International Journal of Engineering & Technology, 7 (4) (2018) 4823-4828

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.20057
Research paper

Scalable and enhanced key-aggregate cryptosystem in cloud-based intelligent health monitoring system

K. Aarumugam [1] *, Dr. P. Sumathi [2]

[1] PhD Research Scholar, PG & Research Department of Computer Science, Government Arts College, Coimbatore- 641 018
[2] Assistant Professor, Department of Information Technology, Government Arts College, Coimbatore- 641 018
**Corresponding author E-mail: aarumugamphd2017@gmail.com*

Abstract

Cloud based Intelligent Health Monitoring system (CIHMS) is a fashionable technology that enables the patients to retrieve health care details directly without visiting the hospital. This can be accomplished by storing the health care details of the patients in the cloud environment. But securing the healthcare details is a challenging problem. In this manuscript, Scalable and Enhanced Key-Aggregate Cryptosystem (SE-KAC) is proposed to provide efficient security for healthcare details. This method addresses the prob-lem of leakage of sensitive information and designs a Secure Cloud-based Intelligent Health Monitoring system for providing the security of the concerned parties and their data. This method allows the patient and healthcare institutions (HIs) to store the health and medical prescription data in encrypted format. For encrypting the data, the double encryption method with ciphertext-id called classes for improving the security. The key owner has a master secret key that is used to extract the secret keys for different classes. The extracted key is aggregated and sends as a single aggregate key to the patient for the decryption process. Elliptic curve is used to generate the ciphertext-id dynamically depends on the data size. An experimental result shows that proposed SE-KAC achieves high security and less complexity.

Keywords: *Cloud Based Intelligent Health Monitoring System (CIHMS); Cloud Computing; Data Sharing; Healthcare Instructions; Key-Aggregate Encryption.*

1. Introduction

Planning to use the modern technologies in the healthcare institutions is s significant approach in many healthcare organizations to improve the healthcare services [1-3]. There is an enormous demand on healthcare services whereas there is high shortage in healthcare professional like doctors, nurses and pharmacists. Additionally, diseases are becoming difficult and it is necessary to develop new technologies for recovering the patients at the emergence situations. Cloud based Intelligent Health Monitoring system (CIHMS) System is a famous technology that provides a better solution for the patients at an emergency situation. CIHMS reduces the burden of the patients to visit the hospital at every time. This system also enables the patients to retrieve the health care details at the emergency situation without the need the visiting the hospital directly.

In the CHIMS, the patient health data is sensed by using WBSN and stored in the cloud storage. The data stored in the cloud can be accessed by anywhere and anytime through internet. The healthcare institutions access the stored data from the cloud storage and provide the medical prescriptions based on the patient health data [4]. The data gathered by sensor networks and medical prescriptions provided by healthcare institutions are highly sensitive and it should be managed correctly for ensuring patient privacy. As a result, it is necessary to ensure security of data during transmission and also storage in the cloud environment. Practical difficulties like security management and scalability with the data size also to be concentrated. Various methods are suggested for securing the health data and medical prescription during the transmission and storage of cloud data. Key-aggregate Cryptosystem [5] is one of the public-key cryptosystems that encrypts the message using public key and also with an identifier of cipher text called class. The key holder has a master secret key that is utilized to extract the secret keys for various classes. The extracted key is an aggregated key which is a compressed as a secret key for single class.

In this work, Scalable and Enhanced Key-Aggregate Cryptosystem (SE-KAC) is proposed to provide efficient security for healthcare data with high scalability. In this method patient and health care institutions store the health data and medical prescriptions in the encrypted format. The double encryption method is used for encrypting the data and also the cipher text id is used which is called classes. The key owner has a master secret key that is used to extract the secret keys for various classes. The extracted secret key is aggregated and compact as a single key for the decryption process. Depends on the data size, the cipher text is generated dynamically. The data is given to the elliptic curve and generates the cipher text id based on the data size. The following contributions are:

1) The WBAN is utilized to sense the patient health data and it is stored in the cloud storage. The patient health data is encrypted by using double encryption method and also with cipher text id called classes. In the double encryption method, two types of secret keys are used called normal key and the semi-functional key. Along with two secret keys the cipher text id called classes is also used for encryption. The cipher text id is generated dynamically based on the data size. The elliptic curve is used to generate the cipher text id. The master secret key is used by the patient for extracting secret keys for various classes and it is aggregated for reducing complexity. The encrypted data is stored in the cloud storage.
2) The encrypted data stored in the cloud storage is accessed by the healthcare institutions and it is decrypted by using the

aggregated key. The healthcare institutions diagnosed the healthcare information and provide the medical prescriptions for the patients.

3) The healthcare institutions provided the medical prescriptions with encrypted format by using as similar as the double encryption method with cipher text id and it is stored in the cloud storage. The master key is used by the patient for extracting secret keys for various classes and it is aggregated for reducing complexity. The encrypted data is stored in the cloud storage.
4) The, the patient access the medical prescriptions stored in the encrypted format by using the aggregated key.
5) The Health Insurance authority (HIA) takes responsible for making security policies for both patients and healthcare institutions.
6) Finally, the experimental result is analyzed for the proposed SE-KAC and evaluates the performance in terms of security and computational complexity.

2. Literature review

A system called Cloud-based Mobile Health Monitoring system [6] was presented. It presents an interface between the mobile communication and cloud computing technologies for the healthcare services. Providing patient privacy is a challenging problem in the cloud-based mobile health monitoring system. This work conquers the trouble of cloud-based privacy preserving for mobile health monitoring system. Cloud-enabled WBAN architecture and its application in pervasive healthcare systems were presented [7]. This method considers the problem of energy-efficient routing, cloud resource allocation and data security mechanisms in the cloud storage.

A method called secure cloud-based mobile healthcare system [8] was presented by using wireless body area networks. There are two phases in this method: In the first phase, the multi-biometric based key generation method is used for inter-sensor communication. Secondly, the electronic medical records are securely stored in the cloud server. A method called Fully Homomorphic Encryption (FHE) [9] was presented for storing healthcare details in the cloud securely. This FHE method enhances the efficiency of the method. Hash based message authentication code (MAC) and MD-5 algorithm technique [10] was presented for cloud assisted mobile health monitoring system that can preserve data integrity. This method utilizes AES method and outsourcing decryption technique for better privacy and security. Privacy-aware cloud assisted healthcare monitoring system [11] was presented by using the concept of compressive sensing. In this design, the sensitive data samples are obtained and give protection to their data. Preserved samples are send to the cloud for storage, processing and differentiate the reconstructed the data.

A method called an effective and flexible security method [12] was presented which assures confidentiality, integrity and also fine grained access control to outsourced medical data. Key-aggregate Cryptosystem is one of the public-key cryptosystems [5] was suggested which encrypts the message using public key and also with an identifier of cipher text called class. The key holder has a master secret key that is utilized to extract the secret keys for various classes. The extracted key is an aggregated key which is a compressed as a secret key for single class.

3. Materials and methods

3.1. Framework

In this section, the architecture of the proposed system is described which enables Health care Institutions like hospital to organize the data gathered by the WBAN. This proposed method is highly scalable and it is capable to store huge amount of data collected by sensors. Hence, the security is an important concept for providing secure communication in the healthcare services.

To accomplish the security in the cloud-based Intelligent Health Monitoring system, the architecture is described in Fig.1. This architecture considers the patients, Healthcare Institutions, Healthcare Insurance Authority and Cloud Storage. In this framework, the WBAN is used to gather information from patients. The gathered information is encrypted by using the double encryption method with the cipher text id which is called classes for enhancing the security. In the double encryption method, there are two secret keys will be generated for encrypting the message twice, so that attackers cannot easily reveal the contents of the message that is transmitted. The two secret keys are called as normal key and semi-functional key. The normal key is used to generate the cipher text which is called as normal cipher text. Then, this normal Cipher text is again encrypted by using the semi-functional key. The encrypted data is stored in the cloud storage and it is accessed by the Healthcare institutions. The encryption is done by using the double encryption and also with cipher text id called classes. Then, using the master secret key a particular set of cipher text classes are extracted and send to the healthcare Institutions. The healthcare Institutions access the data in the cloud storage by decrypting the data using the aggregated key and semi-functional key. The Healthcare Institutions provide the medical prescriptions to the patients based on their health data. The medical prescriptions are encrypted as same as the double encryption method and using the cipher text id and stored in the cloud storage and send the aggregated key to the patients through E-mail.

The patient access the encrypted data stored in the cloud storage and decrypts it by using the aggregated key and semi-functional key. Then, the patients get the medical prescriptions from the cloud storage. In the encryption process, the cipher text id is generated based on the data size dynamically. The original data is given to the elliptic curve cryptography. In the Elliptic curve concept is used that determines the number of cipher text classes to be generated by using the specific classes. In this method, before deciding the number of cipher text classes, first the communication will be initialized between the user and the server. The user will send the amount of data needs to be transmitted and the server will send the number of cipher text classes need to have for processing the corresponding data. This will be decided based on the number of specific classes present in the elliptic curve.

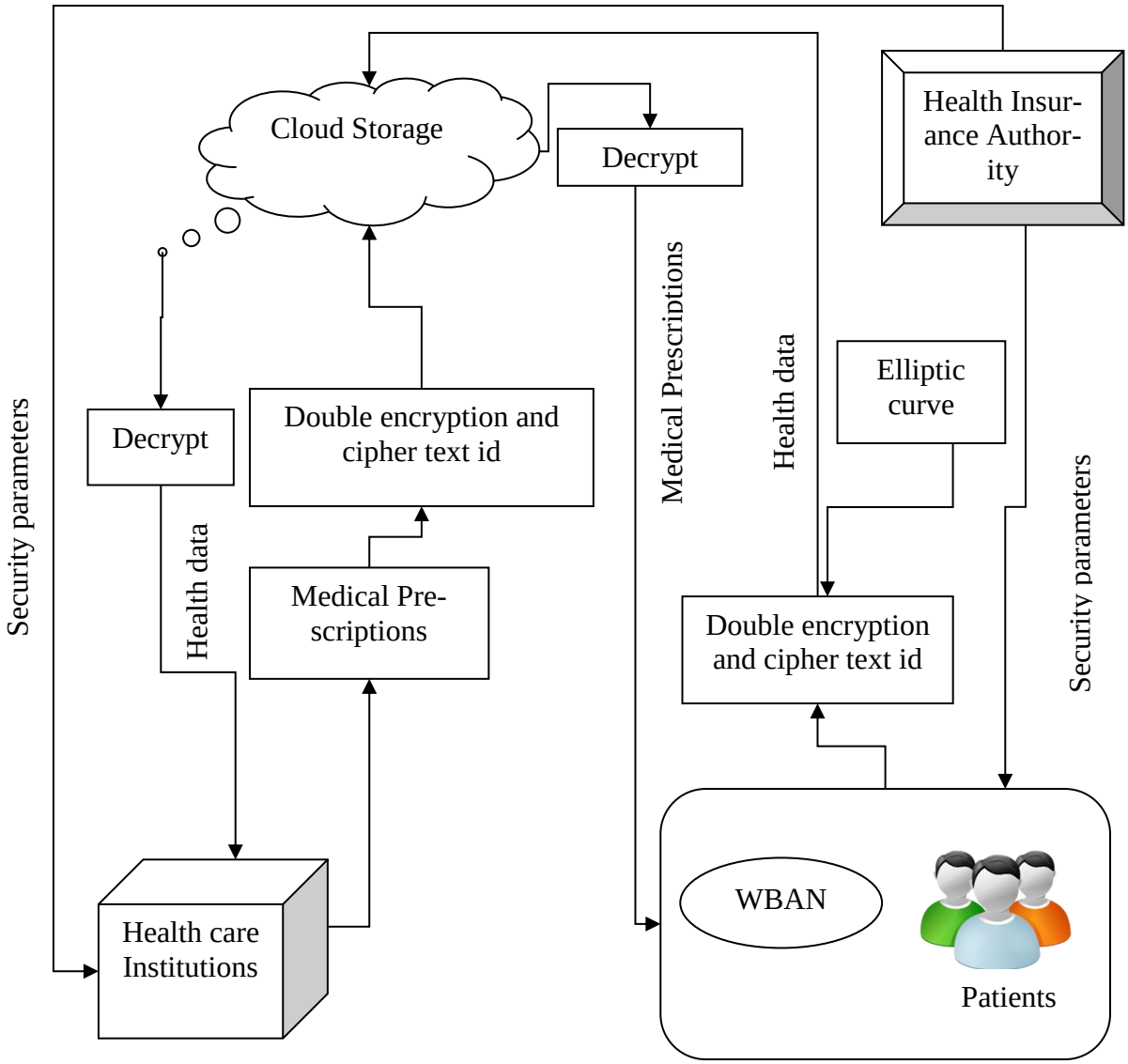

Fig. 1: Proposed Architecture.

3.2. Key-aggregate cryptosystem with double encryption method

In this section, the key-aggregate cryptosystem with double Encryption Method is used in the communication between the Healthcare Institutions and patients in the CIHMS. The process is as follows:

KeyGen: In the Key Generation process, the Health Insurance Authority provides the two secret keys called normal key and semi-functional key. Along the two secret keys, the master secret key is also generated for the healthcare institutions and the patients. The security parameters are distributed to both healthcare institutions and patients. In this process, the information gathering process, the WBAN is used to gather the information from the patients.

Encrypt1: The messages are encrypted firstly with the normal key to generate the normal-cipher text.

Encrypt2: Then the cipher text is again encrypted by using the semi-functional key and also with cipher text classes which is decided by elliptic curve. The cipher text classes are decided dynamically based on data size which is explained in section 3.3. Then, the patients stored the encrypted data in the cloud storage. The patients use the master secret key for extracting particular set of cipher text classes and send the aggregated key to the healthcare Institutions. The healthcare institutions access the stored data which is in encrypted format.

Decrypt: The data is decrypted by using aggregated and semi-functional key to access the data. The Healthcare Institutions process the health data and provides the medical prescriptions to the patients which are encrypted format. The patients access the stored data, decrypted it and get the medical prescriptions.

Step 1: Patient $\rightarrow$ Cloud Storage - Patient encrypts the information and stored in the cloud storage.

KeyGen: In the key generation process, the healthcare Insurance Authority (HIA) provides the security parameters such as normal key (NK), semi-functional key (SK) and master secret key (MS) to the healthcare institutions and patients.

Encrypt $1(\mathrm{NK}, \mathrm{HD})$: In the first encryption process, the patient uses the normal key and a Health data (HD). Then the normal cipher text $\mathcal{NC}$_HD is generated for the health data.

Encrypt $2(\mathrm{SK}, \mathrm{i}, \mathcal{NC}\_\mathrm{HD})$: In the second encryption process, the cipher text, index i which represents the cipher text classes and the semi-functional key is used for encryption. Then, the semi-cipher text $\mathcal{SC}$_HD is generated for the health data.

Extract(MS, S): In this process, a particular set of cipher text classes are only delegated. The input in the extraction process is master-secret key and set S of indices regarding to the various classes and it gives the output as the aggregate key (AK) for the set S denoted by KS. The aggregated key is send to the healthcare institutions through E-mail.

Then, the encrypted data is stored in the cloud storage.

Step 2: Cloud Storage → Healthcare Institutions – The Healthcare Institutions access the data stored in the cloud storage which is in encrypted format.

Decrypt($\mathcal{SC}$_HD, i, KS, AK) : In the decryption process, the healthcare institutions received the aggregated key for the set KS by extracting process. The input of the decryption process is specific set (KS), aggregated key (AK), index i and semi-cipher text $\mathcal{SC}$ for the health data and get the original information.

The healthcare institutions access the encrypted data stored in the cloud storage and provide the medical prescriptions (MPs) in the encrypted format. The encrypted data is stored in the cloud storage.

Step 3: Healthcare Institution → Cloud Storage : The healthcare institutions get the data from the cloud storage and provide the medical prescriptions. The medical prescriptions are also encrypted and stored in the cloud storage.

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

Encrypt 2(SK, i, $\mathcal{NC}$_MP): In the second encryption process, the cipher text, index i which represents the cipher text classes and the semi-functional key is used for encryption. Then, the semi-cipher text $\mathcal{SC}$_MP is generated for the medical prescriptions.

Extract(MS, S): In this process, a particular set of cipher text classes are only delegated. The input in the extraction process is master-secret key and set S of indices regarding to the various classes and it gives the output as the aggregate key (AK) for the set S denoted by KS. The aggregated key is send to the patients through E-mail.

The encrypted medical prescriptions are stored in the cloud storage. The medical prescriptions are accessed by the patients.

Step 4: Cloud Storage → Patients – The patients access the data stored in the cloud storage which is in encrypted format, decrypt it and get the medical prescriptions.

Decrypt($\mathcal{SC}$_MP, i, KS, AK): In the decryption process, the patients received the aggregated key for the set KS by extracting process. The input of the decryption process is specific set (KS), aggregated key (AK), index i and semi-cipher text $\mathcal{SC}$ for the medical prescriptions and get the original information.

3.3. Elliptic curve cryptography-based cipher class generation

In this section, the cipher text classes are generated by using the elliptic curve cryptography. The cipher text classes are created according to the data size. In this method, before determining the number of cipher text classes, the communication will be initialized between the user and the server. Then, the sends the amount of data necessitates to be transmitted and server replies to the user about the number of cipher text classes. This will be determined based on the number of specific classes present in the elliptic curve.

Number of Cipher text classes = ECC(Original data).

Let E is the fixed elliptic curve over a finite field F_p^k and supposeN = |E|. That is, for any point P ∈ E , P added t itself N times creates the identity; NP=id, where the notation nQ for integer and point Q ∈ E means the n-fold addition of Q with itself. The original message is denoted as m as a point X_0 on the elliptic curve E. The elliptic curve problem is based on the fact that this process can only be reversed through the equation,

$$r = qk \ mod \ p$$

In this equation, k is the key, r and q are arbitrary points on the elliptic curve, p is some prime number that defined the elliptic curves finite field.

Algorithm for SE-KAC in CIHMS

1) Input as the patients information gathered from WBAN
2) P_i send the data to the S //S=Server, P_i=Patients
3) Server gives the data to ECC
4) $Number\ of\ Cipher\ text\ classes = ECC(Original\ data)$ //ECC=Elliptic curve
5) S sends the $Number\ of\ Cipher\ text\ classes$ to the P_i
6) 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
7) // P_i encrypts the HD
8) $\mathcal{NC}$_HD ← Encrypt 1(NK, HD) // $\mathcal{NC}$_HD =Normal cipher text for health data, HD=Health data
9) $\mathcal{SC}$_HD ← Encrypt 2(SK, i, $\mathcal{NC}$ − HD) // $\mathcal{SC}$_HD= Semi-cipher text for health data, i=index
10) KS ← Extract(MS, S) //KS=Particular set of cipher text classes, S=Set of cipher text classes
11) P_i encrypt the data and stored in cloud storage
12) // Healthcare Institutions decrypt the data
13) HD ← Decrypt($\mathcal{SC}$_HD, i, KS, AK) //AK=Aggregated key
14) Healthcare Institutions decrypt the data and provide the medical prescriptions
15) $\mathcal{NC}$_MP ← Encrypt 1(NK, MP) // $\mathcal{NC}$_MP =Normal cipher text for Medical prescriptions, MP= Medical prescriptions
16) $\mathcal{SC}$_MP ← Encrypt 2(SK, i, $\mathcal{NC}$_MP) // $\mathcal{SC}$_MP = Semi-cipher text for Medical prescriptions
17) KS ← Extract(MS, S)
18) Healthcare Institutions encrypt the data and stored in cloud storage
19) // P_i decrypt the data
20) MP ← Decrypt($\mathcal{SC}$_MP, i, KS, AK)
21) P_i get the medical prescriptions

Algorithm 1. Describes the SE-KAC in CIHMS. In this algorithm, patient's health data is sensed using WBAN and stored in the cloud storage. The data is stored in the encrypted format. For the encryption process, the dual encryption method is used with cipher text classes. The particular cipher text ids are aggregated, generate the aggregated key and send to the healthcare Institutions via E-Mail. The health care Institutions access the decrypt the data and using aggregated key. The health care Institutions provide the medical prescriptions in the encrypted format by using as same as the dual encryption method with cipher text classes. Then, the patients decrypt the data using the aggregated key. Finally, the patients get the medical prescriptions.

4. Results and discussion

The experimental results are analyzed for the existing and the proposed system. The performance evaluation of the work is done by comparing the proposed work with the existing algorithm based on some parameter. Existing method presented a method called Key-aggregate Cryptosystem (KAC) which is one of the public-key cryptosystems that encrypts the message using public key and also with an identifier of cipher text called class. In the proposed method, Scalable and Enhanced Key-Aggregate Cryptosystem (SE-KAC) is proposed to provide efficient security for healthcare details. The performance is analyzed in terms of confidentiality and integrity in terms of percentage.

Table1 shows the comparison for the existing KAC and the proposed SE-KAC in terms of confidentiality. If the delegation ratio is 0.9, the confidentiality is 96% in the SE-KAC and 88% in KAC method.

Table 1: Confidentiality

Confidentiality (%)		
Delegation ratio (%)	KAC	SE-KAC
0.1	15.1	25.2
0.2	25	38
0.3	32	44
0.4	45	58
0.5	50	69
0.6	62	78
0.7	75	80
0.8	84	87
0.9	88	96

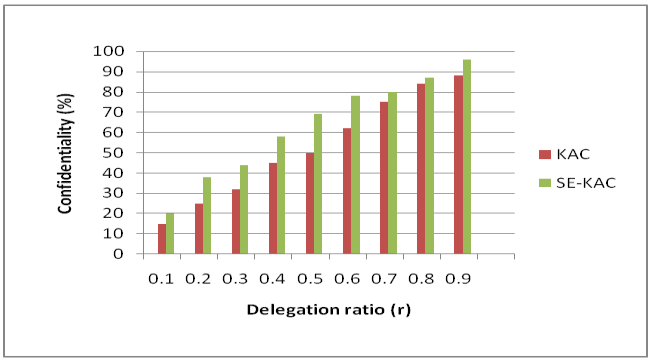

Fig. 2: Confidentiality.

Fig.2 shows the comparison for the existing KAC method and the proposed SE-KAC method in the CIHMS. In the X-axis delegation ratio is taken. In the Y-axis, confidentiality is taken. Delegation ratio is defined as the ratio of the delegated cipher text classes to the total classes. Existing system presented a method called KAC that is the public-key cryptosystems that encrypts the message using public key and also with an identifier of cipher text called class. Proposed method presented a method called SE-KAC that uses double encryption method with an identifier of cipher text called class. The numerical results demonstrate shows that SE-KAC method achieves high confidentiality when compared to the KAC method.
Table2 shows the comparison for the existing KAC and the proposed SE-KAC in terms of integrity. If the delegation ratio is 0.9, the integrity is 95.8% in the SE-KAC and 92.3% in KAC method.
Fig. 3 shows the comparison for the existing KAC method and the proposed SE-KAC method in the CIHMS in terms of integrity. In the X-axis delegation ratio is taken. In the Y-axis, integrity is taken. Delegation ratio is defined as the ratio of the delegated cipher text classes to the total classes. Existing system presented a method called KAC that is the public-key cryptosystems that encrypts the message using public key and also with an identifier of cipher text called class. Proposed method presented a method called SE-KAC that uses double encryption method with an identifier of cipher text called class. The numerical results demonstrate shows that SE-KAC method achieves high integrity when compared to the KAC method.

Table 2: Integrity

Integrity (%)		
Delegation ratio (%)	KAC	SE-KAC
0.1	15.6	21.4
0.2	22.9	27.5
0.3	32.5	38.4
0.4	42.1	45.9
0.5	51.3	54.9
0.6	62.3	68.3
0.7	72.3	78.3
0.8	85.2	88.3
0.9	92.3	95.8

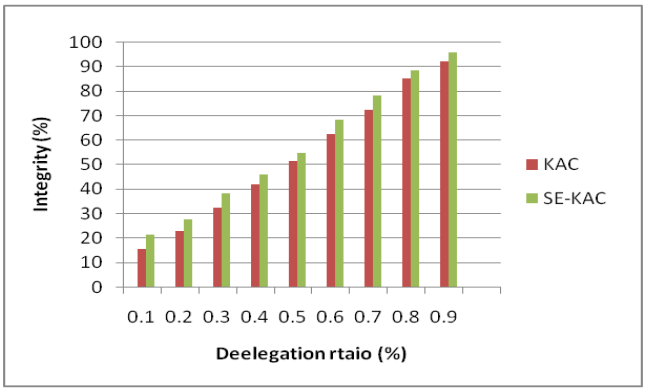

Fig. 3: Integrity.

5. Conclusion

CIHMS reduces the burden of the patients which is used to retrieve the medical records without going to the hospital. Providing efficient security in the Cloud based Intelligent Health Monitoring system (CIHMS) is a significant issue. This work proposes a new method called Scalable and Enhanced Key-Aggregate Cryptosystem (SE-KAC) that provides efficient security in the CIHMS. This method provides high security for the concerned parties who are involved the communication in the CIHMS. This method uses the double encryption method for encrypting the data twice and also uses the cipher text classes for encryption process. Then, the cipher text id are aggregated and used for the decryption. The cipher text classes are generated according to the data size. The cipher text classes are created dynamically using the elliptic curve. So, this method supports enormous amount of data's because it generates the cipher text classes dynamically. Experimental results are analyzed for the proposed SE-KAC and the existing KAC method in the CIHMS. Results show that the proposed method achieves high security in terms of confidentiality and integrity, high scalability when compared to the existing method.

References

[1] Goldschmidt PG (2005), HIT and MIS: implications of health information technology and medical information systems. *Communications of the ACM*, 48(10), pp. 68-74. https://doi.org/10.1145/1089107.1089141.

[2] Davidson E, & Heslinga D (2006), Bridging the IT adoption gap for small physician practices: An action research study on electronic health records. *Information Systems Management*, 24(1), pp. 15-28. https://doi.org/10.1080/10580530601036786.

[3] Klein R (2007), An empirical examination of patient-physician portal acceptance. *European Journal of Information Systems*, 16(6), pp. 751-760. https://doi.org/10.1057/palgrave.ejis.3000719.

[4] Lounis A, Hadjidj, A, Bouabdallah A, and Challal Y (2012), Secure and Scalable Cloud-based Architecture for e-Health Wireless Sensor Networks, In *IEEE Conference on Computer Communications and Networks (ICCCN)*, pp. 1 – 7. https://doi.org/10.1109/ICCCN.2012.6289252.

[5] Chu CK, Chow SS, Tzeng WG, Zhou J, and Deng RH (2014), Key-aggregate cryptosystem for scalable data sharing in cloud storage. *IEEE transactions on parallel and distributed systems*, 25(2), pp. 468-477. https://doi.org/10.1109/TPDS.2013.112.

[6] Lin H, Shao J, Zhang C, and Fang Y (2013), CAM: cloud-assisted privacy preserving mobile health monitoring. *IEEE Transactions on Information Forensics and Security*, 8(6), pp. 985-997. https://doi.org/10.1109/TIFS.2013.2255593.

[7] Wan J, Zou C, Ullah S, Lai CF, Zhou M, and Wang X (2013), Cloud-enabled wireless body area networks for pervasive healthcare. IEEE Network, 27(5), pp. 56-61. https://doi.org/10.1109/MNET.2013.6616116.

[8] Khan FA, Ali A, Abbas H, and Haldar NAH (2014), A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. *Procedia Computer Science*, 34, pp. 511-517. https://doi.org/10.1016/j.procs.2014.07.058.

[9] Page A, Kocabas O, Ames S, Venkitasubramaniam M, and Soyata T (2014), Cloud-based secure health monitoring: Optimizing fully-homomorphic encryption for streaming algorithms. In *Globecom Workshops (GC Wkshps)*, pp. 48-52. https://doi.org/10.1109/GLOCOMW.2014.7063384.

[10] Pawar SS, and Phursule RN (2014), Protect integrity of data in cloud assisted privacy preserving mobile health monitoring. *International Journal of Information & Computation Technology*, 4(13), pp. 1329-1334.

[11] Wang C, Zhang B, Ren K, Roveda JM, Chen CW, and Xu Z (2014), A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing. In *INFOCOM, 2014 Proceedings IEEE*, pp. 2130-2138. https://doi.org/10.1109/INFOCOM.2014.6848155.

[12] Lounis A, Hadjidj A, Bouabdallah A, and Challal Y (2012), Secure and scalable cloud-based architecture for e-health wireless sensor networks. In *21st international conference on Computer communications and networks (ICCCN), IEEE*, pp. 1-7. https://doi.org/10.1109/ICCCN.2012.6289252.