Cluster Computing
https://doi.org/10.1007/s10586-018-2000-y

Secured and memory overhead controlled data authentication mechanism in cloud computing

A. Pugazhenthi[1] · D. Chitra[1]

Received: 8 December 2017 / Revised: 20 January 2018 / Accepted: 2 February 2018

Abstract

Cloud based intelligent health monitoring system (CIHMS) is smart equipment which facilitates the patients to repossess the health care information without going to the hospital. By recording the health care information of the patients in the cloud environment, this could be attained. Nevertheless, while coming to the part of security of healthcare information is a difficult issue. Cloud computing gives a means of storing and distributing the huge amount of data's from the several users. Storing and distributing data contents via third party server will bring about more security problems. The care should be taken on those contents that are dealing via the cloud storage and the illegal access made by malevolent users must be observed and retracted. In the previous research, Bi-directional storage verification in cloud storage (BD-SVCS) is presented for the cloud environment that will validate each user beforehand giving them authentication. Nevertheless, this technique still found to be short of the safe and competent authentication. Here encryption information could be hacked simply. These issues are eliminated in the proposed methodology called scalable and enhanced key-aggregate cryptosystem (SE-KAC), in which the safe and consistent dealing of data contents is guaranteed. It gives competent security for healthcare information. This technique deals with the issue of outflow of sensitive information and implements a safe CIHMS for giving the security of the related parties and their data. By utilizing this technique, the patient and healthcare institutions could record the health and medical prescription data in encrypted format. For encryption, the double encryption technique with cipher text id known as classes for enhancing the security. The key owner contains a master secret key which is utilized to extract the secret keys for various classes. The extracted key is accumulated and forwards as a single aggregate key to the patient for the purpose of decryption. In addition, unique data shared by numerous users are found out that would be given via the similar set of resources with the intention of evading the annoying resource wastage. This is accomplished by taking the similar data contents needed by the users in the identical virtual machine. An experimental result proves that proposed research methodology SE-KAC attains higher security and less complexity.

Keywords Cloud computing · Cloud based intelligent health monitoring system (CIHMS) · Data sharing · Key-aggregate encryption

1 Introduction

Utilizing the recent technologies in the healthcare organizations is an important method so as to enhance the healthcare services [1–3]. There is a massive demand on healthcare services although there is also a huge unavailability in healthcare professional for instance doctors, nurses and pharmacists. Furthermore, diseases are turn out to be challenging and it is indispensable to develop novel technologies for getting better the patients at the emergence conditions. Cloud based intelligent health monitoring system (CIHMS) system is presented to bring about a healthier solution for the patients at an emergency condition which lessens the problem of the patients to go to the hospital at each and every time. It as well lets the patients to repossess the health care information at the emergency condition devoid of going to the hospital directly.

In the CHIMS, the patient health information is identified by WBSN and kept in the cloud storage and it could be

✉ A. Pugazhenthi
pugal268@gmail.com

[1] Department of Computer Science and Engineering, P. A. College of Engineering and Technology, Pollachi, India

Published online: 16 February 2018

accessed by everywhere and all the time via internet. The healthcare organizations access the data stored in the cloud and give the medical prescriptions dependent upon the patient health details [4]. The data collected by sensor networks and medical prescriptions given by healthcare organizations are extremely subtle and it must be managed properly for guaranteeing patient privacy. Accordingly, it is essential to guarantee the data security all through transmission and similarly storage in the cloud environment. Real-world problems such as security management and scalability with the data size should be focused. Key-aggregate cryptosystem [5] is one among the public-key cryptosystems, which encrypts the message by utilizing public key and likewise with an identifier of cipher text known as class. The key holder contains a master secret key, which is used to take the secret keys for several classes. The extracted key is an aggregated key that is a trampled as a secret key for single class [6].

In this research, scalable and enhanced key-aggregate cryptosystem (SE-KAC) is introduced to offer effective security for healthcare information with high scalability. In this method, Patient and health care organizations record the health data and medical prescriptions in the encrypted format. The double encryption technique is utilized for encrypting the data and furthermore the cipher text id known as classes is utilized. The key owner contains a master secret key, which is utilized to take out the secret keys for several classes. The extracted secret key is combined and compressed as a single key for decryption. Based on the size of the data, the cipher text is produced vigorously. At this point it produces the cipher text id dependent upon the size of the data. The subsequent contributions are as follows:

(1) The WBAN is used to intuit the health data of the patient and it is kept in the storage space of the cloud. The patient health information is encrypted by utilizing double encryption technique and then with cipher text id known as classes. In the double encryption technique, two kinds of secret keys are utilized. First one is normal key and second one is the semi-functional key. The cipher text id is produced animatedly dependent upon size of the data. The master secret key is utilized by the patient for taking out the secret keys for several classes and it is combined for decreasing complexity. The encrypted data is then kept in the storage space of the cloud.

(2) The encrypted data kept in the storage space of the cloud is accessed by the healthcare organizations and by utilizing the aggregated key, it is decrypted. The healthcare organizations analyzed the healthcare data and give the medical prescriptions for the patients.

(3) The healthcare organizations given the medical prescriptions with encrypted format by utilizing as alike as the double encryption technique with cipher text id and it is kept in the storage space of the cloud. The master key is utilized by the patient for taking out the secret keys for several classes and it is combined for decreasing complexity. The encrypted data is kept in the storage space of the cloud.

(4) Then, the patient access the medical prescriptions kept in the encrypted format by utilizing the aggregated key.

(5) The Health Insurance authority (HIA) takes accountable for creating security policies for patients as well as healthcare organizations.

(6) As a final point, the experimentation outcome is examined for the presented SE-KAC and assesses the performance in regard to security and computational complexity.

The research paper is structured in this manner. In section II related works has been discussed. In section III the proposed methodology is presented. Section IV gives the SE-KAC for safeguarding the subtle information. In section V, experimental outcomes are examined. In section VI gives the conclusion and upcoming ideas.

2 Related works

This part discusses about numerous techniques for giving security to the healthcare data kept in the cloud servers.

A method known as cloud-based mobile health monitoring system provides an interface amid the mobile communication and cloud computing techniques for healthcare services. Offering privacy to the patient is a difficult issue in the cloud-based mobile health monitoring system. This method surmounts the difficulty of cloud-based privacy preserving for mobile health monitoring system. Cloud-enabled WBAN architecture is presented by Wan et al. [7] and its applications in pervasive healthcare systems. This technique regards the issue of energy-efficient routing, cloud resource allocation and data security techniques in the cloud storage.

A technique known as secure cloud-based mobile healthcare system is introduced by Khan et al. [8] by utilizing wireless body area networks. There are two stages in this technique: In the primary stage, the multi-biometric based key generation technique is utilized for inter-sensor communication. Next, the electronic medical records are safely kept in the cloud server. A technique known as fully homomorphic encryption (FHE) is introduced by Page et al. [9] for keeping healthcare information in the cloud safely. This FHE technique improves the effectiveness of this technique. Hash based message authentication code (MAC)is suggested by Pawar et al. [10] and MD-5 algorithm for cloud aided mobile health monitoring system, which could conserve data integrity. This technique uses AES technique and outsourcing decryption method for improved privacy and security.

Privacy-aware cloud aided healthcare monitoring system is introduced by Wang et al. [11] by utilizing the notion of compressive sensing. In this plan, the sensitive data samples are got and provide guard to their data. Conserved samples are forwarded to the cloud for storage, processing and distinguish the rebuilt data. Lounis et al. [12] introduced a technique known as an efficient and lithe security technique, which guarantees confidentiality, integrity and likewise fine grained access control to outsourced medical data. Key-aggregate cryptosystem presented by Chu et al. [5] is one among the public-key cryptosystems which encrypts the message by utilizing public key and furthermore with an identifier of cipher text known as class. The key holder contains a master secret key which is used to take out the secret keys for numerous classes. The extracted key is an aggregated key that is a compacted as a secret key for single class.

Li et al. [13] presented a new cryptographic primitive called attribute-based encryption scheme with outsourcing key-issuing and outsourcing decryption, which can implement keyword search function (KSF-OABE). The proposed KSF-OABE scheme is proved secure against chosen-plaintext attack (CPA). Vurukonda and Rao [14] discussed various features of ABE mechanisms by addressing Features like access policy, Attributes Fine graininess access control, Overhead Computation, Efficiency, User Revocation, Scalability and Collision- Resistance.

Nagpal et al. [15] introduced Methods and systems for selective encryption and secured extent quota management for storage servers in cloud computing. Li et al. [16] presented a searchable CP-ABE with attribute revocation, where access structures are partially hidden so that receivers cannot extract sensitive information from the ciphertext. Xu et al. [17] proposed a lightweight searchable public-key encryption (LSPE) scheme with semantic security for CWSNs. LSPE reduces a large number of the computation-intensive operations; thus, LSPE has search performance close to that of some practical searchable symmetric encryption schemes.

Patranabis and Mukhopadhyay [18] provided a novel, efficient and secure solution to this problem by introducing a new public-key searchable encryption primitive referred to as the key-aggregate searchable encryption (KASE). Godle et al. [19] implemented the double encryption and key aggregation on virtual cloud. Here they used the cloud where it will upload the files to cloud. So in that the files will be encrypted and uploaded to cloud.

3 Scalable and enhanced key-aggregate cryptosystem (SE-KAC) for cihms

3.1 Framework

In this part, the architecture of the presented system is explained that facilitates Health care Organizations such as hospital to arrange the data collected by the WBAN. This research technique is highly scalable and it can able to store vast quantity of data gathered by sensors. Henceforth, the security is a significant notion for giving secure communication in the healthcare services.

In order to achieve the security in the CIHMS, the architecture is illustrated in Fig. 1. This architecture takes the patients, Healthcare Organizations, Healthcare Insurance Authority and Cloud Storage. In this structure, so as to collect the details from the patients, the WBAN is utilized. The collected data is encrypted by utilizing the double encryption technique with the usage of the cipher text id that is known as classes for improving the security. In the double encryption technique, usually two secret keys would be produced for encrypting the message two times, with the intention that attackers couldn't simply disclose the contents of the message which is communicated. The two secret keys are known as normal key and the other one is semi-functional key. The normal key is utilized to produce the cipher text known as normal cipher text. At that point, this normal Cipher text is then encrypted by utilizing the semi-functional key. The encrypted data is kept in the cloud storage and it is accessed by the Healthcare organizations. The encryption is accomplished by the double encryption method and with cipher text id known as classes. Then and there, by utilizing the master secret key a specific set of cipher text classes are taken out and forward to the healthcare Organizations. It accesses the cloud storage data by decrypting the data by utilizing the aggregated key as well as semi-functional key. The Healthcare Organizations give the medical prescriptions to the patient dependent upon their health information. The medical prescriptions are encrypted similar to the double encryption technique and by utilizing the cipher text id and stored in the cloud storage and forward the aggregated key to the patients over E-mail.

The encrypted data in the cloud storage could be accessed by the patient and decrypts it by utilizing the aggregated key as well as semi-functional key. At that time, the patients acquire the medical prescriptions from the cloud storage. In the encryption process, the cipher text id is produced dependent upon size of the data vigorously. In this technique, previously determining the amount of cipher text classes, primarily the communication would be set amid the user and the server. The user would forward

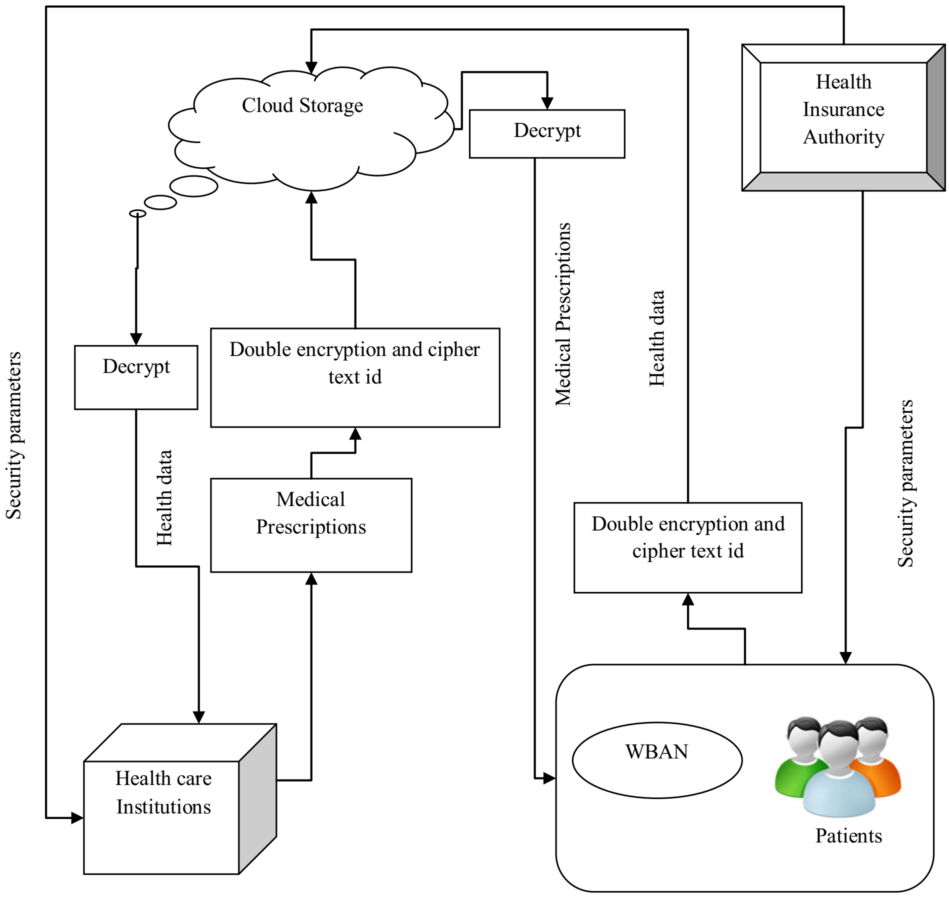

Fig. 1 Proposed Architecture

the quantity of data and the server will send back the amount of cipher text classes that is required to processing the data.

3.2 Key-aggregate cryptosystem with double encryption method

This part focuses on the key-aggregate cryptosystem with double Encryption Technique, which is utilized to communicate amid the healthcare organizations and patients in the CIHMS. The process is in this manner:

KeyGen: In the Key Generation process, the Health Insurance Authority gives two secret keys known as normal key and the semi-functional key. Together with the two secret keys, the master secret key is as well produced for the healthcare organizations and the patients. The security parameters are dispersed to healthcare organizations as well as patients. In this procedure, the WBAN is utilized to collect the data from the patients.

Encrypt 1: The messages are encrypted initially with the normal key to produce the normal-cipher text.

Encrypt 2: At that time the cipher text is then encrypted by utilizing the semi-functional key and likewise with cipher text classes. The cipher text classes are selected vigorously dependent upon the size of the data. At that moment, the patients kept the encrypted data in the storage space of the cloud. The patients utilize the master secret key for taking out the specific set of cipher text classes and forward the aggregated key to the healthcare Organizations. And then it accesses the stored data that is in encrypted format.

Decrypt: The data is decrypted by utilizing aggregated and semi-functional key to access the data. The Healthcare Organizations process the healthcare information and gives the medical prescriptions to the patients that are in encrypted format. The patient access the data stored and decrypts it to acquire the medical prescriptions.

Step 1: Patient → CloudStorage - Patient encrypts the information and kept in the cloud storage.

KeyGen: In this process, the healthcare Insurance Authority (HIA) gives the security parameters for instance normal key (NK), semi-functional key (SK) and master secret key (MS) to the healthcare organizations and patients.

$\mathbf{Encrypt1}(\mathbf{NK}, \mathbf{HD})$: In this process, the patient utilizes the normal key and a Health data (HD). Afterward, the normal cipher text $\mathcal{NC}$_HD is produced for the health information.

$\mathbf{Encrypt2}(\mathbf{SK}, \mathbf{i}, \mathcal{NC}\_\mathbf{HD})$: In this process, the cipher text, index i that denote the cipher text classes and the semi-functional key are utilized for encryption. After that, the semi-cipher text $\mathcal{SC}\_\mathrm{HD}$ is produced for the health information.

$\mathbf{Extract}(\mathbf{MS}, \mathbf{S})$: In this extraction process, a specific set of cipher text classes are surrogated. The input in this process is master-secret key and set S of indices concerning to the numerous classes and it provides the output as the aggregate key (AK) for the set S represented by KS. The aggregated key is forwarded to the healthcare organizations over E-mail.

Afterward, the encrypted data is kept in the cloud storage.

Step 2: CloudStorage → HealthcareInstitutions—The Healthcare Organizations access the data kept in the cloud storage in encrypted format.

$\mathbf{Decrypt}(\mathcal{SC}\_\mathbf{HD}, \mathbf{i}, \mathbf{KS}, \mathbf{AK})$: In this process, the healthcare organizations got the aggregated key for the set KS by extraction process. The input is specific set (KS), aggregated key (AK), index i and semi-cipher text $\mathcal{SC}$ for the health data and acquire the original information.

The healthcare organizations access the encrypted data in the cloud storage and give the medical prescriptions (MPs) in the encrypted format. The encrypted data is kept in the cloud storage.

Step 3: HealthcareInstitution → CloudStorage: The healthcare institutions (HIs) get the data from the cloud storage and provide the medical prescriptions. The medical prescriptions are also encrypted and stored in the cloud storage.

$\mathbf{Encrypt}1(\mathbf{NK}, \mathbf{MP})$: In the first encryption process, the HIs use the normal key and the medical prescriptions (MPs). Then, the normal cipher text $\mathcal{NC}\_\mathrm{MP}$ is generated for the medical prescriptions.

$\mathbf{Encrypt}2(\mathbf{SK}, \mathbf{i}, \mathcal{NC}\_\mathbf{MP})$: In this process, the cipher text, index i that denote the cipher text classes and the semi-functional key is utilized for encryption. Afterward, the semi-cipher text $\mathcal{SC}\_\mathrm{MP}$ is produced for the medical prescriptions.

$\mathbf{Extract}(\mathbf{MS}, \mathbf{S})$: In this extraction process, a specific set of cipher text classes are surrogated. The input is master-secret key and set S of indices concerning to the numerous classes and it provides the output as the aggregate key (AK) for the set S represented by KS. The aggregated key is forwarded to the patients over E-mail. The encrypted medical prescriptions are kept in the cloud storage. Then the medical prescriptions are accessed by the patients.

Step 4: CloudStorage → Patients—The patients access the data in the cloud storage in encrypted format, decrypt it and acquire the medical prescriptions.

$\mathbf{Decrypt}(\mathcal{SC}\_\mathbf{MP}, \mathbf{i}, \mathbf{KS}, \mathbf{AK})$: In this process, the patients obtained the aggregated key for the set KS by extracting process. The input is specific set (KS), aggregated key (AK), index i and semi-cipher text $\mathcal{SC}$ for the medical prescriptions and acquire the original information.

Algorithm for SE-KAC in CIHMS

```
Input as the patients information gathered from WBAN
$P_i$ send the data to the S//S = Server, $P_i$ = Patients
Server gives the data to ECC
Define Number of Cipher text classes
S sends the Number of Cipher text classes to the $P_i$
$P_i$ gets the NK,SK, MS from HIA//NK = Normal key, SK = Semi-functional key, MS = Master secret key and HIA = Health Insurance Authority
// $P_i$ encrypts the HD
$\mathcal{NC}\_\mathrm{HD} \leftarrow \mathrm{Encrypt}\ 1(\mathrm{NK}, \mathrm{HD})$ // $\mathcal{NC}\_\mathrm{HD}$ = Normal cipher text for health data, HD = Health data
$\mathcal{SC}\_\mathrm{HD} \leftarrow \mathrm{Encrypt}\ 2(\mathrm{SK}, \mathrm{i}, \mathcal{NC} - \mathrm{HD})$ // $\mathcal{SC}\_\mathrm{HD}$ = Semi-cipher text for health data, i = index
$\mathrm{KS} \leftarrow \mathrm{Extract}(\mathrm{MS}, \mathrm{S})$ //KS = Particular set of cipher text classes, S = Set of cipher text classes
$P_i$ encrypt the data and stored in cloud storage
//Healthcare Institutions decrypt the data
$\mathrm{HD} \leftarrow \mathrm{Decrypt}(\mathcal{SC}\_\mathrm{HD}, \mathrm{i}, \mathrm{KS}, \mathrm{AK})$ //AK = Aggregated key
Healthcare Institutions decrypt the data and provide the medical prescriptions
$\mathcal{NC}\_\mathrm{MP} \leftarrow \mathrm{Encrypt}\ 1(\mathrm{NK}, \mathrm{MP})$ // $\mathcal{NC}\_\mathrm{MP}$ = Normal cipher text for Medical prescriptions, MP = Medical prescriptions
$\mathcal{SC}\_\mathrm{MP} \leftarrow \mathrm{Encrypt}\ 2(\mathrm{SK}, \mathrm{i}, \mathcal{NC}\_\mathrm{MP})$ // $\mathcal{SC}\_\mathrm{MP}$ = Semi-cipher text for Medical prescriptions
$\mathrm{KS} \leftarrow \mathrm{Extract}(\mathrm{MS}, \mathrm{S})$
Healthcare Institutions encrypt the data and stored in cloud storage
// $P_i$ decrypt the data
$\mathrm{MP} \leftarrow \mathrm{Decrypt}(\mathcal{SC}\_\mathrm{MP}, \mathrm{i}, \mathrm{KS}, \mathrm{AK})$
$P_i$ get the medical prescriptions
```

Algorithm 1 explains the SE-KAC in CIHMS. In this method, patient's health information is sensed by utilizing WBAN and kept in the cloud storage. The data is kept in the encrypted format. Intended for the encryption process, the dual encryption technique is utilized with cipher text classes. The specific cipher text ids are combined, produce the aggregated key and forward to the healthcare Organizations through E-Mail. The health care Organizations access the decrypted data by utilizing aggregated key. The health care Organizations give the medical prescriptions in the encrypted format by utilizing the double encryption technique with cipher text classes. Then and there, the patients decrypt the data by utilizing the aggregated key. Lastly, the patients acquire the medical prescriptions.

4 Numerical results

The experimentation outcomes are examined for the previous and the proposed methodology. The performance assessment of the research is accomplished by matching the research method with the previous methods dependent upon certain parameter. Previous technique introduced a technique known as Bi-directional storage verification in cloud storage (BD-SVCS) is one among the public-key cryptosystems, which encrypts the message by utilizing public key and with an identifier of cipher text known as class. In the current work, SE-KAC is introduced to give effective security for healthcare information. The performance is examined in regard to confidentiality, integrity, user satisfaction degree and resource utilization rate.

4.1 Confidentiality comparison

Table 1 displays the contrast for the previous KAC and BD-SVCS with the current research method SE-KAC in regard to confidentiality. In case the delegation ratio is 0.9, the confidentiality is 96% in the SE-KAC and 88% in KAC technique.

Figure 2 depicts the contrast for the previous KAC and BD-SVCS technique and the presented SE-KAC technique in the CIHMS. X-axis considers delegation ratio. Y-axis considers the confidentiality. Delegation ratio is called as the proportion of the delegated cipher text classes to the total classes. Previous technique known as KAC and BD-SVCS is the public-key cryptosystems, which encrypts the message by utilizing public key and with an identifier of cipher text known as class. Proposed technique known as SE-KAC utilizes dual encryption technique with an identifier of cipher text known as class. The experimental outcomes validates that SE-KAC technique attains high confidentiality while matched up with the KAC and BD-SVCS techniques.

4.2 Integrity comparison

Table 2 displays the evaluation for the previous KAC, BD-SVCS and the presented research SE-KAC in regard to integrity. In case the delegation ratio is 0.9, the integrity is 95.8% in the SE-KAC and 92.3% in KAC technique.

Figure 3 illustrates the evaluation for the previous KAC and BD-SVCS technique with the research SE-KAC technique in the CIHMS in regard to integrity. X-axis considers the delegation ratio. Y-axis considers integrity. Delegation ratio is called as the proportion of the surrogated cipher text classes to the total classes. Previous technique known as KAC and BD-SVCS is the public-key cryptosystems, which encrypts the message by utilizing public key and with an identifier of cipher text known as class. Presented research method SE-KAC utilizes dual encryption technique with an identifier of cipher text known as class. The experiment proves that the SE-KAC technique attains high integrity while matched up with the KAC technique.

Table 1 Confidentiality comparison values

Confidentiality (%)			
Delegation ratio (%)	KAC	BD-SVCS	SE-KAC
0.1	15.1	25.2	27
0.2	25	38	41
0.3	32	44	46.8
0.4	45	58	62.5
0.5	50	69	72
0.6	62	78	79.8
0.7	75	80	83.4
0.8	84	87	89.6
0.9	88	96	98

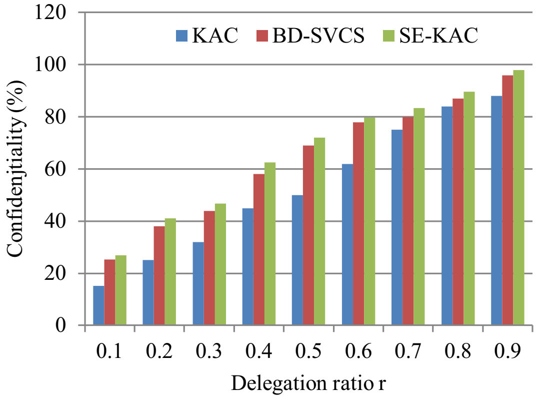

Fig. 2 Confidentiality

4.3 User satisfaction degree

The degree of user satisfaction with a cloud resource can be typically defined as the quality of service offered by the resource to the user. There are generally two ways to evaluating the quality of a service: subjective and objective. A subjective approach demands the feedback information collected from users upon the completion of their resource usage. In this research, we choose to use an objective approach, where a higher degree of satisfaction means a closer match between a user's resource demand and the capability of selected resource.

Table 2 Integrity comparison values

Integrity (%)			
Delegation ratio (%)	KAC	BD-SVCS	SE-KAC
0.1	15.6	21.4	23.5
0.2	22.9	27.5	29
0.3	32.5	38.4	39
0.4	42.1	45.9	47
0.5	51.3	54.9	58
0.6	62.3	68.3	69.8
0.7	72.3	78.3	79.2
0.8	85.2	88.3	89.5
0.9	92.3	95.8	97.2

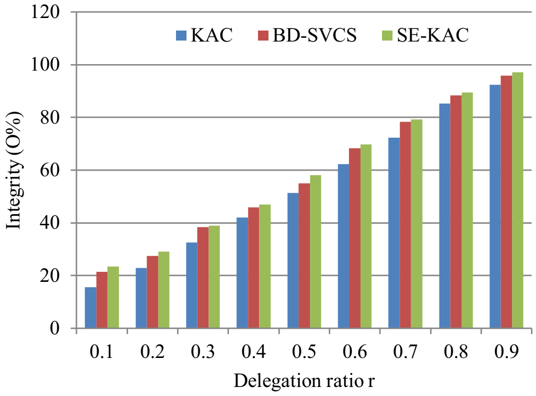

Fig. 3 Integrity

It can be seen from Fig. 4, SE-KAC can achieve more than 80% user satisfaction degree after just two iterations, and it reaches nearly 90% as the two iterations increases to 4. This is due to the SE-KAC algorithm, mechanism implemented and user preference is assigned to each clusters based on the resource requirements of users, which is able to select a sequence of resources where the last one can be closer to the user's request than the previous selections. Assert here that such a continuous feedback integration process would enable the cloud provider to incrementally elicit a user's real need from his/her submitted resource request. Of course, the investigation of this assertion demands human subject analysis and it is left for future studies.

As shown in Fig. 5, with the value of matching threshold changing from 0 to 90%,the user satisfaction degree produced by CUP decreased about 10%.

4.4 Resource utilization rate

Resource utilization rate can be defined differently in different cloud computing environments. Here we simply

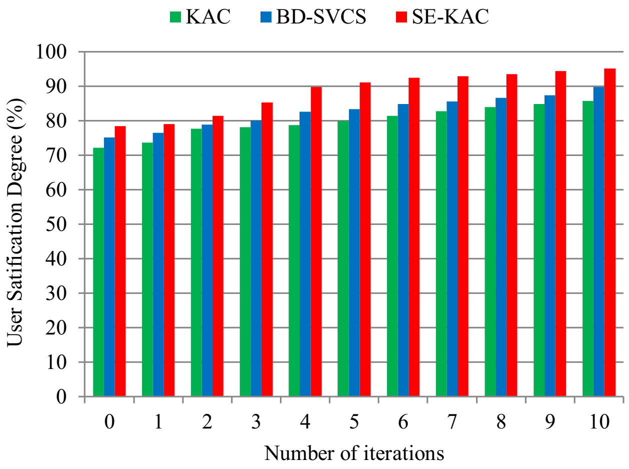

Fig. 4 User satisfaction degree as number of iterations

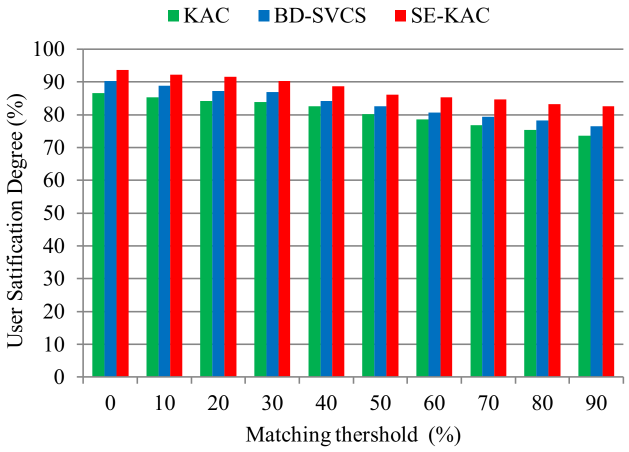

Fig. 5 User satisfaction degree as matching threshold varies

define it as the ratio of the total number of assigned resources to the total number of available resources as CUP starts. This is a critical performance indicator, directly related to the profit a cloud provider can gain.

In this section, perform comparison experiment among KAC, BD-SVCS and SE-KAC to illustrate the performance on resource utilizations rate. It can be seen from Fig. 6 that the resource utilization rate of all methods have increases as the number of users increases from 50 to 300. This is because more user tasks mean more resources will be occupied. However the resource utilization rate of SE-KAC is always higher when compare to other existing methods such as KAC and BD-SVCS. Thus, SE-KAC can achieve a better resource utilization rate by avoiding assigning a higher capability resource to a user task with a lower demand and high priority, leaving more high-capability resources to high-demanding users.

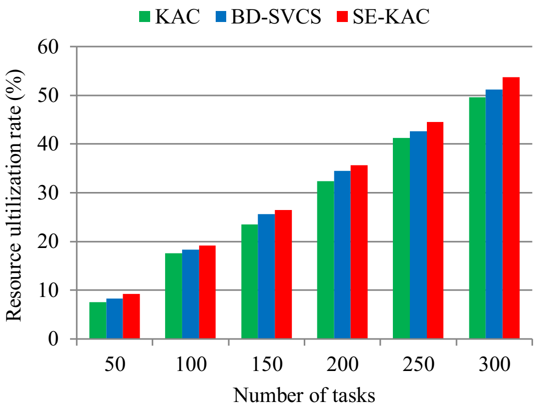

Fig. 6 Resource utilization rate

5 Conclusion

CIHMS decreases the problem of the patients that is utilized to take out the medical records devoid of visiting the hospital. Security in the CIHMS is a noteworthy problem. This research presents a novel technique known as SE-KAC which gives effectual security in the CIHMS. This technique gives high security for the related parties those are included the communication in the CIHMS. This technique utilizes the dual encryption technique for encrypting the data two times and makes use of the cipher text classes for the purpose of encryption. Afterward, the cipher text id are combined and utilized for the purpose of decryption. The cipher text classes are produced in relation to the size of the data. Consequently, this technique aids massive quantity of data's since it produces the cipher text classes vigorously. Experimental outcomes are examined for the research SE-KAC and the previous KAC and BD-SVCS technique in the CIHMS. Outcomes prove that the research technique attains high security in regard to confidentiality and integrity, high scalability while matched up with the previous techniques. In future work, privacy of users can be considered to provide the anonymous and secured authentication of users. Recent encryption algorithms have been applied to prevent the hackers from stealing information. In future it will be better to integrate with the hadoop environment to support the large volume of health care information.

References

1. Goldschmidt, P.G.: HIT and MIS: implications of health information technology and medical information systems. Commun. ACM **48**, 69–74 (2005)
2. Davidson, E., Heslinga, D.: Bridging the IT adoption gap for small physician practices: an action research study on electronic health records. Inf. Syst. Manag. **24**, 15–28 (2006)
3. Klein, R.: An empirical examination of patient-physician portal acceptance. Eur. J. Inf. Syst. **16**, 751–761 (2007)
4. Lounis, A., Hadjidj, A., Bouabdallah, A. and Challal, Y.: Secure and scalable cloud-based architecture for e-health wireless sensor networks. In: *IEEE Conference on Computer Communications and Networks (ICCCN)*, pp. 1–7 (2012)
5. Chu, C.K., Chow, S.S., Tzeng, W.G., Zhou, J. and Deng, R.H.: Key-aggregate cryptosystem for scalable data sharing in cloud storage. In: *IEEE Transactions On Parallel And Distributed Systems*, vol. 25, no. 2 (2014)
6. Lin, H., Shao, J., Zhang, C. and Fang, Y.: CAM: cloud-assisted privacy preserving mobile health monitoring. In: *IEEE Transactions on Information Forensics And Security*, vol. 8, no. 6 (2013)
7. Wan, J., Zou, C., Ullah, S., Lai, C.F., Zhou, M. and Wang, X.: Cloud-enabled wireless body area networks for pervasive healthcare. In: *IEEE in Networks*, vol. 27, no. 5, pp. 56–61, (2013)
8. Khan, F.A., Ali, A., Abbas, H. and Haldar, N.A.H.: A cloud-based healthcare framework for security and patients data privacy using wireless body area networks. In: *The 9th International Conference on Future Networks and Communications (FNC'14)/ The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC'14)/Affiliated Workshops*, vol. 34, pp. 511–517, (2014)
9. Page, A., Kocabas, O., Ames, S., Venkitasubramaniam, M. and Soyata, T.: Cloud-based secure health monitoring: optimizing fully-homomorphic encryption for streaming algorithms. In: *IEEE Globecom 2014 Workshop on Cloud Computing Systems, Networks, and Applications (CCSNA)*, Austin, TX (2014)
10. Pawar, S.S., Phursule, R.N.: Protect integrity of data in cloud assisted privacy preserving mobile health monitoring. Int. J. Inf. Comput. Technol. **4**(13), 1329–1334 (2014)
11. Wang, C., Zhang, B., Ren, K., Roveda, J.M., Chen, C.W. and Xu, Z.: A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing. In: *The 33rd IEEE Conference on Computer Communications (INFOCOM)*, Toronto, Canada (2014)
12. Lounis, A., Hadjidj, A., Bouabdallah, A. and Challal, Y.: Secure and scalable cloud-based architecture for e-health wireless sensor networks. In: *21st International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–7 (2012)
13. Li, J., Lin, X., Zhang, Y., Han, J.: KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Trans. Serv. Comput. **10**(5), 715–725 (2017)
14. Vurukonda, N., & Rao, B. T.: Secure sharing of outsourced data in cloud computing with comparison of different attribute based encryption schemes: a review (2017)
15. Nagpal, A.R., Patil, S.R., Ramanathan, S., Shukla, D., Trevathan, M.B:. *U.S. Patent No. 9,712,495*. U.S. Patent and Trademark Office, Washington, DC (2017)
16. Li, J., Shi, Y., Zhang, Y.: Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage. Int. J. Commun Syst **30**(1), 1 (2017)
17. Xu, P., He, S., Wang, W., Susilo, W., Jin, H.: Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks. IEEE Trans. Ind. Inf. (2017)
18. Patranabis, S., Mukhopadhyay, D.: Key-aggregate searchable encryption with constant-size trapdoors for fine-grained access control in the cloud. IACR Cryptol ePrint Arch **2017**, 318 (2017)
19. Godle, S., Kakade, S., Ithape, K., Giri, S. (2017). double encryption and key aggregation on virtual cloud

A. Pugazhenthi Assistant professor, Dept of Computer Science and Engineering, P.A. College of Engineering and Technology, Pollachi completed his M.E. (Computer Science and Engineering) in 2011 from Pavendar Bharathidasan College of Engineering and Technology, Trichy and another Master degree M.Sc. Software Engineering in Dr. Mahalingam College of Engineering and Technology, Pollachi. he is having 6 years of experience in teaching and also research Experience. he has published 2 papers in International Journals and 8 in National Conferences.

D. Chitra Professor and Head, Dept of Computer Science and Engineering, P.A. College of Engineering and Technology, Pollachi completed her M.E. (Computer Science and Engineering) in 2007 from Kongu Engineering College, Erode, and Ph.D. (Information and Communication Engineering) in Image processing in 2012 from Anna University, Chennai. She has put in 17 years of experience in teaching and research. She has published two patents, 77 papers in International Journals, National and International Conferences, and three more national books for her credit.