Computer Systems Science & Engineering
DOI:10.32604/csse.2022.021717
Article

Tech Science Press

Improved Key Agreement Based Kerberos Protocol for M-Health Security

P. Thirumoorthy[1,*], K. S. Bhuvaneshwari[2], C. Kamalanathan[3], P. Sunita[3], E. Prabhu[4] and S. Maheswaran[5]

[1]Department of Computer Science and Engineeirng, Nandha Engineering College, Erode, 638052, India
[2]Department of Computer Sceince and Engineering, Karpagam College of Engineering, Coimbatore, 641032, India
[3]Department of Electrical, Electronics and Communication Engineering, GITAM University, Bengaluru Campus, 561203, India
[4]Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, 641112, India
[5]Department of Electronics and Communication Engineering, Kongu Engineering College, Perundurai, 638060, India
*Corresponding Author: P. Thirumoorthy. Email: pthirumoorthyresearch1@gmail.com
Received: 12 July 2021; Accepted: 23 August 2021

Abstract: The development of wireless sensor network with Internet of Things (IoT) predicts various applications in the field of healthcare and cloud computing. This can give promising results on mobile health care (M-health) and Telecare medicine information systems. M-health system on cloud Internet of Things (IoT) through wireless sensor network (WSN) becomes the rising research for the need of modern society. Sensor devices attached to the patients' body which is connected to the mobile device can ease the medical services. Security is the key connect for optimal performance of the m-health system that share the data of patients in wireless networks in order to maintain the anonymity of the patients. This paper proposed a secure transmission of M-health data in wireless networks using proposed key agreement based Kerberos protocol. The patients processed data are stored in cloud server and accessed by doctors and caregivers. The data transfer between the patients, server and the doctors are accessed with proposed protocol in order to maintain the confidentiality and integrity of authentication. The efficiency of the proposed algorithm is compared with the existing protocols. For computing 100 devices it consumes only 91milllisecond for computation.

Keywords: Health monitoring; authentication; preparation protocol; kerberos; key agreement

1 Introduction

Today information technology and communication system highly involved in developing the IoT related applications, smart electronic health system, and smart mobile health system etc. In these applications sensors are bounded in patient's body to monitor the health condition via wireless body area network (WBAN). Huge storage demands are assisted by cloud servers through various medical service providers by improving the operational efficiency. Some Telecare based information system collects patient data from their sensor and transferred to their doctor for diagnosing. After diagnosis of final report, it is stored

in the cloud server with accessing permission to patients and secured users. Final health report is very sensitive and transmission happens in public distributed network. Most important function of M-Health system is to keep the sensitive information without any loss or data addition/modification due to unwanted interruption and attacks. Information from sensors is prone to life saving aspects. It must not be attacked or modified in good communication environment in IoT.

Big data analytics, IoT, mobile communications provides intelligent services for comfortable and Safety life for residents [1]. The urbanization is a composed of various sectors which helps to build smart city. These sectors provide sustainable information by observing the all activities in real time. Real time sensor information are analyzed contextually for providing great opportunities in mobile health care networks [2]. Traditional medical practices are extended to new ideology at patient door step using m-health provisions. Where ever patient stay, this m-health monitoring system helps physician to monitor their patient condition and provide treatment at earlier. Still date there is much innovation in wearable devices and body sensors. These devices serve smart city with m-health services by increasing the efficiency of social interactions [3]. These interactions help and assist patient in emergency situation. Traditional system of centralized hospital lacks in early stage emergency predicting and treating patients before losing their life [4]. The distributed nature of m-health system helps to diagnose the diseases in time and monitor their patients continuously. Sensors and wearable devices collects health data and transmit to doctors for further diagnosis process. It helps to see easy notes on patient's historical health details. Also sensor monitors the heath place to place, time to time where ever he moves [5]. Inspite of these advantages, major challenging in m-health social network is data authentication and security. Simple change in health data may cause serious injuries to patient by wrong diagnosis and treatment.

This article mainly focuses on security protocol for transferring health data in M-health environment. Security is ensured by following contributions:

- Key management is major problem for maintaining security and provided security protocol for distributing the key among two parties.
- This research article suggests new improved key agreement based Kerberos protocol with fingerprint biometric over the cloud centralized network on m health.
- Biometric with Kerberos protocol ensures the high security, integrity and authentication of users data in m-health environment.

Rest of the research section arranged as follows: Section 2 describes about related literature survey on security of m-health. Section 3 describes about proposed methodology and Section 4 evaluates the result and outcome. Finally Section 5 concludes the research work with future scope.

2 Related Work

A paper for publication Patients medical health information is considered as a Personal health records (PHRs) which patient feels more privacy and unwilling to share with anyone. Protecting the PHR from unknown access is main research concern over years [6]. Security for maintain PHR [7] is achieved using consent-based access control scheme. Here only authorized user can generate consent using PRE. Recently many research focus on using ABE for protecting the PHR records in cloud server. Data sharing in the network considers ABE as promising scheme using one-to-many flexible cryptographic method [8]. IBE was introduced by Sahai and Waters as new fuzzy based identity encryption [9]. The security of M-Health data [10] contains control policies for encryption. Based on policies cipher text and keys are ascribed. Security infrastructure based on attributes [11] for PHR patients file uses variant of broadcasting cipher text policy. In policy they execute ABE functionalities. The new novel ABE framework [12] suggests secured centric sharing of patient's information in the cloud computing network. Sharing of

cipher text between doctors [13] in cloud m-health platform is secured using CP-ABE, and it tends to deploy attribute based PRE (ABPRE) security techniques. Most defined problem in CP-ABE technique is high computational overhead results in complex computation. Some networks have only limited sensors, which will be affected worse by complex computational strategy.

Protocols always doest not consider the auxiliary authentication services in cloud environment. Cryptographic techniques of [14,15] proposes asymmetric and symmetric techniques. They develop the security system for m-health applications. This system processes by three steps as a) Initialize the service b) Registration of service and user c) Authentication during transfer. In these asymmetric techniques achieves all security concerns and objectives while symmetric techniques has problem of data stealing and confidentiality problems.

The m-health security in [16–18] considers only user communication channel and network for acquiring security. It also follow the asymmetric cryptographic techniques. Main problem is, it could not solve issues like integrity, authentication in network due to lagging of protocol. So if we study the protocol based security techniques which are initialized in IoT security, then IoT can be developed in secured environment. Most security objectives are achieved in these articles. But it has some security flaws when mobile device are stolen or lost. Finally it is concluded that can provide m-health security requirement by using our proposed improved key agreement based Kerberos protocol with fingerprint biometric. This proposed work acquires less time to process, consumes minimum energy and less cost than existing discussed in this section.

3 Proposed Improved Kerberos Methodology

While transmitting the data over the network in a secure way, symmetric key cryptography and their variations are used widely. With this, sharing the secret key between the sender and receiver in a secure way is the main challenge. Existing algorithm still lacks in terms of proving the security, reliability and confidentially in network. To overcome the problem of key management and the distribution of the key over the two parties, this paper proposed a new protocol called improved key agreement based Kerberos protocol with fingerprint biometric over the centralized network such as cloud on m health. From the main server, the data is transmitted over the link trough the trust node. The trust node is responsible for sharing the sender and receiver key in a secure way to access the transmitted data. The security of this trust node is managed using the proposed key agreement based Kerberos protocol. The architecture of the proposed work is shown in Fig. 1.

The proposed healthcare system consist of an wearable devices of the patients, local healthcare center (LHC) and the healthcare server which is connected to the LHC through cloud center which is a centralized database of all hospitals. The sensor nodes retrieve the health parameters of the patients and send to the LHC through wireless devices. The LHC is also a portable device like mobile or laptop which is responsible for the authentication process. In this proposed work, the Kerberos authentication with the removable fingerprint pattern to improve the authentication process more secure, since biometrics proven to be best secure and authentication mechanism in all application areas. There is a trust node between the LHC and healthcare server (HS). The request from the LHC is authenticated through the trust node.

The trust node is responsible for analyzing the request and authentication procedure and then forwards the request to the server for processing. If it is authenticated, the related confidential reply is sent to the healthcare server through the trust node to improve the security at LHC. The trust node of LHC in between the LHC and HS will have the combination of symmetric key with the fingerprint template. This removable fingerprint template of both sender and receiver is transmitted with public key cryptography and the fingerprint privacy is protected through the removable fingerprint template of both parties.

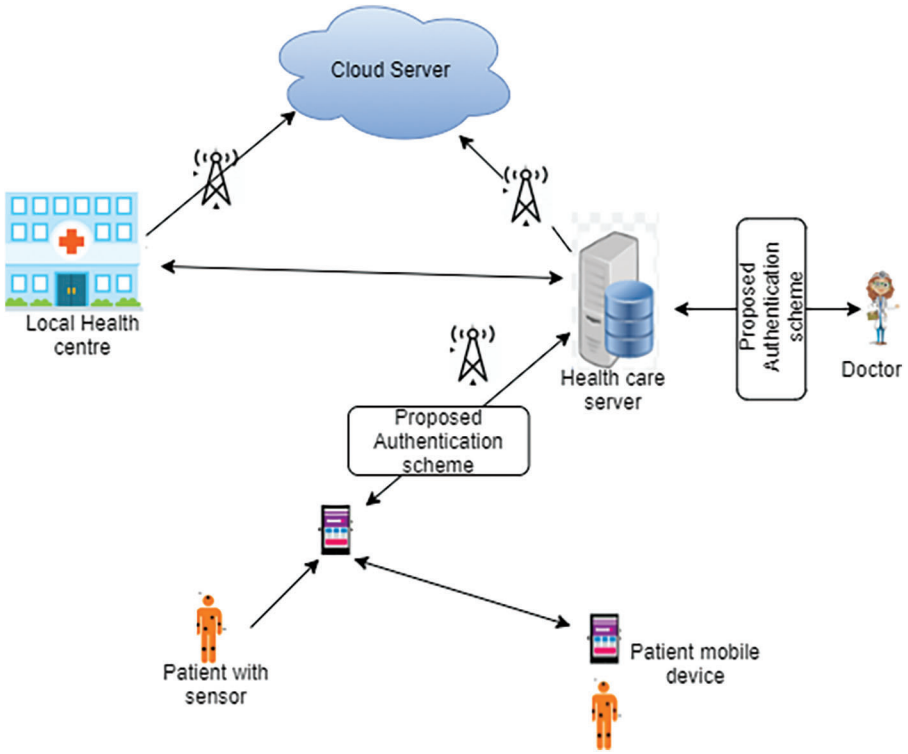

Figure 1: Proposed kerberos system model

3.1 Improved Key Agreement Based Kerberos Authentication Protocol

Each user of the LHC through the devices register with the authentication server and permitted with the identity and the key between the LHC and HS. The authentication server accesses the database from the central cloud.

The IKAP consist of LHC and trust nodes. The request from the LHC is processed by the trust node, which authenticates the LHC requests by applying the proposed algorithm. Once authenticated it examine the data from the server through cloud environment that is responsible to provide the access to the healthcare server. The request from the LHC is authenticated using the key agreement with removable fingerprint (FP) template to maintain the security. The fingerprint data of the patient is used here not for biometric authentication but for the process of increasing the randomness of the key generated by the protocol. Authentication is performed in two phases such as the LHC and the trust node at authentication server and trust node with the HS database. During the authentication, a random integer called r_i with ephemeral (temporary) key called K_a have been chosen with the interval of [1, n−1] where n is the number of request, the LHC request process is declared as,

$$P_a = r_i \times L \tag{1}$$

$$Q_a = -K_a \times L \tag{2}$$

where Q_a is defined as the request on LHC. This request is sent to the authentication server trust node and processed with the random number r_j and key K_b with the interval [1, n−1]which is defined as,

$$P_b = r_j \times L \tag{3}$$

$$Q_b = -K_b \times L \tag{4}$$

The encryption by the trust node is declared as,

$$ET_b = h(X_{P_b},\ X_{Q_b},\ X_{Q_a},\ ID_a,\ ID_b) \tag{5}$$

where,

X_{P_b}- X coordinate of P_b, X_{Q_b}- X coordinate of Q_b, X_{Q_a}- X coordinate of Q_a, ID_a- combined identity of the LHC, ID_b – Identity of the HS. Then the decryption process is declared as follows

$$DT_b = r_j + e_b.K_b + e_b.s_b \tag{6}$$

where, e_b, s_b and Q_b are the secret information sent by trust node to the LHC. While the LHC receives response from the trust node then the request from the trust node is declared as,

$$U_b = DT_b.L + e_b.Q_b + e_b.Y_b \tag{7}$$

Then the verification is declared as,

$$e_b + h(X_{U_b},\ X_{Q_b},\ X_{Q_a,}\ ID_a,\ ID_b) \tag{8}$$

If the LHC failed in the verification process then it's terminated. Or else, the client process the request as,

$$K_a = -K_a \times Q_b \tag{9}$$

The secret key is K=K_a=K_b ensures the authentication process. The algorithm for the key agreement based Improved Kerberos authentication protocol is declared as,

Algorithm: 1

Initialize trust node, random number r_i , and ephemeral key K_a and request L

Step 1: LHC send request to the trust node which is in between of the HS server and LHC.

Step 2: key is generated from both LHC and HS using the proposed algorithm as,

For i= 1 to n

Choose random number r_j and ephemeral key K_b for the request L

Trust node process the request using Eqs. (5) and (6)

Generate the secret information e_b, s_b and Q_b

Key generation using (9) and sent to trust node

Combine the key with the removable template using algorithm 2

Authenticate and verification using (7) and (8)

Share the key

End

Step 3: LHC send the key with the template to the server through trust node.

Step 4: HS received the request and authenticated with the key from the trust node and decrypt the message using the secret key with removable template.

Step 5: HS also generates fingerprint template using algorithm 2.

(Continued)

Algorithm: 1 (Continued)

Step 6: LHC decrypts the information using the secret key after the verification by trust node. Both LHC and HS have removable biometric template of both.

Step 7: Both LHC and HS combined their biometric template with the secret key by using the XOR operation and generated the combined template key. Now both LHC and HS have combined template and the key provided by the central server.

Step 8: LHC and HS can generate their final key using step 2. As both LHC and HS generate the same secret key through the trust node then it is no longer need to share the key through in secure nodes. The workflow sequence diagram of proposed work is shown initially, the LHC sent request to the trust node for accessing the HS through cloud.

The request from the client is declared as,

$$LHC_{req}: \{ts\},\ .K_c,\ tags\{T_{c.tag}\}\},\ V,\ time_{exp},\ n \tag{10}$$

where, K_c, *tags*- LHC key and related tag information such as id, template. V- verifier (trust node), $time_{exp}$- request time interval. While trust node received the request, the process of key agreement based kerboros is authentication is performed and response to LHC is granted to access the information of the HS. This response from trust node to LHC is declared as,

$$TN_{res}: \{K_c,\ V,\ time_{exp},\ n \ldots\} K_c,\ tags,\ \{T_{c.v}\},\ K_v \tag{11}$$

where, $K_{c,v}$ key of the HS to access the information with the time interval $time_{exp}$.

Before establishing the access to HS from LHC, the LHC with trust node and trust node with HS are authenticated using the ID. Further key and template using the key agreement process and then the authentication on both ends are verified mutually. Then the key and tags are provided to the LHC to grant authenticated access between the LHC and HS through trust node authentication server. With this, the authenticated request is forwarded to the HS and reply from the HS to LHC is forwarded using the proposed enhanced Kerberos protocol in the authentication server. Thus the way the improved secure Kerberos protocol ensures the security.

3.2 Generation of Template for Fingerprint Removable

Templates are generated using minutiae feature from fingerprint image of LHC and HS users. Process of extracting minutiae acquires following steps: a) Image Enhancement b) Image Binarization c) Morphological process, d) Image Thinning e) Minutiae feature extraction. Image enhancement of Fingerprint: The input images can contain redundant copies of image pixels. Enhancement technique tends to remove redundant copies of pixels and increase the contrast of original image. It helps to enhance the quality of received fingerprint image. After enhancement, original image can be used for further analysis process to improve the clarity.

Binarization of image: binarization is a process of filtering the image based on threshold value. When the pixels obtain greater than threshold value are colored as white and lesser value pixels below threshold are colored as black Image Morphological process: Shape of input image is considered for morphological process such as dilation and erosion. Adjacent pixels of the input images are taken to form new output image. Adjacent pixel are dilated for received input image and boundary pixels are removed by erosion.

Image Thinning: In formed binary image, particular part is selected and removed. This process is termed as skeletonization, which erode pixels of image into the single pixels.

Minutiae are a feature extracted from fingerprint image. This feature is composed of ridge ending and bifurcation of enhanced image of fingerprint. The fingerprint of users LHC and HS is fed as input image in principal curve algorithm for extracting the minutiae [19–21]. This curve algorithm returns value as (a, b, $\boldsymbol{\theta}$, p). where as (a.b) are values of a and b coordinates of minutiae, $\boldsymbol{\theta}$-represents angle, p represents quality of minutiae. The values (a, b) are considered as points of minutiae and given as vector (A,B). The vector coordinates of $\boldsymbol{V_a}$–has a selected minutiae coordinate values of the points and $\boldsymbol{V_b}$–has a selected minutiae coordinate values of the points. Finally feature vectors of minutiae are represented as,

$$\boldsymbol{V_a} = [\boldsymbol{a_i}]\boldsymbol{i} = 1 \ldots \boldsymbol{n} \tag{12}$$

$$\boldsymbol{V_b} = [\boldsymbol{b_i}]\boldsymbol{i} = 1 \ldots \boldsymbol{n} \tag{13}$$

Generation of Template for Removable Fingerprint: After receiving the features of extracted image, LHC and HS user template is modified to removable template. Once its consider as unique biometric data, then it cannot be used longer. To overcome this problem, irreversible data must be converted to reversible biometric data trait. This conversion must take place before using data in security protocol for authentication. Finally both LHC and HS user have own template of fingerprint as,

A: {a1, a2, an}, B:{b1, b2, bn} where as a and b are considered as minutiae coordinate point values.

3.3 Generation of Key for Combined Template and Fingerprint

After fingerprint template generation, it is send from LHC user to HS user with encrypted key using algorithm 1. HS repeats the same action vis versa. The XOR techniques used to form combined template for both the users. Now they have combined the removable template as representing as follows,

$$\boldsymbol{CTP_{(LHC+HS)}} = \boldsymbol{CTP_{LHC}} \oplus \boldsymbol{CTP_{HS}} \tag{14}$$

Now key for join template is available to users of LHC and HS for processing data with authentication via trust node. The LHC request is processed via trust node with our proposed improved key agreement based Kerberos protocol with fingerprint biometric. The combined template secret key are acquired using algorithm 1 and algorithm 2 equations for both users. Data security of users is highly ensured using combined template key by blocking the interference of unknown intruder's access. Our proposed key Kerberos protocol helps to share the key with high authentication among LHC and HS users. if the key is authenticated with template, then LHC user can get access in cloud network to communicate with HS.

Hence, our proposed improved key agreement based Kerberos protocol with fingerprint biometric template key helps to improve the data confidentially in cloud, data integrity while communicating in m health system. The key of combined template at two ends will increase the security to next level than existing algorithms.

4 Result and Discussions

The proposed authentication protocol with FP template is evaluated using network attached storage and the evaluated results in terms of computational complexity, energy and communication cost are discussed in this section. The performance of the proposed system is further evaluated with the comparative analysis on existing algorithms such as Chiou et al. [22], Mohit et al. [23] and Lopes et al. [24]. For the analysis the data are taken from the reference [25,26]. There are n numbers of wireless devices from LHS are executed using the proposed algorithm for authentication. The results in terms of computational cost, communication and energy cost are listed in Tab. 1.

The proposed IKAP-FP protocol obtain less computational cost, communication cost and energy cost than the existing algorithms. due to the number of parameters exchanged between LHC and HS is low,

the proposed work obtained this result. Various the existing algorithms obtained high cost due to the costly exchange of parameters. The proposed protocol enhance the M-health security with low computational overhead. In terms of number of devices, the computational cost comparison is shown in Tab. 2.

Table 1: Comparison of authentication protocols

Authentication protocols	Computational cost (s)	Communication cost (s)	Energy cost (MJ)
Chiou et al. [2]	2.3 n	6822 n bits	23.43 n
Mohit et al. [3]	1.32 n	4730 n bits	14.41 n
Lopes et al. [4]	0.52 n	3052 n bits	4.91 n
Proposed IKAP-FP protocol	0.13 n	2100 n bits	1.35 n

Table 2: Computational cost (ms) comparison of analyzed algorithms

Authentication protocols	Number of devices				
	20	40	60	80	100
Chiou et al. [2]	48.91	79.1	92.04	154.2	181.2
Mohit et al. [3]	42.46	76.52	91.92	1724	204.7
Lopes et al. [4]	35.9	65.4	90.2	106.8	195.3
Proposed IKAP-FP protocol	8.3	25.02	45.8	82.45	91.23

The evaluated results from Fig. 2. shows the proposed IKAP-FP obtained low computational cost of 91.23 s for 100 devices. The obtained results is low than other existing algorithms such as Chiou et al., Mohit et al. and Lopes et al., of 181.2, 204.7 and 195.3 s respectively for 100 devices.The analysis in terms of communication cost is shown in Tab. 3 with the illustration in Fig. 3.

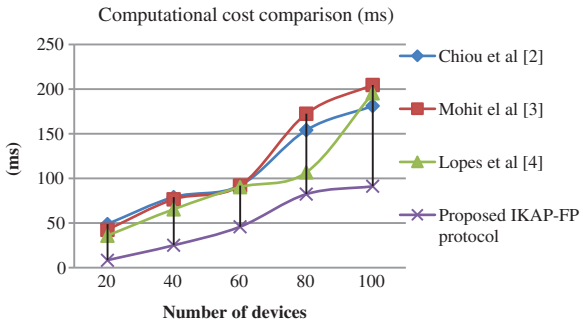

Figure 2: Computational cost comparison of authentication protocols

The experimented result of the analysis represent that our proposed IKAP-FP obtains low communication cost of $4.3*10^5$ bits on executing 100 devices than existing protocols such as Chiou et al. [2] obtains $7.3*10^5$, Mohit el al [3] obtains $6.9*10^5$ and Lopes et al. [4] obtains $6.2*10^5$.

Table 3: Communication cost (bits * 105) comparison of analyzed protocols

Authentication protocols	Number of devices				
	20	40	60	80	100
Chiou et al. [2]	2.3	2.1	3.8	5.9	7.3
Mohit el al [3]	1.5	1.8	2.9	4.8	6.9
Lopes et al. [4]	1.4	1.2	2.3	3.5	6.2
Proposed IKAP-FP protocol	0.45	0.92	1.7	2.65	4.3

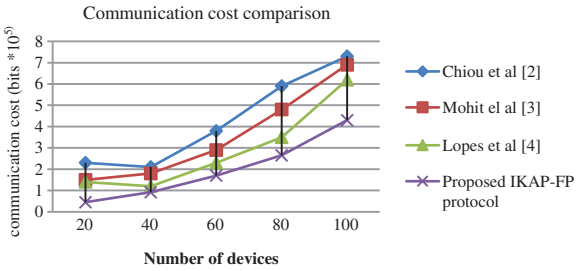

Figure 3: Communication cost comparison of analyzed protocols

In terms of energy cost, the result obtained from the experimentation is shown in Tab. 4. The energy is calculate as energy cost = CCtotal*W where, CCtotoal–computational time calculated using Tab. 2. and W-CPU power of the devices.

Table 4: Energy cost comparison of analyzed protocols

Authentication protocols	Number of devices				
	20	40	60	80	100
Chiou et al. [2]	590	1100	1600	1900	2100
Mohit et al. [3]	400	880	1400	1600	1800
Lopes et al. [4]	300	480	550	690	880
Proposed IKAP-FP protocol	80	140	210	290	460

The energy cost of existing and proposed protocols are evaluated. The result shows that our proposed IKAP-FP protocol obtains 460 MJ for executing 100 devices which is lower than other existing approaches such as Chiou et al. [22] obtains 2100 MJ , Mohit et al. [23] obtains 1800 MJ and Lopes et al. [24] obtains 880MJ for executing 100 devices request. The graphical representation of the results is shown in Fig. 4.

Hence, the best results are obtained from the security and evaluation proven that our proposed IKAP-FP performs better in terms of computational cost, communication cost and energy cost than the literature [22–24]. The proposed protocol is symmetric cryptography rather than existing approaches are asymmetric. Compare to existing algorithms, the proposed protocol enhance the M health security with secret key combined with fingerprint template [27–29]. Hence, the authenticated registered users only gain access to patients data which improves the confidentiality of the proposed M-health system.

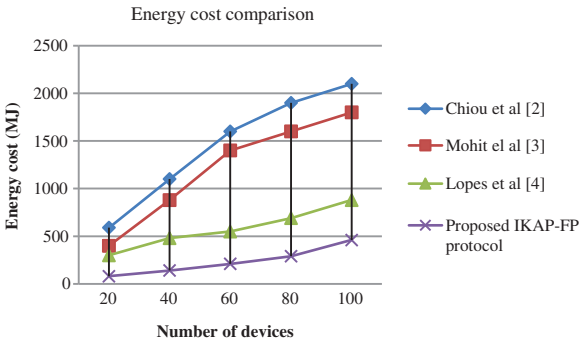

Figure 4: Energy cost comparison in terms of number of devices

5 Conclusions

A smart application based on heath care is main project to various developing industries in medical field. Day to day its important for urban people to monitor their health level due to work pressure and unhealthy food infrastructures. Our proposed work aims to recover and build M-Health application with high security. Maintaining the data secretly in open network is not easy. Because cloud like infrastructure have accessing its data minute by minute. Sometime information may fetched wrongly or update incorrectly. This research article introduced improved key agreement based Kerberos protocol with fingerprint biometric template key helps to improve the data confidentially in cloud. Biometric with security protocol can able implement high authentication in network system. Our result implementation shows very less computational cost, as of our proposed IKAP-FP protocol communication cost of $4.3*10^5$ bits on executing 100 devices. Where as existing techniques consumes more than $7.1*10^5$. During biometric authentication process with protocol execution consumes only less energy cost of 460 MJ for 100 devices. Where as existing techniques consumes more than 1000 MJ. In future this work can be extended with other security protocols with biometric for best result.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. S. Hossain, G. Muhammad, W. Abdul, B. Song and B. Gupta, "Cloud-assisted secure video transmission and sharing framework for smart cities," *Future Generation Computer Systems*, vol. 83, pp. 596–606, 2018.

[2] B. Tang, Z. Chen, G. Hefferman, S. Pei, T. Wei *et al.,* "Incorporating intelligence in fog computing for big data analysis in smart cities," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2140–2150, 2017.

[3] J. Zhou, Z. Cao, X. Dong, X. Lin and A. Vasilakos, "Securing m-healthcare social networks: Challenges, countermeasures and future directions," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 12–21, 2013.

[4] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen *et al.,* "Security and privacy for mobile healthcare networks: From a quality of protection perspective," *IEEE Wireless Communications*, vol. 22, no. 4, pp. 104–112, 2015.

[5] H. Huang, T. Gong, N. Ye, R. Wang and Y. Dou, "Private and secured medical data transmission and analysis for wireless sensing healthcare system," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1227–1237, 2017.

[6] T. L. Chen, Y. T. Liao, Y. F. Chang and J. H. Hwang, "Security approach to controlling access to personal health records in healthcare service," *Security and Communication Networks*, vol. 9, no. 7, pp. 652–666, 2016.

[7] A. Zhang, A. Bacchus and X. Lin, "Consent-based access control for secure and privacy-preserving health information exchange," *Security and Communication Networks*, vol. 9, no. 16, pp. 3496–3508, 2016.

[8] Q. Huang, Y. Yang and M. Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing," *Future Generation Computer Systems*, vol. 72, pp. 239–249, 2017.

[9] A. Sahai and B. Waters, "Fuzzy identitybased encryption," in *Proc. ICTACT, Aarhus*, Denmark, pp. 457–473, 2005.

[10] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. ISSP*, California, USA, pp. 321–334, 2007.

[11] S. Narayan, M. Gagn and R. SafaviNaini, "Privacy preserving system using attribute-based infrastructure," in *Proc. CCSW*, Chicago, USA, pp. 47–52, 2010.

[12] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[13] M. H. Au, T. H. Yuen and J. K. Liu, "A general framework for secure sharing of personal health records in cloud system," *Journal of Computer and System Sciences*, vol. 90, pp. 46–62, 2017.

[14] A. M. H. Yuen, T. H. Liu, J. K. Susilo, W. Huang, X. Xiang *et al.,* "A general framework for secure sharing of personal health records in cloud system," *Journal of Computer and System Sciences*, vol. 90, pp. 46–62, 2017.

[15] X. Li, J. Niu, M. Karuppiah, M. Kumari, S. Wu *et al.,* "Secure and e_cient two-factor user authentication scheme with user anonymity for network based e-health care applications," *Journal of Medical System*, vol. 40, pp. 1–12, 2016.

[16] Q. Jiang, K. M. Khan, X. Lu, J. Ma and D. He, "A privacy preserving three-factor authentication protocol for health clouds," *Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

[17] P. Mohit, R. Amin, A. Karati, G. P. Biswas and M. K. Khan, "A standard mutual authentication protocol for cloud computing based health care system," *Journal of Medical System*, vol. 41, no. 4, pp. 50, 2017.

[18] S. Chiou, Z. Ying and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," *Journal of Medical System*, vol. 40, no. 4, pp. 101, 2016.

[19] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian *et al.,* "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth,"*Journal of Medical System*, vol. 40, no. 11, pp. 1–10, 2016.

[20] R. Amin, S. K. Islam, G. P. Biswas, D. Giri, K. M. Khan *et al.,* "A more secure andprivacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments," *Security and Communication Networks*, vol. 9, pp. 4650–4666, 2016.

[21] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan *et al.,* "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[22] A. Sarkar and B. K. Singh, "A novel session key generation and secure communication establishment protocol using fingerprint biometrics," *In Handbook of Computer Networks and Cyber Security*, 1st ed., Springer, Cham, Kurukshetra, india, 2020.

[23] P. Mohit, R. Amin, A. Karati, G. P. Biswas and M. K. Khan, "A standard mutual authentication protocol for cloud computing based health care system," *Journal of Medical System*, vol. 41, no. 4, pp. 1–9, 2017.

[24] S. Chiou, Z. Ying and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," *Journal of Medical System*, vol. 40, no. 4, pp. 101–110, 2016.

[25] G. Lopes and A. P. Gondim, "Mutual authentication protocol for D2D communications in a cloud-based E-health system," *Sensors*, vol. 20, no.7, pp. 2072–2085, 2020.

[26] T. Baratsanjeevi, S. Deepakkrishna, M. P. Harrine, S. Sharan and E. Prabhu, "Iot based traffic sign detection and violation control," in *Proc. ICIRCA*, Coimbatore, India, pp. 333–339, 2020.

[27] M. Karthikeyan, V. Manesh, L. S. Krishna, B. Vijay, R. Vishwabharan *et al.,* "Iot based accident detection and response time optimization," in *Proc. ICCMC*, Erode, India, pp. 358–363, 2021.

[28] N. Chidambaram and D. Vijayan, "Detection of exudates in diabetic retinopathy," in *Proc. ICACCI*, Bangalore, India, pp. 660–664, 2018.

[29] V. Iyer, B. Ganti, A. M. Hima Vyshnavi, P. K. Krishnan Namboori and S. Iyer, "Hybrid quantum computing based early detection of skin cancer," *Mathematics*, vol. 23, no 2, pp. 347–355, 2020.