International Journal of Computer Sciences and Engineering
Vol.**11**, Special Issue.**1**, pp.**107-113**, November **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Paper

An improved algorithm with Multifactor Authentication Scheme for Telecare Medical Information System (TMIS)

Asit Kumar Nayek[1*], **Radha Krishna Jana**[2], **Arpan Adhikary**[3]

[1,3]Dept. of Computer Science & Engineering (AIML),Haldia Institute of Technology, Haldia, India
[2]Computer Science & Engineering, JIS University, Kolkata, India

**Corresponding Author: asit.nayek@gmail.com*

Abstract: Telemedicine and its base, Telecare Medical Information System (TMIS), are becoming popular trend in the post COVID days. Faster Internet services and wireless technologies essentially provide faster data transfer facilities in Internet of Things (IoT) environment. To provide remote healthcare services, wearable and household medical devices are connected to form IoT networks. Thus, private data are exposed over the Internet and privacy maintenance is an issue. Elliptic Curve Cryptographic (ECC), a public key system, may be used since it can handle lightweight keys for small devices. One way hash-functions are very useful to protect any data but are irreversible. Hashing is useful to implement for data integrity. Our proposed system will use public key cryptosystem where keys are generated in ECC over a cyclic field. Beside this, One Time Password (OTP) will be used to provide another layer of user verification that will be transmitted in the GSM like telephone network. We will expect to provide security at different levels for all kind of users in a TMIS environment.

Keywords: Internet of Things (IoT), Elliptic Curve Cryptography (ECC), One Time Password (OTP), Hashing, Encryption and Decryption.

1. Introduction

In the realm of 5G networks, Internet bandwidth is increased in many folds to support huge data transfer among data processing nodes. In support of this evolution, Internet of Things (IoT) plays a vital role in several applications which are directly associated with various domains in human life. Starting from agriculture, healthcare, weather forecasting, manufacturing industries, mining industries, etc., are few of them. In the recent past, outbreaks of human transmissible diseases compelled us to lean towards remote healthcare system and telemedicine services. Telemedicine and Telecare Medical Information System (TMIS) are becoming necessary for remote areas where usual transportation facilities are limited. Even, these applications are mostly welcome by elderly people who are apart from their near and dears. Privacy and data security maintenance are major challenges in this environment since these kind of systems shall be personally secured as well as to be secured from the health care providers' end. A typical TMIS environment is shown in figure-1.

As shown in the above figure, a TMIS environment consists of personal area network (PAN) where IoT devices are connected through a wireless sensor network (WSN) or via GSM network or via Wi-Fi networks. These devices are able to collect data and transmit them via local switches to cloud computers or to some other local servers.

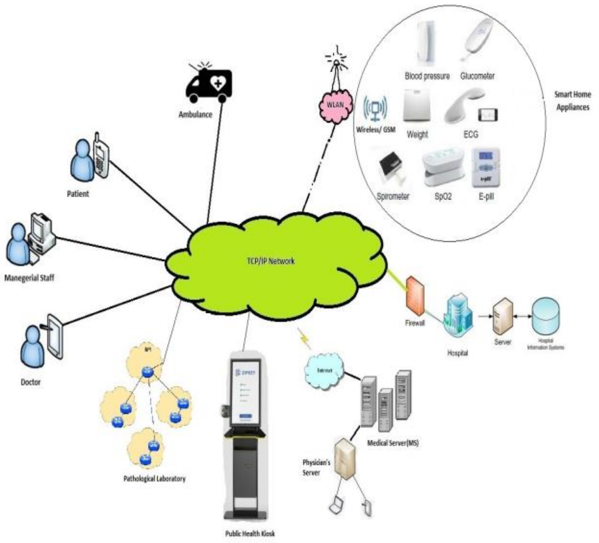


Fig 1. A typical TMIS environment

In a typical TMIS environment, sensory devices are distributed at different geographical locations that are connected by network devices over the Internet. Often the devices may turn into point of fires for the intruders to steal valuable data that mislead different users. Security measures shall be taken at different levels that protect user information as well as stored data at remote servers. Many schemes have been proposed so far in this direction that are discussed in section 2. Abbreviations that used in the discussion are summarised in subsection 2.1. In subsection 2.2, we described a little bit of technical preliminaries which are relevant to our present literature. Models that are proposed for authentication purposes are discussed in section 3 and its underlying subsections. Performance analysis of the proposed scheme from different points as given in Table 2, are described in section 4 and its subsequent paragraphs. Conclusion and future direction to this concern are discussed in section 5. Overall, in this paper we try to convince our scheme with mathematical notions.

2. Related Work

In [1], the authors proposed a two-factor authentication scheme where user ID & password are used for authentication and shared session key is used for secured conversation between patient and doctor. User ID and Password are stored within smart card in hashed form while a fresh registration is made. Here, a user couldn't change a password by any means. Their proposal may suffer from stolen card attack since a card is used for the anonymity of a user.

In [2], Anjali Singh, et. al., reviewed the scheme proposed by R. Amin, et.al., scheme [3], where user anonymity, perfect forward secrecy and mutual authentication was not maintained. However, the authors assumed that the content of a card is recoverable even if they are stored in the memory in hashed form.

In [4], the authors reviewed a three-factor authentication scheme as proposed by Jongseok Ryu, et. al., and proposed a solution for session key exchange between communicating parties using Elliptic Curve Cryptography (ECC). According to their proposal, public key pairs are computed with ECC. Rest of the encryption scheme was kept identical.

In [5], the authors had proven that a smart card based TMIS system may face a problem of password guessing attack which also make challenges of user anonymity. From their view, session key, user id and all other necessary key communicating parameters are one way hashed. But they are not emphasising on node add/remove services. They relied upon two-factor authentication scheme. Public keys are generated and protected by EC-DLP (Discrete Logarithmic Problem) mechanism.

In [6], the authors proposed a three-factor authentication scheme based on Chaotic Map for the public key cryptosystem. User's biometric information is used for authentication and provides anonymity for a user. As a proof of concept, they used BAN (Burrows–Abadi–Needham) logic.

In [7], Shuyun Shi, et.al. , described an authentication scheme for multi-server environment using block-chain technology. They relied on physical unclonable function (PUF) to share sensitive user information between any two servers. Their proposal is significant while we consider a multi server environment among several health care providers. In fact, PUF is a hardware based security module that create TRNs (True Natural Numbers) which is highly depended on a particular physical device.

Lijun Xiaoa, et.al. in [8] also preferred PUF as a session key generator in combination with ECC. Even though, PUF generates TRNs with hardware circuitry embedded with a device, unfortunately it suffers from instability. Hardware aging is another problem that limits the generating power of the PUF circuit. The remedy to this problem is to add a refresh circuitry inbuilt to this PUF.

The authors in [9] proposed the REAS-TMIS scheme based on authenticated encryption with associative data (AEAD), one way hash function and authenticated key exchange (AKE) for maintaining session key among communicating parties with repository server. They concentrated on session establishment prior to data transfer activities.

In [10], the authors were leaning towards three-factor authentication scheme which was based on ECC. They also relied on patients' fingerprint as biometric signature along with conventional authentication mechanisms. Abraham Isiaho, et.al. in [11], reviewed a large set of recent works and concluded that perfect forward secrecy is a major challenge in many algorithms. They also mentioned about lower order computational complexity is a major challenge to the IoT environment like TMIS.

Multi-server environment is a common platform where users' data are stored centrally from multiple TMIS operators. A user can make a switch over from one health service provider to another after comparing his conveyances. In such environment, privacy of a user and user's data protection, are very crucial and challenging. In [12], the authors relies on public key generation using ECELP and ECCDHP. But still they are depending on login ID and password as credentials to enter into the system for any user. But in todays' digital age, it is quite difficult to remember his credentials, especially during ailment and for the elderly people. In [13], the authors proposed two factor authentication scheme that relies on password and smart card. They proposed the access mechanisms for medical files that are stored and transmitted over internet like insecure public channel. Bilinear Deffie-Hellman (BDH) algorithm is used for public key generation between two communicating parties. We may review their proposal while we will create public keys for server(s) and users.

Password is used as a credential for any user in [14] in combination with biometrics. Sometimes passwords are used as dictionary words or type of phrases that are related to his surroundings. By knowing his personal details, an intruder may try to guess the password. But enabling biometric authentication which is supposed to be unique for every user, is a good choice. Authors proposed user registration phase where the stored biometric data directly be accessible if the smart card is stolen. From that, any insider of a TMIS environment can get biometric data and duplicate them for later use without the actual physical biometrics.

In [15], the authors prescribed an important concept of signcryption along with elliptic curve. Key generation and authentication process is very significant. They concentrated on smart card architectural development and inclusion of hardware security mechanisms into that. They proposed for a key of huge length which is subdivided into two parts and the first part is used for message encryption and remaining part is used for authentication. But for user registration, they proposed to use password as user credential which is vulnerable. P. Nayak, et.al. in [16], also proposed user authentication scheme based on smart card and password. But using a robust terminal that is used for card reader as well as alphanumeric character input is costly. They also relied on password which is difficult to manage as stated earlier. In [17], the authors proposed that user information will be transmitted in hashed form and from that message they will retrieve User ID. But, in generic sense hashing is an irreversible function. It is not possible to extract information from hashed data by XOR operation.

The authors in [18] reviewed on the architecture of TMIS layers and their probable components. Their comments on already existing algorithms are interesting. Especially, in multi-server environment which is a key feature of any Remote Healthcare System. In [19], [20], the authors also applied password as a user credential to protect user privacy and to maintain user anonymity. But still some practical issues related to password exits which are inconvenient to many users.

Therefore, our approach is to focus on removing password as user credential and in place of that finding a practical solution which is approximately unique to every human being, i.e., biometric data, e.g., thumb impression, iris scanning etc.

2.1 Abbreviation Used in the scheme:

Table 1. Abbreviations used

Notations	Definitions
IDi	Identity of user Ui
SIDj	Identity of server Sj
Ek(.), Dk(.)	A symmetric encryption/decryption algorithm with secret key k
hk(.)	Collision-resistance secure one-way keyed chaotic hash function
PWi	Password of user Ui
$\oplus$	Exclusive OR (XOR) operation
Bio_i	Biometric template of user Ui
H(.)	Collision-resistant one-way hash functions
H(.)	Collision-resistant one-way hash functions
MAC_A	Message authentication code algorithm of A
b_{ij}	Number of the authentication time
Bio_i	Biometric template of user U_i
Bio_i	Biometric template of user U_i
||	Concatenation operation

2.2. Technical Preliminaries:

A one-way hash function h : x→y is a function with the following properties:

- The function h takes messages of variable length as the input and converts them into an output of a fixed-length message digest.
- The function h, is an one-way function in the sense that, given x, it is trivial to compute h(x) = y. However, given y, it is difficult to compute $h^{-1}(y) = x$.

Cryptographic one-way hash function satisfies the following properties:

1. *Easiness:* Given $m \in X$, it can be easily compute y such that $y = h(m)$.
2. *Preimage Resistant:* It is hard to find m from given y, where $h(m) = y$.
3. *Second-Preimage Resistant:* It is hard to find input $m \in X$ such that $h(m) = h(m')$ for given input $m \in X$ and $m \neq m$.
4. *Collision Resistant:* It is hard to find a pair $(m,m') \in X \times X$ such that $h(m) = h(m')$, where $m \neq m'$
5. *Mixing-Transformation:* On any input $m \in X$, the hashed value $y = h(m)$ is computationally indistinguishable from a uniform binary string in the interval $\{0, 2n\}$, where n is the output length of hash $h(\cdot)$.

Elliptic curve cryptography (ECC):
ECC is a public key cryptography approach which is based on finite fields in Discrete Mathematics. An elliptic curve is a plane curve defined over a finite fields, but not real numbers, which consists of real points satisfying the following equation:

$$Y^2 = x^3 + ax + b.$$

The set of points chosen from a finite field, will form an Abelian group. ECC support smaller key size in comparison with other security protocols. For this reason, it becomes quite popular. For ECC, key length is varied from 160 bit to 521 bit whereas in RSA the key size ranges from 1024 to 15360 bit to achieve same level of security.

ECC has several variants in Discrete Logarithm Problem (DLP) to offer different security options, viz., EC Digital Signature Algorithm (ECDSA), EC Diffie-Hellman (ECDH), EC Integrated Encryption Scheme (ECIES) , EC Menezes–Qu–Vanstone (MQV), etc.

3. MODEL DESCRIPTION:

3.1 User Registration Phase:

This phase is the initial interaction between a user and the TMIS environment.

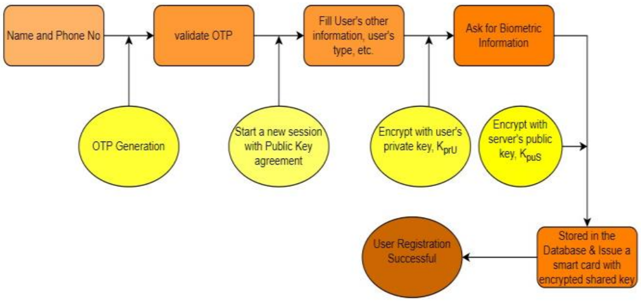

Name and Phone No
validate OTP
Fill User's other information, user's type, etc.
Ask for Biometric Information
OTP Generation
Start a new session with Public Key agreement
Encrypt with user's private key, K_{prU}
Encrypt with server's public key, K_{puS}
Stored in the Database & Issue a smart card with encrypted shared key
User Registration Successful

Fig 2. User registration process

As described the scheme in fig 2, the Registration Server (RS) of the TMIS environment generates a key pair (RSK_{Pr}, RSK_{Pu}) over a finite field in ECC. While transmitting Name, Phone No. and his Public key (U_{pubi}) over the Internet, a user

encrypts this using RSK_{Pu}. This encrypted massage is decrypted only by the RS using RSK_{Pr}. Thus identity and reliability of the server (SID_i) is authenticated.
i.e., The initial massage requesting for registration becomes

$$M= < Id_i \| \; TNo_i | \; |U_{pubi} >$$

Receiving this token, RS generates an OTP, typically an alphanumeric code of length 8-10 characters, with a session key, date-timestamp with a timer and Server ID. This complete massage is encrypted by user's public key (U_{pubi}). This massage is represented by

$$R= E(OTP \| SKU_i \| DateTimeStamp \| SID_i) \qquad (1)$$

This reply (R) has been hashed H(R) and that to be sent with R. From the massage R, user extracts all fields including SKU_i and OTP by XOR (⨁) logic. Validating the OTP, user information has been shared with the server. In this transaction, public key encryption is still to be used for maintaining secrecy. To maintain integrity, one way hash function H(.) will be used. While the biometric information is to be captured, converted and transmitted over the Internet, then special care be taken since for future login, it is very much sensitive. Biometric template of user U_i (Bio_i) is first hashed and then encrypted with PK of the Registration Server (RSK_{Pu}) to transmit to the server. This has been now stored in the RS database and a copy of the same will be stored in the Smart Card. To resist privileged insider attack and stolen verifier attack, hashed biometric information may be a choice. i.e. T= Ek(H(Bio_i).

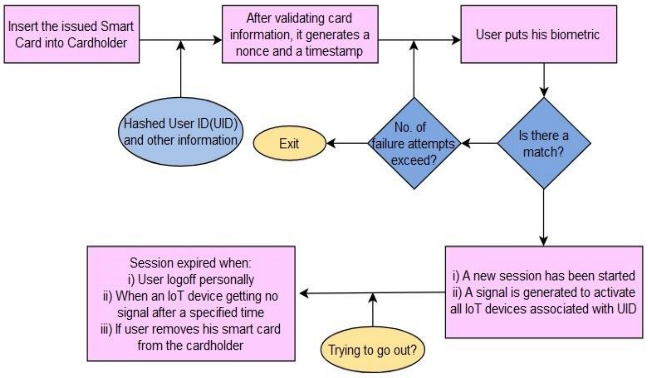
$$SCU_i = \; H(<H(Bio_i \;))| \; | \; ID_i >) \qquad (2)$$

While we are creating a User ID, User type shall be noted since they will capable of doing different operations in the system. We are proposing auto-generated or system generated ID for any kind of users to avoid UID clash. An ID may be generated with this logic for easy remembering:

$$ID_i = (FirstName \| DDMM(DOB) \| ServerSeqenceNo) \quad (3)$$

3.2 User Authentication and Login phase:

The following flowchart (fig. 3) depicts the process of user verification process.



Insert the issued Smart Card into Cardholder
After validating card information, it generates a nonce and a timestamp
User puts his biometric
Hashed User ID(UID) and other information
Exit
No. of failure attempts exceed?
Is there a match?
Session expired when:
i) User logoff personally
ii) When an IoT device getting no signal after a specified time
iii) If user removes his smart card from the cardholder
Trying to go out?
i) A new session has been started
ii) A signal is generated to activate all IoT devices associated with UID

Fig 3. User verification & authentication process

In this multifactor scheme, we propose for smart card, biometric data and OTP based authentication system. After successful registration, a user will try for login to the system. As a smart card holds user information in hashed form, after inserting it into the cardholder, that data along with a nonce will be transmitted over the Internet. This complete data will be hashed to avoid third party intrusion or man-in-the middle attack. This scheme also guarantees user anonymity. i.e.,

$$K = H(H(UID_i \| CardNo | DeviceID_i) \| RandomNonce) \qquad (4)$$

After satisfying on K, it will ask for biometric data for user authenticity. It can resist stolen smart card issue as well. As there is nothing to remember about the user accounts related information, elderly and ailing people can easily activate their accounts. Other users like doctors and hospital staffs may use other verification methods but choice is very limited compared to this scheme. Here, by limiting the no. of failure attempts and encrypting session information from the server side, privileged insider attack and session hijacking attack can be prevented. An active session can be created by the following procedure:

$$SKU_i = E_{PKUi}(K \| DateTimeStamp \| RandomNo) \qquad (5)$$

After getting the session key, user decrypt it using $PrKU_i$, i.e.,

$$Session \; Key(SKU_i \;) = D_{PrKUi} \; (SKU_i) \qquad (6)$$

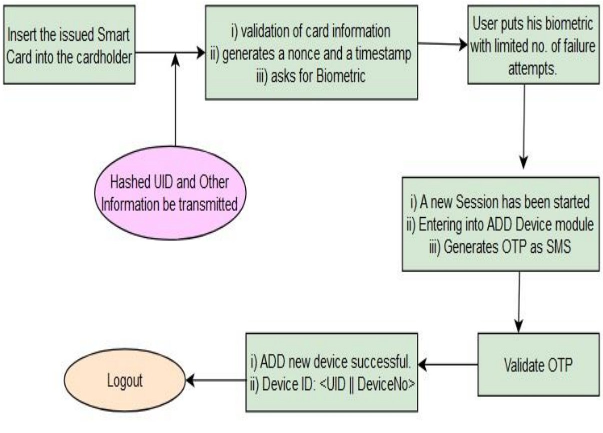
From this, user extracts the RandomNonce by

$$RandomNonce = SKU_i \oplus K \qquad (7)$$

Thus, user U_i will be verified and the registration-cum-authentication server also be authenticated. And hence, presence of man-in-the middle can be reduced.

3.3 New device to add to the Personal IoT Network:

Proposed scheme for adding new IoT device the network is shown in the figure 4 and modifying the personal IoT network is shown in figure 5. These schemes are very similar to login phase except that the verification of OTP.



Insert the issued Smart Card into the cardholder
i) validation of card information
ii) generates a nonce and a timestamp
iii) asks for Biometric
User puts his biometric with limited no. of failure attempts.
Hashed UID and Other Information be transmitted
i) A new Session has been started
ii) Entering into ADD Device module
iii) Generates OTP as SMS
Logout
i) ADD new device successful.
ii) Device ID: <UID || DeviceNo>
Validate OTP

Fig 4. New IoT sensor/ device registration process

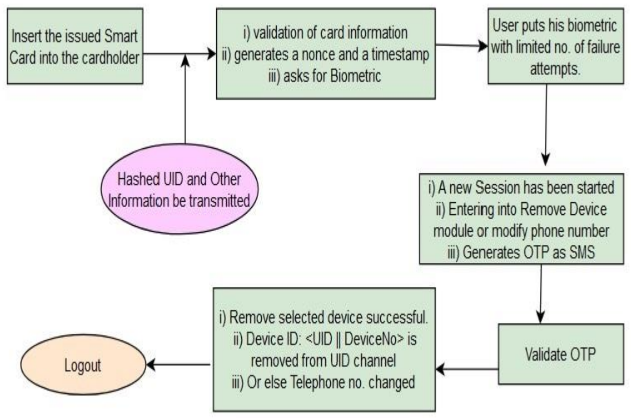

Insert the issued Smart Card into the cardholder
i) validation of card information
ii) generates a nonce and a timestamp
iii) asks for Biometric
User puts his biometric with limited no. of failure attempts.
Hashed UID and Other Information be transmitted
i) A new Session has been started
ii) Entering into Remove Device module or modify phone number
iii) Generates OTP as SMS
Validate OTP
i) Remove selected device successful.
ii) Device ID: <UID || DeviceNo> is removed from UID channel
iii) Or else Telephone no. changed
Logout

Fig 5. Modification of the network

Before addition of an IoT node, NodeID, NodeType, etc. will be verified. But until the OTP is verified, that device will not be incorporated into the network of user U$_i$. Similar actions also be performed when we will try to remove an IoT node. In both the cases, the user will get acknowledged about addition or removal of a node. Until the SIM card is cloned, this system will be secure against man-in-the-middle attack.

3.4 Logout Phase:

In this phase, all the random nos. will reset along with the system clock. Our proposal also include the expiry of inactive sessions to relinquish the load on data server. Also, in non-active sessions, intruders may start a parallel session in disguise of a legitimate user. So, inactive sessions must be turned down after expiry of limited amount of time. By limiting no. of active sessions, DDoS can be prevented.

4. PERFORMANCE ANALYSIS:

Table 2 shows the point of concern from where we may measure the performance of our scheme. Since the TMIS environment works in the public channel of the Internet, then all the schemes shall protect the resources of the entire environment.

Table 2. Evaluation criteria

Evaluation criteria
User anonymity and non-traceability
Stolen smart card attack
Offline password guessing attack
Insider attack
Replay attack
Impersonation attack
Multilevel authentication
Forward secrecy
Denial of service attack
Known session-specific temporary information attack
Server free password change

4.1 User anonymity and non-traceability:

The proposed system can protect user anonymity since every smart card will hold UID in hashed form such that by stealing the card, none can retrieve the information by reversing it. Every user ID is unique as the combination of name, date of birth and a server sequence no. is unique.

4.2 Stolen smart card attack:

As every session starts with a smart card verification followed by biometric verification of a user, by stealing a smart card or by guessing the UID only, a trespasser couldn't get entry to the system. Not only that by knowing only a UID, none will be able to add an unknown device to intrude into the system. This is because, an OTP verifier will acknowledge about the intrusion.

4.3 Offline password guessing attack:

As our system will not use any password directly, there is no chance of this event. If hospital personnel will accept a password as the login credential, then OTP verifier may be enabled for every login along with a random captcha. This random captcha can resist an automated program that will try for an intrusion.

4.4 Insider attack: User data is supposed to be stored in hashed form which is irreversible. Simple XOR operation could not produce the biometric template of a user (Bio$_i$) and hence it will be unknown to any internal person also. Thus insider attack can be prevented.

4.5 Replay attack: During login, session key(SKU$_i$) is generated by using a hash code of card information along with a nonce. Let an adversary *A* produces its own random nonce and replay to the user. Thus K' will be reproduced by *A* and will asks for biometric template of the user. While creating a session ID, we relied on public key cryptosystem. Using eq. (6), the authentication server (AS) is verified by the user and the random nonce which is created by the user in eq. (4) is verified. After satisfying on both the parameters mentioned in eq.(6) and eq.(7), the user starts transmitting data. Once rejected, *A* could not get any IoT data from the user.

4.6 Impersonation attack: As cardholder only be the account holder, he will be treated as a legitimate user. His credentials and biometric information is anonymous. Impersonation attack will not be possible in this proposed system.

4.7 Multilevel authentication: In our proposed system, there is a provision for multilevel authentication like biometric authentication and OTP verification.

4.8 Forward secrecy: According to eq. (5), every time a session is created in SKU$_i$, a time stamp and a random nonce is required which are unique always. Once a session is terminated, SKU$_i$ and its derived part Session ID, will be destroyed. This session would not be revived anymore and hence perfect forward secrecy will be maintained.

4.9 Denial of service attack: While logging into the authentication server, an adversary may masquerade as a legitimate user and may trigger an automated attack by knowing many UID. Such many login requests put the AS busy and DoS may be occurred. But here we are limiting no. of failure attempts to biometric authentication. If no. of attempts (b$_{ij}$) exceeds, then that UID will be blocked for half-an-hour or alike. Not only that, UIDs are stored in hashed form within smart cards, which are usually unknown to us, i.e., they are not public information. Hence DoS attack is less probable to the proposed system.

4.10 Server free password change: Server free password change or offline password guessing attack is not possible here. To change any password or to modify a User IoT network, OTP verification is imposed. So the offline password guessing or server free password change is not possible.

5. CONCLUSION AND FUTURE SCOPE:

In this paper we try to authenticate both the server end and the user end. TMIS environment consists of many data transactions and storage of sensed-data. To protect these storage structures, other mechanisms shall be devised. We may extend our study in the authentication process and controlled access mechanisms of user data in multi-server environment. A multi-server environment is a combination of systems where any user can migrate from one hospital-service provider to another without registering into another TMIS environment. This environment will demand for protection of user data. So the storage structure and file access mechanism must be enquired and deployed carefully. Our proposed mechanism requires additional hardware like smart card reader and finger print recognizer along with other IoT based health care devices. In our scheme, we proposed for addition of a new sensor node under a particular user. If we design such kind of structure in public domain as part of a smart city, then anonymous users can checkup their health status without creating any User ID and user identification will be done in different way. Not only that, any new device will be connected via legitimate users; otherwise any eavesdroppers can connect into the data server and may make a hazard.

Data Availability
None.

Conflict of Interest
This is to declare that there is no conflict of interest with other authors in relation to the discussed article.

Funding Source
None

Authors' Contributions
The first author was conceived the thing under discussion and made a proposal with the second author. Second author reviewed the literature and earmarked the research gaps. With the third author, first author conceptualize the article and the article was reviewed by all the authors. In fact, the topic under consideration was selected on sue-moto basis and security of the proposed system is supposed to be continued for transmitted data.

Acknowledgements
We are thankful to Prof. Debasish Giri, Associate Professor, Maulana Abul Kalam Azad University of Technology, Haringhata, Kolkata, West Bengal, Inida, for his valuable advice to start thinking in this matter.

References

[1] Poornima Naga, Preeti Chandrakarb, Karan Chandrakar,"An Improved Two-Factor Authentication Scheme for Healthcare System, International Conference on Machine Learning and Data Engineering", Procedia Computer Science, Elsevier, 1079–1090, 2023, DOI: 10.1016/j.procs.2023.01.087.

[2] Anjali Singh, Marimuthu Karuppiah , Rajendra Prasad Mahapatra, "Cryptanalysis on a secure three-factor user authentication and key agreement protocol for TMIS with user anonymity ", Cyber Security and Applications , Elsevier B.V., 2022, https://doi.org/10.1016/j.csa.2022.100008.

[3] R. Amin, G.P. Biswas, "A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity", J. Med. Syst., Springer, 39 (8), 1–19, 2015, DOI 10.1007/s10916-015-0258-7.

[4] C. Madan Kumar , Ruhul Amin, M. Brindha., "Cryptanalysis of Secure ECC-Based Three Factor Mutual Authentication Protocol for Telecare Medical Information System", Cyber Security and Applications, Elsevier B.V, 2023, https://doi.org/10.1016/j.csa.2023.100013.

[5] Niranchana Radhakrishnan and Amutha Prabakar Muniyandi, "Dependable and Provable Secure Two-Factor Mutual Authentication Scheme Using ECC for IoT-Based Telecare Medical Information System", Journal of Healthcare Engineering, Hindawi, 2022, https://doi.org/10.1155/2022/9273662.

[6] Tzu-Wei Lin1 and Chien-Lung Hsu, "Chaotic Maps-based Privacy-Preserved Three-Factor Authentication Scheme for Telemedicine Systems", International Journal of Network, Vol.25, No.2, PP.194-200, Mar. 2023, DOI: 10.6633/IJNS.202303 25(2).02).

[7] Shuyun Shi, Min Luo ,Yihong Wen, Lianhai Wang, and Debiao He , "A Blockchain-Based User Authentication Scheme with Access Control for Telehealth Systems", Security and Communication Networks, Volume, Hindawi, 2022, https://doi.org/10.1155/2022/6735003.

[8] Lijun Xiaoa, Songyou Xie, Dezhi Han, Wei Liang, Jun Guo & Wen-Kuang Choul., "A lightweight authentication scheme for telecare medical information system", Connection Science, Taylor & Francis, VOL.33,NO.3, pp. 769–785, 2021, DOI: 10.1080/09540091.2021.1889976.

[9] Muhammad Tanveer, Abd Ullah Khan, Ahmed Alkhayyat, Shehzad Ashraf Chaudhry, Yousaf Bin Zikria, Sung Won Kim, "REAS-TMIS: Resource-Efficient Authentication Scheme for Telecare Medical Information System", IEEE Access, February, 2022, DOI:10.1109/ACCESS.2022.3153069.

[10] Jongseok Ryu, Jihyeon Oh, Deokkyu Kwon, Seunghwan Son , Joonyoung Lee, Yohan Park, And Youngho Park.,"Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System", IEEE Access, Vol- 10, January, 2022, DOI: 10.1109/ACCESS.2022.3145959.

[11] Abraham Isiaho *, Kelvin Kabeti Omieno and Hillan Rono , "Tele-care medical information systems security techniques: A critical review of the state of the art techniques", WJAETS, 07(02), P240–P254.,December,2022, https://doi.org/10.30574/wjaets.2022.7.2.0136.

[12] Guosheng Xu, Shuming Qiu, Haseeb Ahmad, Guoai Xu, Yanhui Guo, Miao Zhang and Hong Xu, "A Multi-Server Two-Factor Authentication Scheme with Un-Traceability Using Elliptic Curve Cryptography", Sensors, MDPI, 18, 2394; doi:10.3390/s18072394.

[13] Fairouz Sherali, Sarhan Falah, "An Efficient Two Factor User Authentication and Key Exchange Protocol for Telecare Medical Information System", International Journal of Mathematics and Computer Science, 15(2020), no. 4, 1015–1027, 2020, ISSN 1814-0432.

[14] Yohan Park, "A Secure User Authentication Scheme with Biometrics for IoT Medical Environment", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 11,pp 607-615, 2018, .

[15] Anuj Kumar Singh , Arun Solanki , Anand Nayyar, and Basit Qureshi, "Elliptic Curve Signcryption-Based Mutual

Authentication Protocol for Smart Cards", Applied Science, MDPI, 10, 8291; doi:10.3390/app10228291

[16] Priyank Nayak, Ravi Singh Pippal, "A Robust Patient Authentication Scheme For Telecare Medicine Information Systems (Tmis) Against Smart Card Security Breach", VOL 7, ISSUE 19, ISSN- 2394-5125 ,2020.

[17] Mourade Azrour , Jamal Mabrouki , and Rajasekhar Chaganti, "New Efficient and Secured Authentication Protocol for Remote Healthcare Systems in Cloud-IoT", Security and Communication Networks, Hindwai, Volume 2021, Article ID 5546334, 12 pages ,2021, https://doi.org/10.1155/2021/5546334.

[18] Vani Rajasekar, Premalatha Jayapaul, Sathya Krishnamoorthi, Muzafer Saračević, "Secure Remote User Authentication Scheme on Health Care, IoT and Cloud Applications:A Multilayer Systematic Survey", Acta Polytechnica Hungarica, Vol. 18, No. 3,pp 97-106, 2021.

[19] Niranchana Radhakrishnan, Marimuthu Karuppiah, "An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems", Informatics in Medicine Unlocked, Elsevier B.V., https://doi.org/10.1016/j.imu.2018.02.003, 2018

[20] Arezou Ostad-Sharif1 & Dariush Abbasinezhad-Mood1 & Morteza Nikooghadam, "Journal of Medical Systems (2019) 43: 10 https://doi.org/10.1007/s10916-018-1120-5, 2019.

AUTHORS PROFILE

Mr. Asit Kumar Nayek received his M.Tech from Jadavpur University, Kolkata, India and pursuing his Ph.D. at Maharaja Sriram Chandra Bhanjadeo University (erstwhile North Odisha University), Baripada, India. Presently, he is working as Assistant Professor in the department of Computer Science & Engineering (AI&ML) at Haldia Institute of Technology, Haldia, India. He has more than 10 years of teaching experience and 4 years of administrative experiences at different organizations. His area of interests include computer hardware development, IoT design for different applications and Artificial Intelligence. He is a senior member of IEEE.

Radha Krishna Jana Earned B.E and M.Tech from Burdwan University and Jadavpur University and pursuing Ph.D in Computer Science and Engineering from JIS University.His research area includes Social Network Analysis, AI in Medicine & Healthcare, Big Data Analytics in Healthcare &Medicine. Mr. Jana has 19 years' rich experience in teaching, research and industry. He has authored more than 40 papers in the referred Journals and Conferences. He published one book also. He is a life member of Indian Society of Technical Education and Member of Institute of Engineers (India).

Mr. Arpan Adhikary received his MTech from Maulana Abul Kalam Azad University of Technology, West Bengal, India in 2022. Presently, he is working as Assistant Professor in the department of Computer Science and Engineering (AI&ML) at Haldia Institute of Technology, Haldia, India. He has nearly 1 year of teaching experience. His area of interests include Machine Learning, Deep Learning and IOT based smart Healthcare industries.