Enhanced Authentication Scheme for Mobility Model in Medical Wireless Sensor Networks

[1]B. Naresh Kumar, [2]Malladi srinivas

[1]Research scholar, Department of CSE, koneru lakshmaiah Educational Foundation, Vaddeswaram, AP,India.
[2]Professor, Department of CSE, koneru lakshmaiah Educational Foundation, Vaddeswaram, AP,India.
Mail Id: [1]bgvthm38@gmail.com, [2]srinu_cse@kluniversity.in

Abstract

The advent of wireless sensor networks has brought significant advancements in healthcare, enabling remote interactions between medical professionals and patients. However, ensuring the security of communication in Medical Wireless Sensor Networks (WSNs) poses different challenges. To address this, this paper introduces a novel authentication framework designed for doctors and patients. The proposed mechanism incorporates essential features such as mutual authentication, anonymity, and data integrity, safeguarding the Medical Wireless Sensor Networks (MWSN). Symmetric encryption techniques are employed to maintain the overall security of the system.

Keywords: Authentication, Data Security, Encryption, Medical Sensors, Communication.

1. Introduction

The rise of the medical-WSN has greatly impacted how patients and doctors communicate [1]. Due to the increasing number of countries that are adopting home-based treatment for their patients, there is a concern that the security and privacy of these individuals are being compromised.

The rapid emergence and evolution of the medical-WSN has highlighted the need for secure communication. There are various issues that need to be resolved in order to ensure that the data collected and used by the system is protected. Most of the research that has been conducted on the security of the medical-WSN has focused on the use of authentication principles and cryptographic mechanisms [2].

The authors in [3] presented a system that enables real-time monitoring of patients' heart rate and sends data to medical facilities. The researchers in [4] proposed a method that allows doctors to analyze a patient's condition remotely by monitoring their sleep. They were able to accomplish this through the use of the Internet of Things. The immense amount of data collected by sensor devices has created a huge amount of privacy concerns. This is why it is important that the security of the data is improved. Unfortunately, in the present era, it is still not easy to implement effective measures to protect the privacy of the users. The researchers in [5] looked into different technologies and presented methods for capturing and presenting data from the generation stage to the storage. They also studied how to secure the information in wireless networks.

Medical-WSN applications typically rely on the location of the patients and doctors to determine the appropriate service [6]. But, since the users are often mobile, there could be security issues if they change their locations. The main objective of this paper is to ensure that the authenticity and integrity of the users while they are in different locations. Section 2 explains about the related work regarding the authentication mechanism in wireless sensor networks. Section 3 explains about the user mobility enhanced authentication method for MWSN. Section 4 deals with the security analysis of the proposed method. Section 5 explains about the experimental analysis of the proposed and existing methods. Section 6 concludes the research work.

2. Literature Survey

Healthcare facilities rely on different equipment's to gather patient information and implementing a mutual authentication system in medical applications can help protect their networks against unauthorized access [7]. User authentication methods can be used to access data from remote locations. However, analyzing different security techniques reveals the need to implement multiple measures to protect the networks [8].

Several password-based authentication schemes have been introduced in [9-11]. However, these schemes are susceptible to various security threats and are not considered secure against attacks. In contrast, the author in [12] has proposed an innovative and effective user authentication scheme that has been demonstrated to withstand different attacks, including replay and man-in-the-middle attacks, ensuring enhanced security.

In their work, the authors put forth an E-SAP scheme for two-factor authentication, leveraging smart card identity [13]. They asserted that their scheme provides security against DoS attacks. To address the challenges of multi-factor authentication, they introduced a biometric feature and proposed a three-factor-based scheme for health-care IoT networks. Furthermore, the authors in [14] presented an enhanced version of the previous work [15]. They developed a client verification mechanism that incorporates biometrics within a sensor network, resulting in improved reliability and security compared to existing approaches.

For various authentication purposes, key exchange protocols have demonstrated to be more effective than current methods. The authors of this study [16] analyzed a particular scheme for smart devices and found that it provided insufficient protection. They then implemented an improved scheme for the cloud-connected Internet of Things network. The authors in [17] improved the security of a smart card-based authentication system. However, it was not suitable for use in medical IoT networks due to its lack of forward secrecy and password validity. The authors in [18] designed an improved authentication system that addresses these issues. They used an RFID-based scheme with a hash function that can effectively handle various attacks. Despite its improved design, the system still remains vulnerable to various attacks. These include denial of service, synchronization, and impersonation.

The authors in [19] introduced a method that enables secure communication by sharing secret keys. Unfortunately, this approach lacks the necessary authentication to protect the data. The authors in [20] talked about methods that can protect the privacy of medical IoT devices. By hashing the user's information and identity, this approach can help prevent unauthorized access. The authors in [21] paper also introduced a two-factor authentication method that can be used for medical IoT networks. This method addresses the security and privacy concerns of the devices. The authors of the paper also presented a framework that can be used to monitor the data collected by medical IoT devices. However, these frameworks are prone to man-in-the middle attacks. In particular, they are vulnerable to user impersonation and denial of service attacks. In order to address these issues, the authors of the paper suggested using a secure approach for ad hoc networks. However, this method is still prone to offline attacks and device theft due to its lack of identity tracking features.

3. Proposed Method

Nomenclature

Symbol	Description
Y	Local Server
Z	Remote Server
Tkn	Token
TKT	Ticket
A_H	Health care Authority
T_R	Routing table
S	Secret key
TS	Time stamp
$K_{i, ID.j}$	Users subliminal ID
K_i	It might be patient or doctor
N_K	Nonce generated by K
$[..]_s$	Symmetric key

	encryption
TM_{key}	Temporary key
PT	Patient
DT	Doctor

3.1 Network model

In the medical system, we typically have the healthcare authority, doctors, and patients. Within the Medical-WSN, there exists an authentication server managed by the healthcare authority, where users register their accounts. The primary aim of the proposed model is to ensure the mobility of users while also protecting their privacy and security. Figure 1 shows the network model, which consists of a remote and a local server that can provide services depending on the users' status.

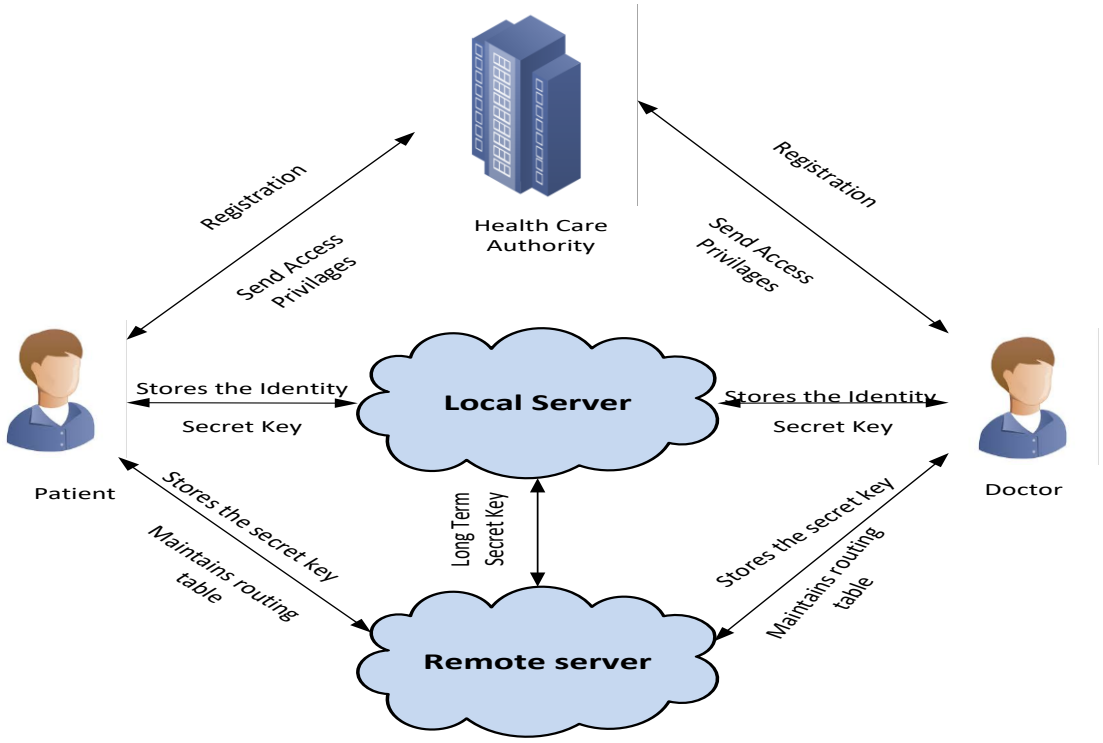

Fig.1. Proposed Network Model for Medical WSN

3.2 Preliminaries

The proposed model maintains three major servers. These are the Remote, User Registration, and Local servers. Each of these serves a specific function within the system.

Remote Server: A remote server is a global hub that operates from a central location. It enables data exchange and communication between various networks and locations. It ensures that users have easy access to the system regardless of their location.

Local Server: User requests and network services are handled by a local server, which is responsible for providing those services and interacting with users within a specific region or network. This server ensures efficient data management and communication within its chosen area.

Healthcare Authority Server: The healthcare authority's registration server handles the process for new users. It keeps track of the users' information, such as their authentication credentials and personal details. After they've registered, they can then access the system by establishing their identity.

The three servers collaborate to create a streamlined and proficient model for organizing user activities, data processing, and privileged access management.

3.3 Authentication Protocols for the Proposed System

The objective of this research study is to establish a secure communication channel between patients and doctors, regardless of whether they are in the same or different locations. The communication can be achieved using either wireless or wired methods, depending on the users' preferences and requirements. In this protocol, three distinct authentication conditions are thoroughly analyzed and examined, and they are outlined as follows:

i. PT-Y-DT condition
ii. PT-Z-Y-DT condition
iii. PT-Z-DT condition

3.3.1 PT-Y-DT condition

Algorithm 1 shows the procedure used to facilitate communication between a doctor DT and patient PT who are both in the same vicinity. This is accomplished through a local server that is managed by the A_H. The consultation phase and ticket generation are the two phases of this process.

Ticket Generation Phase: This module provides communication between users by requiring them to mutually authenticate using a local server Y. This type of communication is carried out through the participation of both the doctor DR and the patient PT. The procedure for the patient PT and the local server Y is outlined in the following steps. The patient will use a ticket, which is denoted by $TKT_{PT,\ DT}$ in order to communicate with the doctor.

$$TKT = [S_k, PT, PT_{i,ID.1}, DT, TS]_{S_{dt,Y}} \quad (1)$$

Consultation Phase: The patient (PT) initiates the connection by sending a ticket TKT to the doctor (DT). The doctor (DT) acknowledges the connection by responding to the patient (PT). The patient (PT) can then communicate with the doctor DT using the local server (Y). The data exchanged between the doctor DT and the patient PT are secured using an encrypted key (S_k). The proposed authentication method for patients in the PT-Y-DT scenario follows the Algorithm 1.

Algorithm 1: PT-Y-DT scenario

i. $PT \rightarrow Y : PT_{i,ID.1}, Y, DT, N_{PT}, VMAC_{S_{PT,Y}}(PT_{i,ID.1}, Y, DT, N_{PT})$

ii. $Y \rightarrow PT : PT_{i,ID.1}, Y, N_{PT}, [S_K, PT_{i,ID.2}]_{S_{PT,Y}}, TKT, VMAC_{S_{PT,Y}}(PT_{i,ID.1}, Y, S_k, N_{PT}, PT_{i,ID.2}, TKT)$

iii. $PT \rightarrow Y \rightarrow DT : PT_{i,ID.1}, DT, N_{PT}, TKT, VMAC_{S_{PT,Y}}(PT_{i,ID.1}, DT, N_{PT}, TKT)$

iv. $DT \rightarrow Y \rightarrow PT : PT_{i,ID.1}, DT, N_{PT}, Grant, VMAC_{S_{PT,Y}}(PT_{i,ID.1}, DT, N_{PT}, Grant)$

v. $PT \rightarrow Y \rightarrow DT : Medicare\,\mathrm{Re}\,quest$

vi. $DT \rightarrow Y \rightarrow PT : \mathrm{Re}\,ply$

3.3.2 PT-Z-Y-DT condition

Algorithm 2 shows that the patient PT and the doctor DT both in different locations. The doctor DT is at their home while the patient PT is at a remote location. The patient PT wants to consult the doctor DT. In this scenario, they must first communicate with local server Y to gain access to S. The patient PT and the doctor DT performs the authentication process using S which is shared between the Z and Y. The remote and local servers each have a long-term secret key. This means that the authentication process is carried out from Z to the Y and back to the doctor DT.

Ticket Generation Phase: The patient PT is situated in a distant location and needs to establish communication with the doctor DT through the remote server Z. In order to authenticate this interaction, both the remote Z and local Y servers are involved. The primary challenge in this scenario is how to verify the patient's identity without prior information. To address this, a secret key and encryption mechanism are employed to secure the patient's

data. The Y shares a temporary key TM_{key} with Z to facilitate identity verification.

Consultation Phase: In this phase, the patient PT initiates contact with the doctor DT using a ticket. The communication process between the patient PT and doctor DT is similar to that of the PT-Z-Y-DT condition, but with the involvement of the Z and Y servers.

Algorithm 2: PT-Z-Y-DT Scenario

i. $$PR \rightarrow Z : PR_{i,ID.1}, Z, DT, N_{PR}, Tkn, VMAC_{TKey}(PR_{i,ID.1}, Z, DT, N_{PR}, Tkn)$$
$$where\, Tkn = [PR_{i,ID.1}, Y, Z, N_{PR}]_{S_{PR,Y}}$$

ii. $$Z \rightarrow Y : Z, Y, PR_{i,ID.1}, DR, N_{PR}, Tkn, VMAC_{Tkey}(Z, Y, PR_{i,ID.1}, DR, N_{PR}, Tkn)$$

iii. $$Y \rightarrow Z : Y, Z, PR_{i,ID.1}, [PR_{i,ID.1}, T_{key}, N_{PR}]_{S_{Z,Y}}, VMAC_{Tkey}(Y, Z, PR_{i,ID.1}, T_{key} N_{PR}),$$
$$[PR_{i,ID.2}, DR, S_k, TKT]_{S_{PR,Y}} \quad where\ TKT = [PR, PR_{i,ID.1}, DR, S_k, TS]_{S_{dr,Y}}$$

iv. $$Z \rightarrow PR : Z, PR_{i,ID.1} N_{PR}, VMAC_{Tkey}(Z, PR_{i,ID.1}, N_{PR}), [PR_{i,ID.2}, DR, S_k, TKT]_{S_{PR,Y}}$$

v. $$PR \rightarrow Z \rightarrow Y \rightarrow DR : Medicare\,\mathrm{Re}\,quest$$

vi. $$DR \rightarrow Y \rightarrow Z \rightarrow PR : \mathrm{Re}\,ply$$

3.3.3 PT-Z-DT condition

Algorithm 3 explains that the doctor DR and patient PR are both in a different locations. In the ticket generation phase, the PR is similar to the one who had PR-Z-DR. The Y server, which is the local one, authenticates DR by sending request to Z. The patient PT and the doctor DT need to communicate with Y to ensure the secure communication. The authentication procedure for PT is common as second condition. In this case, Z will use the help of Y to verify DR identity. The procedure for consultation and authentication is explained below.

Authentication Phase: In the first stage, doctor DR connects with a remote server Z using a temporary key T_{key} and token *Tkn*, which is obtained from a local server Y. After connecting, the remote server Z sends the *Tkn* to the Y to confirm the details of DR. It then requests a temporary key T_{key} from the server. The local server Y then forwards the T_{key} to the remote server Z, which will then check the authenticity of the DR.

Algorithm 3: PT-Z-DT Scenario

i. $$DR \rightarrow Z : DR, Z, Y, N_{dr}, Tkn, VMAC_{T_{Key}}(DR, Z, Y, N_{PR}, Tkn)$$
$$where\, Tkn = [DR, Z, Y, N_{PR}]_{S_{dr,Y}} \quad and\ T_{key} = f(S_{dr,Y}, N_{dr}, DR)$$

ii. $$Z \rightarrow Y : Z, Y, DR, N_{dr}, Tkn, VMAC_{Tkey}(Z, Y, DR, N_{dr}, Tkn)$$

iii. $$Y \rightarrow Z : Y., Z, DR, [DR, T_{Key}, N_{dr}]_{S_{Y,Z}}, VMAC_{S_{Z,Y}}(Y, Z, DR, T_{key}, N_{dr})$$

iv. $$Z \rightarrow DR : DR, Z, N_{dr}, Decision, VMAC_{T_{Key}}(Z, DR, N_{dr}, Decision)$$

v. $$PR \rightarrow Z \rightarrow DR : PR_{i,ID.1}, DR, N_{pr}, TKT, VMAC_{T_{Key}}(PR_{i,ID.1}, DR, N_{pr}, TKT)$$

vi. $DR \rightarrow Z \rightarrow PR : DR, PR_{i,ID.1}, N_{pr}, Accept, VMAC_{K_s}(DR, PR_{i,ID.1}, N_{pr}, Accept)$

vii. $PR \rightarrow Z \rightarrow DR : Medicare\ \text{Re}quest$

viii. $DR \rightarrow Z \rightarrow PR : \text{Re}ply$

4. Security Analysis of the Proposed Method

4.1 Anonymity

The proposed model employs a user ID that is known as a subliminal ID. It is sent and received in intervals and can be decrypted only by the user. Even if an attacker possesses the user's key, they would be unable to find them. The subliminal ID of the users is encrypted with the help of Y. It can only be decrypted using the user's key. Exploits cannot find the user's key even if they possess it.

4.2 Replay Attacks

The proposed method for authentication utilizes nonces in communication. A new set of random numbers is generated every time the two parties communication. Since the nonce for each interaction is unique, the data from previous sessions is not utilized in the current session. This method ensures that the information is always fresh.

4.3 Data Confidentiality

The proposed model ensures the maintenance of data confidentiality by securely sharing the user's long-term secret key with the local server. This approach guarantees that sensitive information remains protected, as the key is securely transmitted and stored, preventing unauthorized access to the data. The user has to provide the local server with the key in order to access the data. This method ensures that the data's confidentiality is maintained.

4.4 Data Integrity

The proposed model can maintain its data integrity through the use of VMAC. This mechanism uses authentication procedure to secure the communication using hash function. The long-term secret key generated by the VMAC can be shared between the server and the user. The user can then use the VMAC key to establish communication between the server. This method ensures that the data is protected.

5. Performance Evaluation

Table 1 shows the performance evaluation of the proposed system. The proposed system is compared with the PAM[22], MAUT[23] and ICAS[24]. In the PAM [22], the authors didn't addressed the issue of mutual authentication in the medical cloud platform. In MAUT [23], the authors are not considered the data integrity, mutual authentication and user privacy. In ICAS[24], the authors are failed to address the issue of confidentiality, authentication, Data integrity and User privacy. The proposed method is executed using the AWS SDK i.e., BOTO3 which uses the python 3.3. The server which is selected for communication are AWS EC2 instances which is having the configuration of Xeon processor @ 3.3 GHz with 32GB RAM. The BOTO3 sample code is given below:

```
" for i in ec2.instances.all():
    if i.state['Name'] == 'stopped':
        i.start() "
```

Table 1: Security parameter for performance Evaluation

Parameters	PAM [19]	MAUT [20]	ICAS [21]	Proposed model
Mutual authentication	×	×	×	✓
User privacy	✓	×	×	✓
Data Integrity	✓	×	×	✓
Data confidentiality	✓	✓	×	✓
Replay attacks	✓	✓	✓	✓

The cost of running a server during the authentication process for doctors and patients is shown in Figure 2. The proposed method of authentication can be significantly lower than existing methods. The computation cost of the various phases of the authentication process is shown in Figure 3. The results of the study revealed that the proposed method of authentication can be used to facilitate mutual authentication in various conditions.

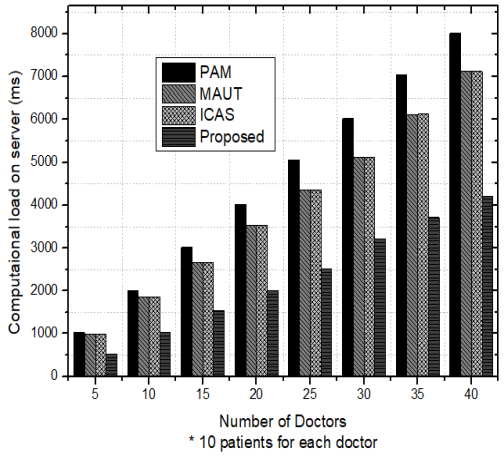

Figure 2: Computational load Vs Number of Doctors

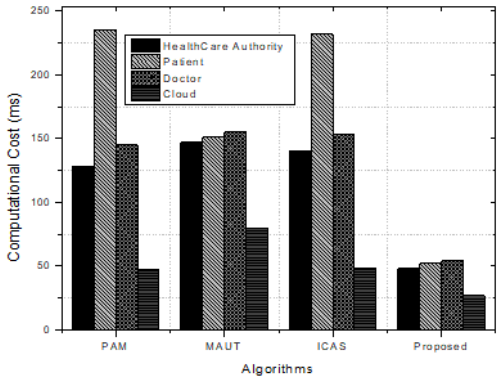

Figure 3 Computational Cost of the Proposed and Existing Algorithms

6. Conclusion

This research paper introduces an authentication mechanism specifically designed for the MWSN. It aims to establish a secure communication channel between doctors and patients, regardless of whether they are in the same or different locations. Both wired and wireless communication methods are supported in this mechanism. The proposed authentication mechanism offers several advantages, including anonymity, confidentiality, integrity, and mutual authentication. This solution addresses the issue of user mobility, as existing mechanisms are limited by their high cost and computation speed. It utilizes a symmetric key encryption algorithm for added security..

References

[1] Singh, Deepti, Bijendra Kumar, Samayveer Singh, and Satish Chand. "A secure IoT-based mutual authentication for healthcare applications in wireless sensor networks using ECC." *International Journal of Healthcare Information Systems and Informatics (IJHISI)* 16, no. 2 (2021): 21-48.

[2] Kwon, Deok Kyu, Sung Jin Yu, Joon Young Lee, Seung Hwan Son, and Young Ho Park. "WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks." *Sensors* 21, no. 3 (2021): 936.

[3] Hathaliya, Jigna J., Sudeep Tanwar, and Richard Evans. "Securing electronic healthcare records: A mobile-based biometric authentication approach." *Journal of Information Security and Applications* 53 (2020): 102528.

[4] Yang, Sheng-Kai, Ya-Ming Shiue, Zhi-Yuan Su, and Chuan-Gang Liu. "A novel authentication scheme against node captured attack in WSN for healthcare scene." In *2019 IEEE Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*, pp. 39-42. IEEE, 2019.

[5] M. A. Murillo-Escobar, L. Cardoza-Avendaño, R. M. López-Gutiérrez, "A double chaotic layer encryption algorithm for clinical signals in telemedicine", J. Med. Syst., vol. 41, pp. 1-17, 2017.

[6] D. Yin, W. Huanzhen, Z. Zixia, "Research on medical image encryption in telemedicine systems", Technol. Health Care, vol. 24, no. s2, pp. S435-S442, Jun. 2016.

[7] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, W. Lou, "Secure deduplication with efficient and reliable convergent key management", IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 6, pp. 1615-1625, Jun. 2014.

[8] Z.Y. Wu, Y. Lee, F. Lai, H. Lee, Y. Chung A secure authentication scheme for tele care medicine information systems J. Med. Syst., 36 (3) (2012), pp. 1529-1535.

[9] . W. John Bethencourt, Amit Sahai, Cp-abe library, Online at http://acsc.cs.utexas.edu/cpabe/.

[10] C.Medaglia and A. Serbanati, “An overviewof privacy and security issues in the internet of things,” in Proceedings of the 20th TyrrhenianWorkshop on Digital Communications, pp. 389–395, Sardinia, Italy, September 2009.

[11] A. Groce and J. Katz, “A new framework for efficient password based authenticated key exchange,” in Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS ’10), pp. 516–525, ACM, Chicago, Ill, USA, October 2010.

[12] . Chen, R. Liau, L. Chang Applications of multi-channel safety authentication protocols in wireless networks J. Med. Syst., 40 (1) (2016), pp. 26:1-26:15

[13] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, Y. Yang, A bilinear pairing based anonymous authentication scheme in wireless body area networks for mhealth. J. Med. Syst., 40 (11) (2016), pp. 231:1-231:10.

[14] D. Mishra, J. Srinivas, S. Mukhopadhyay. A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems. J. Med. Syst., 38 (10) (2014), p. 120

[15] H. Yang, H. Kim, K. Mtonga. An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system. Peer-to-Peer Network. Appl., 8 (6) (2015), pp. 1059-1069.

[16] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.

[17] Z. Ding, J. Li, and B. Feng, “Research on hash-based RFID security authentication protocol,” Computer Research and Development, vol. 46, no. 4, pp. 583–592, 2009.

[18] Z.-Q. Wu, Y.-W. Zhou, and J.-F. Ma, “A security transmission model for internet of things,” Chinese Journal of Computers, vol.34, no. 8, pp. 1351–1364, 2011.

[19] Sinha, Samman, Abhilasha Singh, Ritu Gupta, and Shreyya Singh. "Authentication and Tamper Detection in Tele-medicine using Zero Watermarking." Procedia computer science 132 (2018): 557-562.

[20] A. B. Reddy and R. Y. R. Kumar, "Performance and Security Analysis in Cloud Using Drops and T-Coloring Methods," *2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Mandya, India, 2022, pp. 1-7, doi: 10.1109/ICERECT56837.2022.10060014.

[21] R.Senthamil Selvan,Tumor Infiltration of Microrobot using Magnetic torque and AI Technique” by 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), ISSN:0018-9219,E-ISSN:1558-2256,26 June 2023.

[22] Bahache, Anwar Noureddine, Noureddine Chikouche, and Fares Mezrag. "Authentication schemes for healthcare applications using wireless medical sensor networks: A survey." *SN Computer Science* 3, no. 5 (2022): 382.

[23] S. Y. Chiou, Z. Ying, and J. Liu, “Improvement of a privacy authentication scheme based on cloud for medical environment,” Journal of Medical Systems, vol. 40, no. 4, pp. 1–15, 2016.

[24] C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, “A privacy authentication scheme based on cloud for medical environment,” Journal of Medical Systems, vol. 38, article 143, 2014.

[25] X. F. Cheng, X. L. Zhang, and J. F. Ma, “ICASME: an improved cloud-based authentication scheme for medical environment,” Journal of Medical Systems, vol. 41, no. 3, pp. 1–14, 2017.