Computer Systems Science & Engineering
DOI: 10.32604/csse.2022.022329
Article

Tech Science Press

Fingerprint Agreement Using Enhanced Kerberos Authentication Protocol on M-Health

A. S. Anakath[1,*], S. Ambika[2], S. Rajakumar[3], R. Kannadasan[4] and K. S. Sendhil Kumar[5]

[1]School of Computing, E.G.S. Pillay Engineering College, Nagapattinam, 611002, India
[2]Department of Computer Science and Engineering, University College of Engineering Ariyalur, Ariyalur, 621705, India
[3]Department of Mathematics, University College of Engineering Ariyalur, Ariyalur, 621705, India
[4]Department of Software Systems, School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology University, Vellore, 632014, India
[5]Department of IoT, School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology University, Vellore, 632014, India
*Corresponding Author: A. S. Anakath. Email: asanakath21@gmail.com

Received: 04 August 2021; Accepted: 10 November 2021

Abstract: Cloud computing becomes an important application development platform for processing user data with high security. Service providers are accustomed to providing storage centers outside the trusted location preferred by the data owner. Thus, ensuring the security and confidentiality of the data while processing in the centralized network is very difficult. The secured key transmission between the sender and the receiver in the network is a huge challenge in managing most of the sensitive data transmission among the cloud network. Intruders are very active over the network like real authenticated user to hack the personal sensitive data, such as bank balance, health data, personal data, and confidential documents over the cloud network. In this research, a secured key agreement between the sender and the receiver using Kerberos authentication protocol with fingerprint is proposed to ensure security in M-Healthcare. Conditions of patients are monitored using wireless sensor devices and are then transferred to the server. Kerberos protocol helps in avoiding unnecessary communication of authenticated data over the cloud network. Biometric security process is a procedure with the best security in most of the authentication field. Trust node is responsible in carrying data packets from the sender to the receiver in the cloud network. The Kerberos protocol is used in trust node to ensure security. Secured communication between the local health center and the healthcare server is ensured by using a fingerprint feature called minutiae form, which refers to the fingerprint image of both sender and receiver. The computational and communicational cost of the proposed system is lesser when compared with other existing authentication methods.

Keywords: Protocol security; m-health; cloud computing; biometric; fingerprint; kerberos protocol

1 Introduction

Emerging applications in big data, such as cloud computing, intelligent businesses, and mining applications, are the reason for future business enterprise needs. Free resources along with the Internet are polled as cloud storage and used for various applications over the Internet. Cloud computing works dynamically in the Internet all over the world by offering the storage spaces and processing software in run time. When compared with existing distributed system environments, cloud computing, as a utility of distributed computing, provides lesser investment and better scalability and efficiency. Due to the advancement of cloud technologies, the need and usage of grid computing and supercomputing are reduced. Although the cloud environment satisfies the users and data owners in all perspectives, it still faces security issues. Thus, providing high security over the confidential data processing is an important field of research in distributed infrastructure. In this work, security for storing personal identities over the cloud network is processed. Issues exist in the transmission of sensitive data in traditional distributed domain is addressed and discussed about the advantages of privacy and security in the big data infrastructure [1,2]. Huge data over the Internet may interfere with sensitive information, thereby creating privacy problems.

High-security processing techniques in cloud computing is not an easy task. Sharing confidential data to the destination is a big challenge because of the wide network accessing capability of cloud computing [3]. Sometimes, data are shared outside the current domain to requested users. Today, social media, health applications, e-commerce, business enterprise, and educational applications increases number of users, storage devices over the cloud infrastructure leads to high growth in access and control in that field. Network intruders are ready to hack the data and modify the originality of data in the cloud [4]. Therefore, the protection of the original data from deletion, modification, and fabrication is very challenging.

The security of the sharing system is classified as two types, namely, the privileged base access control [5] and the key management process. The group key security [6] is processed by authorized group of users to protect the shared information along the network. However, this system cannot afford security for cloud users. Group key is shared with third-party authentication. However, the authorization of a third party in cloud is not always guaranteed. In this proposed work, we introduce an agreement-based security key using Kerberos protocol. This protocol is strongly attached with secured features using biometric fingerprint information. This Kerberos protocol with biometric security is highly confidential and accessed in the cloud network.

The research contribution in this work is presented as follows:

- The implementation of Kerberos authentication with removable fingerprint pattern to improve the authentication process.
- Trust node, which carries security information with data to be processed.
- The fingerprint feature called minutiae is used to create templates from the fingerprint images of the users of the local healthcare center (LHC) and the healthcare server (HS).
- Once the biometric features are matched between the user and the server, biometric information is removed, and protocol allows securing the transmission of data.

The remainder of the research article is organized as follows: The second section presents the study of previous works in cloud security in m-health. The third section discusses the working principle of Kerberos and biometric security protocol during data authentication. The fourth section explains the result evaluation process. Finally, the last section concludes the paper.

2 Related Work

Paper [7–9] proposed a standard mutual authentication protocol for a cloud computing-based health care system. To overcome issues, such as the lack of security of patient anonymity, the authors developed light weight authentication protocol for the Telecare medical information system in cloud environment. The results ensure the security and prevents the system from major attacks. Moreover, the performance of the protocol is compared with existing results to prove the efficiency of the proposed protocol. Chiou et al. [10] proposed a mutual authentication protocol for Device-to-Device (D2D) communication in cloud-based e-health system. The proposed work ensures security in terms of the development of safe e-health systems to protect the patient's data and identities.

The work proposed by Lopes et al. [11] have the cloud server that store the patient's data, which are collected from the sensors that are fixed with the human body. These data are encrypted and transferred through the public channel and cloud server with the mutual authentication and session key. They formed a protocol based on four phases, namely, health center upload, patient upload, treatment, and checkup. A two-way authentication protocol is proposed to authenticate the client and server anonymously in Paper [12]. This mechanism preserves the identity of the user in the cloud and fulfils the authentication. A novel RSA algorithm for secured key transmission in a centralized cloud environment is proposed in [13]. This algorithm encrypts the keys used in a group environment. Both these algorithms are computationally efficient.

Jiang et al. [14] developed a protocol for e-health based on symmetric cryptography. Li et al. [15] and Gunes et al. [16] built their e-health protocol based on three phases, namely, initialization, registration, and authentication. Their protocols are susceptible to stealing the patient's device information and confidentiality issues. Stallings developed a long-term evolution D2D model that are integrated into 3GPP LTE architecture with the development of the discovery model to establish the communications based on proximity services are proposed in Paper [17]. This work does not focus on m-health architecture and needs further improvement.

Ueshige et al. proposed a multiple challenge-response protocol that enabled user interaction. These protocols are also similar to Kerberos protocol with the issues of maintaining the secret key, and the owner is not established [18]. Abid et al. [19] developed a one-time biometric authentication protocol with biometric authentication that requires the storage of biometric templates. This protocol is based on a one-time transformation with unique session. Barni et al. [20] developed a protocol for e-Passport authentication based on elliptic curve cryptography by using fingerprint biometrics to generate the parameters used for e-passport authentication. No proper evaluation is performed in this work. Paper [21–23] proposed authentication protocols for the authentication of the user in the system. However, they did not provide the cryptographic key for secured transmissions. The other protocols found in Paper [24] shared the same secure secret key for all the sessions.

Liu et al. [25] recommended the transport layer security, which provided the symmetric key for secure transmission generated in every session. Public key cryptographic protocols are used to share the key. Attribute-based cipher text policy is proposed to share secured schemes along the cloud environment. Restricting the unauthorized persons in the network is the main focus in this sign-based encryption scheme. The policy of access control in cloud with personal data is controlled in Huang et al. [26]. Here, central trusted authority is responsible for key management and generation. Novel encryption technique using public key is used to authorize data with cipher text process [27].

Wu et al. introduced identity encryption technique to improve cloud security. In this research, the identity of the users is collected and encrypted to securely share data in cloud [28]. Cipher text security with access control and bilinear data paring in attribute-based cipher text are used for secured searching [29]. In the peer-to-peer cloud storage and process, data security is assured using ACPC scheme [30]. Attribute-based cipher text has low performance problem. This problem is improved by using a framework called RAAC scheme. Cloud storage is highly affected by privacy problems [31]. The scheme, called privacy aware data sharing, is computed as attribute encryption and re-encryption process in which the key is often updated secretly without the interference of a third party.

3 System Model and Preliminaries

While making the data transaction over different networking environments, security and authentication are the crucial parts of the process. During the transmission of the data over the network, two persons, namely, the sender and the receiver, are involved, and data must be protected from third-party access networks. The authentication process is an important part to ensure that the transaction is highly secured in the network. This security and authentication can be provided through cryptographic techniques. While transmitting the data over the network securely, symmetric key cryptography and their variations are widely used. With this, sharing the secret key between the sender and receiver securely is the main challenge. Existing algorithms still lack in proving security, reliability, and confidentially.

3.1 System Model

To overcome the problems of management and the distribution of the key over the two parties, this chapter proposes a new protocol called secure key agreement-based enhanced Kerberos authentication protocol (EKAP) with fingerprint biometric over centralized networks, such as cloud on healthcare application. From the main server, the data are transmitted over the link through the trust node. The trust node is responsible for sharing the sender and receiver key securely to access the transmitted data. The security of this trust node is managed using the proposed key agreement-based Kerberos protocol. The architecture of this work is shown in Fig. 1.

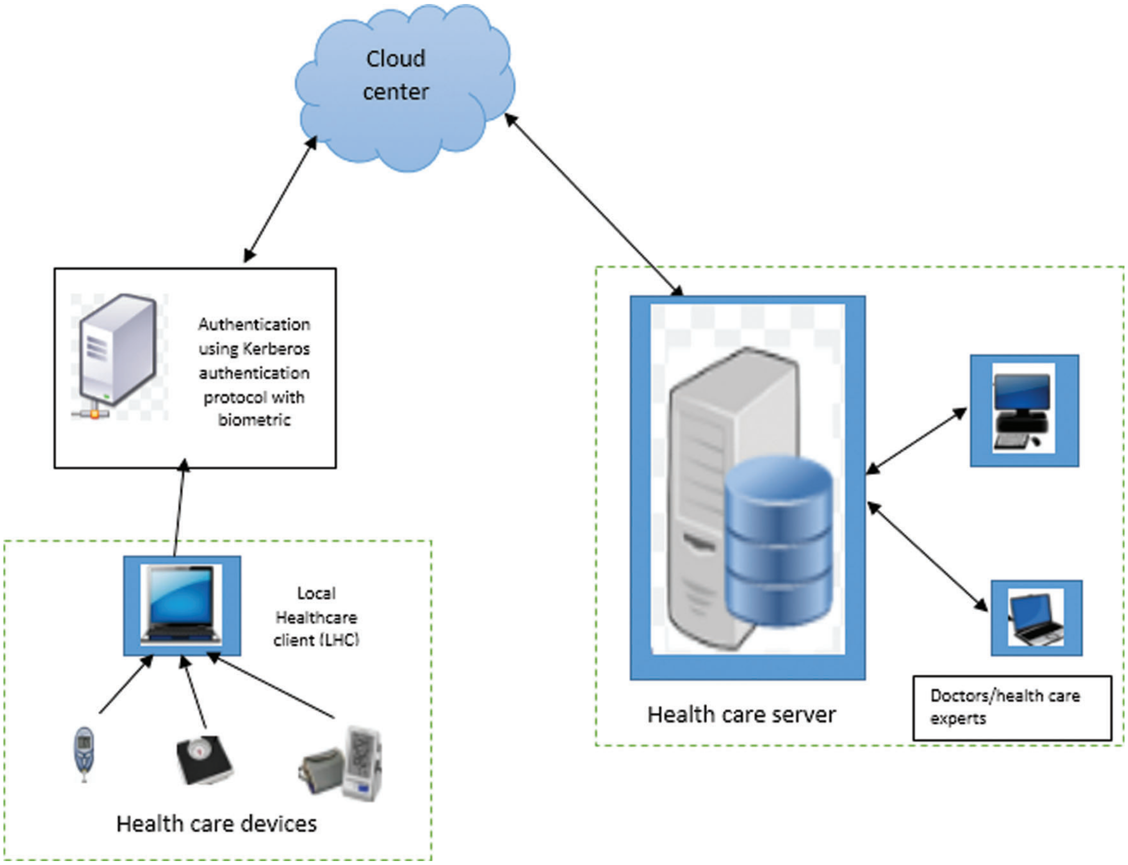

Cloud center
Authentication using Kerberos authentication protocol with biometric
Local Healthcare client (LHC)
Health care devices
Health care server
Doctors/health care experts

Figure 1: Overall architecture of the proposed system

The proposed healthcare system consists of wearable devices of the patients, LHC and the HS. HS is connected to the LHC through a 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 that is similar to mobile phones or laptops, which are involved in the authentication process. In this proposed work, the Kerberos authentication with the removable fingerprint pattern is used to improve security level of the authentication process because biometrics are proven to be the best secured authentication mechanism in all application areas.

A trust node exists between the LHC and the 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. Once authentication is completed, the related confidential reply is sent to the HS through the trust node to improve the security at LHC. The trust node exists in between the LHC and HS with 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.

3.2 EKAP

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

The EKAP consists of LHC and trust nodes. The request from the LHC is processed by the trust node, and the trust node authenticates the LHC requests by applying the proposed algorithm. Once authenticated, it examines the data from the server through cloud environment, and it is responsible in providing access to the healthcare server. The request from the LHC is authenticated using the key agreement with removable fingerprint template to maintain the security. The fingerprint data of the patient are used here not for biometric authentication but for increasing the randomness of the key generated by the protocol. Authentication is performed in two phases: First, between the LHC and the trust node at authentication server; second, the trust node with the HS database. During the authentication, a random integer called r_i with ephemeral (temporary) key called EK_a is selected with the interval of [1, n−1] where n is the number of request, and the LHC request process is declared as,

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

$$Q_a = -EK_a \times L, \tag{2}$$

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 E_{Kb} with the interval [1, n−1], which is defined as follows:

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

$$Q_b = -EK_b \times L. \tag{4}$$

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:

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

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, 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 LHC fails in the verification process, then it is terminated. Otherwise, the client processes the request as:

$$EK_a = -EK_a \times Q_b. \tag{9}$$

The secret key EK = EK_a = EK_b ensures the authentication process. The algorithm for the key agreement based EKAP is given in Algorithm 1.

Algorithm 1: Enhanced Kerberos authentication protocol-key agreement

```
  Initialize trust node, random number $r_i$, ephemeral key $EK_a$ and request L
Step 1: LHC sends request to the trust node which is in between the healthcare 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 $EK_b$ for the request L
        Trust node processes the request using Eqs. (5) and (6)
        Generate the secret information $e_b$, $s_b$ and $Q_b$
        Key generation using Eq. (9) and is sent to the trust node
        Combine the key with the removable template using Algorithm 2
        Authentication and verification using Eqs. (7) and (8)
        Share the key
End
Step 3: LHC sends the key with the template to the server through trust node.
Step 4: The HS receives the request and checks whether it is authenticated with the key from the trust node and decrypts the message using the secret key with removable template.
Step 5: The HS generates biometric template using Algorithm 2.
Step 6: LHC decrypts the information using the secret key after the verification done by the trust node. Both LHC and HS have removable biometric template of both.
Step 7: Both LHC and HS combine their biometric template with the secret key by using the XOR operation and generate the combined template key. Now both LHC and HS have combined key 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, it is not necessary to share the key through the secure nodes. The workflow sequence diagram of proposed work is shown in Fig. 2. Initially, the LHC sent request to the trust node for accessing the HS through cloud. The request from the client is declared as,
```

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

where, EK_c, *tags*- LHC key and related tag information such as id, template. V- verifier (trust node), $time_{exp}$- request time interval. The trust node receives the request, and performs the key agreement based Kerberos authentication and responses to LHC by granting to access the information of the HS. This response from trust node to LHC is declared as,

$$TN_{res}\colon \{EK_c,\ V,\ time_{exp},\ n\ldots\}EK_c,\ tags,\ \{T_{c.v}\},\ EK_v \tag{11}$$

where, EK_c, *V*- key of the HS to access the information with the time interval $time_{exp}$.

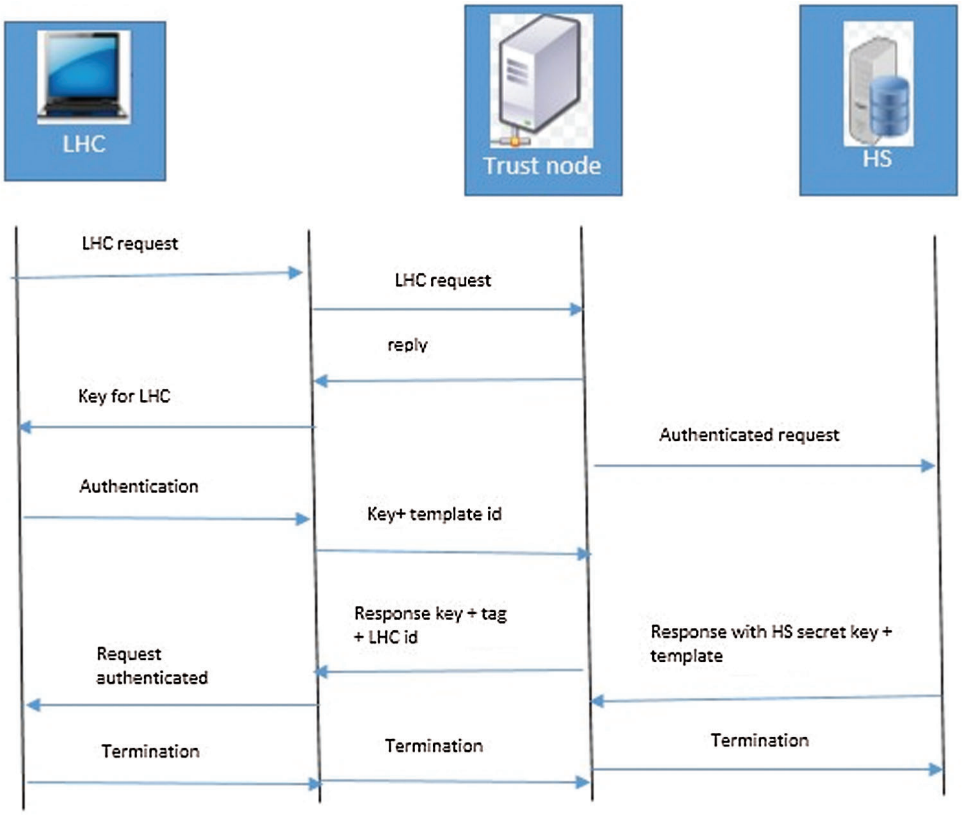


Figure 2: Workflow sequence diagram of the proposed work

Before establishing the access to HS from LHC, the LHC with trust node and the trust node with HS are authenticated using the ID, key, and template using the key agreement process. Finally, 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 the trust node authentication server. With this, the authenticated request is forwarded to the HS, and the reply from the HS to LHC is forwarded using the proposed enhanced Kerberos protocol in the authentication server. In this way, the EKAP protocol ensures security by establishing mutual authentication process.

3.3 Removable Fingerprint Template Generation

For the user of LHC and the experts in the HS, fingerprint templates are created using the fingerprint feature called minutiae form of the fingerprint image. The process of this minutiae extraction is performed using the steps, such as enhancement, binarization, morphological operation, thinning, and minutiae extraction.

Fingerprint Image enhancement: This step is performed to improve the quality of the obtained fingerprint feature. The original captured images are obtained and need to be enhanced to improve for further processing. Enhancement process is used to remove the redundant pixels of the input image and increase the brightness and contrast of the raw image.

Fingerprint Image binarization: The enhanced image is then binarized using the threshold value. The pixel above the threshold are declared as white, and the pixel value below the threshold are declared as black. Hence, the fingerprint image is binarized.

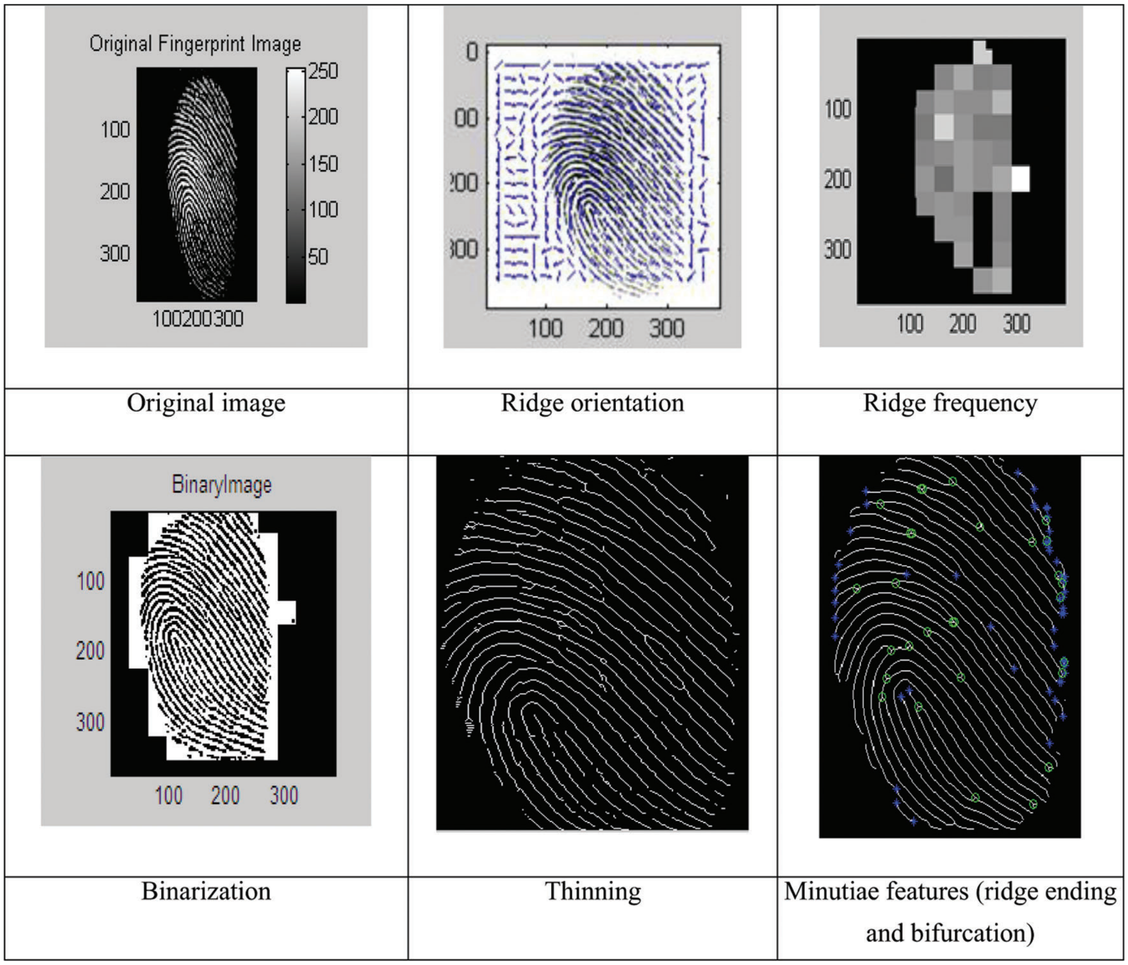
Morphological operation: This process is based on the shape of the input image. Each pixel of the input image with its adjacent pixels in the output image using the operations, dilation, and erosion, as necessary. Dilation refers to the addition of pixels while erosion means the removal of the pixels at the boundaries.

Thinning: This process is also called skeletonization, which is used to remove the selected part of the image from the binary image. This step erodes the pixels into the single pixel form.

Minutiae feature extraction: Minutiae features, such as ridge ending and bifurcation, are the features extracted from the enhanced fingerprint image. From the given input image of user of LHC and HS, the minutiae points are extracted using the principal curve algorithm (Sarkar et al. 2020). This algorithm returns the point as (x, y, θ, q) where x and y are the coordinate values of the minutiae point (x, y), θ is the angle, and q is the quality of the minutiae feature point. The (x, y) values are measured as the minutiae points, and these are represented as a vector called (X,Y). The vector V_X consists of x coordinate values of the selected minutiae points, and V_Y consists of y coordinate values of the selected minutiae points. These extraction process is represented in Fig. 3. These featured vectors are represented as follows:

$$V_X = [x_i] i = 1 \ldots n, \tag{12}$$

$$V_Y = [y_i] i = 1 \ldots n. \tag{13}$$



Original image

Ridge orientation

Ridge frequency

Binarization

Thinning

Minutiae features (ridge ending and bifurcation)

Figure 3: Fingerprint image feature extraction process

Removable fingerprint template generation: Once the image features are extracted, the template of the users from LHC and HS is altered as a removable template. If the unique biometric data are considered, then the biometric data will no longer be in use. Therefore, the irreversible data should be converted into reversible biometric trait before it is used in the authentication protocol for security. Both the users of LHC and HS possess their own removable fingerprint template as, X: {x1, x2,..xn}, Y: {y1, y2,..yn} where x and y are the coordinate values of minutiae points.

Algorithm 2:

```
Input: A[] – random array of the size 1 to 32, X[] – x coordinate value of minutiae points, Y[] – y coordinate value of minutiae points, n – total number of minutiae points.
Output: C[] – Integer array of the removable template
Step 1: Read the input image of the users
Step 2: Store the first 32 x coordinate values of the minutiae point (x, y)
Step 3: Store the first 32 y coordinate values of the minutiae point (x, y)
Step 4: If ( i mod 2 == 0) //even number
    $T(A[i]) = (x(i) \bmod 256)) + 1$    (14)
Step 5: Else
    $T(A[i]) = (y(i) \bmod 256)) - 1$    (15)
Step 6: End if
```

3.4 Combined Template of Key and Fingerprint Generation

After generating the fingerprint template of LHC users, it is sent to the HS with the encryption key using Algorithm 1. The same procedure is also performed by HS users. The combined template is formed using XOR operation of both templates of users. Now, both users have the combined removable template with them, which is represented as,

$$CT_{(LHC+HS)} = CT_{LHC} \oplus CT_{HS}. \tag{16}$$

Now, both the users of LHC and HS have this combined template with the key for their authentication process through the trust node. The work flow diagram of our proposed authentication protocol is shown in Fig. 4. The request from the LHC is processed through trust node using the proposed key agreement based on enhanced Kerberos with biometric template protocol. The key with the combined template of both the users is generated using the equations in Algorithms 1 and 2. The combined template at both ends improves the security by not allowing any interference of unknown access. The key agreement based on protocol shares the key between the user of the LHC and HS securely to authenticate the request. Once authenticated with the key and the template, the LHC user is granted access to the HS through the cloud network.

Hence, our proposed key agreement based on EKAP with biometric template improves the confidentially and integrity with secure communication over the healthcare system. The combined template at both ends assures improved security to the next level of normal authentication algorithms.

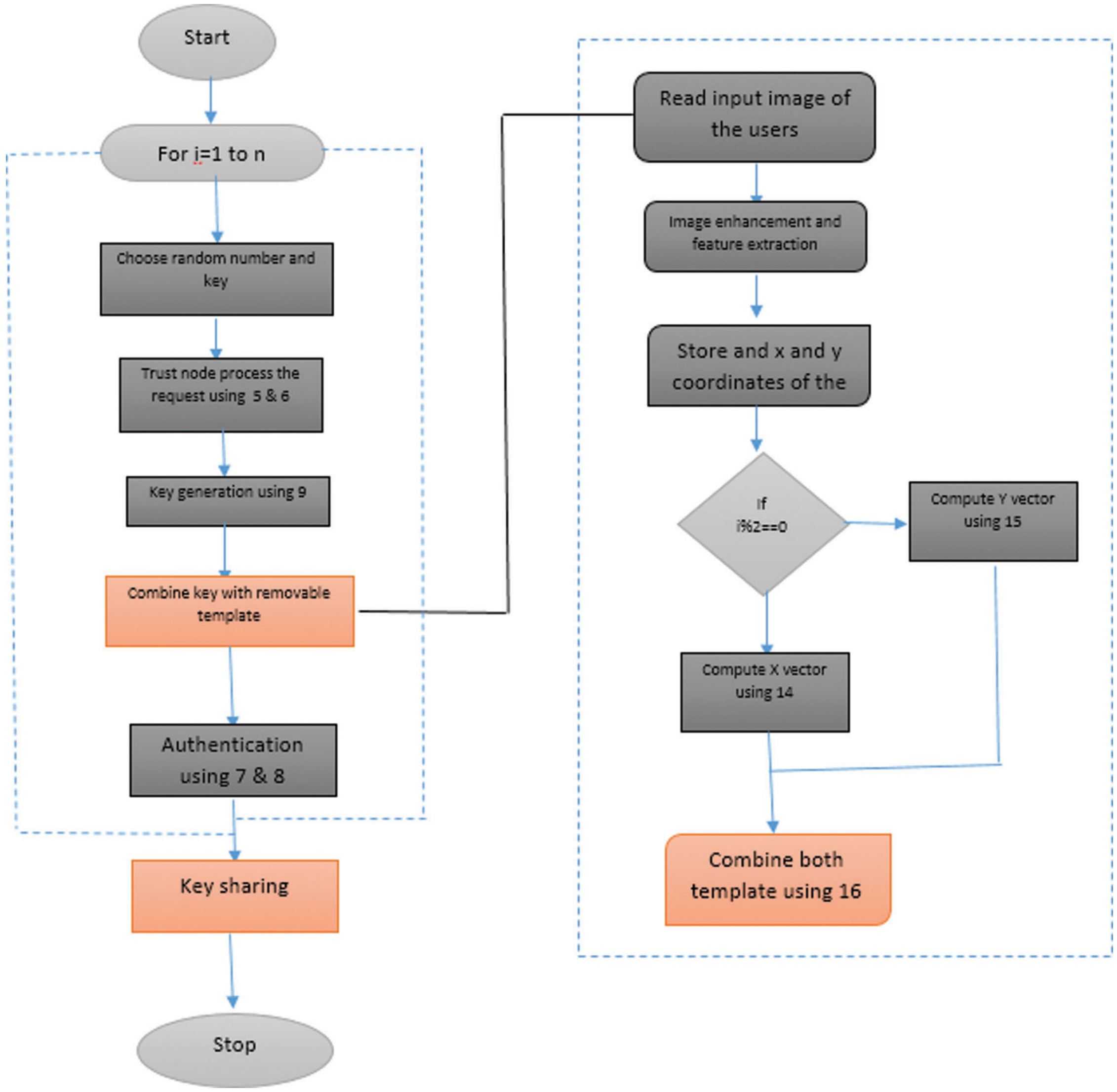

Start
For i=1 to n
Choose random number and key
Trust node process the request using 5 & 6
Key generation using 9
Combine key with removable template
Authentication using 7 & 8
Key sharing
Stop
Read input image of the users
Image enhancement and feature extraction
Store and x and y coordinates of the
If i%2==0
Compute Y vector using 15
Compute X vector using 14
Combine both template using 16

Figure 4: Workflow of our proposed work

4 Result and Discussion

This section describes the results of experiment and evaluation of the proposed authentication protocol for key agreement, which is based on the EKAP with biometric template on healthcare system. It is implemented using network attached storage. The proposed work is evaluated in terms of computational complexity, communication cost, and energy cost. It has also been compared with existing algorithms to prove that its efficiency is superior to those of existing systems. Thenumber of devices from LHC are executing the authentication using the proposed algorithm to the HS through trust node and cloud server. Tab. 1. represents the computational, communication, and energy costs of the proposed system and the existing systems.

Tab. 1 shows that our proposed authentication protocol incurs low computational, communication, and energy cost because of the lesser number of parameters exchanged between the LHC and HS than the existing approaches due to the costly exchange of parameters. Our protocol consumes less computational time and enhanced the performance of the system. Tab. 2 represents the comparison of computational costs in terms of the number of device requests for access to the system (Fig. 5).

Table 1: Comparison of authentication protocols

Protocols	Computational cost (ms)	Communication cost (ms)	Energy cost (MJ)
Chiou et al. (2016)	2.43 n	6920 n bits	26.43 n
Mohit et al. (2017)	1.42 n	4832 n bits	15.45 n
Lopes et al. (2020)	0.21 n	3072 n bits	2.93 n
Proposed protocol	0.15 n	2134 n bits	1.65 n

Table 2: Computational cost comparison of analyzed algorithms

Protocols	Number of devices				
	20	40	60	80	100
Chiou et al. (2016)	50	80	150	200	250
Mohit et al. (2017)	40	78.54	127.4	189.3	220.43
Lopes et al. (2020)	20.43	57.34	90.32	112.42	198.34
Proposed protocol	9.4	30.42	56.24	89.23	91.24

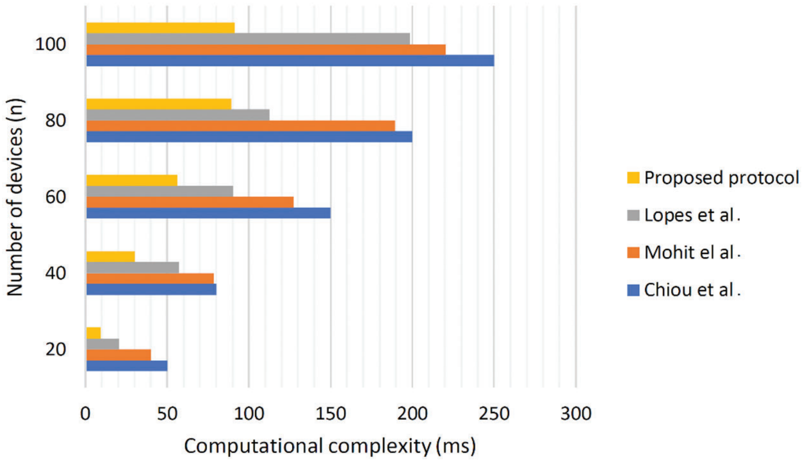


Figure 5: Computational cost comparison

The graph illustrates the analysis of the results of the existing protocols with proposed enhanced Kerberos authentication protocol (EKAP) with biometric template. The proposed algorithm incurs a low computational cost of 91.24 ms for 100 access devices, the other existing protocols proposed in terms of communication cost, the results of the analysis are shown in Tab. 3 and illustrated in Fig. 6.

The experimental results of the analysis show that our proposed EKAP obtains low communication cost of 5.4 × 105 bits on executing 100 devices. Other existing protocols, such as obtains 8 × 105 bits.

Table 3: Communication cost comparison of analyzed protocols

Protocols	Number of devices				
	20	40	60	80	100
Chiou et al. (2016)	2	2.5	4	6	8
Mohit et al. (2017)	1.5	2	3.5	5	7.5
Lopes et al. (2020)	1	1.5	2.5	3.8	6.5
Proposed protocol	0.5	1	2	3.2	5.4

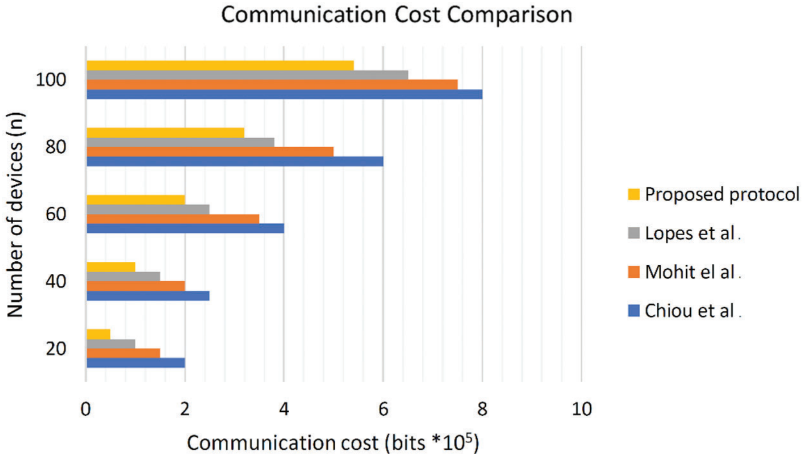


Figure 6: Communication cost comparison of analyzed protocols

The results of energy cost analysis experiment are shown in Tab. 4. The energy cost is computed using the following formula: energy cost = CCtotal*W, where CCtotal is the computational time calculated using Tab. 2 and W-CPU power of the devices.

Table 4: Energy cost comparison of analyzed protocols

Protocols	Number of devices				
	20	40	60	80	100
Chiou et al. (2016)	600	1200	1800	2200	2600
Mohit et al. (2017)	400	900	1500	1700	1900
Lopes et al. (2020)	200	400	500	700	900
Proposed protocol	90	150	220	300	570

The energy cost of the existing and proposed protocols are evaluated. The results show that our proposed EKAP protocol obtains 570 MJ for executing 100 devices, which is lower than those of other approaches. The protocol proposed obtained 2600, 1900, and 900 MJ for executing 100 devices. The graphical representation of the results is shown in Fig. 7.

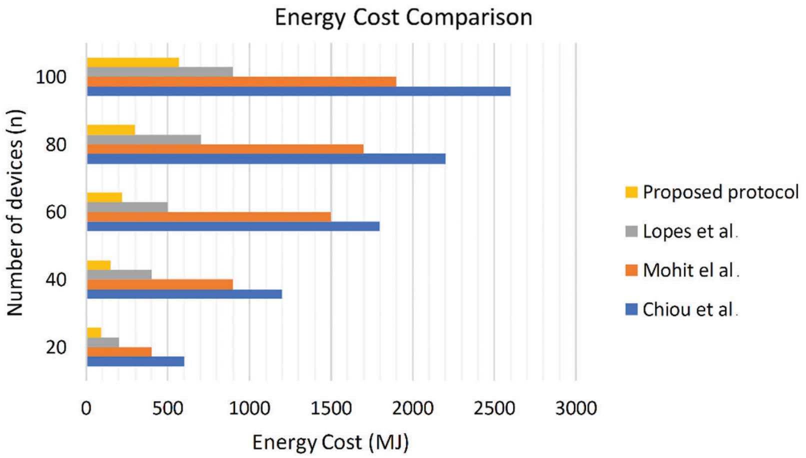


Figure 7: Energy cost (MJ) comparison of analyzed protocols

5 Conclusions

In this paper, an authentication protocol using Kerberos combined with fingerprint for a healthcare system is presented. The security issues of the data transmitted over the cloud network between the LHC and the HS are considered. To address this issue, the key is computed using the Kerberos authentication protocol by combining the key with the fingerprint template. The LHC and the HS computes and verifies the keys of each other. Hence, the security of the system is achieved by exploring the mutual authentication of LHC and HC by gently exchanging the secure key between them. The performance of the system exhibits remarkable results. The computational cost of the proposed system for 100 nodes is computed and found the improvement of 54%, 58.6%, 63.5% compared with the works proposed by Lopes et al. (2020), Mohit et al. (2017), and Chiou et al. (2016), respectively. The communication cost of the proposed system for 100 nodes is determined and found better performance of 17%, 28%, and 32.5% compared with the works proposed by Lopes et al. (2020), Mohit et al. (2017), and Chiou et al. (2016), respectively. The energy cost of the proposed system is calculated and obtained increased efficiency of 36.7%, 70%, and 78% compared with the works proposed by Lopes et al. (2020), Mohit et al. (2017), and Chiou et al. (2016), respectively. Hence, this proposed system is inferred as a secure and efficient healthcare system in distributed cloud network environment.

An authentication protocol using Kerberos combined with fingerprint for a healthcare system is proposed in a distributed environment. The security issues of the data transmitted over the cloud network between the LHC and the HS are considered. To address this issue, the key is computed using the Kerberos authentication protocol by combining the key with the fingerprint template. In the proposed work, we create the template for clients, as well as servers in the cloud. In the future, various biometric parameters can be used with Kerberos protocol (EKAP) for high security in the network.

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] X. Chen and J. H. Jiang, “A method of virtual machine placement for fault-tolerant cloud applications,” *Intelligent Automation & Soft Computing*, vol. 22, no. 4, pp. 587–597, 2016.

[2] X. Li, Y. Zhuang and S. X. Yang, “Cloud computing for big data processing,” *Intelligent Automation & Soft Computing*, vol. 23, no. 4, pp. 545–546, 2017.

[3] 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*, Springer, Cham, pp. 777–805, 2020.

[4] A. S. Anakath, S. Rajakumar and S. Ambika, “Privacy preserving multi factor authentication using trust management,” *Cluster Computing*, vol. 22, no. 5, pp. 10817–10823, 2019.

[5] A. S. Anakath, R. Kannadasan and S. Ambika, “Application of boolean algebra in security systems like captcha,” *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, no. 7, pp. 941–946, 2018.

[6] K. Y. Teng, S. A. Thekdi and J. H. Lambert, “Risk and safety program performance evaluation and business process modeling,” *IEEE Transactions on Systems, Man, and Cybernetics-Part a: Systems and Humans*, vol. 42, no. 6, pp. 1504–1513, 2012.

[7] Y. Tang, C. Lee, C. S. Lui and R. Perlman, “Secure overlay cloud storage with access control and assured deletion,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 903–916, 2012.

[8] J. Shao, R. Lu and X. Lin, “Fine-grained data sharing in cloud computing for mobile devices,” in *Proc. INFOCOM*, Hong Kong, China, pp. 2677–2685, 2015.

[9] 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 Systems*, vol. 41, no. 4, pp. 50, 2017.

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

[11] G. Lopes and P. R. Gondim, “Mutual authentication protocol for D2D communications in a cloud-based e-health system,” *Sensors*, vol. 20, no. 7, pp. 2072, 2020.

[12] A. Arasan, R. Sadaiyandi, F. Al-Turjman, A. S. Rajasekaran and K. S. Karuppuswamy, “Computationally efficient and secure anonymous authentication scheme for cloud users,” *Personal and Ubiquitous Computing*, pp. 1–11, 2021.

[13] S. Ambika, S. Rajakumar and A. S. Anakath, “A novel RSA algorithm for secured key transmission in a centralized cloud environment,” *International Journal of Communication System*, vol. 33, no. 5, pp. 1–9, 2020.

[14] Q. Jiang, X. Lian, C. Yang, Y. Tian and Y. Yang, “A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth,” *Journal of Medical Systems*, vol. 40, no. 11, pp. 1–10, 2016.

[15] X. Li, J. Niu, M. Karuppiah, S. Kumari and F. Wu, “Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications,” *Journal of Medical Systems*, vol. 40, no. 12, pp. 1–12, 2016.

[16] T. T. Gunes and H. Afifi, “Hybrid model for LTE network-assisted d2d communications,” in *Proc. ICANANW, Benidorm*, Spain, pp. 100–113, 2014.

[17] W. Stallings, “Cryptography and network security Principles and Practices,” 5th ed., Boston, Upper Saddle River, Prentice Hall, 2010.

[18] Y. Ueshige and K. Sakurai, “A proposal of one-time biometric authentication,” in *Proc. Security and Management*, Las Vegas, United States, pp. 78–83, 2006.

[19] M. Abid and H. Afifi, “Towards a secure e-passport protocol based on biometrics,” *Journal of Information Assurance and Security*, vol. 4, no. 4, pp. 338–345, 2009.

[20] M. Barni, T. Bianchi, C. M. Dario, R. D. Raimondo, P. Labati *et al.*, “Privacy-preserving finger code authentication,” in *Proc. ACMMS*, Rome, Italy, pp. 231–240, 2010.

[21] M. Upmanyu, A. M. Namboodiri, K. Srinathan and C. V. Jawahar, “Blind authentication: A secure crypto-biometric verification protocol,” *IEEE Transactions Information Forensics and Security*, vol. 5, no. 2, pp. 255–268, 2010.

[22] J. Bringer, H. Chabanne, M. Izabachène, D. Pointcheval, Q. Tang *et al.*, “An application of the goldwasser-micali cryptosystem to biometric authentication,” in *Proc. CISP*, Perth, Australia, pp. 96–106, 2007.

[23] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky and A. Smith, “Secure remote authentication using biometric data,” in *Proc*, ICTACT, Darmstadt, Germany, pp. 147–163, 2005.

[24] Q. Tang, J. Bringer, H. Chabanne and D. Pointcheval, "A formal study of the privacy concerns in biometric-based remote authentication schemes," in *Proc*, ICISPE, Nanjing, China, pp. 56–70, 2008.

[25] H. liu, Y. huang and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," *Future Generation Computer System*, vol. 52, pp. 67–76, 2015.

[26] K. Huang, R. Tso, C. Yu Chi, M. D. Rahman, A. Almogren *et al.*, "PKE-Aet: Public key encryption with authorized equality test," *The Computer Journal*, vol. 58, no. 10, pp. 2686–2697, 2015.

[27] L. Wu, Y. Zhang, K. K. R. Choo and D. He, "Efficient and secure identity based encryption scheme with equality test in cloud computing," *Future Generation Computer. System*, vol. 73, pp. 22–31, 2017.

[28] Q. Xu, C. Tan, Z. Fan and W. Zhu, "Secure multi-authority data access control scheme in cloud storage system based on attribute-based sign encryption," *IEEE Access*, vol. 6, pp. 34051–34074, 2018.

[29] H. He, R. Li, X. Dong and Z. Zhang, "Secure, efficient and fine-grained data access control mechanism for P2P storage cloud," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 471–484, 2014.

[30] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue *et al.*, "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 953–967, 2017.

[31] Z. Pervez, A. M. Khattak, S. Lee and Y. K. Lee, "SAPDS: Self-healing attribute-based privacy aware data sharing in cloud," *Journal of Supercomputer*, vol. 62, no. 1, pp. 431–460, 2012.