Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 4, 755-761

Enchanced Environmental Security Awareness Data Storing In Cloud Provider

S Selvakumar*, K Manikandan, S Giriranjan
*Associate Professor,Dept. of CSE,Agni college of Technology,Chennai.
Assistant Professor,Dept. of NWC,SRMIST,Kattankulathur.
Assistant Professor,Dept of CSE,VelTech Rangarajan Dr. Sangunthala R&D Institute of science and Technology,Chennai.

Abstract

The Security and Scalability aware Key based Encryption Scheme (SS-KES) is proposed in this research effort to provide efficient security for healthcare and environmental data while also allowing for great scalability. This approach encrypts health data and medical prescriptions and is used by patients and health-care institutions. Encrypting data is accomplished by the use of a double encryption mechanism, as well as cypher text ids or classes. The primary key, known as the master key, is held by the key holder and is used to extract secret keys for each class. The extracted key is a merged key that is used as a single key during the decryption process. It is determined by the amount of data and the cypher employed.

Keywords—*SS-KES; CIHMS; Cipher text id*

I. INTRODUCTION

A well-known technology is the Cloud-based Intelligent Health Monitoring System (CIHMS), which provides patients with a better solution in emergency situations. In the CHIMS, WBSN is utilised to interpret patient health data, which is then saved in the cloud. Data in the cloud can be accessed anytime, anywhere via the internet. Cloud storage is used by healthcare organisations to access data and give medical prescriptions based on patient health information. Healthcare facilities' sensor network data and medical prescriptions are particularly sensitive, and they must be appropriately managed to preserve patient privacy. As a result, data security must be guaranteed both during transmission and storage in the cloud. Practical challenges like as data accessibility and protection must also be addressed..

II. SECURITY AND SCALABILITY CONCERNED DATA MANAGEMENT IN CLOUD ENVIRONMENT

The architecture of the proposed system is outlined in this part, which allows healthcare facilities such as hospitals to organise the data collected by the Wireless Body Area Networks (WBAN). This approach is extremely accessible and capable of storing large amounts of data collected by sensors. As a result, security is a crucial notion in enabling secure communication in healthcare.

To accomplish this, security has been utilised on the internet Smart Monitoring And Diagnosis. This method takes into account patients, healthcare facilities, healthcare insurance authorities, and cloud storage. Throughout this framework, the WBAN is employed to collect patient information. Using the second encryption process, the acquired data is encrypted with the unique id of the cypher text and named classes for improved security. Two secret keys are generated for encrypting the communication twice in the double encryption strategy, making it difficult for attackers to decrypt the contents of the transmission. The private keys are the standard and semi-secret keys.

The semi-functional key is used to encrypt the standard encryption technique once more. Health systems may have access to the encrypted data because it is kept in the cloud. Dual encryption and cypher text named classes are used to encrypt the files. The secret key of the masters is used to retrieve a specified collection of cypher text classes and deliver them to medical institutions. An aggregated key and a semi-functional key are used by the health systems to decrypt data in cloud storage. Patients are given medical prescriptions based on their health data by healthcare facilities. The medical prescriptions are encrypted using a two-factor authentication mechanism.

The patient decrypts the encrypted data stored in the cloud storage with the uniform key and semi-

function key. The patient then calls the doctor's prescription from the cloud. During encryption, the ciphertext identifier is dynamically generated according to the size of the data. Elliptic curve encryption is used to encrypt raw data. The number of cypher text classes that can be created using classes is calculated using the elliptic curve concept. The user and server's communication will be allotted before deciding on the amount of cypher text classes. The user will send and the service will receive the massive amount of data that will be transferred.

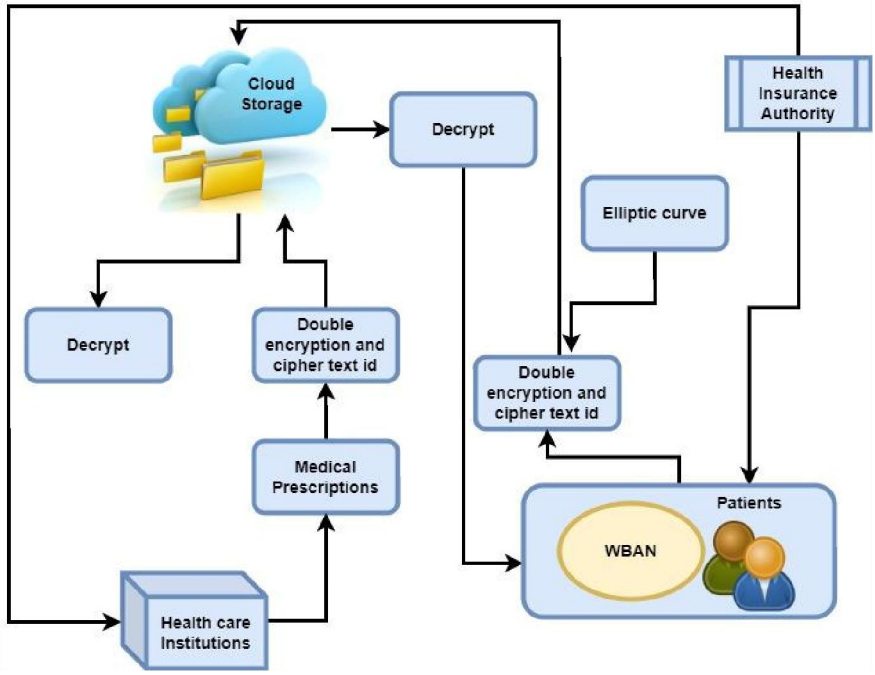


Fig-1Secured Data Storing in Cloud Service Providers

III. DOUBLE ENCRYPTION METHOD IN A KEY-AGGREGATE CRYPTOSYSTEM

The decryption key is made more powerful in this research work via allow it to decrypt multiple cypher texts without altering its size. to "create an effective public key encryption method that supports supple delegation in the sense that any subset of the cypher texts (generated by the encryption method) can always be reversed by a constant-size decryption key (created by the master secret key owner)". They propose the Security and Scalability aware Key-based Encryption Scheme to address this issue (SS-KES).

The user wants the information to be encrypted in SS-KES, and it comes under the public key, which is also beneath the class, which is an individual identifier of cypher text. The cypher texts are also classified into various types of classes in this case. The master secret key belongs to the owner of the key, and it is used to secretly extract keys from a variety of classes. Most significantly, these keys serve as an aggregate key, allows the secret key for a single class to all be compact without using the keys' energy. Decryption energy for some other cypher text groups, on the other hand, is reduced. The information can be passed to Bob as a sibling based on this result.

To get the most out of the improved methodology, the cypher text classes for various types of needs should be suitable for various types of public keys. For the time being, this is reasonable, and it rejects the way of hierarchy that a successful hierarchy requirement desired to a primary information sharing procedure. pk1 and pk2 are appropriate for "personal" and "work" when this parameter is used. It has subparts beneath that it decide whether it may distribute both parameters. "Music" and "game" are some other instances.

In this section, the CIHMS uses a key-aggregate cryptosystem with a double encryption method for communication between healthcare institutions and patients. The steps are as follows:

KeyGen: The health insurance authority offers secret keys, referred to as "normal" and "semi-functional," respectively, during the key generation process. The master secret key is generated in addition to two secret keys for healthcare institutions and patients. Both

healthcare institutions and patients are given the security parameters. The WBAN is used to collect information from patients in this process, which is called as the information collection process.

Encrypt1: To generate the normal-cipher text, the messages are first encrypted with the normal key.

The cypher text is then encrypted a second time, this time using the semi-functional key and elliptic curve-determined cypher document classes. The document classes for cypher are determined dynamically based on the size of the data. The encrypted data is then stored in the cloud by the patients. Patients use the master keys to extract the specified set of cypher text classes and provide the aggregated key to the medical facility. The encrypted data that has been saved is accessible to healthcare facilities. The data is decrypted using aggregated and semi-functional keys.

Step 1:

While uploading the data to the cloud, the patient encrypts it.

The Healthcare Insurance Authority (HIA) provides security parameters such as normal key (NK), semi-functional key (SK), and master secret key (MS) to healthcare institutions and patients during the key creation process.

The patient uses the standard key and health data in the first encryption stage (HD).

The health information is then encoded using standard cypher text.

The cypher text, index I, which represents the cypher text classes, and the semi-functional key are employed in the second encryption procedure.

The semi-cipher text for the health data is then generated.

Step 2:

Healthcare organisations can benefit from the encrypted data saved in cloud storage.

During the decryption procedure, the healthcare institutions extracted the aggregated key for the set KS.

The decryption method requires a certain set (KS), aggregated key (AK), index I, and semi-cipher text as input for the health data and to obtain the original information. Medical prescriptions (MPs) are issued in encrypted form by health authorities, who process encrypted data stored in cloud storage. The information is saved in the cloud and is encrypted.

Step 3:

Medical prescriptions are issued after data is downloaded from cloud storage. In addition, medical prescriptions are encrypted and stored in the cloud.

Healthcare organisations utilise a standard key and medical prescriptions in the first encryption procedure.

After that, the standard cypher text for medical prescriptions is formed.

The cypher text, index I, which represents the cypher text classes, and the semi-functional key are employed in the second encryption procedure.

After that, the semi-cipher text for medical prescriptions is produced.

Only a subset of cypher text classes is delegated in this procedure.

In the extract, the master-secre is viewed as an input.

Step 4:

Patients have access to encrypted data stored in cloud storage, and they decrypt or use to obtain medical prescriptions.

The patients extracted the aggregated key for the set KS during the decryption process.

For medical prescriptions and getting the original information, the decryption process uses a specific set (KS), aggregated key (AK), index I and semi-cipher text as input.

CRYPTOGRAPHY BASED ON CIPHER CLASS GENERATION To ELLIPTIC CURVES :

The cypher text classes in this section are created using elliptic curve cryptography. For public key cryptography based on algebraic structure, elliptic curve cryptography (ECC) using defined elliptic curves in excess of finite fields is utilised. To distinguish itself from non-ECC cryptography, the ECC required a few fundamental keys. ECC employs a relatively small encryption key—a value that must be input into the encryption process—to decode an encrypted message. Other first-generation public key encryption techniques necessitate more processing power than this small key.

IV. PROPOSED ENCRYPTION PROCEDURE

The size of the data determines the structure of the ciphertext class. This procedure establishes communication between the user and the server before determining the number of ciphertext classes. The data is then sent to the server. This is important and the server answers user questions about ciphertext classes. This is determined by the number of different classes of elliptic curves, as shown in the following equation.

$$Number\ of\ Cipher\ text\ classes = ECC(Original\ data)$$

Assume that E is a fixed circular curve that extends beyond the boundary of a finite field. To put it another way, adding P to itself N times produces the identity; NP=id, where nQ signifies integer and point denotes the n-fold addition of Q to itself. The symbol m is a point on the elliptic curve E that represents the original message. The basis for the elliptic curve issues is this execution, which is inverted throughout the Equation below.

$$r = qk \bmod p$$

The key is k, r and q are random points on the elliptic curve, and p is represented by prime numbers that describe the finite fields of elliptic curves.

V. Algorithm for SS-KES in CIHMS

Input as the patients' information acquired from WBAN and transfer the data to the S /S=Server, according to the SS-KES algorithm in CIHMS. =Patients

ECC receives the data from the server /ECC=Elliptic curve

S delivers the message to the HIA, who then receives the NK, SK, and MS from the HIA /NK=Normal key, SK=Semi-functional key, MS=Master secret key, and HIA=Health Insurance Authority.

Encrypts the HD with / =Normal cypher text for health data, HD=Health data / = Semi-cipher text for health data, i=index

Encrypt the data and save it to the cloud.

The data is decrypted by healthcare institutes.

/The abbreviation AK stands for aggregated key.

Healthcare organisations decrypt the information and issue medical prescriptions.

/ =Cypher text for medical prescriptions, MP=Medical Prescriptions / Semi-cipher text for medical prescriptions

Healthcare organisations encrypt data and store it in the cloud. / decrypt the data

Obtain prescriptions from doctors.

The SS-KES in CIHMS is defined by the method above. Patient health data is recorded in WBAN and stored in the cloud using this technology. Information is stored in encrypted form. The double crypto approach is used in the crypto text class of the crypto process. Aggregated keys from each encrypted text ID and by email to the medical facility. The data is acquired and decrypted by health authorities using the aggregated key. Prescriptions are provided in a format encrypted by the medical institution that uses the same double encryption approach as the double encryption method using encrypted text classes. The patient then makes a decision.

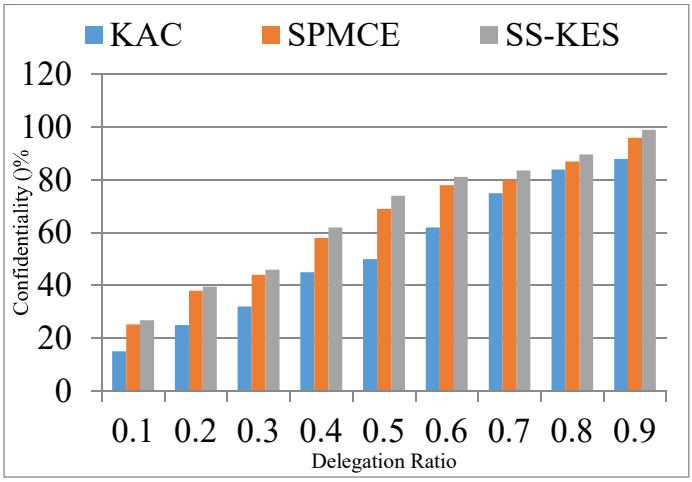
VI. NUMERICAL RESULTS

For both existing and new systems, the experimental results are analysed. Work performance is evaluated by comparing the proposed work with existing parameter-based algorithms. Existing approaches include Keyaggregate Cryptosystem (KAC). This is a public key cryptosystem that encrypts messages using a public key and an encrypted text identifier called a class.To ensure efficient security for healthcare details, the proposed method proposes the Security and Scalability aware Key based Encryption Scheme (SS-KES). In terms of percentage, the performance is evaluated in terms of confidentiality and honesty. The end product is

- Delegation ratio Vs Confidentiality
- Integrity
- Response time
- Security Level
- Processing cycle

Delegation Ratio Vs Confidentiality

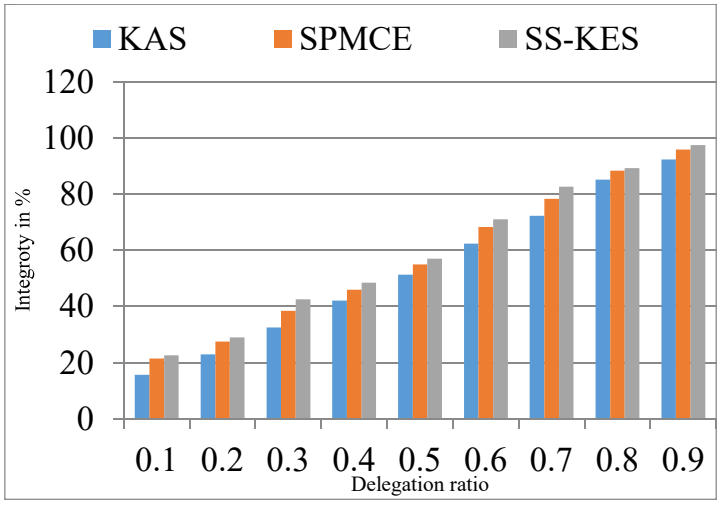
- The delegation ratio is the ratio of cipher content classes to overall classes..
- Increased delegation ratio would increase the confidentiality level which should be higher for the proposed method



- The proposed method SS-KES shows 5% better result than SPMCE and 24% better result than KAC methods

Integrity

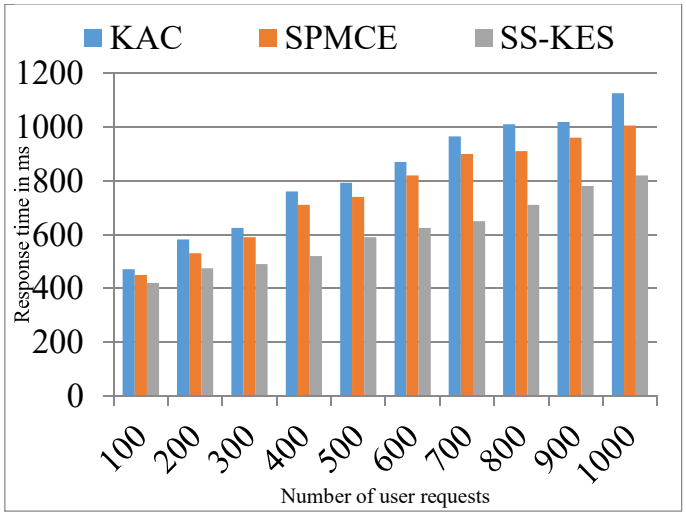
- Integrity is ability of system to preserve the original quality of the cloud stored health data contents



- It shows SS-KES is 4% better result than SPMCE and 13% better result than KAC

Response Time

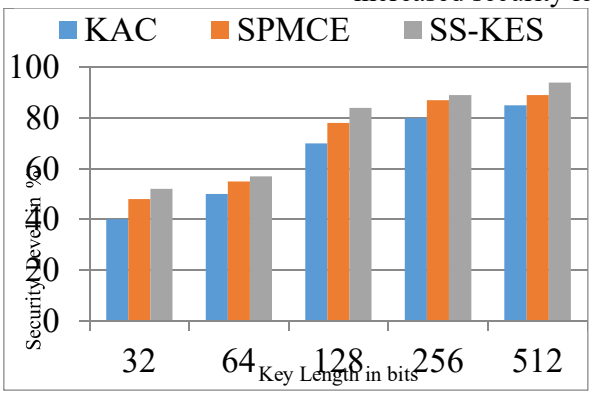
- Response time is described as the amount of time that is consumed to accept and process the user submitted requests



- SS-KES is showing 2% better result than SPMCE and 9% better result than KAC

Security Level

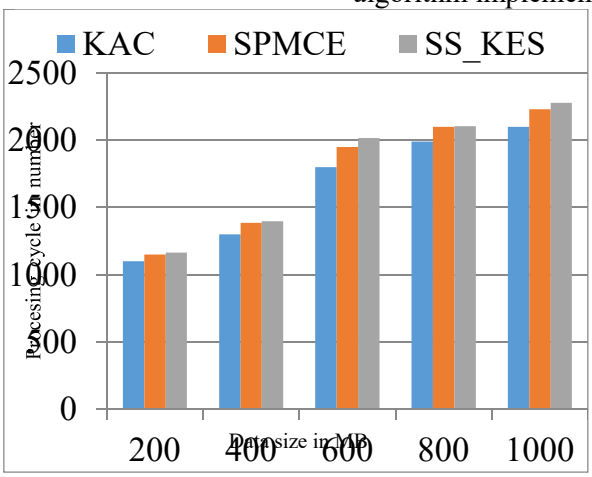
- The symmetric cryptosystem security is a function of the length of the key
- Longer key length would also increase the security level where the proposed system should have increased security level



- The proposed SS-KES shows 5% better result than SPMCE and 16% better result than KAC

Complexity

- Complexity defines the presentation of the present and existing methodologies with respect to the number of processing steps required to complete the algorithm implementation



- SS-KES Shows 2 % better result than SPMCE and 8% better result than KAC method

VII. CONCLUSION

Patients' responsibilities have been reduced by CIHMS, which enables users to access their hospital documents without having to seek medical attention. Quality security in the Cloud-based Intelligent Health Monitoring System (CIHMS) is a major concern. This paper introduces the Protection and Flexibility aware Key based Encryption Scheme, a novel technique for offering appropriate security in the CIHMS (SS-KES). This method guarantees a secure network for all parties involved in CIHMS communication. This procedure encrypts the data twice using the double encryption method and the cypher text classes. After that, the cypher text IDs are computed.

VIII. REFERENCES

[1] Bourouis, A., Feham, M and Bouchachia, A. (2012). A new architecture of a ubiquitous health monitoring system: a prototype of cloud mobile health monitoring system.

[2] Chen D and Zhao H., (2012). Data security and privacy protection issues in cloud computing. International conference on computer science and electronics, engineering, pp. 647–651.

[3] Chu, C.K., Chow, S.S., Tzeng, W.G., Zhou, J and Deng, R.H., (2014). Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 468-477.

[4] Habib, S.M., Varadharajan, V and Mühlhäuser, M., (2013). A trust-aware framework for evaluating

security controls of service providers in cloud marketplaces. In 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 459-468.

[5] Delerablée, C., Paillier, P and Pointcheval, D., (2007). Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In International Conference on Pairing-Based Cryptography, pp. 39-59.

[6] Hwang, K and Li, D., (2010). Trusted cloud computing with secure resources and data coloring. IEEE Internet Computing, vol. 14, no. 5, pp. 14-22.