Computer Systems Science & Engineering
DOI:10.32604/csse.2022.022024
Article

Tech Science Press

QKD in Cloud-Fog Computing for Personal Health Record

L. Arulmozhiselvan* and E. Uma

Department of Information Science and Technology, Anna University, Chennai, 600025, India
*Corresponding Author: L. Arulmozhiselvan. Email: arulmozhiselvan@auist.net

Received: 25 July 2021; Accepted: 08 October 2021

Abstract: Cloud computing is a rapid growing technology which delivers computing services such as servers, storage, database, networking, software and analytics. It has brought a new way to securely store and share information and data with multiple users. When authorized person access these clouds, the released data should not compromise any individual's privacy and identity should not be revealed. Fog Computing is the extension of cloud with decentralized structure which stores the data in locations somewhere between the data source and cloud. The goal of fog computing is to provide high security, improve performance and network efficiency. We use quantum key distribution to produce and distribute key which change its quantum state and key, when key is known by mediator and it has ability to detect presence of mediator trying to gain lore of the key. In this paper, we introduced sugar-salt encryption which overcomes brute-force attack in effect delivers phony data in return to every incorrect guess of the password or key.

Keywords: Security; cloud computing; fog computing; quantum key distribution; sugar-salt encryption

1 Introduction

Cloud computing is everywhere. Cloud components are made up of three elements such as client, datacenter and distributed servers. Each of them has several purposes and functional role in delivering cloud service. The term service in cloud computing denotes the reusable and components across network. It is paid for used service and has following advantages: low barrier, large scalability, multitenancy and device independence. Cloud provides Software as a Service (SaaS) where we use software which is not managed and maintained by us.

The provider does all upgrades and run infrastructure. Some applications include analytics, accounting, video conferencing, IT service management, customer resource management and web content management. The benefits of using SaaS are better marketing, security, reliability and more bandwidth. Platform as a Service (PaaS) is another delivery model that provides all the resources needed to build the applications and service from internet. It is found on systems: add-on developmental facilities, standalone environment and application delivery environments. Infrastructure as a Service (IaaS) provides resources such as server, network equipment, memory, CPU and storage. It involves service level agreement, hardware, network, internet connectivity, platform virtualization environment and utility computing. These applications help business in operational, economic and staffing.

Cloud has responsibility in securing data not only in security issue but also with operating teams and development. Businesses in today are ready to provide application that protects financial data, personal data and medical data. To avoid risk, cloud service provider should provide security at each level from data collection to data delivery. Various vulnerabilities are solved by skilled specialist. There are requirements to develop mechanism in order to preserve security of medical data in healthcare system integrated with cloud-fog-edge architecture in IoT applications [1]. The growth of storage continues at momentous rate. Due to workload of data in analytics and multimedia applications, storage demand is becoming high.

Most of IT organizations came forward to use shared cloud services by reducing their cost of IT infrastructure. As cloud provides flexibility, it matches requirement of workloads and provides better solution to storage demand. No matter where data, hardware, platform and format but it can be accessed through cloud. It is impossible for person to sit alone to manage and analyze data in hardware.

To protect cloud system, data and infrastructure, cloud security has policy, controls, procedures and technologies. These measures are to protect data and privacy of patient/user by authentication. For business data protection, they transfer data to cloud but in-between transition they face many security threats. It is evolving day by day and researchers still trying to find better solution. It is necessary that cloud service provider must provide best security in no way to compromise the user. Methods to provide security to some extent include VAPT (Vulnerability Accessibility Penetrating Testing), Firewall, Data encryption and BIOS password.

Any cyber-attacks can be categorized as follows: client side, network and server side. Major threats include data breaches, data loss, network hijacking and insecure application [2]. Cloud introduces more privacy concern in identity of persons. The privacy can be about personal information, behavior, communication and privacy of person [3]. Various technology and methods are integrated to solve privacy issues faced by cloud. The major techniques and methods include encryption and decryption, information hiding is tested and used till now [4,5].

Fog is extension of cloud that contains multiple nodes which are directly connected to physical devices. It acts as mediator between hardware and servers. It regulates the process of data which is sent to server and data with less security are processed in the fog node itself. It helps cloud server to process data, analyze and store efficiently.

By integrating fog with cloud, it achieves low latency, power efficiency and low bandwidth. It provides high security with better user experience to data stored in fog and cloud. Fog has various components and functions which are used for multiple purposes. IoT devices collects data which is passed through the gateways. It includes endpoints, routers and switches of both wired and wireless. Edge nodes are used to collect data from patient or user. The fog nodes are connected with core network, servers, routers and cloud devices.

Honey encryption (HE) is to encrypt messages using low min-entropy keys such as passwords. HE is designed to produce ciphertext, when decrypted with number of incorrect keys, returns tenable but sham plaintexts called honey messages. It provides high security which withstands brute-force attacks. It can also provide fence against partial disclosure of high min-entropy keys. To showcase this improvement, built a concrete HE schemes for password-based encryption of RSA secret keys and credit card numbers. The key challenges are development of applicable instances where new type of randomized message is encoded using scheme called Distribution-Transforming Encoder (DTE) and analysis of expected maximum loading of bins in various kinds of balls-and-bins games.

Quantum Key Distribution (QKD) is used to transmit cryptographic keys using quantum property of photons in beam of laser securely. It uses individual photons for each data that are exchanged between two users. Each photon holds single bit of data. The photons are coded in binary 1's and 0's which are determined using the states of the photon as polarization or spin. It makes possible to transmit keys without being hijacked.

Quantum Key Distribution exploits mechanics of quantum to transmit keys between two parties securely. The key challenge is getting both parties in a communication to agree same key without being hijacked by mediator. Quantum key distribution uses beam of lasers to transmit keys. While mediator interrupts the beam, grasping wisdom of key, there is a change in quantum property, making keys useless to an assailant.

At the sender's side, laser engenders a sequence of photons, each in horizontal or vertical of two polarizations. The polarization of photon is measured at receiver's side. If a listener hijacks the photon to regulate its polarization, the photon is destroyed in process and the listener had to generate new photon to send the newly created duplicate photon to the receiver. To determine the error rate, the states of photons are compared by receiver and sender in separate channel and determine if the session is secure. Due to comparison of process, the photons are destroyed which is not able to use while generating key. If the session is secure, an applicable number of photons are elected as cryptographic key that are used by both the sender and receiver.

2 Related Work

2.1 Cloud Healthcare

Cloud computing is emerging technology with on-demand service and virtualization which provides scalable features and suitable in medical service. Researchers reported that cloud computing provides high performance with health data. Health data refers to Electronic Health Record (EMR), Personal Health Record (PHR) are stored and retrieved securely in cloud with the use of Fog Computing. Fog Computing is the extension of Cloud where data are stored temporarily and analyzed. Electronic Health Record consists of both real and non-real time data whereas Personal Health Record includes microsensors which monitor the health status of patients regularly with chronic disease. Personal health monitoring is a growing trend because of our growing older population, decreasing medical manpower, and numerous innovative healthcare applications.

Healthcare e-services include chronic disease, Electrocardiography (ECG), personal wellness and body fitness monitor. Other innovative products such as headsets, etc., that measure brainwaves to clothes which completely incorporate sensing devices. These monitoring devices are mostly designed to be wearable which is easy and doesn't feel different to measure and monitor health status like other tools present in hospital and Centre [6]. PHR systems offer new ways for personalized healthcare management, but with privacy issues and confidentiality risks. Patients always worry about their data used for other purpose, which destroys confidentiality in a PHR [7]. To access feasibility in e-healthcare lot of works and efforts are required. Researchers in existing system categorized data based on techniques used [8].

There are security issues in mobile computing as attackers hack messaging center and read content where more confidential information is shared *via* SMS. So, an intelligent management system is introduced to avoid such hacks and data breaches [9]. Next, cloud-based, Electronic Health Record (EHR) system was proposed in order to solve the traditional data integration and interoperability problems [10]. In [11], a new cloud framework for medical services was proposed which is pervasive in nature. This platform is used to manage message in case of emergency assistance and establish connection in health care service.

Also, a cloud-based system was proposed in order to avoid risk of trust as third party view the data was reported in [12]. A framework based on cloud with sensor which is app-based is used to collect data in real time for monitoring the health status of patient with chronic disease was presented in [13]. Health data needs high security in order to protect information about patient so the possible approaches to provide security is reviewed in [14]. To address this, a novel cloud-fog based framework for health care services the honey encryption was proposed.

2.2 Honey Encryption

Password Based Encryption (PBE) is used in many applications with encryption and used by most of the system. PBE is used to protect user's confidential data and key is derived from password and salt value. This system is not beyond the brute force attack. Passwords that are stored in database server are easily cracked by attacks. PBE is used to protect the sensitive data which are protected by server database.

If the database breaches, then the database holding the password of sensitive data are taken and there is no use in securing the data. HE connects cryptography to secure the health data which provide high security. Cryptography machinery are applied to decode the message where HE provides security to impart [15]. Different applications have different capability in protecting sensitive data provided by honey encryption. Whether the key is correct or wrong, the decryption process takes message from message space. Due to this feature some valid messages are leaked [16].

Honey Encryption (HE) is introduced which overcomes the problem of traditional Password-based Encryption (PBE). Honey encryption provides security beyond brute-force attack. It is used to protect important data and provide plausible looking data with wrong key. Honey encryption provides security to set of messages that have features like credit card numbers or messages.

Message space consists of message set. It is determined before encryption and all messages are arranged in some order. Then PDF and CDF for each message that occurs in message space are needed. For distribution-transforming encoder (DTE) seed space is needed where each message is mapped to seed range (n-bit binary string). The seed ranges are determined for each message based on PDF and CDF. A message can be transferred to multiple seeds and n-bit seed space is enough to map at least one seed.

Honey Encryption provides two security properties: Semantic security and Message recovery security. In Semantic security, if the keys are used it is impossible to recover original message and in message recovery security, it is impossible to distinguish whether recovered message is valid or not after decryption. In [17], message recovery security has some deficiencies in providing modern security for encryption and has some robust issues in providing the security for authenticated encryption schemes [18,19]. It is clear that by using this type of encryption it is impossible for attacker to gain original message and fooled by honey encryption [20]. The goal of hiding information is achieved by using honey encryption [21].

2.3 Quantum Key Distribution

The most popular cybercrime are identity theft and authentication where attackers enter into user account to steal most sensitive information is increased. The concept of Quantum Key Distribution (QKD) was first proposed in the year 1970s. Security of data on both during communication and storage is highly dependent by digital society.

Computational problems like prime factorization is one of the main reason for security of existing protocols in key distribution for access control [22]. A model QCMC is proposed to strengthen privacy of data security based on quantum cryptography applied in mobile computing devices and protocol is introduced for security based on quantum keys and distance-bounding protocols [23]. The QKD system guarantees security at data transmission. When we discuss the security of network system, we have to consider how to identify [24]. Introducing QKD in cloud is different and new which overcomes all security issues faced and it is verified by using AVISPA tool where intruder is present in order to check its security level [25,26].

QKD is the secure communication to exchange encryption keys only between known parties. The communication uses quantum physics properties which is used to exchange keys and provides high security which is proved. This process involves creation of key and share between them to encrypt and decrypt messages.

QKD works by transmitting photons over fiber optic cables between known shared parties. Each photon consists of quantum state in which photons are sent as stream of zeros and ones called qubits. When photon reaches its receiver end, it travels through beam splitter and force the photon to select random path into collector of photons. Then receiver responds to sender with sequence of photons and compared. This sequence of bits is used to encryption.

In our paper, we proposed sugar-salt encryption and Quantum Key Distribution (QKD) for secure storage and retrieval of Electronic Health Record (EMR) in cloud using fog computing. These implementations overcome the brute force attack and improved performance. This achieves fast response time, low latency and reliability.

3 Proposed Work

Fog computing is extension of cloud computing which works at edge devices from distributed computing. It performs basic data analysis, aggregation and management between gadgets and server. This administration makes up Internet of Things (IOT) to send data to cloud for further analysis and process. Existing system drawbacks are high latency, low response time, lack of resource and low QOS. Multi-level intrusion detection system is implemented for active IDS in cloud computing. The proposed method increases resource availability and contributes optimal use of resources. It also addresses potential threats and manages user.

Fog devices perform storage, computation and communication. It connects sensors with cloud system. It manages all data and cloud connectivity. The cloud-fog gateway is used to send collected data to cloud for storage and data analysis process which is not performed by fog. Fog combined with IoT applications are used in health domain. IoT is easiest goal for attacker to access sensitive data. So, fog assisted IoT used to secure data from attacker. The focus is on confidentiality, integrity, and authentication which is achieved by our methodology. Fog device collect non-real time health data from user through fog terminals and end device that are connected through internet. Fig. 1. describes architecture of proposed system in which collected data are moved to fog layer. The fog layer consists of QKD layer and fog server. Fog server is for temporary storage of data which holds non-sensitive data. QKD layer consists of qkd devices which generate n-bit strings of qubits for sensitive data which detects the presence of mediator trying to gain lore of the key and changing its quantum state on every incorrect guess of key. The key generated by the QKD devices are stored in the fog server. This achieves authentication which is drawback in existing system.

The collected data in fog layer are segmented based on security level and migrated to cloud. The file uploaded in cloud are replaced by alternate data and swapped using sugar-salt encryption technique which overcomes brute force attack. Sugar-salt encryption serves up fake/similar/phony data on every incorrect guess of key. The swapped data are encrypted using AES algorithm. This achieves confidentiality and privacy of data. The query is passed by authorized user to view individual record. The records are maintained by Cloud service provider (CSP). Data users who want to access data need to request data to CSP. The CSP accept request only for authorized user. Once CSP accepts the request send OTP to user to view the data. The user enters OTP in cloud to view file. Key generated by Quantum Key

Distribution and AES algorithm is sent to user through mail along with OTP. The user uses both the key to decrypt and access file. Finally, file is displayed to user by aggregating the data from both cloud and fog.

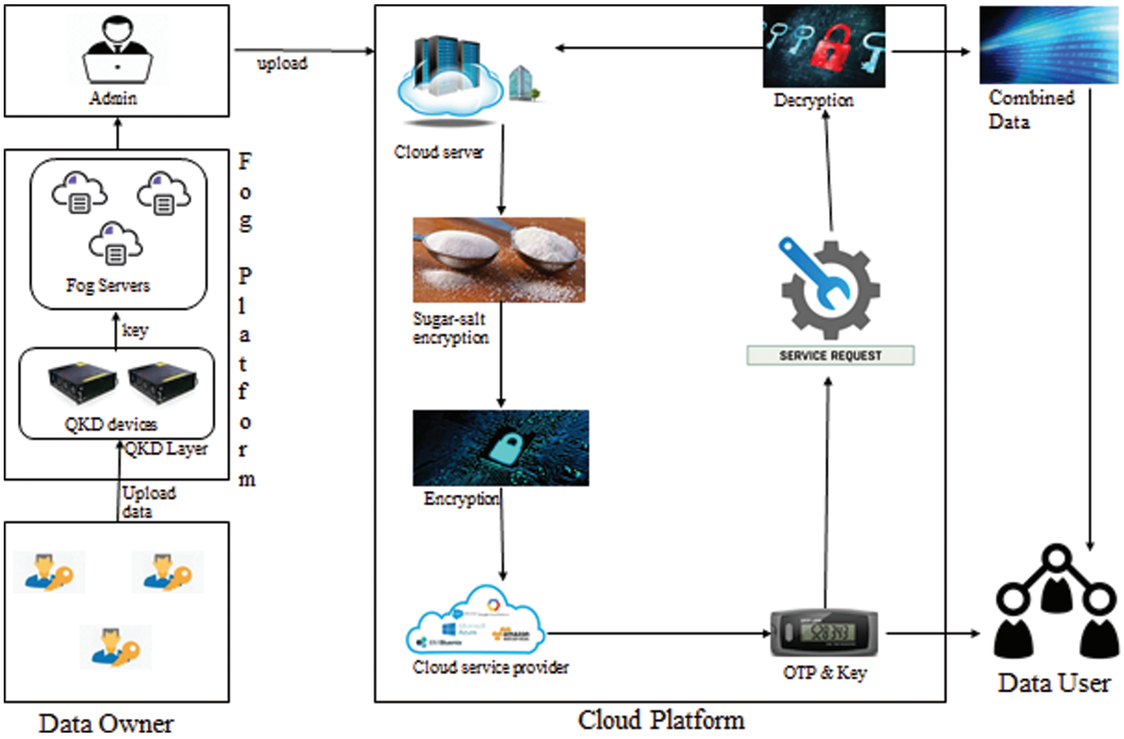

Figure 1: Architecture of sugar-salt encryption in cloud-fog environment

Cloud computing is easy for attacker to target. Fig. 2. depicts overall process of proposed system in flowchart. Proposed system provides efficient resource allocation, better QOS and efficient service. Cloud-fog computing secures the medical data more efficiently as it segments the data based on security level. Data with non-sensitive are stored in the fog layer and more sensitive data are stored in cloud. The attacker either gains the fog data nor cloud data but not the complete report. As he/she needs to find two keys where one is for the fog and another for the cloud. We evaluated the performance of the existing system. We measured the time needed to generate key, time taken to upload the files and memory utilization. Our proposed system takes less time to generate key and for uploading the file. Most of the time are utilized for file upload and download to cloud as it contains more data and files. Thus, the proposed system achieves better performance than traditional methods. It also overcomes brute force attack by implementing sugar-salt encryption.

3.1 Encoding and Decoding Using Distribution

In encoding and decoding, statistical methods are used by SSE, CMF (.) to encode plaintext p_i to ciphertext c_i and decode ciphertext c_i to plaintext p_i. This CMF works as the statistical code

$$c_i = \mathrm{CMF}(\mathrm{p_i}), \text{for encoding}, (\mathrm{c_i}) \in \{0, 1, \ldots, \mathrm{n}\}$$

$$p_i = \mathrm{CMF}^{-1}(\mathrm{c_i}), \text{for decoding}, (\mathrm{p_i}) \in \{0, 1, \ldots, \mathrm{n}\} \tag{1}$$

Therefore, each data in a file can be encoded or decoded in shared files based on statistical properties. Let us take **a** for fog data and **R** for cloud data are matrices of L size, and A and r represents their corresponding vectorized forms. In this paper, p(A|R, ¬) denotes density function which is same as the DTE of Honey Encryption. This distribution is incorporated with Bayesian rule. By using Bayesian chain rule,

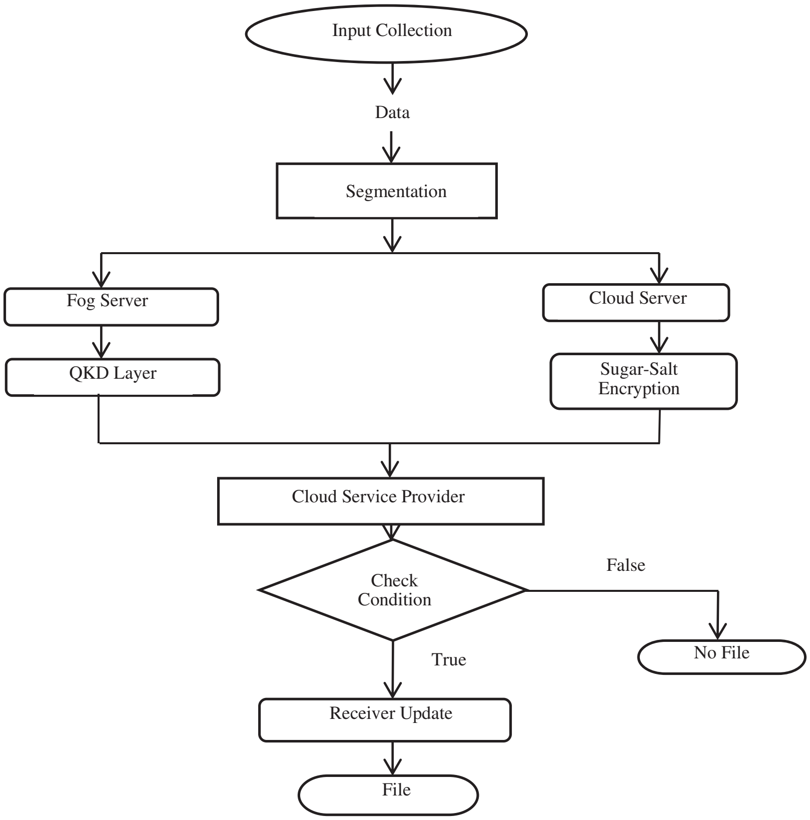

Figure 2: Flowchart of proposed system

$$\mathrm{p}(\mathrm{A}|\mathrm{R},\Psi) = \prod_{\mathrm{i}=1}^{\mathrm{L}} \mathrm{p}(\mathrm{a_i}|\mathrm{A}_{1:\mathrm{i}-1},\mathrm{R},\Psi) \tag{2}$$

In general, the file has the images have grid structure and related with Markovian (two-dimensional) structure because it reduces the complexity of time and space using Markovian blankets.

$$\mathrm{p}(\mathrm{A}|\mathrm{R},\Psi)=\prod_{i=1}^{L} p(a_i|A_{MB(i)},\mathrm{R},\Psi) = \prod_{i=1}^{L} p(a_i|A_{ne(i)},\mathrm{R},\Psi) \tag{3}$$

Here a_i is the n th value of the file, MB(i) and ne(i) denotes the Markov blanket and related values of the n th value. Both encoding and decoding are performed sequentially. The conditional density of the n th value can be further reduced by independence of values in the cloud data such that

$$\mathrm{p}(a_i|A_{ne(i)},\mathrm{R},\Psi) = \mathrm{p}(a_i|A_{ne(i)},r_i,R_{\sim i},\Psi) \tag{4}$$

This distribution can be written by

$$\mathrm{p}(\mathrm{a_i}|\mathrm{A}_{\mathrm{ne(i)}},\mathrm{R},\Psi)=\mathrm{p}(\mathrm{a_i}|\mathrm{A}_{\mathrm{ne(i)}},\mathrm{r_i},\mathrm{R}_{\sim\mathrm{i}},\Psi)\alpha(\mathrm{r_i}|\mathrm{a_i},\Psi)\mathrm{p}(\mathrm{a_i}|\mathrm{A}_{\mathrm{ne(i)}},\Psi) \tag{5}$$

In Eq. (5), there are two factors such as likelihood function and prior function which are explained in Bayesian framework. Both the factors are used in relating the probability of how it fits the cloud data and corresponding related values. Eqs. (2) and (5) are to single cloud data R and its vectorized form r. In this case, both factors have the same influence on posterior function. There are multiple data in cloud instead of single data. So, the equation can be written as

$$\mathrm{p}(\mathrm{A}|\mathrm{R},\Psi) = \prod_{i=1}^{L} p(a_i|A_{ne(i)},\mathrm{R},\Psi) \,\alpha\, \prod_{i=1}^{L}[\prod_{n=1}^{N} p(r_i^{(n)}|a_i,\Psi)]\; p(a_i|A_{ne(i)},\Psi) \tag{6}$$

Now the likelihood and prior factor are defined using normal distribution by

$$\mathrm{p}(r_i^{(n)}|a_i,\Psi) \;=\; N\;(r_i^{(n)};a_i,h^2) \;=\; N\,(a_i;r_i^{(n)},h^2)$$

$$\mathrm{p}(a_i|A_{ne(i)},\Psi) = N\,(a_i;f(A_{ne(i)},\rho^2) \tag{7}$$

It is known that the product of normal distribution becomes normal distribution. Therefore, it can be written as

$$\mathrm{p}(a_i|A_{ne(i)},\mathrm{R},\Psi) = N\,(a_i;\,\mu,\sigma^2) \tag{8}$$

Now the cumulative mass function of the n th value is defined by

$$p_{cmf}^{(i)}(z_k) = \sum_{k=0}^{2^{k-1}} p \frac{p(a_{i=}z_k|A_{ne(i)},R,)}{\sum_{j=0}^{2^{d-1}} p(a_{i=}z_f|A_{ne(i)},R,)} \tag{9}$$

For encryption and decryption with keys, the symmetric algorithm is used as follows,

Let S be a set. A distribution on S is a function p:S = {0, 1…., n}. A Symmetric Encryption scheme SE = (Enc, Dec) is a pair of algorithms for encrypt and decrypt which is defined based on key space K and message space M. The Encryption algorithm Enc takes as input key K ∈ k and message M ∈ m and output ciphertext C ∈ c. The Decryption algorithm Dec takes as input key K ∈ k and ciphertext C ∈ c and outputs message M ∈ m.

SSE = (SSEnc, SSDec) with key space K_1 & K_2 and message space M_1 & M_2.

SS Encryption

```
SSEnc ($K_1$, $K_2$, $M_1$, $M_2$)
$S_1$ ← encode ($M_1$)
$C_1$ ← Enc ($K_1$, $S_1$)
return $C_1$
$S_2$ ← encode ($M_2$)
$C_2$ ← Enc ($K_2$, $S_2$)
return $C_2$
```

SSDecryption

```
SSDec ($K_1$, $K_2$, $C_1$, $C_2$)
$S_1$ ← Dec ($K_1$, $C_1$)
$M_1$ ← decode ($S_1$)
return $M_1$
$S_2$ ← Dec ($K_2$, $C_2$)
```

```
$M_2$ ← decode ($S_2$)
return $M_2$
```

SSCom with message space M_1 and M_2 gives the original message (plaintext) by collecting the data of related items from both Fog and Cloud.

```
SSCom ($M_1$, $M_2$)
O ← $M_1 + M_2$
return O
```

Algorithm 1: Segmentation of Data

```
Input: Files
Output: segmented data
Migrate to fog layer
if qubits are generated {
    Data are segmented
        upload to cloud server based on security
}
```

Algorithm 1 describes the segmentation of data in the fog layer. In fog, the data which are available in local public database are stored. These data require less security which matches the stored record of other patients where the hackers try to steal the data based on this common information. To avoid such situation fog layer segment the data and generate the key using QKD stored in the key generator and in cloud server the other data's are uploaded. The segmented data uploaded to cloud by fog server needs more security as it contains the reports and medicines prescribed by doctors.

Algorithm 2: Secure Storage of Data Using SSE

```
Input: segmented data
Output: report
Begin
Replace file by alternate data and swap
encrypt data using sugar-salt Encryption
for each input data
key generated using AES
online query for collection of data
decrypt using quantum and AES key
end
end
```

Algorithm 2 depicts how to secure the uploaded data securely using SSE. The file contains data and images are changed based on the sugar-salt encryption (SSE) techniques. Once it is changed, encrypt using AES and key is generated which is stored by the cloud service provider. If there is mediator who tries to access the data, it gives the irrelevant data which appears as original similar file. So, the data are more secure which is revealed to only the authorized data user.

The data analysis report of existing and proposed system is given in Tabs. 1 and 2. Based on number of personal records uploaded the overall performance is analyzed considering the time taken for the process for encryption, decryption, computation and performance.

Table 1: Data analysis report (existing system)

No of personal records	Encryption time (sec)	Decryption time (sec)	Computation time (sec)	Performance (sec)	Storage (mb)
10	4.5	4.65	5.836	9.8	23.36
50	5.529	5.756	5.824	8.542	26.45
100	7.902	8.026	4.857	7.265	30.24
200	9.458	9.978	4.582	6.685	35.78
300	11.065	12.036	3.587	6.102	40.36
400	13.258	14.577	3.25	5.268	50.34
450	14.964	16.598	2.894	5.004	62.25
500	15.345	17.854	2.534	4.329	69.74

Table 2: Data analysis report (proposed system)

No of personal records	Encryption time (sec)	Decryption time (sec)	Computation time (sec)	Performance (sec)	Storage (mb)
10	3.45	3.548	5.748	9.504	25.32
50	4.365	4.576	5.736	7.259	25.35
100	6.602	6.789	4.689	6.587	25.24
200	8.625	8.754	4.269	5.874	30.21
300	10.045	11.024	3.254	4.859	34.85
400	12.548	13.847	3.105	3.662	48.54
450	13.987	14.859	2.536	3.425	60.78
500	14.253	15.784	2.102	2.589	58.74

Storage is important paradigm because cloud holds billions of data of several users across the world. Here, it needs less storage as it segments the data and stores in fog sever.

Fig. 3. shows the data analysis report which overcomes the existing system and provides better security. Encryption is used to protect medical records of patients which is stored in cloud prevents from brute force attack and cyber-attacks. The amount of time taken to encrypt is compared with existing algorithms. AES encrypt data in less time i.e., as number of records increases, the time to encrypt decreases and vice versa for decryption and the percentage of encryption and decryption are 90.06% and 88.49%. Computational time is time required for completing process. Based on the rule applied, the computation time calculated which achieves 94.22% and it is low compared to other methods. The overall performance of proposed system is 82.56%. Storage is comparatively low than existing methods and it achieves 91.28% because it segments the data and store data in cloud and as well as in fog based on security level.

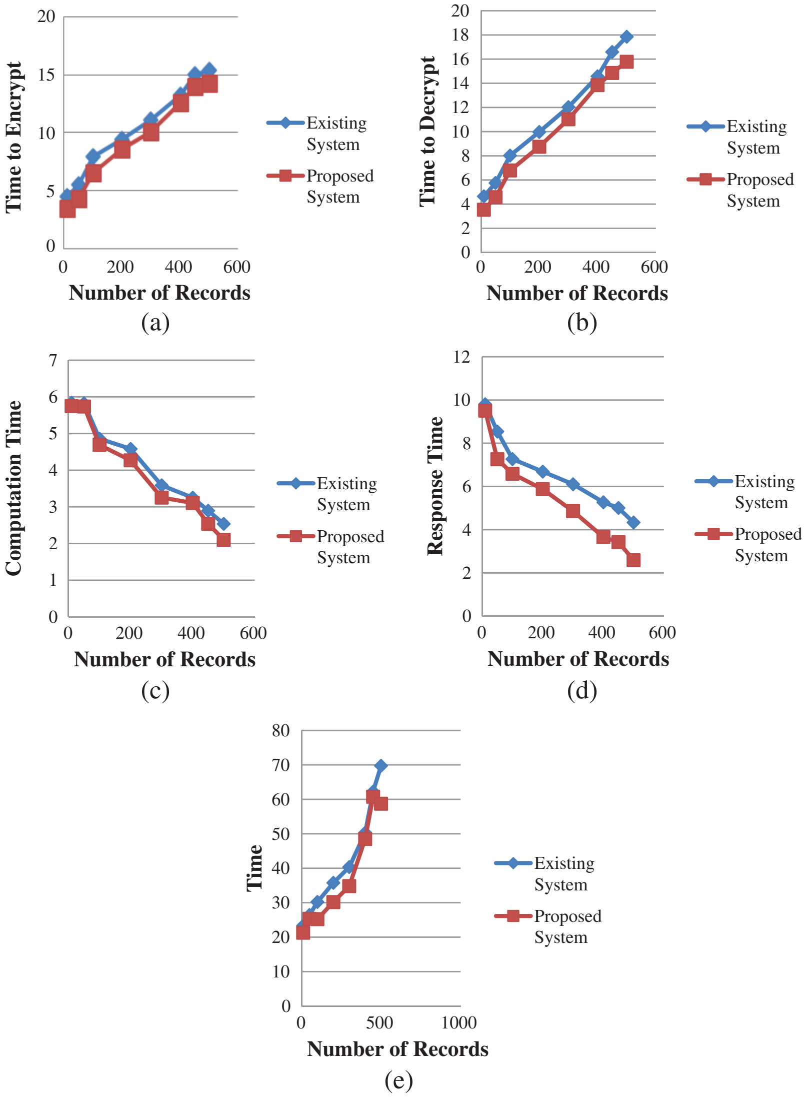

Figure 3: Comparison of data analysis (a) Encryption (b) Decryption (c) Computation (d) Performance (e) Storage

4 Conclusion

Having studied the latest research, it is observed that single technique does not overcome all privacy concern. In this paper, we proposed sugar-salt encryption and Quantum Key Distribution (QKD) which will be better solution for security of medical data. QKD in fog layer collects EMR records and segment based on security level. It generates the key which is stored in key center and moved to cloud. In cloud it encrypts data based on sugar-salt encryption technique where it provides plausible looking data on every incorrect guess of the key. At decryption it uses both quantum key and AES key. Our experimental result shows fast response time and low latency compared to existing system. It resolves the various privacy concerns such as brute force attack, security and reliability. Thus, performance of the system is improved by sugar-salt encryption technique.

Acknowledgement: We show gratitude to anonymous referees for their useful ideas.

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] R. Saha, G. Kumar, M. K. Rai, R. Thomas and S. J. Lim, "Privacy ensured e-healthcare for fog-enhanced IoT based applications," *IEEE Access*, vol. 7, no. 4, pp. 44536–44543, 2019.

[2] X. Wu, R. Jiang and B. Bhargava, "On the security of data access control for multiauthority cloud storage systems," *IEEE Transactions on Services Computing*, vol. 10, no. 2, pp. 258–272, 2015.

[3] E. Mok, A. Samsudin and S. F. Tan, "Implementing the honey encryption for securing public cloud data storage," in *First EAI Int. Conf. on Computer Science and Engineering*, Malaysia, pp. 1–9, 2017.

[4] N. Tyagi, J. Wang, K. Wen and D. Zuo, "Honey encryption applications," 6.857 *Computer & Network Security (Massachusetts Institute of Technology)*, pp. 1–16, 2015.

[5] C. H. Tseng, S. H. Wang and W. J. Tsaur, "Hierarchical and dynamic elliptic curve cryptosystem based self-certified public key scheme for medical data protection," *IEEE Transactions on Reliability*, vol. 64, no. 3, pp. 1078–1085, 2015.

[6] J. Li, "Ensuring privacy in a personal health record system," *Computer*, vol. 48, no. 2, pp. 24–31, 2015.

[7] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab *et al.,* "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, no. 10, pp. 464–478, 2017.

[8] R. Sahu and M. S. Ansari, "Securing messages from brute force attack by combined approach of honey encryption and blowfish," *International Research Journal of Engineering and Technology*, vol. 4, no. 9, pp. 1019–1023, 2017.

[9] A. Bahga and V. K. Madisetti, "A cloud-based approach for interoperable electronic health records (EHRs)," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 5, pp. 894–906, 2013.

[10] C. He, X. Fan and Y. Li, "Toward ubiquitous healthcare services with a novel efficient cloud platform," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 1, pp. 230–234, 2012.

[11] N. Penghao, C. Yuan and L. Chong, "Quantum authentication scheme based on entanglement swapping," *International Journal of Theoretical Physics*, vol. 55, no. 1, pp. 302–312, 2016.

[12] A. Benharref and M. A. Serhani, "Novel cloud and SOA-based framework for e-health monitoring using wireless biosensors," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 1, pp. 46–55, 2013.

[13] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 4, pp. 1431–1441, 2014.

[14] A. Juels and T. Ristenpart, "Honey encryption: Encryption beyond the brute-force barrier," *IEEE Security & Privacy*, vol. 12, no. 4, pp. 59–62, 2014.

[15] W. Yin, J. Indulska and H. Zhou, "Protecting private data by honey encryption," *Security and Communication Networks*, vol. 2017, no. 11, pp. 1–9, 2017.

[16] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," *Journal of Cryptology*, vol. 21, no. 4, pp. 469–491, 2018.

[17] V. T. Hoang, T. Krovetz and P. Rogaway, "Robust authenticated-encryption AEZ and the problem that it solves," in *Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, pp. 15–44, 2015.

[18] P. Rogaway and T. Shrimpton, “A provable-security treatment of the key-wrap problem,” in *Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, pp. 373–390, 2006.

[19] P. P. Vinayak and M. A. Nahala, “Avoiding brute force attack in manet using honey encryption,” *International Journal of Science and Research*, vol. 4, no. 3, pp. 83–85, 2015.

[20] J. Jaeger, T. Ristenpart and Q. Tang, “Honey encryption beyond message recovery security,” in *Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, pp. 758–788, 2016.

[21] L. Qiu, X. Sun and J. Xu, “Categorical quantum cryptography for access control in cloud computing,” *Soft Computing*, vol. 22, no. 19, pp. 6363–6370, 2018.

[22] J. Han, Y. Liu, X. Sun and L. Song, “Enhancing data and privacy security in mobile cloud computing through quantum cryptography,” in *IEEE Int. Conf. on Software Engineering and Service Science (ICSESS)*, Beijing, China, pp. 398–401, 2016.

[23] Y. Okabe, M. Eto, D. I. K. Nakao, J. S. J. Nakazato, K. O. K. Nakao *et al.,* “List of published presentation papers of network security research institute and cybersecurity research center,” *Information Sciences*, vol. 181, no. 11, pp. 2071–2085, 2011.

[24] G. Sharma and S. Kalra, “Identity based secure authentication scheme based on quantum key distribution for cloud computing,” *Peer-to-Peer Networking and Applications*, vol. 11, no. 2, pp. 220–234, 2018.

[25] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner and N. Gisin, “Device-independent quantum key distribution with local bell test,” *Physical Review X*, vol. 3, no. 3, pp. 1–11, 2013.

[26] J. Han, Y. Liu, X. Sun and L. Song, “Quantum key management algorithm based on sliding window,” *Journal of Jilin University (Engineering and Technology Edition)*, vol. 46, no. 2, pp. 535–541, 2016.