International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume ***14*** *Issue* ***02 Year 2022*** *Page* ***273:284***

Multifactor Authentication Key Management System based Security Model Using Effective Handover Tunnel with IPV6

[1]Dhoma Harshavardhan Reddy, [2]Dr.N Sirisha
[1]Trainee Security Analyst, JunoClinic, Davman Technology Services Private Limited
[1]dhreddy2001@gmail.com
[2]Professor - Department of Computer Science and Engineering, MLR Institute of Technology, Dundigal, Hyderabad, India
nallashirisha@mlrinstitutions.ac.in

Article History

Received: 24 March 2022
Revised: 28 July 2022
Accepted: 29 August 2022

Abstract

In the current modern world, the way of life style is being completely changed due to the emerging technologies which are reflected in treating the patients too. As there is a tremendous growth in population, the existing e-Healthcare methods are not efficient enough to deal with numerous medical data. There is a delay in caring of patient health as communication networks are poor in quality and moreover smart medical resources are lacking and hence severe causes are experienced in the health of patient. However, authentication is considered as a major challenge ensuring that the illegal participants are not permitted to access the medical data present in cloud. To provide security, the authentication factors required are smart card, password and biometrics. Several approaches based on these are authentication factors are presented for e-Health clouds so far. But mostly serious security defects are experienced with these protocols and even the computation and communication overheads are high. Thus, keeping in mind all these challenges, a novel Multifactor Key management-based authentication by Tunnel IPv6 (MKMA- TIPv6) protocol is introduced for e-Health cloud which prevents main attacks like user anonymity, guessing offline password, impersonation, and stealing smart cards. From the analysis, it is proved that this protocol is effective than the existing ones such as Pair Hand (PH), Linear Combination Authentication Protocol (LCAP), Robust Elliptic Curve Cryptography-based Three factor Authentication (RECCTA) in terms storage cost, Encryption time, Decryption time, computation cost, energy consumption and speed. Hence, the proposed MKMA- TIPv6 achieves 35bits of storage cost, 60sec of encryption time, 50sec decryption time, 45sec computational cost, 50% of energy consumption and 80% speed.

Keywords- Security, Authentication, Tunnelling, Healthcare 5.0, Key Management

1. Introduction

The use of modern advanced information technologies has grown progressively in storing and distributing enormous health data in order to minimize the computational cost and to provide more medical facilities [1]. Arrival of e-Health clouds provide easy and remote accessibility to health data. Moreover, several risk factors are also experienced due to this advancement which includes providing security, integrity, and maintaining confidentiality of medical data [2]. This situation is to be handled

smartly by determining more smart ways where existing healthcare approaches are integrated with smart medical devices and advanced technologies of communication like 5.0. To satisfy these necessities, WBANs architecture are presented in different ways [3]. In general, WBAN consists of personal controller (PC), healthcare center (HC), and several wireless medical sensors deployed in or out of the patient's body. More useful biomedical information is obtained with these sensors in different aspects [4]. Thus, physiological data of patients like temperature, heartbeat, blood pressure were effectively measured by the help of these sensors. Then, this information is processed in Health centers [5]. Thus, the record containing the status of user health is generated and maintained which helps in providing medical services to the patients on-time and simultaneously to many patients. It is noted that HC is a secured center for data and the role of valid entity is to distribute vital key information [6]. The confidential key for every sensor and PC is stored securely in HC. The PC is portable which aggregates sensor data of the individuals. Then, the sensitive biomedical information is transmitted through PC to the remote server [7]. Healthcare sensors, namely wearable and implantable sensors, are wireless low-power sensors which are restricted to storage, power, computation and communication [8]. In particular, implantable sensors are unfeasible as built-in battery is changed or recharged frequently. Moreover, as computation and transmission load are increased, sensors dissipate power into heat which generally harm organs of the body [9]. Consequently, WBAN sensors prefer slow-cost operations. Practically in WBANs, exchanging data between sensors and PC takes place in open wireless environment, where biometric data transmitted is subjected to several attacks towards security and privacy particularly in WBAN where more devices are involved [10]. Thus, more advanced security and privacy approaches are important for WBAN [11,12]. Efficient authentication methods for wireless environment are more important to protect the communication in WBAN [13]. Hence, uncharted and charted secure threats like impersonation, eavesdropping, and replaying can be prohibited. Thus, private biometric information was delivered securely. Transmission of messages between PC and every legitimate sensor was also secured [14].

Research contributions in this work are:

- The protocol coined in this paper provides improved security that is required for e-Healthcare environment. Further, this novel protocol is totally lightweight, thus feasible for e-Healthcare system.
- The user anonymity for every entity involved is achieved by authentication and preventing illegal access to sensors. The electrocardiogram signal obtained from ECG sensors and smart devices is analyzed and used as biometric data while authentication.

The rest of the paper is arranged as described: Section 2 presents a brief note on the works related to this research. Section 3 elaborates the designed system model and the proposed Multifactor Key management-based authentication by Tunnel IPv6 (MKMA- TIPv6) scheme. Then, section 4 illustrates the performance analysis and this work is concluded with future enhancements in section 5.

2. Related Works

Several research works were carried out on group key management related to wireless body networks and thus numerous approaches were developed. Traditional Public Key Cryptosystem (TPKC) was employed previously in healthcare applications. The principle of identity-based public key cryptography (ID-PKC) [15] was applied in many works, and was the first cryptography technique introduced in [16] which had the ability to handle certificate management issues of TPKC. Public key for the user was generated in ID-PK causing their known identity, whereas the secret key was created using a trusted key generation center (KGC). In [17], key management scheme based on ID-PKC was designed for mobile devices. In [18], demonstrated that their model was susceptible to impersonation attack. Moreover, key agreement protocols based on ID was coined. Two centralized protocols for group key management were framed on the basis of correlation analysis [19]. Here, transmission passes were reduced while distributing group key. In [20], group key distribution strategy based on key tree and CRT was introduced where root keys of the group member sub trees were used by key server and CRT was involved in the distribution of group key. In [21], centralized CRT-based group key management on was presented for secured multicast communication which reduced the computational complexity of key server. Introduced Pair Hand protocol, a handover authentication protocol, was developed based on the pairing-based cryptographic approach which improved communication ability and reduced the problems of AS. Pair Hand protocol required two handshakes between MN and AP for key

establishment and mutual authentication. An elliptic curve cryptography-based authentication scheme was developed based on three factors namely smart card, password, and biometrics. The flaws observed in the scheme of Fan and Lin namely(i) design flaws in privacy while using biometrics (ii) verification table was not maintained thus vulnerable to attacks like stolen-verifier, modification and insider attacks were focused. Linear Combination Authentication Protocol (LCAP) was constructed for minimizing the number of signatures acquired related to the identical pseudo-ID of key recovery attack. By linear iterative combination of arbitrarily captured two signatures related to the identical pseudo-ID, attacker estimated the private key of MN with higher probability.

3. Proposed Security Scheme in Healthcare

Improving the security and performance of the 5.0 core mobile virtual path network consists of three stages. In first stage is developing the security scheme for the network. The developed security model will be based on tunnel support for IPv6 and encryption scheme with increased key size. In second stage to improve performance of communication planned to utilize the multifactor authentication based on the secret key process. In final stage is to improve the system performance by using one-way hash as well as bio-hash functions.

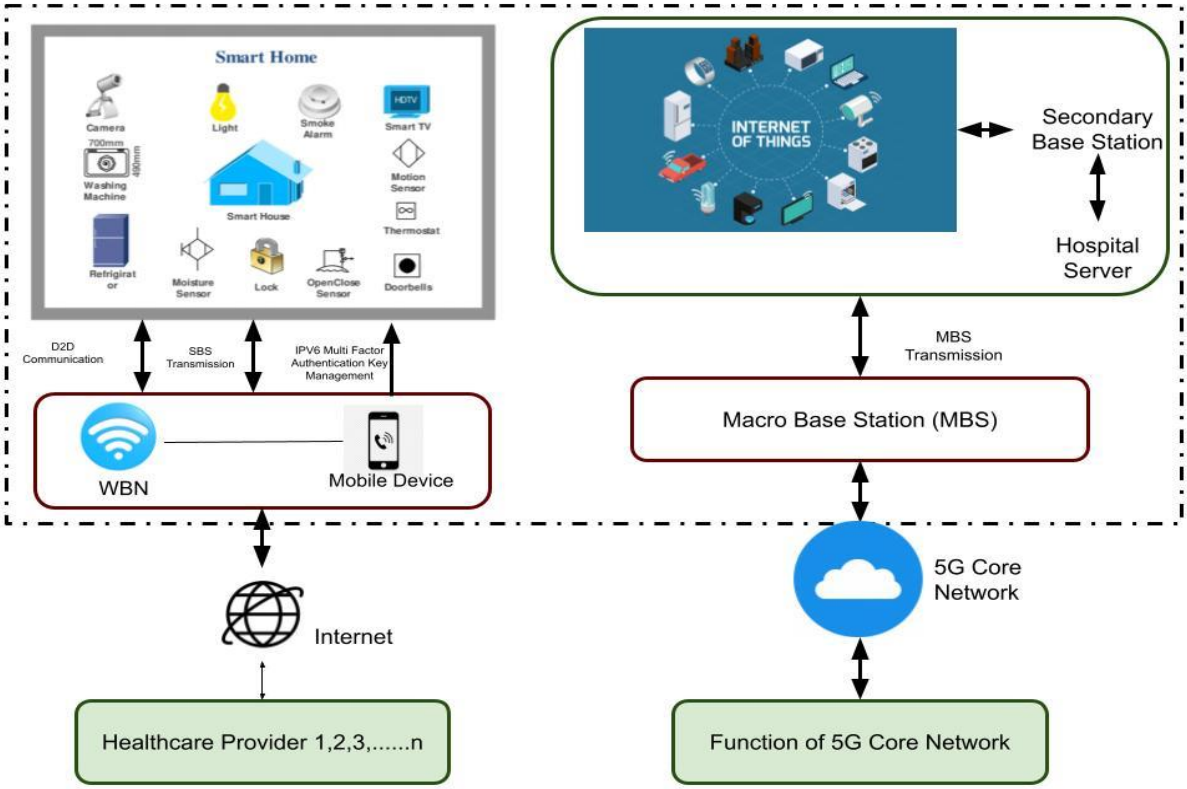

Figure 1. Proposed Architecture for Security In 5G Healthcare Networks

3.1 System model

While constructing the E-health service, two major roles considered are users *Ui* and servers *Sj* which are service providers. With only one login, several servers *Sj*s end services to *Ui.* A personal care domain contains different wearable sensors like electroencephalogram, sensors detecting respiratory rate, fall, and gait which are deployed in the user's body within a WBAN. These sensors gather health information of the user for monitoring their health continuously with no constraints on their day-to-day normal activities. Sensed data are then transmitted through wireless technologies like Bluetooth, to the mobile devices of *Ui* for further communications. A home care domain consists of *Ui's* who are

registered with *Sj* with the help of password, smartcard, and biometrics. After authenticating mutually, a secret group key is distributed by *Sj* to *Ui*. This key helps in encrypting the data sensed from personal care domain and uploaded securely to the systems for monitoring remotely. Here, when 5G networks are involved, the communication can be quick for real-time process. Here, *Sj* are family doctors or private medical experts. Moreover, this secret group key can be used by *Sj*to encrypt health related data which are the results of medical tests or treatment and then forwards these data to *Ui*.

3.2Developing Security scheme:

Tunneling support configuration of IPv6 connects LAN (Local Area Network) using native IPv4 gateway provided by ISP (Internet Service Provider). Tunneling, security approach, requires Private Key Generator (PKG) which is a trusted third party. PKG maintains the private keys of the correspondence node (CN) created for encryption. Additionally, it provides data confidentiality along with integrity, authorization, and non-repudiation. IPv6 tunnels are provided by tunnel brokers to the clients over intervening IPv4. Many tunnel brokers do not charge for promoting broadcasting and installing IPv6. Sign-up procedure in any form is required by most of the providers, particularly for prefixes of network with larger size. Transitional tunnels have to be terminated in order to support IPv6 either in the network security perimeter and firewalls or outside, and natively routed over the firewall where suitable rules are applied and tested. Moreover, attacks like false binding, man-in-the-middle, amplification and replay are prevented. Once the path probing is done for n times, the average time of the tunnel IPv6 path (z'n)is estimated by,

$$Z'_n = \beta \min(n) + (1-\beta) z'_{n-1} \qquad (1)$$

Figure 2. Protocol Stack of Ipv6 with Tunneling

The proposed model is based on some assumptions listed below:
Initially, Mobile Node (MN) registers with Corresponding Node (CN) to get the public key of CN. A secure IPSec tunnel exists between MN and Home Agent (HA). There exists a secure path between CN and Key Generation Center (KGC)as every client are authenticated by KGC. Encryption- A symmetric encryption scheme Encryption Key (EK). Here, all combinations of block ciphers and modes of operation recommended in this technical guideline are suitable. Message Authentication Code Key Management (MACKM). A key derivation function H can simply be a hash function if its output has at least the length of the total symmetric key material to be derived.

3.3 Key management

Once the tunnel base security architecture is constructed. The authorized users from the requisition phase generate a separate key. With the unique identity of the user, every attribute is traced. This identity and attributes of the user are hidden from users. No information about the matching or mismatching of attributes can be obtained using this from the cipher texts. These attributes are categorized as Hidden Normal attributes (HN) and Hidden Identity Attributes (HIA).
Generate cryptographically strong system parameters (p, a, b, P, q,i), Choose d randomly and uniformly distributed in $\{1, \ldots, q-1\}$. Set $G = d \cdot P$. Then, the encryption system parameters (p, a, b, P, q,i), together with G, form the public key and d the secret key. A Distributed Key Distribution Center (DKDC) is a group of n servers present in the network which combined performs the task of KDC. Here, users have secure point-to-point channels with every server. User transmits a key-request message to communicate securely with other users of their own. This model removes the focus on secret and slow down aspect present in the network with a single KDC. Secret keys are unknown by the server as they are shared among n servers. Further, every user, in parallel, transmits a key-request to several

servers. Hence, generating a key takes only less time, than the centralized set up. At last, users get the required keys even if few servers are not possibly connected to the user.

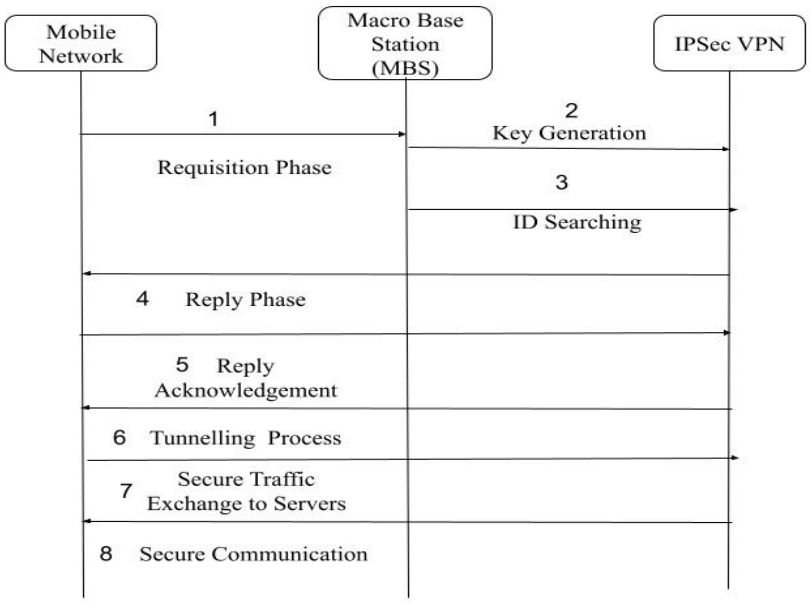

Figure 3 Key Management in Ipv6 VPN Network

4. Multifactor Key management-based authentication

On the service side, multi-factor authentication module receives the message from the first phase and obtain International Mobile Subscriber Identity (IMEI) and (International Mobile Station Equipment Identity (IMSI) information of the mobile. With this information, an authentication request is sent to management service process which in turn executes the instructions related to query the database and decides whether permission is to be given for the mobile device access, and returns to VPN gateway; If access is allowed, gateway either follows the consultations, or transmit an error message to the terminal. Multifactor authentication type chosen here is token-based security but a virtual device is a software application running on a mobile device which compete with a physical device. A six-digit numeric code is generated by the device depending on the time-synchronized one-time password principle. The valid code has to be entered by the user on a second webpage while logging in from the device. Every MFA device of the user has to be unique; and the user is not allowed to enter the code from any other device for authentication.

Figure 4 Registration Request Packet

4.1 Registration phase

- *Step R*1 V *Ui* gives his/her identity, password and biometrics represented as *IDi*, *PWi* and *Bi* respectively and then estimates *BW* D*H* (*PWi*, *HBio*(*Bi*)) and *P* D *H*(*H*(*PWi*)jj(*H*(*IDi_IDSj*). After then, *Ui* forwards (*IDi*; *B*; *P*) to *Sj*.
- *Step R*2 V When (*IDi*;*BW*; *P*) is received, *Sj* utilizes the key of encryption *sj* to calculates *Qj*D*SEsj*(*H*(*sj*)*IDSjIDi*, *BW*j*P*). Next, *Sj* forwards(*nj*;*Qj*) to *Ui*.
- *Step R*3 When (*nj*;*Qj*) message is received, *Ui* calculates *Qj*. At last, the credentials {*IDi*;*PWi*g}and server-related parameters (*j*; *IDSj*; *nj*}are stored by *Ui* in *Sci* and *MDi* accordingly.

5. Message Transfer Phase

The scheme involved in this research work has two messages as described below
*M*1:*Ui*→*Sj*V (*AEnj*(*IDSj, IDi, Qj, m,r*1,*ti*))
*M*2:*Sj*→*Ui*V (*SEki*(*r*2*tj*); [*x*1; *x*2;…..*xu*])
Step-1: These messages are given as idealized form below
*M*1:*Ui*→*Sj*V (h*IDSj*;*IDi*;*Qj*;*m*; *r*1; *tiin*)
*M*2:*Sj*→*Ui*V (h*r*2; *tjikij*; h*x*1; *x*2; ……*xu*i)
Step-2: Once the request message is received in the idealized form {Mi ,σi}, initially, MBS ensures the validity of timestamp ts. If not valid, request is just disallowed. Or else, MBS ensures whether e(σi , P) = e(H2(Mi)· H1(IDpidi), Ppub). When valid, MBS estimates the session key and authentication code which are K2−i = e(H1(pidi), sH1(IDAP2)) and Aut = H2(K2−i ||pidi ||IDAP2) respectively. Next, tuple {pidi , IDAP2, Aut} is forwarded to MNi.
Step-3: Once {pidi , IDAP2, Aut}message is received, MNi estimates the verification code Ver = H2(Ki−2||pidi ||IDAP2) which is compared with Aut. When equal, MNi authorizes that MBS and session key generated are valid. Or else, the connection is cancelled by MNi.
Since q is the system parameter generated at random, messages Mi and M0i are random as well as x1 and x2 are chosen randomly from Zp, q and β = (x1 ·H2(Mi)+x2 ·H2(M0 i))(modq) are roughly viewed as two random numbers which are independent. Therefore, the success probability, Psuccess, of attack for one time, equals the probability of β and q which are co-prime. This is given by

$$P(\text{success})= \prod_{i=1}^{k}(1-\frac{1}{pi})=\prod_{i=1}^{\infty}(1-\frac{1}{pi}2) \quad (2)$$

On these n signatures, the target MBS performs batch verification as:

$$E(\sum_{i=1}^{n}\beta i, p)=e(\sum_{i=1}^{n}(H2(m, ri).sH1(pid)+rip), p \quad (3)$$

6. Hash functions

Usually, the remote database maintains identity-password table for verification at server. The request message for login generally contains either an identity and password or hash values. Once the login message is received, server hunts the database for identity. Once the identity is determined, it is then compared with the respective password or hash value. But the structure of this table may suffer from attacks namely stolen verifier and insider. The request message for login may contain the biometric feature Bi of the user which is scanned on the remote terminal. Using an exclusive-or operation, Bi is integrated with ri, a number randomly generated from smart card. Another random number rj help in generating a dynamic string which locates the respective masked biometric template. Ti·algorithm f(n) is particularly a one-way and collision-free. Two masked strings in the database are then matched by the server. When the output exceeds the threshold, the server terminates the session. Or else, a new⊕ri and Ti⊕Bi rj ' a random number for next login is generated. Then f(rj') replaces f(rj) in the database. In the meantime, the random number rjin the smart card is updated by rj' ri in the request message of login and rj⊕n. Note that during transmission, Bi ' in the response message are not plaintext.
Sku=h(M'/r3/r4)=h(y⊕c1'/r3/c6⊕h(Bi⊕r1')=h(M⊕C1'/r3/r4⊕h(Bi⊕r1')⊕h(Bi⊕r1'))=h(M/r3,r4)=h(h(h_{bio}(C2/S)/C5⊕h_{bio}(C2)/r4=h(M'/r3/r4)=SK_s

7. Algorithm Design

The fixed secret s1 and the static secret seed are pre-shared between the corresponding node (CN) is S1 and mobile node (MN)is S2. The resistant token is given to the corresponding node. Once the tuple (aa, bb, cc) is retrieved, the secret s2 is calculated by invoking Algorithm hash generation.

*ni : Compute Kij = Pnj * Sni*
Compute H hash (Token ni || Kij || r)
Generate $Sign_{ni}$ Sign (H, S_{ni})
$n_i n_j$:AReq ({ Tokenni , Signni , r}) at time t.
n_j : if $Token_{ni}$ validity period is valid then
*{Compute Kji = Pni * Snj Compute H by using hash (Token ni || Kji || r)*
Flag Verify (Sign, H, Pni)
if flag = =accept then
{ nj authenticates ni
Compute H hash (Token nj || Kji || r+1)*
Generate $Sign_{nj}$ Sign (H ,Snj)*
njni : { $Token_{nj}$, $Sign_{nj}$ }
}
else authentication fails
end if
} else rejects
Authentication Request
end

8. Performance Analysis

The experiment is carried out and the parameters used for analysis are storage cost, Encryption time, Decryption time, computation cost, energy consumption and speed. The values obtained for these parameters are compared against three standard methods namely Pair Hand (PH), Linear Combination Authentication Protocol (LCAP), Robust Elliptic Curve Cryptography-based Three factor Authentication (RECCTA) with proposed Multifactor Key management-based authentication by Tunnel IPv6 (MKMA- TIPv6) method.

8.1 Storage cost

The shared session keys which are received from device-to-device communications are stored temporarily by the users. Thus, this temporary storage includes additional cost on the user side.

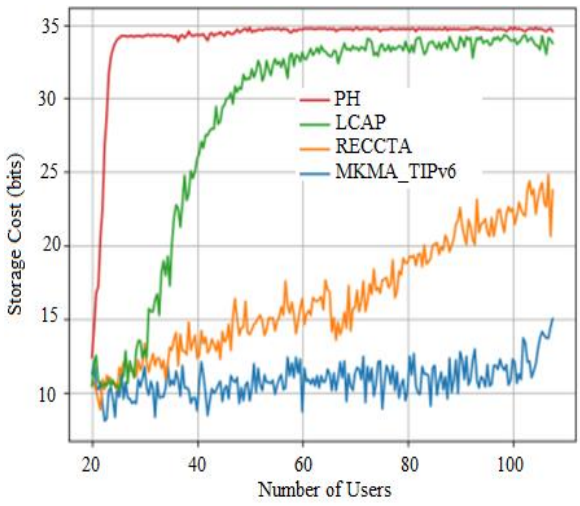

Figure 5. Analysis of Storage Cost

The above figure 5 shows the analysis of storage cost with number of users in x axis and storage cost in y axis. It is found that for the increased number of users the existing methods such as PH,LCAP and RECCTA achieves 39 bits, 38bits and 36 bits and hence the proposed method MKMA- TIPv6 achieves 35bits which is better than PH,LCAP and RECCTA as improved by 4 bits, 3 bits and 1 bit respectively.

8.2 Encryption time

This is the time consumed by the algorithm to generate the cipher text from the plaintext. This is involved in determining the throughput of the encryption method and encryption speed.

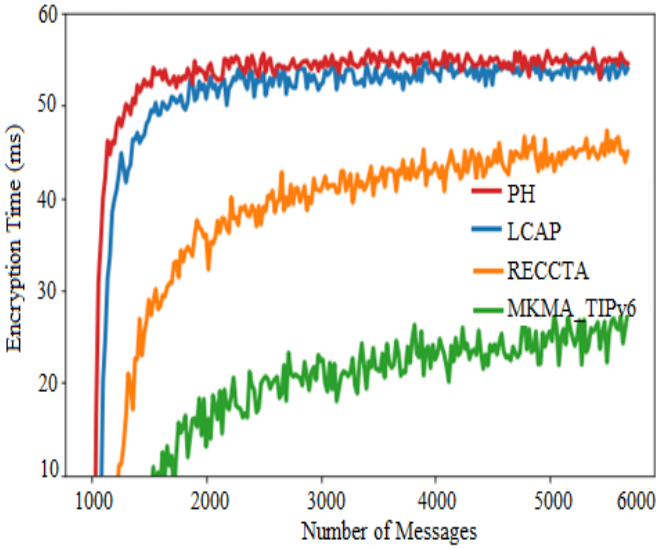

Figure 6. Analysis of Encryption Time

The above figure 6 shows the analysis of encryption time with number of messages in x axis and encryption time in y axis. It is found that for the increased number of messages the existing methods such as PH, LCAP and RECCTA achieves 65 sec, 65sec and 62sec and hence the proposed method MKMA- TIPv6 achieves 60sec which is better than PH, LCAP and RECCTA as improved by 5sec, 5sec and 2sec respectively.

9. Decryption Time

This is the time taken by the algorithm to generate the plaintext from the cipher text. It is involved in determining the throughput of the decryption method and decryption speed.
The figure 7 shows the analysis of decryption time with number of messages in x axis and decryption time in y axis. It is found that for the increased number of messages the existing methods such as PH, LCAP and RECCTA achieves 55 sec, 53sec and 51sec and hence the proposed method MKMA- TIPv6 achieves 50sec which better than PH, LCAP and RECCTA as improved by 5sec, 3sec and 1sec respectively.

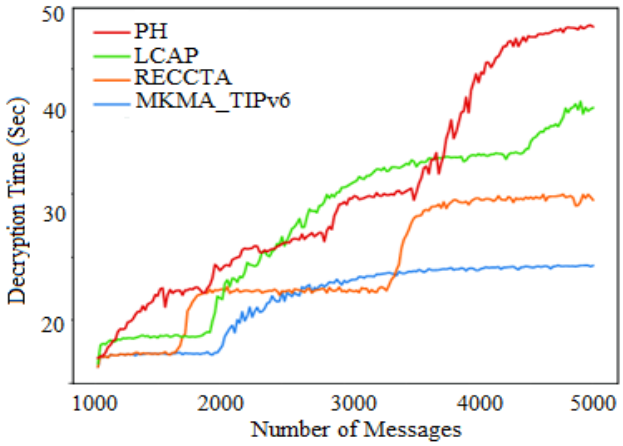

Figure 7. Analysis of Decryption Time

10. Computation Cost

Computational cost is the execution time per time step during simulation. This when represented as a series of rule applications, computational time is proportionate to the total rule applications.

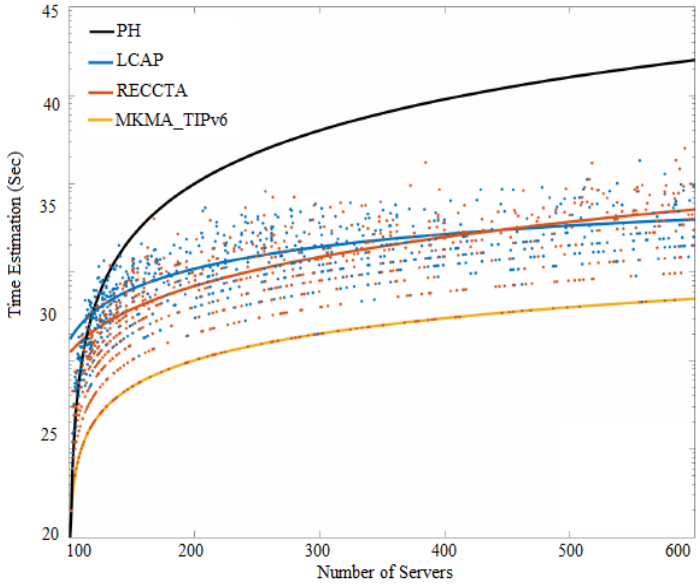

Figure 8. Analysis of Computational Cost

The above figure 8 shows the analysis of computational cost with number of servers in x axis and time estimation in y axis. It is found that for the increased number of messages the existing methods such as PH, LCAP and RECCTA achieves 50 sec, 49sec and 47sec and hence the proposed method MKMA-TIPv6 achieves 45sec which is better than PH, LCAP and RECCTA as improved by 5sec, 4sec and 2sec respectively.

The above figure 9 shows the analysis of energy consumption with number of users in x axis and energy consumption with percentage in y axis. It is found that for the increased number of users the existing methods such as PH, LCAP and RECCTA achieves 55%, 53% and 51% of energy consumption whereas the proposed method MKMA- TIPv6 achieves50% which is better than PH, LCAP and RECCTA as improved by 5%, 3% and 1% respectively.

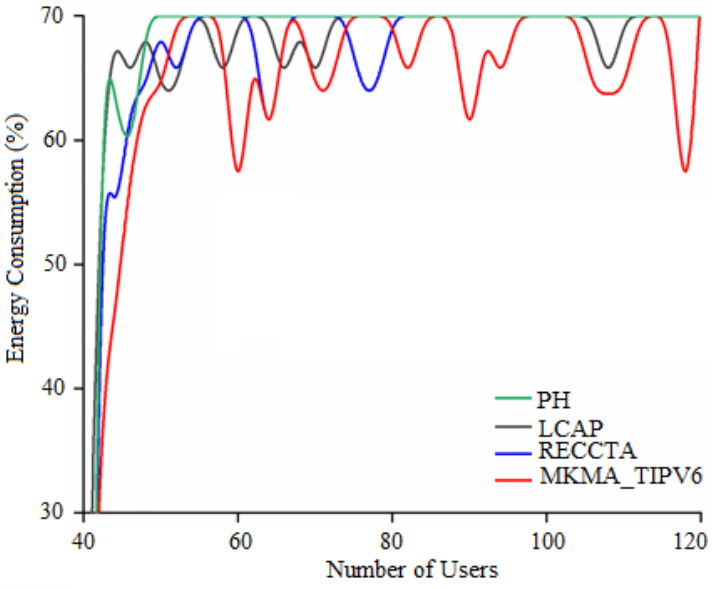

Figure 9. Analysis of Energy Consumption

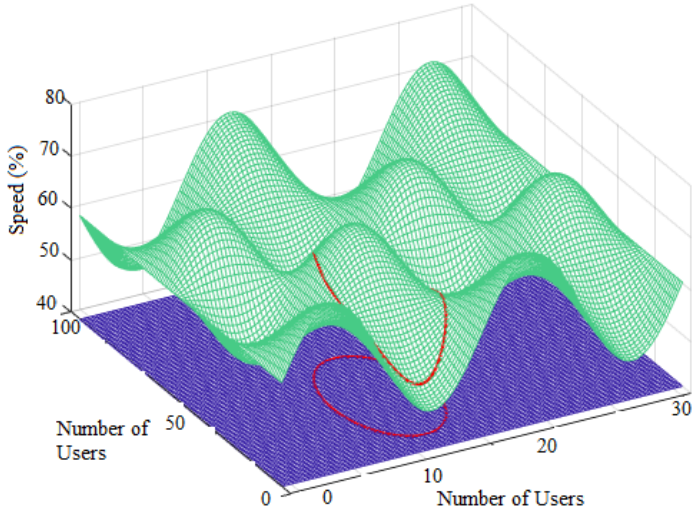

Figure 10. Analysis of Speed

The above figure 10 indicates the analysis of speed for the proposed MKMA- TIPv6 method, where the number of users is in two-dimensional x-axis and speed with percentage in y-axis. The proposed MKMA- TIPv6 achieves 80% speed which is 10% better than PH, 6% better than LCAP and 4% better than RECCTA.

Table 1 shows the overall comparison between proposed MKMA- TIPv6 and existing PH, LCAP and RECCTA method

Table 1. Comparison Between Existing and Proposed Method

Parameters	PH [22]	LCAP [24]	RECCTA [23]	MKMA- TIPv6 (proposed)
Storage cost (bits)	39	38	36	35
Encryption time (sec)	65	65	62	60
Decryption time (sec)	55	53	51	50
Computation cost (sec)	50	49	47	45
Energy consumption (%)	55	53	51	50
Speed (%)	70	74	76	80

11. Conclusion

This paper illustrates the practical challenges experienced with the existing key management protocol while preserving the confidentiality of the user. The limitations of the protocols used so far are concentrated while developing the novel protocol in this paper with enhanced security features. The protocol proposed in this work presents a cost-effective authentication in respect to computational as well as storage cost than recent e-Health cloud authenticating protocols. With informal security analyses, the proposed protocol is not that much able to deal with familiar security attacks. But the performance analyses along with formal security analyses proves that how that this protocol provides more additional security factors. As a result, this protocol is specified to be reliable, efficient and secure than the existing protocols such as Pair Hand (PH), Linear Combination Authentication Protocol (LCAP), Robust Elliptic Curve Cryptography-based Three factor Authentication (RECCTA) and hence

the proposed MKMA- TIPv6protocol achieves 35bits of storage cost, 60sec of encryption time, 50sec decryption time, 45sec computational cost, 50% of energy consumption and 80% speed. The future work is to concentrate on including machine learning based key management method for achieving better encryption and decryption time.

References

[1] P. Pawar, V. Jones, B.-J.F. Van Beijnum, H. Hermens, "A framework for the comparison of mobile patient monitoring systems", *J. Biomed. Inf., vol.*45, no.3, pp. 544-556, 2012.

[2] Z. Xia, X. Wang, X. Sun, Q. "Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data", *IEEE Trans. Parallel Distr. Syst.*, vol.27, no.2, pp.340-352, 2015.

[3] M. Wazid, A. K. Das and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks", J. Netw. Comput. Appl., vol. 123, pp. 112-126, 2018.

[4] W. Drira, É. Renault and D. Zeghlache, "A hybrid authentication and key establishment scheme for WBAN", *Proc. IEEE 11thInt. Conf. Trust Secur. Privacy Comput. Commun.*, pp.78-83, 2012.

[5] D. He, S. Zeadally, N. Kumar and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security", *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590-2601, 2017.

[6] H. Tan, D. Choi, P. Kim, S. Pan and I. Chung, "Comments on 'dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks", *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2149-2151, 2017.

[7] H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks", *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1442-1455, 2015

[8] Liu, Z. Zhang, X. Chen and K. S. Kwak, "Certificateless remote anonymous authentication schemes for WirelessBody area networks", *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, 2014.

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

[10] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks", *Comput. Methods Programs Biomed.*, vol. 135, pp.37-50, 2016.

[11] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He and N. Chilamkurti, "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks", *Int. J. Netw. Manage.*, vol. 27, no. 3, pp. e1937, 2017.

[12] Cao X., Zeng X., Kou W., Hu L. "Identity-Based Anonymous Remote Authentication for Value-Added Services in Mobile Networks", *IEEE Trans. Veh. Technol.vol.*58, pp.3508-3517, 2009.

[13] Shamir A, "Identity-Based Cryptosystems and Signature Schemes", *Proceedings of the Advances in Cryptology; Santa Barbara, CA, USA*, pp. 47–53, 1984.

[14] Yang J., Chang C," An ID-based Remote Mutual Authentication With Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem", *Comput. Secur.vol.*28, pp.138–143, 2009.

[15] Yoon E., Yoo K. "Robust ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC", *Proceedings of the 2009 International Conference on Computational Science and Engineering; Vancouver, BC, Canada*, pp.633-640, 2009.

[16] Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.

[17] Wang H,"Identity-Based Distributed Provable Data Possession in Multicloud Storage", *IEEE Trans. Serv. Comput, vol,*8, pp.328-340, 2015.

[18] Zheng X., Huang C., Matthews M,"Chinese Remainder Theorem Based Group Key Management", *Proceedings of the 45th Annual Southeast Regional Conference; Winston-Salem, NC, USA*, pp.266–271, 2007.

[19] Vijayakumar P., Bose S., Kannan A, "Chinese Remainder Theorem Based Centralized Group Key Management for Secure Multicast Communication", *IET Inf. Secur*. 2014; **8:179**–187. doi: 10.1049/iet-ifs.2012.0352.

[20] Allam, A. M. (2020). Cooperative key establishment protocol for full-duplex relay systems. International Journal of Communication Networks and Information Security, 12(2), 190-197.

[21] Chang, C.-C.; Lee, C.-Y.; Chiu, Y.-C," Enhanced authentication scheme with anonymity for roaming service in global mobility networks",*Comput. Commun.*vol.32, pp.611–618, 2009.

[22] H. L. Yeh, T. H. Chen, K. J. Hu, and W. K. Shih, "Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data", IET *Information Security*, vol.7, pp.247-252, 2013

[23] P. K. Barik, C. Singhal, and R. Datta, "An efficient data transmission scheme through 5G D2D-enabled relays in wireless sensor networks", *Comput. Commun.*, vol. 168, pp.102-113, 2021.