide mutual authentication and Session key agreement, and (iv) Performance comparison with other similar schemes. We have pointed out several security weaknesses in Mishra et al.'s scheme such as Designing Imperfection in login phase, Designing Imperfection in authentication phase, Designing Imperfection in password change phase, Lack of biometric update or change phase, Strong replay attack, and Clock synchronization problem. The performance comparison of the other schemes is also made with which other protocols provide the overview about the respective protocol's feasibility. We even propose the future scope, which the field of security.

1.4 Organization of This Article

The chapter has been in the organized in the following manner. In Sect. 2, the details about the related literature work is discussed, which describes about the similar works and their respective contribution in the domain. The next Sect. 3 details about the Mishra et al.'s [3] scheme and summary of each phase involved in the scheme. Section 4 details about the cryptanalysis of the scheme and pointed out the flaws present in the scheme. Section 5 brings the performance comparison of scheme with the latest

protocols based on the parameter as storage cost, communication, and computation costs. We also address the future scope in Sect. 6 comprising of what the sector might hold. Finally, we arrive at the conclusion in Sect. 7.

2 Literature Review

The area of security is an active area of research and there has been numerous works in this area. After the first-ever authentication-based protocol was proposed in 1981 by Lamport [4] for which password was used for authentication. Many recent works have done in succession [3, 5–13] and few recent ones have been discussed here.

In 2015, Arshad et al. [5] brought an improvement to Bin Muhaya's [14] scheme, which was found to be prone to offline password guessing attack and which even fails in providing the perfect forward secrecy. Improvement provided led to an improvement in computation time by 2.73 times. In 2016, Wazid et al. [15] brought a complete analysis of the security requirements keeping the services into consideration. The analysis provides the mathematical review of methods used along with their future scope of improvement that should be addressed in the near future. Also, Aslam et al. [16] in 2016 proposed a complete summary of the related scheme proposed based on one, two, and three factors with their respective pros and cons. It also points the probable attacks and mathematical requirements to implement these security measures. The analysis enables complete comparison based on features and respective drawbacks wrt to each proposed scheme is made.

Again in 2016, Jiang et al. [17] brought an enhancement to Wu et al. [18] proposed a protocol, which relies on 3-factor remote authentication and which found a vulnerability in offline password guessing, and at the same time prone to user impersonation attack. Additionally, it failed to provide a recovery mechanism if the smart card is lost or stolen. Another proposal was by Wazid et al. [19] which was again an improvement to Amin and Biswas [20] scheme of 2015 who proposed a 3-factor authentication scheme and which was found to be vulnerable to many potholes as privileged-insider attack, replay attack, along with user and server impersonation attack and even stolen smart card attack. Improvement addressed drawbacks and ensured that the scheme is shielded to attack as stated.

In 2017, Jiang et al. [21] brought an improvement to Lu et al. [22] scheme, which relies on 3-factor authentication scheme and claims to be secure from attacks but fails in identity guessing, tracking attack, identity revelation, offline password guessing, and impersonation attack with both user and server. The scheme makes improvements in the drawbacks addressed earlier at the same time making it a balance between security and efficiency. In 2017, again, Wu et al. [23] brought before RFID-based scheme, which enables both forward and backward untraceability. Also, it enables keeping the details of tag and reader anonymous. The scheme meets all the required security milestones and at the same time is applicable for usage across the services.

In 2017, authentication scheme which was based on human biometrics was brought by Jung et al. [24], which was an improvement to Liu et al.'s [25] proposed

scheme in 2016, which used a biometric-based encryption scheme for health care but suffers numerous vulnerabilities as improper identification based on biometrics, spoofing attack and also fails to provide session key verification. The improvement provided by the protocol ensures that the system is secure with these loopholes mentioned in Liu et al. [25] scheme with security being enhanced. In 2017 again, Chatterjee et al. [26] provided an approach to carry out the authentication by setting the access control to the particular users as per requirement. It enables making group-based authentication scheme, which resists attacks and ensures data secrecy.

Another addition was by Mohit et al. [27] in 2017, which was an improvement to cloud-based Chiou et al.'s [28] scheme, which enables the patient and hospital to upload the data to the server which hereby could be used by the doctor for treatment and after further changes could be pushed to the server. It has its own flaw in the name of failing to preserve anonymity and safety against the stolen attack. The contribution of Mohit et al. [27] removes the drawback and improves communication and computation overheads.

In 2018, Kumar et al. [29] found that proposed Mohit et al.'s [27] protocol is a cloud-based system for mutual authentication in the domain of health care. It was found that the scheme has the drawbacks as stolen verifier attack, and many logged into the patient attack, impersonation attack, and failure for session key protection. These attacks are eradicated by Kumar et al. [29] and also improvement in computation and communication overheads. Again in 2018, Li et al. [30] brought before a cloud-based medical service where patients could securely use the service keeping privacy maintained. The scheme is even compared with protocols proposed earlier in a similar direction and proves that the scheme is shielded against the attack and provides a better computation, which makes the scheme practical for usage in cloud-based systems.

3 Overview of Mishra et al. [3] Protocol

We have summarized Mishra et al.'s [3] scheme. It has phases as registration, login, verification, password change, and smart card revocation phase, respectively. The used notations here are addressed in Table 1.

For initializing the system, first, the server S makes a choice for two prime numbers i and j of length 1024 bits, it then calculates n = ij. Then select a prime p and integer X in the form that $pX \equiv 1 \bmod (i-1)(j-1)$. Where i, j, and X are kept as secret while n and p published as public.

3.1 Registration Phase

Here, whenever a new user makes registration. He/she performs the below mentioned steps (Table 2).

Table 1 Meaning of symbols and notations of this manuscript

Notation	Description
U	User
RC	Registration center
S	Server
E	An adversary
ID	User identity
PW	U password
SC	Unique serial number of smart card
B	U's biometric key
X	S's secret(master) key
$h(.)$	Hash function
$H(.)$	Bio-hash function
N_c	U random nonce
N_s	S random nonce
$\|$	Concatenation operator
$\oplus$	*XOR* operator
SK	Session key

Step1: The new user U makes a choice for identity ID and password PW with full liberty. Then, submit the request for registration to the medical server with ID.

Step2: On receiving the request for registration by user U, S checks the uniqueness of ID. If it fails, then the session is aborted. Otherwise, allocates unique SC, it then calculates $J = h(X \parallel ID \parallel N \parallel SC)$, where SC is the unique serial number of smart card and take N = 0 if user is new, else set N to N + 1.

Step3: The S stores values as $\{J, n, e, h(.)\}$ in the smart card and sends smart card to user U. In addition, S keeps record of patient which is stored in the database and the new entry (ID, RID) is added in the database, where $RID = (N \parallel SC \parallel T_r)$ and T_r is the time of registration.

Step4: After the smart card is received, the user U gives biometrics B and calculates $L = J \oplus h(ID \parallel PW)$ & $V = h(ID \parallel H(B) \parallel PW)$, where H is a function which performs bio-hash. Then, swap the parameter L with J and then store the value V in the smart card. At the end, the smart card holds values as $\{V, L, n, e, h(.)\}$.

3.2 Login Phase

Here, whenever the user requires to avail the service, it logs into server, then insertion of smart card into a smart card reader and then the identity ID, password PW, and imprints biometric B as input.

Table 2 Comparison of related works with cryptographic method, their highlights, and year of work

Scheme	Cryptographic method	Highlights	Year
Arshad et al. [5]	ECC	Improvement of Bin Muhayas scheme Faster computation 2.73 times	2015
Wazid et al. [15]	–	Protocols analysis along with their scope of improvement	2016
Aslam et al. [16]	–	Protocol analysis based on one-, two-, or three-factor for authentication with their respective pros and cons Probable attacks and drawbacks known	2016
Jiang et al. [17]	ECC	Improvement to Wu et al. scheme Vulnerabilities due to attacks removed	2016
Wazid et al. [19]	ECC	Improvement to Amin-Biswas scheme Removal of vulnerabilities as replay, user and server impersonation and stolen smart card attack	2016
Jiang et al. [21]	ECC	Improvement to Lu et al. scheme Shield against vulnerabilities as identity guessing, tracking, identity revelation, online password guessing, user and server impersonation attacks	2017
Wu et al. [23]	–	RFID-based scheme which enables untraceability Enables keeping the details of tag and reader anonymous	2017
Jung et al. [24]	ECC	Improvement to Liu et al. scheme Biometric-based authentication Vulnerabilities removal as improper identification, spoofing attack and fails to provide session key verification	2017
Chatterjee et al. [26]	Key policy attribute-based encryption	Authentication by setting access control levels Group-based authentication scheme which resists attacks and enables secrecy	2017
Mohit et al. [27]	Digital signatures	Improvement to cloud-based Chiou et al. scheme Removes drawback and improvement in communication and computation overheads	2017
Kumar et al. [29]	Digital signatures	Improvement to Mohit et al. Vulnerabilities removal as stolen verifier, many patient logged in, user and server impersonation, and failure for session key protection attack	2018
Li et al. [30]	ElGamal signature scheme	Cloud-based medical service usage keeping privacy maintained Secure against probable attack and better computation	2018

Step1: Check for $V == h(ID \parallel H(B) \parallel PW)$. If this condition evaluates to false, the session is then aborted. Else, find $J = L \oplus h(ID \parallel PW)$.

Step2: Choose a random number r_u and find $A = J^{r_u} \bmod n$ & $C_u = h(ID \parallel A \parallel J \parallel T_u)$, then put forwards the login message AID to the S, here and T_u is latest timestamp.

3.3 Verification Phase

Here, both server and user checks the legitimacy of one another and a session key is created for safe transmission of information. Following are the steps involved in verification phase.

Step1: After receiving the message AID, the S calculates $AID^X \bmod n$ and gets $(ID \parallel T_u \parallel A \parallel C_u)$. It takes out the entry $RID = (N \parallel SC \parallel T_r)$ which is equivalent to ID in the recorded table. Next, S checks if $T_u > T_r$. The S then calculates $J = h(X \parallel ID \parallel N \parallel SC)$ and checks if $C_u =?h(ID \parallel A \parallel J \parallel T_u)$. If it fails, the session is terminated. Else, U is identified by S. Furthermore, replacement of RID with $RID^* = (N \parallel SC \parallel T_u)$ is made by S.

Step2: The S makes a choice for random number r_s and computes $D = J^{r_s} \bmod n$, $K_{us} = A^{r_s} \bmod n = J^{r_u r_s} \bmod n$. It then calculates the session key $sk_{us} = h(ID \parallel K_{us} \parallel J \parallel T_u)$ and $C_s = h(ID \parallel sk_{us} \parallel D \parallel T_u)$. At last, S assumes sk_{us} as session key and shares the message as $< D, C_s >$ with user U.

Step3: After the message is received, i.e., $< D, C_s >$, the smart card calculates $K_{su} = D \bmod n = J^{r_s r_u} \bmod n$ and also the session key $sk_{su} = h(ID \parallel K_{su} \parallel J \parallel T_u)$ and also calculate $C_s^{'} = h(ID \parallel sk_{su} \parallel D \parallel T_u)$. Now, check $C_s^{'} =?C_s$. If this condition fails, then terminate the session. Else, S identified by U. Both U and S agree on session keys sk_{us} and sk_{su}, i.e., $K_{us} = J^{r_s r_u} \bmod n = J^{r_u r_s} \bmod n$.

3.4 Password Change Phase

Here, the user is provided with facility to alter password without the aid of server.

Step1: The user U now adds smart card in the reader and then gives biometric B. Again, input for ID, PW, and new password PW_{new} is made.

Step2: The next smart card checks for $V == h(ID \parallel H(B) \parallel PW)$. If this check fails then the session is terminated. Else, calculate $J = L \oplus h(ID \parallel PW)$.

Step3: Then, smart card calculates $L_{new}=J \oplus h(ID \parallel PW_{new})$ and $V_{new}=h(ID \parallel H(B) \parallel PW_{new})$. Replacement of L with L_{new} and V with V_{new} is made.

3.5 Smart Card Revocation Phase

Here, the revocation of smart card is made if the same is lost or damaged by any such reason. Then, the smart is provided by the seever when the request is made.

Step1: The U makes a request to avail a new smart card to S along with an identity ID.

Step2: The S checks for the identity of U. If the U is not genuine or if ID is invalid, the session is then aborted. Else, we head toward the very next step.

Step3: The server S takes out $RID = (N \parallel SC)$ which is similar to ID in stored database.

Step4: S then frames the user specific smart card for U by storing the values $\{J_{new}, n, e, h(.)\}$ in it, where $J_{new} = h(X \parallel ID \parallel N + 1 \parallel SC_{new})$ and SC_{new} is new serial number of the smart card. Then, the smart card is sent to user U through a safe channel and replacement of RID with RID_{new}, where $RID_{new} = (N + 1 \parallel SC_{new})$ is made.

Step5: After gaining smart card, U performs **Step4** of registration phase.

4 Cryptanalysis of Mishra et al. [3] Scheme

4.1 Designing Imperfection in Login Phase

In the phase of login, the verification of $V == h(ID \parallel H(B) \parallel PW)$ will never be obtained because of the bio-hash function $H(.)$ is not present in smart card's memory. So, smart card reader cannot compute $H(B)$. Therefore, without the correct value of $H(B)$, the password verification, i.e., $V = h(ID \parallel H(B) \parallel PW)$ always turns out to be false. Further, computation of $J = L \oplus h(ID \parallel PW)$, $A = J^{r_u} \bmod n$ & $C_u = h(ID \parallel A \parallel J \parallel T_u)$ is done by smart card, which contains the value old identity and password. Therefore, the value of J, A, C_u is not correct without using proper value of identity and password. As a result, login message AID is incorrect. It is clear from the above explanation, Mishra et al.'s [3] scheme fails to verify identity, password, and biometric. This is a very severe drawback in Mishra et al. [3] scheme.

4.2 Designing Imperfection in Authentication Phase

In authentication, denial-of-service (DoS) attack can cause a permanent error on authentication by introducing unexpected data during the procedures of authentication. User U fails to login into the server using valid identity and password owing to the flaw in the authentication phase. This implies that inefficiency in the authentication phase would result in denial-of-service attack. An adversary may perform denial-of-service attack to cause the server to reject the login of a specific user. In Mishra et al.'s [3] protocol, the authentication phase has some design flaws, which is described as follows.

Step1: Let's suppose that user has lost smart card in some way. The user now wants to make the recovery of smart card then the user executes the smart card revocation phase.

Step2: After successful execution of smart card revocation phase, $RID = (N \parallel SC \parallel T_r)$ is replaces with $RID_{new} = (N + 1 \parallel SC_{new})$ and stores RID_{new} into the database.

Step3: In the next login session, the user shares the request for login via message $AID = (ID \parallel T_u \parallel A \parallel C_u)^e \bmod n$ to the server, where T_u is the current login time stamp.

Step4: After the message is received from user, the server in the beginning checks for the novelty of timestamp $T_u > T_r$. After execution of the phase of revocation, the timestamp T_r is not stored in the database. So, the server cannot retrieve the timestamp T_r. Therefore, the server fails to verify the uniqueness of the timestamp and the session is aborted.

4.3 Designing Imperfection in Password Change Phase

In Mishra et al.'s [3] protocol, the same signs of imperfection was found in password change phase as in that of login phase. In password change phase also, the verification is a failure because the bio-hash function is not present in the smart card. So, the reader always fails in verifying the password, identity, and biometrics as well. As a result, inefficient password change phase results in denial-of-service attack. Denial-of-service attack is a decisive attack, where the adversary can use some methods to work upon the server so that the legitimate user's access requests will be denied by the server. An attacker can modify the false verification information of a valid user for the next login phase. Afterward, the valid user will not access the server anymore. So, any illegal person could make changes in the user's password in the following manner.

Step 1: If attacker gains the smart card of user by some method and attempts to change the password of user.

Step 2: He/she then enters a random identity, password, and gives biometric B. After that, reader performs the verification but we know that this password verification always fails. So, a user U is re quested to give a new password PW_{new}.

Step 3: Attacker enters new password PW_{new} and smart card calculates $L_{new} = L \oplus h(ID \parallel PW) \oplus h(ID \parallel PW_{new})$ and $V_{new} = h(ID \parallel H(B) \parallel PW_{new})$. Then, replace its L with L_{new} and V with V_{new}.

Step 4: So, the attacker could change the legal user's password and after that legitimate user would not able to access his/her own account.

The above discussion shows that the Mishra et al.'s [3] scheme has an inefficient phase of password, which also leads to DoS attack.

4.4 Lack of Biometric Update or Change Phase

The biometrics update requires because the biometrics has the problem of the aged deterioration. The most prominent properties in a authentication scheme using biometrics is that a legitimate user should be provided with the opportunity to change or update old password along with biometrics. Mishra et al.'s [3] scheme fails to provide biometric update or change phase.

4.5 Strong Replay Attack

In this attack, an attacker tries to be a legal user by retransmitting the previous executed messages to the desire entity. In Mishra et al.'s [3] protocol, in log-in phase, message $AID = (ID \parallel T_u \parallel A \parallel C_u)^e \bmod n$ is calculated on the patient's end and transmission of this message is made to the server across the public channel, where $A = J^{r_u} \bmod n$ and $C_u = h(ID \parallel A \parallel J \parallel T_u)$, where ID is patient's identity and T_u is current timestamp. It can be shown that Mishra et al. [3] protocol is susceptible to strong replay attack due to following reasons.

Step1: Suppose that the login message AID has intercepted by the attacker and retransmits after a short duration of time.

Step2: Upon obtaining the message from the attacker, the server first decrypts the message AID using the secret key d and retrieves $(ID \parallel T_u \parallel A \parallel C_u)$. Subsequently, server checks the novelty of time interval, i.e., $T_u > T_r$. But T_r does not exist in the database because in the previous user's authentication session, T_r is replaced with T_u. Therefore, the condition $T_u > T_r$ never obtained and server fails to check the originality of the timestamp.

Step3: Afterward, server calculates $J = h(X \parallel ID \parallel N \parallel SC)$ and checks if $C_u = h(ID \parallel A \parallel J \parallel T_u)$ and this condition always holds because AID is a valid message given by the genuine user. Therefore, the adversary is successful to login into the remote server using the previously intercepted message AID.

4.6 Clock Synchronization Problem

Any mutual authentication scheme is avoided from attacks as replay and man in middle with the help of timestamps. Unfortunately, clock synchronization problem [24, 26] arises using timestamp in huge networks like wide area networks, mobile communication, and satellite communication networks. The number of schemes depend on timestamp can resist replay attack by means of systems's timestamp provided the system clock must be synchronized; otherwise, the scheme will not work accurately. Through the network environments and transmission delay is not predictable, the possible replay attack is found in all the existing schemes those used timestamp.

According to the aforementioned explanation, Mishra et al. [3] scheme depends on timestamps. Definitely, it would face the clock synchronization problem.

5 Performance Comparison

To measure the feasibility of the protocol, it is mandatory to analyze the performance in the form of required storage requirement, communication cost, and computation cost. For comparison, a series of protocols in the related domain is taken as represented in Table 3 below.

In Table 4 below, the comparison of the protocol with their respective costs are made. For memory requirement analysis, standards assumed are IDs and timestamps taking 32 bits, random nonce of 64 bits, one-way hash function requiring 256 bits, bio-hash function requiring 160 bits, elliptic curve point consumes 320-bits, and for encryption or decryption, it requires 512 bits. In the comparison of the storage requirements, the cost comprises of storage in database and smart card if protocol makes use of it. Taking protocol P1, the storage requirement in database is of {ID_i, n_i = 96 bits} and for smart card storage, it requires {V_i, K_i, xP, l, h(.), H(.) = 832 bits}. Again, in the similar fashion, the storage requirement for the protocols P2, P3, P4, P5, P6, and P7 are {704 = (256 * 2 + 32 + 160), 672 = (160 * 3 + 32), 1248 = (256 * 3 + 160 * 3), 1216 = (512 + 256 * 2 + 64 * 3), 1280 = (512 * 2 + 256), and 1440 = (256 * 4 + 160 + 512)} bits, respectively.

Again, on the communication front, the requirement is because of the messages shared across the channel to achieve mutual authentication among the participants. Taking protocol P1 messages shared are M1{d_sP = 320 bits}, M2{AID_i, M_1, M_2} = 832 bits, and M3 {M_3 = 256 bits}. Collectively comprising of 1408 bits. Similarly, for P2, P3, P4, P5, P6, and P7 requirement is of {1344, 1442, 1696, 2464, 2240, 2496} bits, respectively.

For calculation of computation cost, the timing requirement for each operation is considered. The operations as hash function, symmetric key encryption, point multiplication, point addition, fuzzy extraction, modular exponentiation, inverse, and bio hashing represented by {T_H,T_S,T_{PM},T_{PA},T_{FE}, T_{ME}, T_{INV}, T_{BH}} whose operation

Table 3 Representation of protocols

Representation	Protocol
P1	Jiang et al. [21]
P2	Qiu et al. [31]
P3	Xu et al. [32]
P4	Arshad et al. [5]
P5	Ostad et al. [33]
P6	Chaudhry et al. [34]
P7	Wazid et al. [19]

Table 4 Comparison of various cost with other protocols

Parameter	P1	P2	P3	P4.	P5	P6	P7
Storage (bits)	928	704	672	1248	1216	1280	1440
Communication (bits)	1408	1344	1442	1696	2464	2240	2496
Computation time	$16T_H + 4T_{BH} + 6T_{PM} + 1T_{INV}$	$18T_H + 4T_{PM}$	$16T_H + 6T_{PM}$	$14T_H + 6T_{PM}$	$26T_H + 5T_{PM} + 2T_{PA} + 3T_S$	$19T_H + 7T_{PM} + 7T_S + 2T_{BH}$	$21T_H + 3T_{PM} + 3T_S + 2T_{FE}$
Time (s)	0.470175	0.2613	0.338645	0.38695	0.35499	0.5519	0.351975

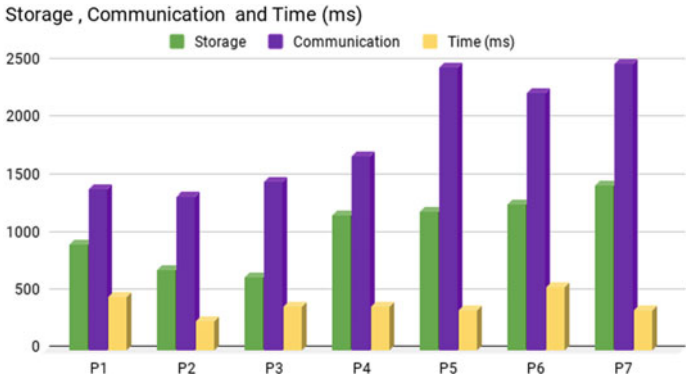

Fig. 2 Storage cost, communication cost, and time comparison chart

Table 5 Feature comparison of protocols

Feature	P1	P2	P3	P4	P5	P6	P7
User anonymity	✓	✓	✓	✓	✓	✓	✓
Impersonation attack	✓	✓	✓	✓	✓	✓	✓
Mutual authentication	✓	✓	✓	✓	✓	✓	✓
Known key security	✓	✓	✗	✓	✗	✗	✓
Perfect forward secrecy	✓	✓	✓	✓	✓	✓	✓
Replay attack	✓	✓	✓	✓	✓	✓	✓
Man-in-middle attack	✓	✓	✓	✓	✓	✓	✓
Offline password guessing attack	✓	✓	✓	✓	✓	✓	✓
Denial-of-service attack	✗	–	–	–	✓	✗	✗

time and corresponding values are (0.0005, 0.0087, 0.063075, 0.000262, 0.063075, 0.522, 0.003725, 0.02 s), respectively. Taking protocol P1, the operations being performed are $16T_H$,$4T_{BH}$, $6T_{PM}$, and 1 TT_{INV} which sums up the entire timing requirement to {16 * 0.0005 + 4 * 0.02 + 6 * 0.063075 + 0.003725 = 0.470175 s}. Similarly, for P2, P3, P4, P5, P6, and P7 requirement is of {0.2613, 0.338645, 0.38695, 0.35499, 0.5519, 0.351975} sec, respectively.

The graphical representation in Fig. 2 below shows the comparison of the protocol when their respective costs is made.

Now, in Table 5 below, the feature comparsion of the protocols is been made with the features which one protocol provides and the other fails to address. The properties such as Mutual authentication, Non-repudiation, User anonymity, Perfect forward secrecy, Biometrics protection, and attacks as Man in middle, Impersonation, Replay attack, Offline password guessing, and Denial of service are considered here.

6 Future Scope

There has been a series of modifications in the protocol itself after the first protocol by Lamport [4] was proposed. The changes have come in the name of factors used ranging from passwords, smart card, and biometrics. They have been successful in providing the security from the numerous attacks but in the upcoming scenario, there have to be some added ways to tackle the security issues. In the future scope, there could be an increase in the biometrics being used for authentication say multiple biometrics. The next scope could be in the name of usage wearable devices which could provide the authentication thus eradicating the use of passwords and ID for authentication. The improvement could be even in the name of usage of hashing function and its implementation which could reduce the computation time as well as the number bits involved. The dependency on any such equipment as the smart card and its reader should be reduced taking into account the capacity of the system to be fault tolerant with smart card and even the server as well.

7 Conclusion

In this work, E-health care domain is addressed with its security implications and taking into account the protocol given by Mishra et al. The overview of the protocol is addressed and a lot of security loopholes in the protocol for respective phases and also prone to some attacks. The security comparison of the similar protocols has been made so that the analysis of the feasibility of the same could be made. There has been a discussion on the scope in the domain of security and with that of added feature and characteristics, which could be utilized to come up with the feasible yet dealing with all the loopholes which could erupt in the time to come.

References

1. Chaki, J., Dey, N., Shi, F., & Sherratt, R. S. (2019, January 24). Pattern mining approaches used in sensor-based biometric recognition: A review. *IEEE Sensors Journal*.
2. Dey, N., Nandi, B., Dey, M., Biswas, D., Das, A., & Chaudhuri, S. S. (2013, February 22). BioHash code generation from electrocardiogram features. In *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 732–735). IEEE.
3. Mishra, R., & Barnwal, A. K. (2015). A privacy preserving secure and efficient authentication scheme for telecare medical information systems. *Journal of Medical Systems*, *39*(5), 54.
4. Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11), 770–772.
5. Arshad, H., Teymoori, V., Nikooghadam, M., & Abbassi, H. (2015). On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. *Journal of Medical Systems*, *39*(8), 76.

6. Ali, R., & Pal, A. K. (2017). Three-factor-based confidentiality-preserving remote user authentication scheme in multi-server environment. *Arabian Journal for Science and Engineering*, *42*(8), 3655–3672.
7. Ali, R., Pal, A. K., Kumari, S., Karuppiah, M., & Conti, M. (2018). A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. *Future Generation Computer Systems*, *84*, 200–215.
8. Ali, R., & Pal, A. K. (2018). An efficient three factorbased authentication scheme in multiserver environment using ECC. *International Journal of Communication Systems*, *31*(4), e3484.
9. Ali, R., & Pal, A. K. (2017). A secure and robust three-factor based authentication scheme using RSA cryptosystem. *International Journal of Business Data Communications and Networking (IJBDCN)*, *13*(1), 74–84.
10. Chandrakar, P., & Om, H. (2017). Cryptanalysis and extended three-factor remote user authentication scheme in multi-server environment. *Arabian Journal for Science and Engineering*, *42*(2), 765–786.
11. Chandrakar, P., & Om, H. (2017). A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. *Computer Communications*, *110*, 26–34.
12. Chandrakar, P., & Om, H. (2017). Cryptanalysis and improvement of a biometricbased remote user authentication protocol usable in a multiserver environment. *Transactions on Emerging Telecommunications Technologies*, *28*(12), e3200.
13. Chandrakar, P., & Om, H. (2018). An efficient two-factor remote user authentication and session key agreement scheme using Rabin cryptosystem. *Arabian Journal for Science and Engineering*, *43*(2), 661–673.
14. Bin Muhaya, F. T. (2015). Cryptanalysis and security enhancement of Zhu's authentication scheme for Telecare medicine information system. *Security and Communication Networks*, *8*(2), 149–158.
15. Wazid, M., Zeadally, S., Das, A. K., & Odelu, V. (2016). Analysis of security protocols for mobile healthcare. *Journal of Medical Systems*, *40*(11), 229.
16. Aslam, M. U., Derhab, A., Saleem, K., Abbas, H., Orgun, M., Iqbal, W., et al. (2017). A survey of authentication schemes in telecare medicine information systems. *Journal of Medical Systems*, *41*(1), 14.
17. Jiang, Q., Khan, M. K., Lu, X., Ma, J., & He, D. (2016). A privacy preserving three-factor authentication protocol for e-Health clouds. *The Journal of Supercomputing*, *72*(10), 3826–3849.
18. Wu, F., Xu, L., Kumari, S., & Li, X. (2015). A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks. *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2015.02.015.
19. Wazid, M., Das, A. K., Kumari, S., Li, X., & Wu, F. (2016). Design of an efficient and provably secure anonymity preserving threefactor user authentication and key agreement scheme for TMIS. *Security and Communication Networks*, *9*(13), 1983–2001.
20. Amin, R., & Biswas, G. P. (2015). A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity. *Journal of Medical Systems*, *39*(8), 1–19.
21. Jiang, Q., Chen, Z., Li, B., Shen, J., Yang, L., & Ma, J. (2018). Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), 1061–1073.
22. Lu, Y., Li, L., Peng, H., & Yang, Y. (2015). An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. *Journal of Medical Systems*, *39*, 32. https://doi.org/10.1007/s10916-015-0221-7.
23. Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., & Shen, J. (2018). A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), 919–930.
24. Jung, J., Moon, J., & Won, D. (2017). Robust biometric-based anonymous user authenticated key agreement scheme for telecare medicine information systems. *KSII Transactions on Internet and Information Systems, 11*(7), 3720–3746. https://doi.org/10.3837/tiis.2017.07.023.

25. Liu, W., Xie, Q., Wang, S., & Hu, B. (2016). An improved authenticated key agreement protocol for telecare medicine information system. *SpringerPlus, 5*(1), 555. Article (CrossRef Link).
26. Chatterjee, S., Roy, S., Das, A. K., Chattopadhyay, S., Kumar, N., Reddy, A. G., et al. (2017). On the design of fine grained access control with user authentication scheme for telecare medicine information systems. *IEEE Access, 5*, 7012–7030.
27. Mohit, P., Amin, R., Karati, A., Biswas, G. P., & Khan, M. K. (2017). A standard mutual authentication protocol for cloud computing based health care system. *Journal of Medical Systems*, *41*(4), 50.
28. Chiou, S. Y., Ying, Z., & Liu, J. (2016). Improvement of a privacy authentication scheme based on cloud for medical environment. *Journal of Medical Systems*, *40*(4), 1–15.
29. Kumar, V., Jangirala, S., & Ahmad, M. (2018). An efficient mutual authentication framework for healthcare system in cloud computing. *Journal of Medical Systems*, *42*(8), 142.
30. Li, W., Zhang, S., Su, Q., Wen, Q., & Chen, Y. (2018). An anonymous authentication protocol based on cloud for telemedical systems. In *Wireless communications and mobile computing*.
31. Qiu, S., Xu, G., Ahmad, H., & Wang, L. (2018). A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. *IEEE Access*, *6*, 7452–7463.
32. Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., & He, L. (2013). A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. *Journal of Medical Systems*, *38*, 1–7.
33. Ostad-Sharif, A., Abbasinezhad-Mood, D., & Nikooghadam, M. (2019). A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications. *Journal of Medical Systems*, *43*(1), 10.
34. Chaudhry, S. A., Khan, M. T., Khan, M. K., & Shon, T. (2016). A multiserver biometric authentication scheme for tmis using elliptic curve cryptography. *Journal of Medical Systems*, *40*(11), 230.