International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

An Adaptive Authentication Schemes based on the user Mobility in Medical-IoT

P. Jyotheeswari, N. Jeyanthi

Abstract: ***The utilization of wireless communication in the medical The utilization of wireless communication in the medical filed led to the quality life of patients. The patients who are residing in the remote areas can consult and communicate with the doctors through the health care authority. However, providing the security at the time of communication is a difficult task in medical-IoT. The researchers developed many schemes for data authentication, but every scheme has their own drawback and they are majorly concentrated on the static communication. This paper developed the different authentication mechanisms between the patient and doctor who are available in different regions. The proposed mechanism provides the authentication, anonymity, data integrity and mutual authentication. It also uses the symmetric encryption techniques to preserve the security in Medical–IoT. The performance of the authentication mechanism is tested with real time environment. The results proved that the proposed algorithm is efficient in resisting the replay attacks and preserves the anonymity, data integrity and authentication.***

Keywords: Medical-IoT, Authentication, Integrity, Confidentiality, Encryption.

I.INTRODUCTION

From the past decade, the Internet of Things (IoT) has been evolved as the major technology in the networking industry. The IoT is defined as the network that connects the items like vehicles, users, home devices and many more through the sensors, tags and actuators. IoT enables the communication between the objects through the digital form. Scenarios like health care, home automation and vehicle systems are more effective with the support of Internet of Things [1]. Medical-IoT (M-IoT) has made an impact on communication among doctors and patients. Many nations are following the trend of home basedtreatment for patients and improving the quality of the patient's life, but along with this, there is a serious concern about the privacy and security of the patients which is disclosed by the health care professional's insecure network [2]. The involvement of wireless communication in health services are increased rapidly to promote the health care applications. There are different issues related to security need to be addressed in the M-IoT. In M-IoT applications, usually the doctors and patients are in fixed locations where the services can be offered, but sometimes they are in mobile. The security issues may arise when the users are changing their locations.

The major motivation behind this work is to provide the privacy and security to the doctors and patients while they are in mobility. The rest of the paper is organized as follows. Section 2 deals with the recent works related to the medical IoT. Section 3 explains about the proposed framework for authenticating the users in they are in the mobility. Section 4 explains about the security analysis in the proposed model. Section 5 deals with the experimental analysis of the authentication mechanisms. Section 6 concludes the research work.

II.RELAED WORK

In recent studies, the researchers proposed many security algorithms in telemedicine. These algorithms proposed authentication protocols to preserve the security in telemedicine. In [4], the authors developed the authentication mechanism for users based on the hashing function. This algorithm allows the authentication between the users, but this mechanism is not supported for distributed environments.In [5], the authors mentioned that the RFID tag carried by the clients is scanned by the RFID reader without their notice and it is simple to the intruders to gain access to the client's personal information. It is easy to the attackers to compromise the information at the time of data transmission from the local server to the remote server. In IoT, almost the communication network uses short number of sensors and also it uses light weight encryption algorithms to encrypt the data [6]. Groce et al. [7] proposed the security protocol that can be proved more secure in general model, but it is not suitable to deal with the medical-IoTapplications.In [8], the authors proposed the key evolution approach for preserving the privacy in telemedicine. The similar mechanism was later applied to the body area networks in M-IoT [9]. However, they are not discussed the mobility of the users in their proposed protocols.

With respect to the above discussion, some of the studies proposed the biometric authentication mechanism where the gateways are introduced to register the users which can identify and restrict the attacks [10]. Some authors considered the patient privacy as a major concern and proposed that attribute based encryption [11]. In [12], Lamport et al. proposed the hash function based authentication method for preserving the privacy. Later on, the authors in [13] proposed the hash based encryption for data protection. Wu et al. [14] proposed the lightweight cryptographic algorithm for data protection in IoT along with that they developed ONS query mechanism for search the data in the IoT applications. In [15], the authors presented the secure data transmission scheme for IoT. They used cooperative algorithm for successful data transmission.
In [16], a secure data transmission method was proposed for IoT.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

P. Jyotheeswari*, Research Scholar, SCOPE, Vellore Institute of Technology, Vellore, Tamilnadu, India,
N. Jeyanthi, Associate Professor, SITE, Vellore Institute of Technology, Vellore, Tamilnadu, India,

This method adopts the trusted third party and only two parties will be authenticated. So this method is not accepted in complex web applications. In [17-18], the researchers concentrated on using the mobile devices and sensor devices to monitor the health conditions of the patients, but they are not security issues related to the connectivity.

III. SECURITY REQUIREMENTS AND PROOSED FRAMEWORK

Nomenclature

Symbol	Description
L	Local Server
R	Remote Server
H_A	Health care Authority
P	Patient
D	Doctor
X_i	X might be the patient or doctor and i the user ID
$X_{i,\,ID.j}$	j denotes the subliminal ID of the user i
$K_{x,y}$	Secret key shared between x and y
Z_R	Denotes the routing table
$[..]_k$	Data encryption using the symmetric key encryption mechanism
N_X	Nonce generated by X
TS	Time stamp
T_{key}	Temporary key
TKT	Ticket
Tkn	Token

A. *Network Model*

In general, we consider the health care authority, doctors and patients in the medical system. The authentication server is maintained in the Medical-IoT, where the health care authority is presented. Users register under this authentication server. The proposed model serves the purpose of mobility of the users and preserves the security and privacy. Fig. 1 shows the proposed model where it contains the local server and remote server which provides the services to the users based on their status. In the proposed model, the users can move in any location and can communicate securely.

B. Preliminaries

The Local server.Remoteserver, User Registration through health care authority is the three major servers maintained in the proposed model. The detailed explanation about the three servers is given below.

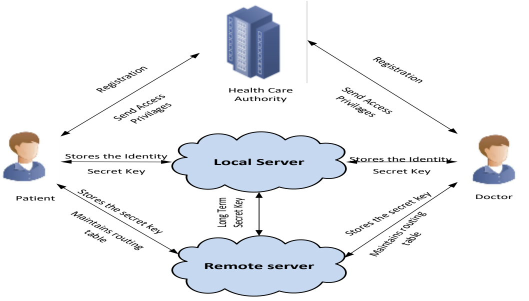

Fig.1. System model for Medical IoT [20]

Local server (L): L is located in the home area network which is responsible to store the doctors and patients IDs along with that its stores the symmetric secret key $K_{X,L}$ which is shared between the user X and local server L. It also maintains the routing table Z_L which stores the real IDs of the user along with the subliminal IDs which maps to them. The L also maintains the secret key $K_{L,R}$ between the local server L and remote server R.

Remote server (R) : R is located outside of the home area network and stores the secret key $K_{L,\ R}$ which is shared between the Local server L and Remote server R. It also stores the secret key $K_{RU,R}$which is shared between the remote user RU and remote server R. It also maintains the routing table Z_R.

Health Care Authority (H_A): H_A deals with the doctor registration and patient registration. The patient performs one time registration with L. The main reason behind the patient registration is to register the ID along with the setup of secret key $K_{P,L}$which is obtained by their own password. The patients ID is stored in to the table and mapped with the subliminal ID. The subliminal ID will be the phone number or IP address which is depends on the system type. The doctor registration is also same as the patents registration, but here were are not using the subliminal ID. The doctors ID is registered under the L and gets the secret key$K_{d,L}$.

C.Proposed authentication Protocols

In this research work, the secure communication channel is established between doctor and patient in different location or same location. The wired or wireless communication is encouraged between the users. The Three different conditions are analysed in the proposed authentication protocol, which is given as follows.

a. P-L-D Condition
b. P-R-L-D Condition
c. P-R-D Condition

A. P-L-D Condition

Figure 2 explains about the patient P and doctor Dcommunication which is resided under same location. i.e., local server L which is managed by the health care authority H_A.There are two phases in this condition, Ticket generation Phase and consultation phase.

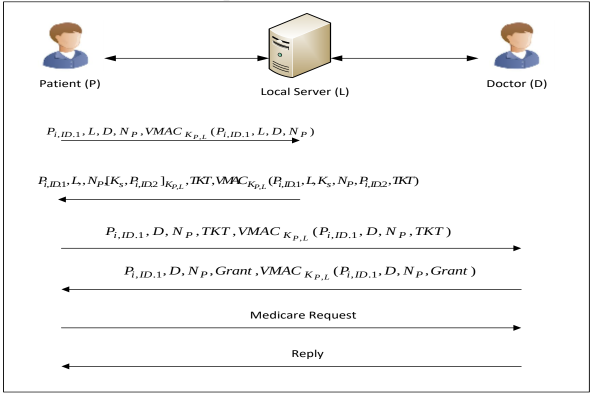
Patient (P)
Local Server (L)
Doctor (D)
$P_{i,ID.1}, L, D, N_P, VMAC_{K_{P,L}}(P_{i,ID.1}, L, D, N_P)$
$P_{i,ID.1}, L, , N_P, [K_S, P_{i,ID.2}]_{K_{P,L}}, TKT, VMAC_{K_{P,L}}(P_{i,ID.1}, L, K_S, N_P, P_{i,ID.2}, TKT)$
$P_{i,ID.1}, D, N_P, TKT, VMAC_{K_{P,L}}(P_{i,ID.1}, D, N_P, TKT)$
$P_{i,ID.1}, D, N_P, Grant, VMAC_{K_{P,L}}(P_{i,ID.1}, D, N_P, Grant)$
Medicare Request
Reply

Figure 2: Ticket generation and Consultation Phase in P-L-D condition

a. Ticket Generation Phase

The major objective of this module is to provide the secure communication by allowing mutual authentication between the users.

This secure communication is carried through the trusted local server Lby patient P and doctor D. The following steps are implemented by P and L to acquire consultation from the D. The P can communicate with the D using the ticket *TKT_{P,D}* which is given as

$$TKT = [K_S, P, P_{i,ID.1}, D, TS]_{K_{d,L}} \quad (1)$$

b. Consultation Phase

In this phase, patent P sends the *TKT* to the doctor D to establish the communication and doctor D confirms the communication establishment by sending the reply to the patient P. The communication between P and D is carried through the trusted server L. The messages transmitted between the patent P and doctor D is encrypted using the secret key K_s. The procedure for proposed authentication protocol in P-L-D condition is given as follows.

i. $P \rightarrow L : P_{i,ID.1}, L, D, N_P, VMAC_{K_{P,L}}(P_{i,ID.1}, L, D, N_P)$

ii. $L \rightarrow P : P_{i,ID.1}, L,, N_P, [K_S, P_{i,ID.2}]_{K_{P,L}}, TKT,$
$VMAC_{K_{P,L}}(P_{i,ID.1}, L, K_S, N_P, P_{i,ID.2}, TKT)$

iii. $P \rightarrow L \rightarrow D : P_{i,ID.1}, D, N_P, TKT,$
$VMAC_{K_{P,L}}(P_{i,ID.1}, D, N_P, TKT)$

iv. $D \rightarrow L \rightarrow P : P_{i,ID.1}, D, N_P, Grant,$
$VMAC_{K_{P,L}}(P_{i,ID.1}, D, N_P, Grant)$

v. $P \rightarrow L \rightarrow D : Medicare\,\mathrm{Re}\,quest$

vi. $D \rightarrow L \rightarrow P : \mathrm{Re}\,ply$

c. P-R-L-D Condition

Figure 3 shows that the patient P is located in remote location and doctor D is in the home location and the patient p is requesting for consultation of the doctor D. In this mechanism, the patient P needs to contact the local server L to get the secret key K, but is not possible without the help of remote server R. Therefore, the local server L and remote server R shares the long term secret key K and authentication is carried through remote server R to local server L and patient P to doctor D.

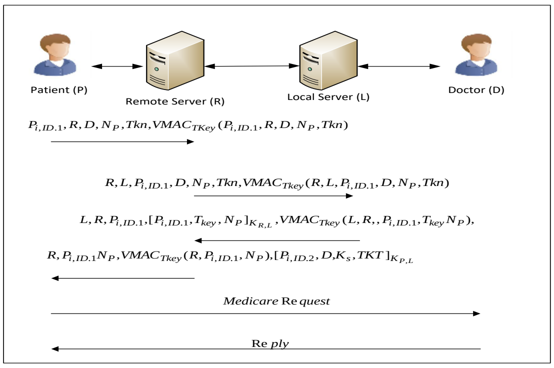
Patient (P)
Remote Server (R)
Local Server (L)
Doctor (D)
$P_{i,ID.1}, R, D, N_P, Tkn, VMAC_{TKey}(P_{i,ID.1}, R, D, N_P, Tkn)$
$R, L, P_{i,ID.1}, D, N_P, Tkn, VMAC_{Tkey}(R, L, P_{i,ID.1}, D, N_P, Tkn)$
$L, R, P_{i,ID.1}, [P_{i,ID.1}, T_{key}, N_P]_{K_{R,L}}, VMAC_{Tkey}(L, R,, P_{i,ID.1}, T_{key} N_P),$
$R, P_{i,ID.1} N_P, VMAC_{Tkey}(R, P_{i,ID.1}, N_P), [P_{i,ID.2}, D, K_S, TKT]_{K_{P,L}}$
$Medicare\,\mathrm{Re}\,quest$
$\mathrm{Re}\,ply$

Figure 3: Ticket generation and Consultation Phase in P-R-L-D condition

a. Ticket Generation Phase

In this module, the patient P is located in the remote location and needs to contact the remote server R to communicate with the doctor D. Therefore, authentication is carried in between the patient and doctor with the help of local server L and remote server R. The major issue faced in this condition is how the R validates the authenticity of the P. Since R doesn't have any information about the P. This issue can be solved by applying the encryption mechanism to the data sent by the P and the temporarysecret key. The local server L shares the temporary secret key with the remote server R to validate the authenticity of the patient P.

b. Consultation Phase

In this phase, the patient P contacts the doctor D with the obtained ticket, the communication between the P and S is same as P-L-D condition, but the difference is the R and L will be involved in this communication.

i. $P \rightarrow R : P_{i,ID.1}, R, D, N_P, Tkn,$
$VMAC_{TKey}(P_{i,ID.1}, R, D, N_P, Tkn)$
$where Tkn = [P_{i,ID.1}, L, R, N_P]_{K_{P,L}}$

ii. $R \rightarrow L : R, L, P_{i,ID.1}, D, N_P, Tkn,$
$VMAC_{Tkey}(R, L, P_{i,ID.1}, D, N_P, Tkn)$

iii. $L \rightarrow R : L, R, P_{i,ID.1}, [P_{i,ID.1}, T_{key}, N_P]_{K_{R,L}},$
$VMAC_{Tkey}(L, R,, P_{i,ID.1}, T_{key} N_P),$
$[P_{i,ID.2}, D, K_S, TKT]_{K_{P,L}}$
$where\ TKT = [P, P_{i,ID.1}, D, K_S, T]_{K_{d,L}}$

iv. $R \rightarrow P : R, P_{i,ID.1} N_P,$
$VMAC_{Tkey}(R, P_{i,ID.1}, N_P), [P_{i,ID.2}, D, K_S, TKT]_{K_{P,L}}$

v. $P \rightarrow R \rightarrow L \rightarrow D : Medicare\,\mathrm{Re}\,quest$

vi. $D \rightarrow L \rightarrow R \rightarrow P : \mathrm{Re}\,ply$

c. P-R-D Condition

Figure 4 shows that the patient P and doctor D are situated in the remote location. The ticket generation phase for patient P is same as that of P-R-L-D condition. The local server L authenticates the doctor D with the help of remote server R. The patient P and doctor D needs to contact the local server L for secure communication, because the remote server R doesn't have any storage to verify the credentials of P and D. The patient authentication is same as that of second condition. Accordingly, R authenticates D to establish the secure communication with P. Here R verifies D by taking the help of L. The procedure for authentication and consultation of D is given as follows.

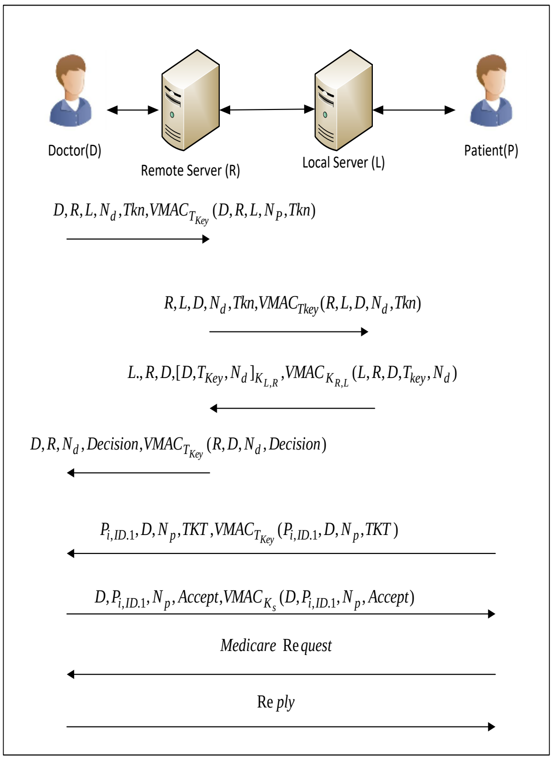
Doctor(D)
Remote Server (R)
Local Server (L)
Patient(P)
$D,R,L,N_d,Tkn,VMAC_{T_{Key}}(D,R,L,N_P,Tkn)$
$R,L,D,N_d,Tkn,VMAC_{Tkey}(R,L,D,N_d,Tkn)$
$L.,R,D,[D,T_{Key},N_d]_{K_{L,R}},VMAC_{K_{R,L}}(L,R,D,T_{key},N_d)$
$D,R,N_d,Decision,VMAC_{T_{Key}}(R,D,N_d,Decision)$
$P_{i,ID.1},D,N_p,TKT,VMAC_{T_{Key}}(P_{i,ID.1},D,N_p,TKT)$
$D,P_{i,ID.1},N_p,Accept,VMAC_{K_s}(D,P_{i,ID.1},N_p,Accept)$
Medicare Request
Reply

Figure 3: Authentication Phase and Consultation Phase in P-R-D condition

Authentication Phase: In the initial stage, doctor D contacts remote server R with token *Tkn* and temporary key T_{key}which is obtained from local server L. As a next step, remote server R forwards token *Tkn* to local server L to verify the information about doctor D and request temporary key T_{key}associated with doctor D. Then local server L forwards T_{key} to remote server R to validate the authenticity of doctor D by remote server R. As a final step, R will verify the authenticity of the doctor D.

i. $D \rightarrow R : D,R,L,N_d,Tkn, VMAC_{T_{Key}}(D,R,L,N_P,Tkn)$
$where Tkn = [D,R,L,N_P]_{K_{d,L}} \ and \ T_{key} = f(K_{d,L},N_d,D)$

ii. $R \rightarrow L : R,L,D,N_d,Tkn, VMAC_{Tkey}(R,L,D,N_d,Tkn)$

iii. $L \rightarrow R : L.,R,D,[D,T_{Key},N_d]_{K_{L,R}}, VMAC_{K_{R,L}}(L,R,D,T_{key},N_d)$

iv. $R \rightarrow D : D,R,N_d,Decision, VMAC_{T_{Key}}(R,D,N_d,Decision)$

v. $P \rightarrow R \rightarrow D : P_{i,ID.1},D,N_p,TKT, VMAC_{T_{Key}}(P_{i,ID.1},D,N_p,TKT)$

vi. $D \rightarrow R \rightarrow P : D,P_{i,ID.1},N_p, Accept,VMAC_{K_s}(D,P_{i,ID.1},N_p,Accept)$

vii. $P \rightarrow R \rightarrow D : Medicare \ Request$

viii. $D \rightarrow R \rightarrow P : Reply$

IV.SECURITY ANALYSIS

A. Replay attacks

The proposed authentication mechanism uses the nonce whenever the two parties are communicated. Every time the new random number is generated using the nonce and it ensures the freshnessof the data after completion of the session. The data from the previous session is not used in the current session, because the nonce of the previous session is different from the current session. It preserves the freshness of the data.

B. Anonymity

In the proposed model, the user subliminal ID is used for achieving the anonymity. In each round, a new subliminal ID is sent to the user and this subliminal ID is encrypted using the local server which will be decrypted only by the corresponding user. Even the attackers have the own key, they are not able to trace the subliminal ID of the User.

C. Data integrity

The data integrity is preserved in the proposed model by using the VMAC algorithm. VMAC is an authentication mechanism which uses the hash function to secure the communication. The VMAC generates the long term secret key which can be shared between the user and the local server. The users who having the key can calculates the VMAC value and establish the communication. This procedure preserves the data integrity in the proposed model.

D. Data confidentiality

The data confidentiality is preserved in the proposed model by sharing the long term secret key by the user to the local server. To retrieve the data, the user has to submit the key to the local server. It is not possible to decrypt the data without the key. Therefore, the data confidentiality is achieved in the proposed model.

V.PERFORMANCE ANALYSIS

The performance of the proposed authentication model is evaluated using the security features which are given in Table 1. The algorithms such as Chiou et al [19], Chen et al [20] and cheng et al [21] are used for performance comparison of the proposed model.

Table I: Comparison of security parameters

Security Parameter	Chiou et al [19]	Chen et al [20]	Cheng et al [21]	Proposed model
Restricting the replay attacks	✓	✓	✓	✓
Protecting the user privacy	✓	×	×	✓
Mutual authentication	×	×	×	✓
Data confidentiality	✓	✓	×	✓
Data Integrity	✓	×	×	✓

In Chiou et al [19], the authors failed to achieve the mutual authentication in the cloud telemedicine system, In Chen et al [20], the model failed to achieve the user privacy, mutual authentication and data integrity.

Furthermore, in cheng et al[21] are failed to satisfy the user privacy, authentication, confidentiality and integrity. The proposed model is implemented in Boto3 which is an AWS SDK used by python 3.3. The AWS EC2 instances use the Xeon CPU @ 3.3GHz with 16GB RAM and Linux 16.04 OS. The sample code to deploy the instances in Boto3 is given as follows:

```
“ for i in ec2.instances.all():

        ifi.state['Name'] == 'stopped':

        i.start() ”
```

Figure 4 shows the computation cost of the server incurred at time of performing authentication of patients and doctors simultaneously. It is observed that the time taken by the proposed method for authentication of users is less compared to the other existing mechanisms. Figure 5 shows the computation cost of complete one round procedure from patient authentication phase to doctor reply phase. It is proved that the proposed method is efficient for providing mutual authentication in three conditions.

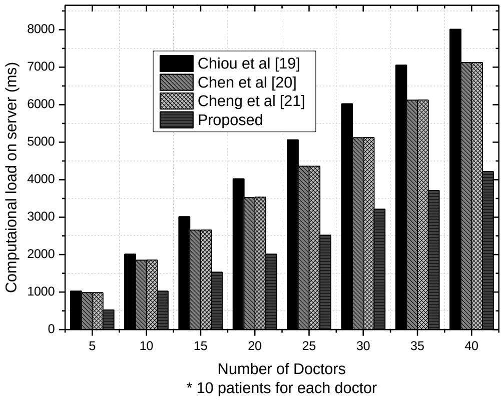

Figure 4: Comparison of Computational Cost in server

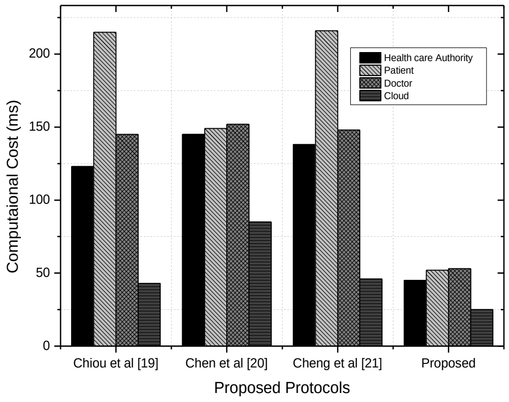

Figure 5: Computation Cost of Complete One Round Procedure

VI.CONCLUSION

This paper proposed authentication mechanism to the Medical-IoT. It Provides secure communication channel between doctor and patient in different location or same location. The wired or wireless communication is encouraged between the users. The proposed authentication mechanism achieved the anonymity, confidentiality, integrity and mutual authentication; along with that it has the ability to handle the user mobility which is not available in the existing mechanisms. The proposed mechanism has the lowest computation cost and high speed and uses the symmetric key encryption mechanism.

REFERENCES

1. 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.
2. 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.
3. 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.
4. Z.Y. Wu, Y. Lee, F. Lai, H. Lee, Y. ChungA secure authentication scheme for telecare medicine information systemsJ. Med. Syst., 36 (3) (2012), pp. 1529-1535.
5. . W. John Bethencourt, AmitSahai, Cp-abe library, Online at http://acsc.cs.utexas.edu/cpabe/.
6. 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.
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.
7. . Chen, R. Liau, L. ChangApplications of multi-channel safety authentication protocols in wireless networksJ. Med. Syst., 40 (1) (2016), pp. 26:1-26:15
8. 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.
9. 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
10. 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.
11. L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.
12. 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.
13. 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.
14. 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.
15. Shen, Jian, ZiyuanGui, SaiJi, Jun Shen, Haowen Tan, and Yi Tang. "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks." Journal of Network and Computer Applications 106 (2018): 117-123.
16. C.-L. Chen, T.-T. Yang, and T.-F. Shih, “A secure medical dataexchange protocol based on cloud environment,” Journal ofMedical Systems, vol. 38, no. 9, article 112, 2014.
17. P. Tudor, W. Martin, B. Natalia, P. Zeeshan, and B. Leon,“Ambient Health Monitoring: the smartphone as a body sensornetwork component,” Innovation in Medicine and HealthcareInmed, vol. 6, no. 1, pp. 62–65, 2013.

18. S. Y. Chiou, Z. Ying, and J. Liu, “Improvement of a privacyauthentication scheme based on cloud for medical environment,” Journal of Medical Systems, vol. 40, no. 4, pp. 1–15, 2016.
19. C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, “Aprivacy authentication scheme based on cloud for medicalenvironment,” Journal of Medical Systems, vol. 38, article 143,2014.
20. X. F. Cheng, X. L. Zhang, and J. F. Ma, “ICASME: an improvedcloud-based authentication scheme for medical environment,”Journal of Medical Systems, vol. 41, no. 3, pp. 1–14, 2017.

AUTHORS PROFILE

P. . Jyotheeswari, received her B.Tech from JNTU Anantapur in 2005 and M. Tech.degrees from MGR university in 2009.. Her interests include Comer networks,, Cyber Security, Data Mining,IoT.

Dr. N. Jeyanthi, is an academician for the past eighteen years at VIT University, Vellore, India. She holds B.E. (CSE), M.Tech. (IT - Networking) and Ph.D. She published around sixty international journal papers and conference papers in the field of Security. Her research work is funded by Department of Science and Technology, India. She is a life member of ISTE. She has been recognized as an active researcher by VIT University for four consecutive years. She also contributed to books and book chapters.She is in the editorial board of International Journals and chaired the sessions in many international conferences.She is a life member of Indian Society of Technical Education.