Robust Security With Strong Authentication in Mobile Cloud Computing Based on Trefoil Congruity Framework

Jerald Nirmal Kumar S., Galgotias University, Greater Noida, India

Ravimaran S., MAM College of Engineering, Tiruchirappalli, India

Sathish A., MAM College of Engineering, Tiruchirappalli, India

ABSTRACT

Mobile cloud computing (MCC) initially draws on cloud and mobile computing principles, where it focuses on wireless networks to provide mobile users with rich computing services. In the modern era, the sharing of secured large-scale data is the major challenging task. However, problems continue to be resolved such that the omnipresent usage and use of mobile cloud computing are feasible. Some of the challenges include security, lossless back-up and data recovery, and computational complexity. To deal with this scenario, a unique combination of the trefoil congruity framework is proposed to secure a privacy-preserving user consent solution by using the backup method to store and recover a huge amount of data. Quantum key fibo privacy approach (QKFPA) encrypts and decrypts the data using the fibonacci chain-leaning matrix along with quantum computation to provide security while transmitting/unloading user information. Consecutively, high-security distribution and rake technology (HSDRT) is enhanced to block the inside attackers and ensures retrieval of saved data without any loss. Once the storage is enhanced, data access is highly secured through the emperor-imperial technique, which generates an imperial label between mobile users and cloud server through the selection of emperor node. The outcome of the work offers great fortification for cyber threats, authentication, and lossless retrieval of data in MCCs.

KEYWORDS

Emperor-Imperial Technique, HS-DRT (High-Security Distribution and Rake Technology), Mobile Cloud Computing (MCC), Quantum Key Fibo Privacy Approach (QKFPA), Trefoil Congruity Framework

1. INTRODUCTION

Mobile cloud computing (MCC) is laurenched as a cloud computing technology that is available for mobile devices like smartphones and tablets (Mollah et al., 2017). In MCC, mobile users can access cloud-specific tools, program and operating performance, and use cloud infrastructure to deploy and implement a range of applications to improve computing power and enhance the storage space and context. Mobile devices are available. The MCC industry is projected to produce $94.75 billion in sales (online, 2018), according to Mordor Intelligence's report in 2023 (Mordor Intelligence Industry Report, 2018). However, the abundance of mobile cloud providers still raises more protection and privacy issues (Chang et al., 2016). The mobile computing world also introduces new security, convenience and privacy requirements. The conventional user authentication method, based on the username and

DOI: 10.4018/JOEUC.20211101.oa11

password, relies on the point of view of the user. For the simplification and convenience of login, the user name and the password have been chosen in the past. However, in recent years people would choose to bring more and more jobs in the mobile terminal due to the huge success of the mobile terminal. As a result, the accounts to be handled are increasing. The findings reveal that on average, every user has 25 accounts in 8 periods of a day and 6.5 passwords and logs. You cannot remember the complex password again but people cannot stop using a plain, weak password and sharing the same password with different network services. If the password of the user is tricked or stolen by the virus and trojan horse, the personal details of the user would be jeopardized (Han et al., 2018).

The protection risks occur for all parties, meaning that the cloud and cloud service providers have problems protecting themselves from possible security attacks for safe sessions, transactions and activities (Gupta & Badve, 2017). It is the responsibility of the cloud service provider to provide its service customers with secured and secure networks to safeguard confidential data, passwords, and applications. In comparison, cloud service providers use sophisticated pin code and strong authentication schemes to deliver stable and uninterrupted services (Chaudhry et al., 2019). Mobile Cloud Computing (MCC) is an evolving technology in which data and information computation, manipulation, and storage take place beyond mobile devices (Xia et al., 2016). This technology is regarded as a cloud itself. MCC has arisen as eminent mobile facilities for effective and economical use of remote computing services and data storage (Oludele & Oluwabukola, 2016). It provides many services, including a network, applications, infrastructure, storage, and reconstruction, etc., and is a very significant cost-effective approach for storage and computation (Pandian & Smys, 2020). The cloud computing services are designed into a replication mechanism to prevent the lack of knowledge about the natural or manmade catastrophe (Gharajeh, 2015). To avoid unintended manipulation and hacking of the information contained in the cloud, it fragments information accompanied by replication to maximize security and to fix concerns of overburdening the cloud. Several times, this scattered information is not well organized but distributed or dispersed changed by random means. This increases the information's recovery time as well as the restored quality (Han et al., 2015).

Mobile cloud computing is split into two methods: the use of online cloud providers and mobile cloud-free resource management (MRM), which combines local mobile device computer and storage facilities. The implementation of external cloud providers is broken down by the creation process which consists of a service-oriented architecture with a cloud link relying on the Internet for mobile devices and agent-client architecture with mobile devices connecting to the cloud through agents like FemtoCell or Cloudlet (Nayak & Bansode, 2016). The MRM should be willing, as the system consists only of mobile devices, to have trustworthy metadata services required for machine and storage resources. Authentication technologies are vital to the correctness of resource knowledge since MRMs can openly be used by mobile users. Conventional techniques of authentication such as methods for authentication based on information, ownership, and biometry are vulnerable to data falsification by man-in-the-middle attacks (MITM's). More potent authentication technology is also important. When 2-factor or multi-factor authentication mechanisms are used the feedback of users is bulky and open to shoulder surf and smudge attacks (Kim & Jeong, 2018).

Researchers have extensively studied security issues such as user authentication and service providers (Huang et al., 2014; Deka & Gharajeh, 2017), outsourcing, safe storage and browsing, data integrity, secure distributed data duplication (Ma et al., 2015) and proof of ownership, due to the increasing use of cloud storage resources. Mobile computer users have access to cloud computing tools, services and apps over unsecured networks of mobile cloud computing. Usually, an individual uses a cloud app built on his or her personal computer to access mobile cloud service services. A cloud service program must authenticate both the cloud service provider and the customer jointly to create faith until the user can access the cloud infrastructure and services (Wang et al., 2015). Network-based systems use authentication mechanisms to avoid unwanted resource entry. Given that authentication schemes are typically intended for the client-server context, their direct use of numerous service providers in distributed environments is unsuitable. In comparison, standard public-key cryptosystems such as RSA and ElGamal, which require high-performance computing resources and broad key lengths, establish most authentication programs. This authentication system is not intended to operate inside the restricted mobile device computing capacity. Also, strict security checks must be enforced as messages are distributed through unknown networks. Key control in remote mobile cloud computing systems is another critical safety issue. Since customers usually access various forms of mobile cloud storage services from various vendors. Consequently, most conventional security mechanisms do not extend to mobile devices (Tsai & Lo, 2015).

Therefore security, data storage and user authentication which include intruder enter inside while uploading data to the cloud, destroy the file, and easily hack the authorized data are the major issues facing in Mobile cloud computing. Moreover the database loses complete protection and gives the user unauthorized access to the three-stage security dilemma. Hence proposed a novel solution that provides high safety and protects the information with lossless retrieval is a forcible need in mobile cloud computing.

The rest of the paper is organized as follows: Section 2 comprises of the related researches, section 3 comprises of the proposed methodology, section 4 comprises of the result and discussion, section 5 comprises the conclusion of the work, followed by the references.

2. RELATED RESEARCHES

Bellini et al (2020) Stakhov offered some fascinating insights about how to take advantage of Fibonacci numbers to achieve a compact representation of an initial error-correcting code. This paper provides an explicit format to measure stakhov redundancy code, describe some of the flows in the initial Stakhov decoding process, which had a critical role in solving a variety of non-trivial diophantine equations, and address in detail how to prevent solving those equations in a few situations, and how to more effectively detect and correct errors. However, this code metric is not used to describe the weight and distance definition of code words.

Boaron et al (2018) presented a 2.5 GHz repetition rate quantum-key delivery system using a one-decoy-coordinated three-state time-bin protocol. To transmit secret key over a cumulative distance of 421 km and achieve secret key speeds of 6.5 bps over 405 km with the help of supreme single-photon detectors designed for quantum key delivery and ultra-low-loss fiber. However, the technical sophistication of these strategies was far greater.

Annane et al (2019) to protect against three well-known attacks on the mobile cloud environment (co-resident attacks, hypervisor attacks, and distributed attacks), present a new security proxy-based approach with three Diffie-Hellman protected hashed keys for user access control and VM deployment and communication control management. The related attacks lead to unauthorized access to sensitive data between different mobile apps being spread while using the cloud as a third party to share resources. The suggested solution was explained using a case study in the area of health care. The sophistication was therefore high for fast operation and new cloud systems cannot be merged with the system.

Sood et al (2019) propose a distinctive EMS solution using Fog and Cloud to store different data types and preserve their co-relationships to avoid numerous breaches of EMD security. A Mobile Fog-based cloud-IoT platform for EMS has been developed in this paper in which only encrypted data is stored in the cloud, and its keys are stored securely on the Fog layer at the company premises. This uses the Advanced Encryption Standard (AES) for encryption, Message Authentication Code (MAC) for data integrity and Secure Socket Layer (SSL) for secure data transfer, tokenize, hashing, and key pointers for simple Fog and Cloud data searches. It stores the encryption/decryption and encryption MAC keys with Master Encryption Key. There was a chance of data occurring when large files exist.

Ghudayyer et al (2017) safety was one of the main concerns of those who want to embrace cloud computing technology and move to it. Security issues posed by cloud technology show that mobile cloud computing poses privacy and security issues such as identification and authentication problems, as sometimes the system owner's identity and authentication, or the cloud owner's data, were not strictly remote. These are some factors that could be viewed as major setbacks to the adoption of mobile cloud computing, and the reason why certain companies are still unwilling to accept, implement, and move to this technology.

Ahmed et al (2019) propose a process state synchronization (PSS)-based execution management. In case of disconnection, calculate analytically an appropriate condition on the synchronization period to ensure a reduction in execution time for mobile applications under PSS. Likewise, calculate the upper bound at the interval of synchronization, whereby a greater interval of synchronization did not result in significant benefits for the mobile application in terms of execution time. Test implementation of PSS with the measured synchronization intervals verified the analytical findings. Also, compare the performance of the proposed solution with cutting-edge solutions. However, there is no separate selection of majesty nodes.

Arul et al (2019) Quantum cryptography was a modern concept that checks for the robustness of Quantum computer security protocols. This paper suggested a security protocol for the complex security association called the QKG-AKA (Quantum Key GRID for Authentication and Key Agreements). In Long Term Evolution (LTE) architecture, this scheme was used effectively without any major improvements in the underlying base structure. The proposed QKGAKA mechanism for stability and protection was evaluated compared with quantum computers. The Internet of Vehicles domain does not, however, guarantee protection.

Sowjanya et al (2019) Data encryption was a challenging job for mobile devices, and a complex connection between the data user and the cloud was a data recovery operation. TEES suggested this post, which encrypted the search over a mobile cloud with greater bandwidth and improved energy consumption. The proposed architecture eliminates computing from personal devices to the cloud and will thus further boost mobile consumer and cloud interactions. The Multi-keyword search framework does not enforce to encrypt mobile cloud search info.

Gosh et al (2019) supervisory systems for controlling production activities, such as power grids, water delivery systems, traffic management, oil and natural gas exploration, space stations and nuclear power plants are used for supervisory control and data acquisition (SCADA) systems. Their stability however is endangered by the growing use of open-access networks. Moreover, a new form of challenge to SCADA systems has been revealed through the advancement of quantum computing. If SCADA systems cannot be secured, the effects can be disastrous. A malicious attack can, for instance, regulate a city's electricity supply, disconnect a water supply grid, or cause a nuclear reactor to fail. The principal objective is to the classification of attacks against SCADA, define a specific form of quantity-based attack, and to devise a new safeguard scheme for both conventional and quantum attacks. The suggested method of "Signcryption" involves the monitoring of intrusion and encryption. However, the properties of quantum mechanics can be used by an eavesdropper for sample attacks in Quantum Key Distribution

However, (Bellini et al., 2020) metric code was not used to describe the weight and distance definition of code words, (Boaron et al., 2018; Annane et al., 2019) the technical sophistication of these strategies were far greater (Sood, 2019). There is a chance of occurring the data when large files exist, (Ghudayyer et al.,2017) and the connection is not fulfill established. (Ahmed et al., 2019) There is no separate selection of majesty nodes, (Arul et al., 2019) and the Internet of Vehicles domain does not, (Sowjanya et al., 2019) Multi-keyword search framework does not enforce to encrypt mobile cloud search info.

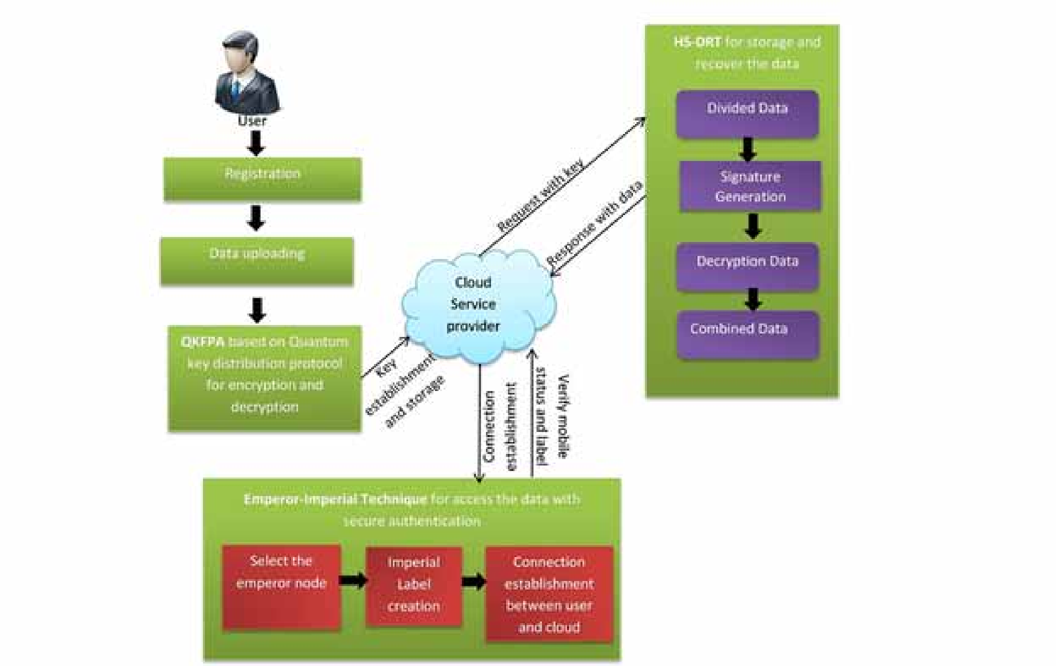
There is a lack of extensive research of MCC data security systems ensuring confidentiality, integrity, authentication, non-repudiation, and access control, which is critical to the development of future safe alternatives and requires further attempts. Hence it is important to design the combined solution for the security problem by adaptive secure privacy-preserving approach for user authorization with aid of backup mechanism to store and recover a large number of data.

3. TREFOIL CONGRUITY FRAMEWORK

With the rise in the challenges of mobile cloud computing during data transmission, User authentication plays a vital role in tackling these issues with the aid of cryptographic solutions. As well storage and retrieval have become a serious issue that has been widely faced daily in our lives nowadays. Whereas, the prior methodologies provide secured data transmission by performing encryption and decryption using the shared secret key, but with increased computational as well as communication overhead. These would simultaneously lead to cyber threat issues and increase data storage complexities. Many quantum security protocols are published for providing cryptography to prove more secure, however, a tangled photon can only bring up to 2 classical bits in those protocols. Additionally, since the photon detectors are randomly selected, trial in two, one must be discarded. Here, the efficiency ratio of enmeshed photons is very low. This leads to data loss or corruption in the data or information stored in the cloud. Though, some recent methodologies recover the corrupted data they don't guarantee lossless data recovery and strong authentication for data access. The security issue in the MCC environment happens from where the data is encrypted then at the time of retrieval and during authentication. Hence it is important to adopt a security mechanism that efficiently protects data at each of these levels so that the communication system can be enhanced. Hence, to cope with all those aforementioned complexities, a novel framework is designed in the proposed work.

This paper proposes an efficient Trefoil Congruity framework, Which includes Quantum Key Fibo Privacy Approach (QKFPA) ensures robust safety and HSDRT attains the lossless backup and retrieval of the data then Emperor-Imperial technique offers the strong authentication for data access which is more indispensable in mobile cloud computing. The overall performance of the proposed system is described in Figure 1.

Figure 1. *Trefoil Congruity framework for MCC*

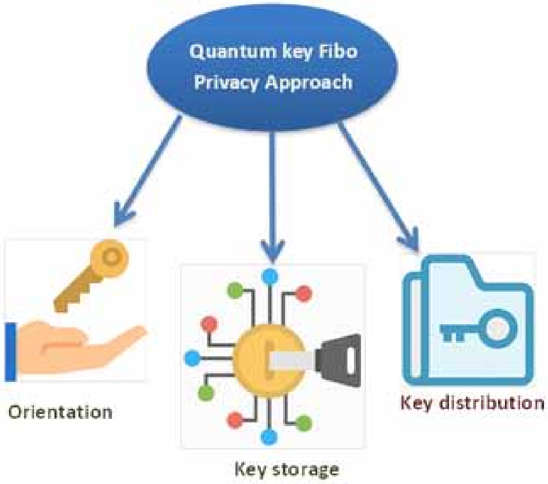

User
Registration
Data uploading
QKFPA based on Quantum key distribution protocol for encryption and decryption
Key establishment and storage
Cloud Service provider
Request with key
Response with data
HS-DRT for storage and recover the data
Divided Data
Signature Generation
Decryption Data
Combined Data
Connection establishment
Verify mobile status and label
Emperor-Imperial Technique for access the data with secure authentication
Select the emperor node
Imperial Label creation
Connection establishment between user and cloud

Initially, the Quantum Key Fibo Privacy Approach (QKFPA) is introduced in the research to perform the encryption and decryption along with the quantum computation. To begin with this, encryption and decryption will be done differently from the existing method. That is QKFPA includes quantum key distribution with the aid of the Fibonacci chain-slanting matrix. Hence it offers great security during encryption and decryption to transmit/upload the user data. Furthermore, a novel HSDRT is utilized, which checks whether any data corruption or loss has occurred or not. If any data corruption or data loss is experienced by the insider's attacker, then the novel method tackles those issues and ensures lossless data recovery. Consequently, the technique offers backup of the stored data without any losses through an ultra-widely distributed data transfer mechanism. Then to enhance the data confidentiality through ensures robust authentication, the research introduces the Emperor-Imperial technique. According to the technique, instead of username and passwords, the imperial label is generated via the emperor node. Once the authorized person gets permission from the emperor node by the imperial label to access the data then the connection is established from the user to the cloud. Thus it provides strong authentication that enhances authorized users only can securely access the data. And the detailed explanation of proposed techniques is described in the following sections.

3.1 Quantum Key Fibo Privacy Approach (QKFPA)

The QKFPA efficiently performs encryption and decryption through quantum coding, thus it offers greater more security for cyber threats. Initially, identified Fibonacci numbers can be directly used for generating the Fibonacci matrices. The major consideration of the Fibonacci matrix is that has the recursive property, therefore the matrix is utilized for quantum coding. The main idea behind that is to use a Vogel encoding spiral, in which participants either Alice or Bob (or even a third party) may be in charge of and encoding a source of entangled orbital angular momentum (OAM) states valued by Fibonacci. Fibonacci-valued entangled pairs then exit the spiral and join the crystal for down-conversion. The down-conversion divides into two lower OAM values for each Fibonacci value (Figure 2).

Figure 2. *Approaches in QKFPA*



There is a beam splitter in both Alice's and Bob's experiments which directs some standard beam proportion to two different types of OAM sorters M and N. Within their experiments, the beam splitters spontaneously pass the entangled photon to either the sorter M or N. The M sorter allows only entangled photons valued by Fibonacci to enter the arrays of a single-photon detector.

The N-sorter is used to make a "diagonal" overlay of the form followed by equation 1 and to filter out any non-Fibonacci-assessed photon.

$$Slanting\,\sup erposition = \frac{1}{\sqrt{2}}\left(\left|FB_{n}\right\rangle + \left|FB_{n-2}\right\rangle\right) \tag{1}$$

There are four possible cases in Alice's (or Bob's) experiment for the sorter that happen. Table 1 details possible cases.

Table 1. Details possible cases

The sorter selected by Alice	L	L	D	D
The sorter selected by Bob	L	D	L	D
Whether photon is used for the key configuration	Yes	Yes	Yes	No

The proposed QKFPA considers the three approaches are Orientation, key distribution, and key storage.

3.1.1 Orientation

In the proposed QKFPA technique, there are two participants Alice and Bob defined as follows,

Alice is a sender, responsible for the processing of entangled states.

Bob is a receiver who detects Alice's entangled photons.

Then Fibonacci numbers (FB_n) are an infinite sequence of integers denoted by the recursion as follows,

$$FB_{n+2} = FB_{n+1} + FB_{n}, \qquad n \geq 0 \tag{2}$$

Where the first two sequence elements are FB0 = 0, and FB1 = 1. Using the Fibonacci sequence's first three integers FB0, FB1, FB2, can construct a 2 x 2 and nth power Fibonacci matrix:

$$Q^{n} = \begin{pmatrix} FB_{n+1} & FB_{n} \\ FB_{n} & FB_{n-1} \end{pmatrix} \tag{3}$$

Therefore, equation 3 can generate the quantum key based on Fibonacci numbers 3, 5, 8, 13, 21, 34, 55, 89. Then the detailed explanation of quantum key distribution follows.

3.1.2 Quantum Key Distribution

In the key distribution phase, the following steps are considered, Step-1: Alice prepares l pairs of entangled states with a source of entangled OAM states based on a Vogel spiral measured by Fibonacci. The l pairs of entangled states are in the form below

$$\sum_{n}\left(\left|FB_{n-1}\right\rangle\left|FB_{n-2}\right\rangle+\left|FB_{n-2}\right\rangle\left|FB_{n-1}\right\rangle\right)_{AB} \tag{4}$$

The first photons in each pair as per Equation (4) constitute SA, and the second photons in each pair as per Equation (4) constitute SB. Alice holds SA and sends SB to Bob.

Step-2: Bob randomly selects the sorters M and N after obtaining SB, and tests the values in SB held by each photon.

Step-3: Alice randomly selects the M and N and sorters to determine the values that every SA photon carries.

Table 2. Possible classical exchange of the Protocol information

Alice obtained Fibonacci value	1	2	3	5	8	13	21	34	55
Alice sending the classical bits	0	0	1	1	0	0	1	1	0

Step-4: Alice moves a series of bits on to Bob. Table 2 shows the contact. Bob will calculate the Alice value when he receives a classical bit from Alice because the value is one of the two adjacent values to his value. Once Bob confirms that Alice's value is even, he transmits a bit to Alice. If the value of Alice is odd, Bob will take the protocol in conjugation with zeros and swapped ones.

Step- 5: Equally, Alice can also confirm the value of Bob after receiving classical information. Which is to say, by sharing classical knowledge, Alice and Bob can convince one another of the detected values. However, classical knowledge is inadequate for an eavesdropper Eve to classify the detected values, as it only achieves vague results in Table 3.

Table 3. Eve has received outcomes in terms of the classical knowledge eavesdropped.

Eve obtained classical information	00	01	10	11
Eve obtained possible outcomes	3, 21, 34, 89	3, 5, 13, 21	8, 55, 89	5, 13, 34, 55

Alice and Bob will create a common key consisting of a series of block-diagonal Fibonacci matrices by knowing the values of Fibonacci in the key distribution process. To be precise, the block-diagonal Fibonacci matrices are formed by both Alice and Bob in terms of the results detected each round including eight Fibonacci numbers (3, 5, 8, 13, 21, 34, 55, and 89). If the available Fibonacci values identified in the first round are 5, 13, 21, 34, then the block-diagonal Fibonacci matrix can be constructed as follows with seeds 5, 13, 21, 34:

$$\begin{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix} & 0 & 0 & 0 \\ 0 & \begin{pmatrix} 21 & 13 \\ 13 & 8 \end{pmatrix} & 0 & 0 \\ 0 & 0 & \begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix} & 0 \\ 0 & 0 & 0 & \begin{pmatrix} 55 & 34 \\ 34 & 21 \end{pmatrix} \end{pmatrix} \tag{5}$$

Where, 0 is a dimension 2 matrix with zero inputs. If the available Fibonacci values identified in the second round are 3, 8, 13, 21, 89, then the block-diagonal Fibonacci matrix can be constructed as follows with seeds 3, 8, 13, 21, 89:

$$\begin{pmatrix} \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix} & 0 & 0 & 0 & 0 \\ 0 & \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix} & 0 & 0 & 0 \\ 0 & 0 & \begin{pmatrix} 21 & 13 \\ 13 & 8 \end{pmatrix} & 0 & 0 \\ 0 & 0 & 0 & \begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix} & 0 \\ 0 & 0 & 0 & 0 & \begin{pmatrix} 144 & 89 \\ 89 & 55 \end{pmatrix} \end{pmatrix} \tag{6}$$

The same method for constructing block-diagonal Fibonacci matrices may be used in n rounds. Also, the determinants of the elements (i.e., dimension 2 Fibonacci matrices) of the central block-diagonal matrices are either 1 or −1, hence the block-diagonal matrices in Fibonacci are invertible. A distributed quantum key is then be stored securely is explained as follows.

3.1.3 Key Storage

Alice and Bob can store the given key using the representation of the Fibonacci matrix reducing the cost of storage. The facts are as follows. Representation of the Fibonacci matrix, consider the representation of positive integers (a b c d …..) with Fibonacci matrices:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \sum_{i=4}^{11} a_i Q^i \tag{7}$$

Where, a i € {0, 1} i = 4, 5, · · ·, 11, and b = c, d = a −b. Since eight different matrices can be formed, the main block-diagonal elements of Equations (5) and (6) can be decompiled using Equation (7) as shown below.

$$\begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix} + \begin{pmatrix} 21 & 13 \\ 13 & 8 \end{pmatrix} + \begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix} + \begin{pmatrix} 55 & 34 \\ 34 & 21 \end{pmatrix} = 0.Q^{4} + 1.Q^{5} + 0.Q^{6} + 1.Q^{7} + 1.Q^{8} + 1.Q^{9} + 0.Q^{10} + 0.Q^{11} \tag{8}$$

$$\begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix} + \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix} + \begin{pmatrix} 21 & 13 \\ 13 & 8 \end{pmatrix} + \begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix} + \begin{pmatrix} 144 & 89 \\ 89 & 55 \end{pmatrix} = 1.Q^{4} + 0.Q^{5} + 1.Q^{6} + 1.Q^{7} + 1.Q^{8} + 0.Q^{9} + 0.Q^{10} + 1.Q^{11} \quad)9($$

The central block-diagonal elements of Equations (5) and (6) are thus stored by Alice and Bob as binary strings 01011100 and 10111001, respectively. Each of the eight Fibonacci numbers is capable of encoding a 3-bit binary string from 000 through 111. That is, at most 24-bit messages can be encrypted in each round. While the message can be divided directly into blocks in the proposed protocol and constitutes digital matrices in terms of the corresponding block-diagonal Fibonacci matrices, thus it is greatly enhanced the coding efficiency.

The QKD is mainly implemented here to improve the transmission security of the cloud. Also, this technique solves the security problems of the traditional key distribution techniques. The working procedure of this technique highly depends on quantum mechanics. During the storage in the CSP, the data may get lost due to some internal failure such as eavesdropping, Denial of Service (DoS), server issues, etc. so a data recovery technique will be implemented in the MCC.

3.2 Mending of Data by HSDRT (High-Security Distribution and Rake Technology)

Due to possible data corruption by internal attacks i.e., insider attacker scrambled data into the encrypted data or even to the encrypted index, the search result may return false data to the user. So there is a need for a security mechanism to verify and retrieve the desirable file. The HS-DRT is an innovative security mechanism, which makes use of an effective ultra-widely distributed data transfer mechanism and high-speed encryption technology. This proposed system follows two sequences one is the Backup sequence and the second is the Recovery sequence. In the Backup sequence, it receives the data to be backed-up, and in Recovery Sequence, when some disasters occur or periodically, the Cloud Server (one of the components of the HSDRT) starts the recovery sequence. However, there is a limitation like security issues secured by the data steaming method as shown in Figure 3.

3.2.1 Secureness Backbone of HS-DRT

The Security level of the HS-DRT does not only depend on the cryptographic technology but also the combined method to specify three factors, such as spatial scrambling, fragmentation/duplication, and shuffling algorithm.

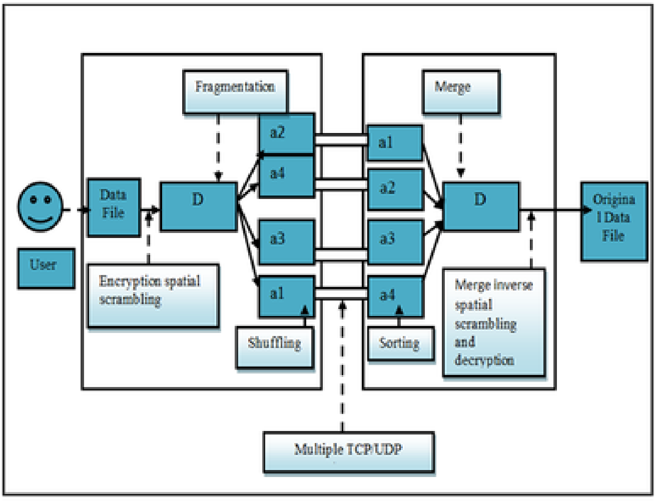
3.2.1.1. Spatial Scrambling

The spatial scrambling procedure can be realized by executing the simple algorithm illustrated as follows. Using the C-style description for(i=1;i<imax;i++){buf[i]=buf[i]+buf[i-1];} buf[0]=buf[0]+buf[imax-1]; The array of buf[ ] is the target data to scramble and Imax is the size of the buf array. This computation process should be repeated several times. To de-scramble, it is only necessary to perform the same operations in the reverse order. By introducing the above mentioned spatial scrambling technology, deciphering by a third party by comparing and combining the encrypted fragments becomes almost impossible according to the fact that the uniform distribution of information can be achieved by this spatial scrambling is performed.

3.2.1.2. Fragmentation/Duplication

One of the innovative ideas of HS-DRT is that the combination of fragmentation and distribution can be achieved in random order. Even if a cracker captured all raw packets between the data center and

Figure 3. *The secure data streaming with HS-DRT*



client nodes, it would be tremendously hard to assemble all the packets in the correct order, because it would be necessary to try about (no. of fragments) attempts.

3.2.1.3. Shuffling

HS-DRT mainly uses the shuffling method with pseudo-random number generators on the distribution to the client nodes. If the shuffled table has a uniform distribution, the table itself is hard-to-guess by the third party. But, if the shuffled tables are biased, there may exist weak points in the corresponding recovery system.

3.2.2 Back-Up Sequence

At the point when the data owner gets the data to be gone down, it encrypts scrambles and separates into a few fragmentations. From these copies, the data to a few degrees fulfill the required recuperation rate as per the pre-decided administration level. The Data Centre encrypts the fragmentations again at the second stage and appropriates them to the customer hubs in a random request. In the meantime, the Data Centre sends the metadata which has been utilized for unraveling the arrangement of parts. The Metadata is made out of encryption keys (both at the first and second stages) related to data of fracture, duplication, and distribution.

3.2.3 Recover the Original Data

The Cloud Server gathers the encoded fragmentations from different proper customers like the rake gathering methodology. At the point when the Cloud Server gathers adequate, several encoded sections, which are not the whole scrambled parts, are decrypted, consolidated, and descrambled in the invert arrange at the second stage and the unscrambling will be finished. After this, the unscrambling data are shared secret keys with the encryption key, the information of fragmentation, and the shuffled tables. The procedure of HS-DRT is illustrated in the below equations.

Generate a random number

$$r = rand(x_t); \tag{10}$$

Create a High-Security HS_t for each Ct and store HS_t at Cs.

$$HS_t = r \oplus client\_ID_t \tag{11}$$

Repeat step equation (18) for all clients. If Ct/Admin Creates/Modifies a D and stores at Mc, then D11 created as

$$D_1^{'} = D_1 \oplus HS_t \tag{12}$$

Store D1 at Cs. If the server crashes a deleted from Mc. then do EXOR to retrieve the original D1 as

$$D_1^{'} = D_1^{'} \oplus HS_t \tag{13}$$

Finally, the D1 returns to the Ct. Where Client-Server: Cs; Clients of Mc: Ct; Data: D1 and D1'; High Security: HS_t; Random Number r;

Clients ID: client_Idt,

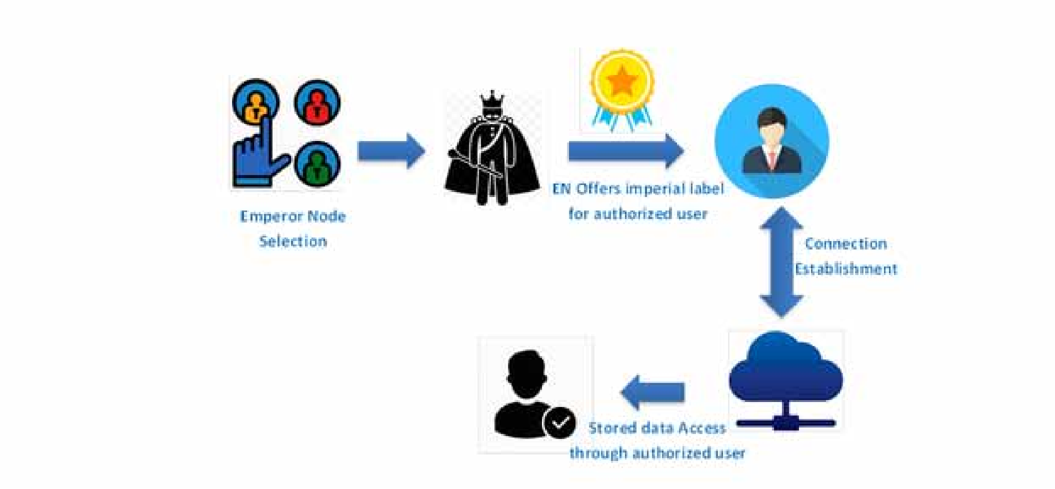
The proposed HS-DRT (High-Security Distribution and Rake Technology) technique is used to store the original data File and recover the data if there is a loss insecure manner by the introduction of spatial scrambling, shuffling, and back up sequence. After this process ends, the signature is generated and then the fragmented data are decrypted separately. Once the user receives the signature, it is matched with the user's signature. If both are the same, the data can be decrypted by using the generated signature. The hashing function is used to perform the signature verification process. The file content requested is given only when the request is authorized. Formally to identify the authorized user, many techniques are identified such as the password, biometrics, etc. although it includes some security concerns. Hence to reduce the security issues during the authorization EI technique is introduced in the next section.

3.3 Emperor-Imperial (EI) Technique

After the data owner has stored the data in CSP, the authorized person may access it. But, due to the vulnerability of the licensed username and password, the data stored can be accessed by an unauthorized person such as hackers. To this end, boost up the security is needed to protect the data by giving a strong authentication. The paper designs the new EI technique that is proposed to assist the Cloudlet manager in strengthening security in the heterogeneous mobile computing environment (Figure 4).

The authentication must be established with two-stages. This includes Mobile and Cloudlet also, between cloudlet and cloud server connections. Thus the multi-stage authentication is ensured. The mobile nodes involved form a virtual backbone in the network that is corroborating with Cloudlet. Any two unconnected mobile nodes exchange their information via a message multicast. A mobile cluster is formed through each node (S) that joins the network. The multicast message ensures that nodes are present and each receiving node(R) will process it and add N(R) = N(R) + K to its neighbor collection. This simple hello protocol includes local information and a constant number of iterative rounds of exchanges of the messages between adjacent hosts. This proposed method is significantly reducing the number of identity theft cases on the MCC due to the need for more information than just the user name and password details.

Figure 4. *process of Emperor-Imperial (EI) Technique*



3.3.1 Emperor Node Selection

The emperor node is an answer for providing end-to-end authentication with Imperial Label. The emperor node chosen should be stronger than other neighbor set nodes. They consider the following features for choosing emperor nodes such as Residual energy, speed, memory available, location, and several adjacents.

After the emperor Node has been picked, the cluster nodes accumulate all Competition Point from their neighboring nodes and select the emperor node with maximum Competition Point. Within all node collection, this information is multi-casted. So if any client node requests a service then it informs the emperor node for the establishment of the connection. The King node includes a token-like Imperial Label. Such tokens may be valid for a One-Time Password on login. It works in the procedure which follows.

1. A requester, RN which is the client who requests access to the network.
2. The emperor node, EN, offers end clients two levels of connectivity.
3. Cloudlet Server, CS, a database that contains the credentials required to allow or deny clients access.

The relation between EN and CS depends on the connectivity from layer III. Once RN joins the network it links to EN physically, but EN only forward authentication packets to CS. So, initial authentication with an EN Imperial Seal token is carried on between RN and CS. Authentication is given by the bidirectional method between CS and RN and that it must generate some fresh shared secrets (Imperial Label) into the endpoints, CS and RN, which will be used as proof of positive authentication. CS communicates to the EN at the end of authentication that RN is an approved unit, and transfers the mutual secret into EN.

In the next section, RN and EN receive a second key that is a connecting key from the Imperial Label and will be used to secure real data contact between these two parties. That time a new connection is enabled, the same authentication takes place within transmission range. This can often happen to consider the possibility of temporary errors or loss of the signal. The re-authentication process has to be shortened to have results consistent with real applications. Algorithms are implemented on the server end and user end.

Preferably the server informs the user, system, and host about the authentication status, and the parties may proceed accordingly based on the authentication results. The Emperor node produces the imperial label authentication tokens in dynamical mode. Whenever a node is connected to the cloud server, the node informs the emperor node of node specifications and passwords, the emperor node provides the node and the Cloudlet architecture with an Imperial Label authentication token. After the imperial label verification with a validity test, Cloudlet guides the connection to the cloud server.

Algorithm-1

Step: 1- Initialize the competition point as zero. If battery charging is applicable, then the competition point will be calculated as initial competition with the addition of 100.
Step: 2- Step 1 is repeated for calculation of competition value up to 70 and 50. After calculating the residual energy competition value, the algorithm wants to calculate the availed memory based on RAM size and CPU speed.
Step: 3- Based on that specific characteristic, finally novel algorithm find out the emperor node. Subsequently, the emperor node generates the imperial label.
Step: 4- once receive the request from services then verify the status of every mobile node. At that time the emperor node generates the imperial label.
Step: 5- After generating the imperial label, to check the device status then check the imperial label matched status.
Step: 6- if the imperial label is not matched error message will be displayed. Or otherwise, the connection is established between the request servicer and cloud server. Continue the authentication for the threshold time limitation of 180 seconds.
Step: 7- After reached the threshold time, process steps 1 to 3 to find out the emperor node. Again the new imperial label verification was performed between the client end and cloud server end.

The token is intended to be impossible to replicate or create through any other node. Finding the emperor node is very hard for attackers to compromise. Even if compromised, CS is unable to obtain Cloudlet Server keys, and it cannot create custom tokens for distribution to other unauthorized devices. The computing power required to generate and validate the token is limited (no public key algorithms used) so that the terminals are not overwhelmed and no new service attacks are implemented. After establishing the connection between the user and cloud users can access the decrypted data.

3.3.2 Data Decryption

The appropriate signature is generated for each data by the cloud service provider after receiving the data from multiple servers for decryption. In this stage, the received quantum key is considered as the master key. The random private key is generated by satisfying the non-abelian property based on the master key. Then, the generated public key is sent to the authorized user at the encryption side. Here, the secret generated by using the received public key is known as the decryption key. At last, the received fragments are separately decrypted at the receiver side and integrated into original data.

Thus the overall framework effectively tackles the cloud data security related issues with the aid of QKD relied on the QKFPA approach. Moreover, the corrupted or the lost data are recovered completely with the aid of HSDRT. Finally, the EI technique is utilized to access the data with high-security authentication. Thus as a whole, the proposed framework ensures highly secured data access from the cloud server, thereby overwhelms the confidentiality and reliability issues faced with the prior methodologies.

Therefore the technique is applied in secret sharing backgrounds, high secure authentication fields for providing safe accessibility and lossless retrieval of data. For example one of the most highly secure authentication fields is banking; hence to transfer the data like bank statements, etc. are highly confidential therefore use the proposed quantum-based encryption and decryption technique in that.

Then from stored data such as transaction details, shares, bonds, etc. to lossless backup and recovery can use the novel HSDrt technique. Finally to access the data securely can be utilized through the proposed EI technique, which provides strong authentication for an authorized person.

4. RESULTS AND DISCUSSION

The efficiency of the proposed framework can be proved further by comparing the results produced by the proposed one with other conventional techniques. Here the comparison is performed with various factors.

4.1. System Specification

The proposed method is implemented in the working platform of java with the following system specification.

Platform: java
OS: Windows 10
Processor: Intel core i5
RAM: 8 GB RAM

4.2 Performance Analysis for the Proposed QKFPA with HS-DRT

To show the efficiency of the proposed method, the following factors are evaluated. The security framework is implemented in JAVA which has been shown in the following Figure 5.

Figure 6 described the quantum key generation, here in the implementation there are three procedures first to generate the quantum key of a specific length, and then analyze the input size based on output key length, finally analyzing the desired key length based on several rounds. Figure 7 described the distribution of quantum keys based on linking.

Therefore, Figure 7 and 8 clearly illustrates the efficiency of the proposed method during encryption and decryption.

Figure 7 illustrates the selection of emperor node and connection establishment between user and cloud. Initially, find the ten most connected elements and determine the neighboring nodes (shortest path) from one element to another as well based on node-specific characteristics the emperor node is selected. Then thus the emperor node generated the imperial label to the authenticated user for establishing the connection. Based on this authentication the proposed methods offer strong security in mobile cloud computing.

4.3 Experimental Analysis

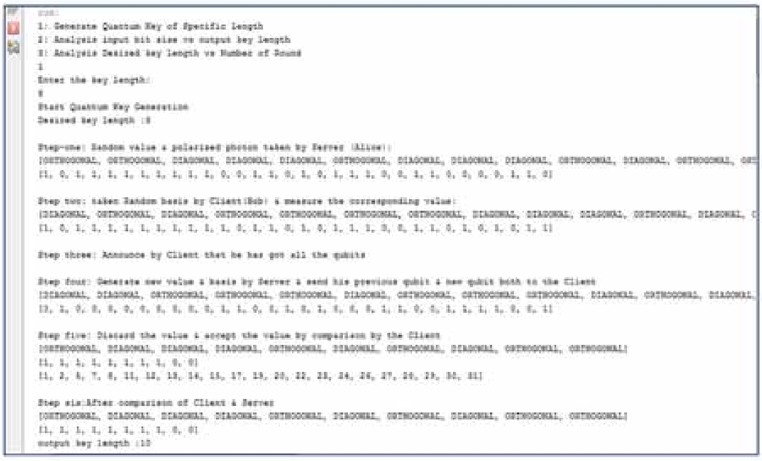
In this section, the work analyzed the performance of the proposed work i.e. encryption time, decryption time, execution time, throughput, key generation time, packet delivery, response time, backup and recovery analysis, buffer size, and key length.

4.3.1 Encryption Time

It is the time taken by the encryption algorithm to convert the plain text into the ciphertext. The encryption time of the data after encrypting it by the proposed technique is compared with the encryption techniques. Encryption time is calculated based on qubit per seconds

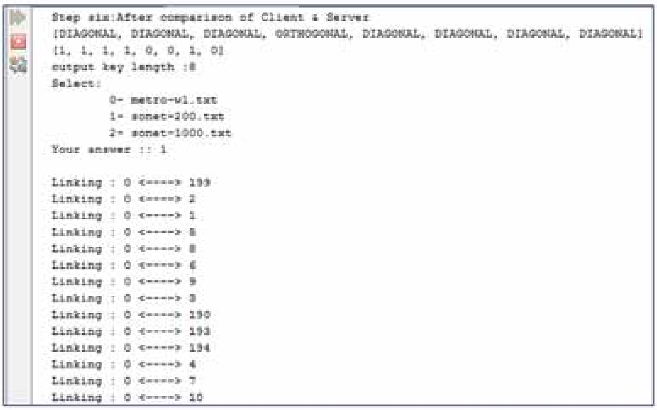
$$\mathrm{E\_time} = \frac{e_c}{\mathrm{r_c}} \tag{14}$$

Figure 5. *Implementation of quantum key generation*



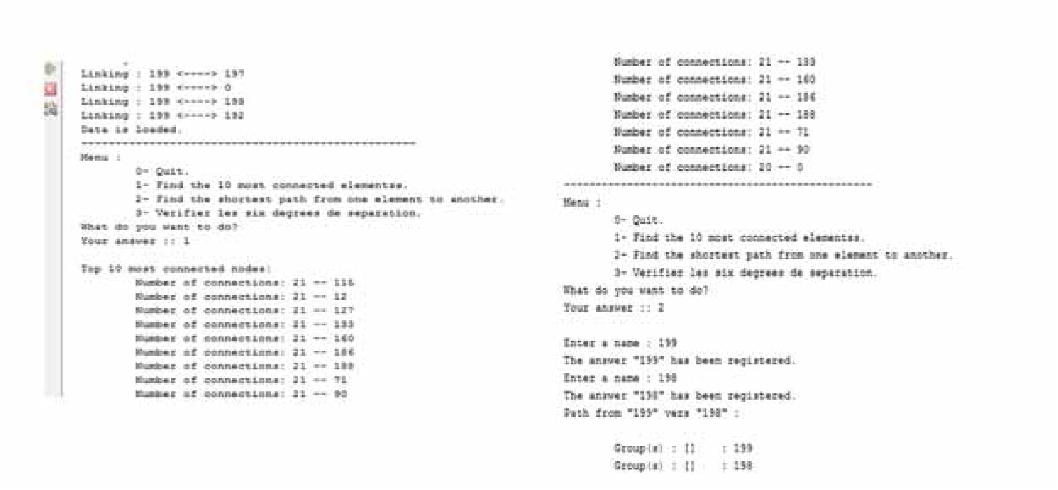
```
run:
1: Generate Quantum Key of Specific Length
2: Analysis input bit size vs output key length
3: Analysis Desired key length vs Number of Round
1
Enter the key length:
8
Start Quantum Key Generation
Desired key length :8

Step-one: Random value & polarized photon taken by Server (Alice):
[ORTHOGONAL, ORTHOGONAL, DIAGONAL, DIAGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL, DIAGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL, ORTHOGONAL, ORT
[1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0]

Step two: taken Random basis by Client(Bob) & measure the corresponding value:
[DIAGONAL, ORTHOGONAL, DIAGONAL, ORTHOGONAL, ORTHOGONAL, ORTHOGONAL, ORTHOGONAL, DIAGONAL, DIAGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL, O
[1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1]

Step three: Announce by Client that he has got all the qubits

Step four: Generate new value & basis by Server & send his previous qubit & new qubit both to the Client
[DIAGONAL, DIAGONAL, ORTHOGONAL, ORTHOGONAL, ORTHOGONAL, DIAGONAL, ORTHOGONAL, ORTHOGONAL, ORTHOGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL,
[0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1]

Step five: Discard the value & accept the value by comparison by the Client
[ORTHOGONAL, DIAGONAL, DIAGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL, ORTHOGONAL, ORTHOGONAL]
[1, 1, 1, 1, 1, 1, 1, 1, 0, 0]
[1, 2, 5, 7, 8, 11, 12, 13, 14, 15, 17, 19, 20, 22, 23, 24, 26, 27, 28, 29, 30, 31]

Step six:After comparision of Client & Server
[ORTHOGONAL, DIAGONAL, DIAGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL, ORTHOGONAL, ORTHOGONAL]
[1, 1, 1, 1, 1, 1, 1, 1, 0, 0]
output key length :10
```

Figure 6. *Implementation of Quantum key distributions and emperor node generation*



```
Step six:After comparision of Client & Server
[DIAGONAL, DIAGONAL, DIAGONAL, ORTHOGONAL, DIAGONAL, DIAGONAL, DIAGONAL, DIAGONAL]
[1, 1, 1, 1, 0, 0, 1, 0]
output key length :8
Select:
        0- metro-w1.txt
        1- sonet-200.txt
        2- sonet-1000.txt
Your answer :: 1

Linking : 0 <----> 199
Linking : 0 <----> 2
Linking : 0 <----> 1
Linking : 0 <----> 5
Linking : 0 <----> 8
Linking : 0 <----> 6
Linking : 0 <----> 9
Linking : 0 <----> 3
Linking : 0 <----> 190
Linking : 0 <----> 193
Linking : 0 <----> 194
Linking : 0 <----> 4
Linking : 0 <----> 7
Linking : 0 <----> 10
```

Figure 7. *Emperor Node selection and connection establishment*



```
Linking : 199 <----> 197
Linking : 199 <----> 0
Linking : 199 <----> 198
Linking : 199 <----> 192
Data is loaded.
----------------------------------------------------
Menu :
        0- Quit.
        1- Find the 10 most connected elementss.
        2- Find the shortest path from one element to another.
        3- Verifier les six degrees de separation.
What do you want to do?
Your answer :: 1

Top 10 most connected nodes:
        Number of connections: 21 -- 116
        Number of connections: 21 -- 12
        Number of connections: 21 -- 127
        Number of connections: 21 -- 133
        Number of connections: 21 -- 160
        Number of connections: 21 -- 186
        Number of connections: 21 -- 188
        Number of connections: 21 -- 71
        Number of connections: 21 -- 90
```

```
        Number of connections: 21 -- 133
        Number of connections: 21 -- 160
        Number of connections: 21 -- 186
        Number of connections: 21 -- 188
        Number of connections: 21 -- 71
        Number of connections: 21 -- 90
        Number of connections: 20 -- 0
----------------------------------------------------
Menu :
        0- Quit.
        1- Find the 10 most connected elementss.
        2- Find the shortest path from one element to another.
        3- Verifier les six degrees de separation.
What do you want to do?
Your answer :: 2

Enter a name : 199
The answer "199" has been registered.
Enter a name : 198
The answer "198" has been registered.
Path from "199" vers "198" :

        Group(s) : []     : 199
        Group(s) : []     : 198
```

Where E_time is the encryption time, e_c is the computation time of encryption and r_c is the response time of encryption. Figure 7 shows the encryption time for different files for the proposed scheme.

4.3.2 Decryption Time

It is the time taken by the decryption to convert the ciphertext into plain text. The decryption time of the data after decrypting it by the proposed technique is illustrated in Figure 8.

$$\mathrm{D\_time} = \frac{d_c}{\mathrm{s}_c} \tag{15}$$

Where D_time is the encryption time, d_c is the computation time of decryption and s_c is the response time of decryption.

Figure 9 shows the decryption time for different files for the proposed scheme. Decryption time is estimated based on the decryption algorithm to convert the ciphertext into the plain text.

4.3.3 Execution Time

It is the process of time taken to establish the connection between user and cloudlet, thus illustrates in Figure 10. The figure here represents up to 100 cloudlet connections that initially established a very less time amount. After some numbers of cloudlet, the execution time is increased, therefore it illustrates the proposed technique efficiently provide the connection establishment in an effective manner of time.

4.3.4 Throughput

Network capacity in data transmission is the amount of data successfully transferred in a given period from one location to another and usually calculated in bits per second (bps). Here in Figure 11 illustrates the throughput of the proposed systems.

Figure 8. *Encryption time*

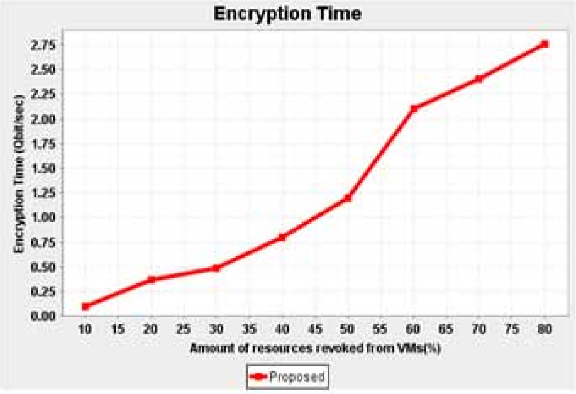


Figure 9. *Decryption time*

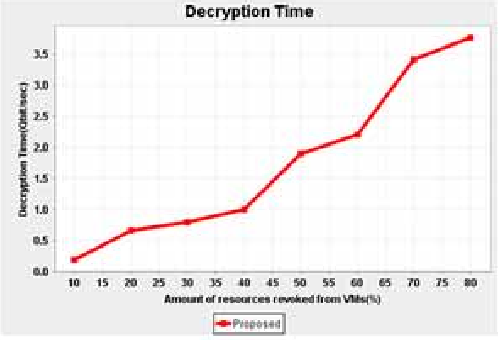


Figure 10. *Execution time*

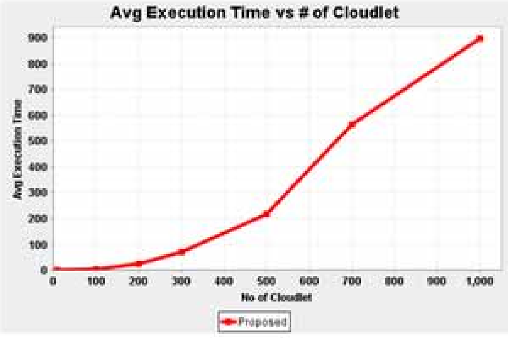
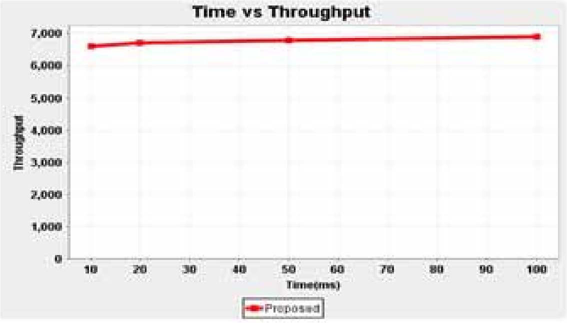


Figure 11. *Throughput*

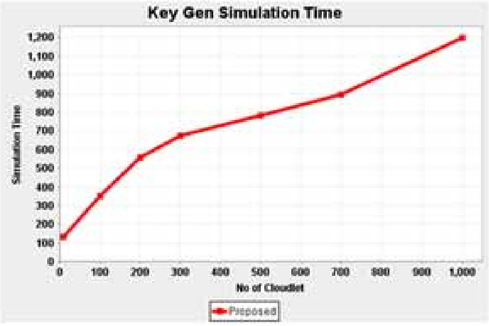


4.3.5 Key Generation Time

Key generation in cryptography is the process of generating keys. A key is used to encrypt and decrypt anything that encrypts/decrypts data. A key generator or keygen is a device or program used to generate the keys. Therefore the time taken for key generation is illustrated in Figure 12.

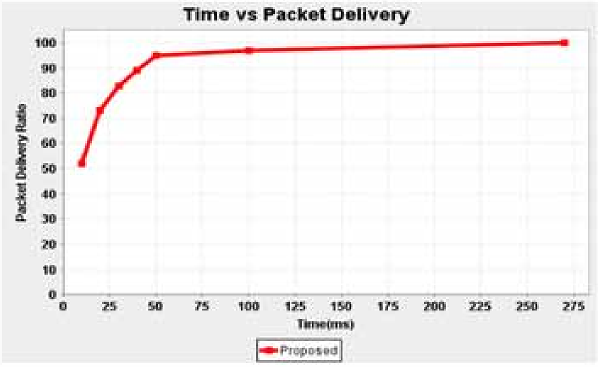
4.3.6 Packet Delivery Ratio

Figure 12. *Key generation time*



Packet delivery ratio is the number of packets sent to a destination successfully, compared to the number of packets sent by the sender. To measure the transmission ratio of the packets, it needs the total number of packets sent and several packets received. In Figure 13 described the packet delivery ratio in the proposed system. Thus it shown the competence of the proposed system in packet delivery based on time.

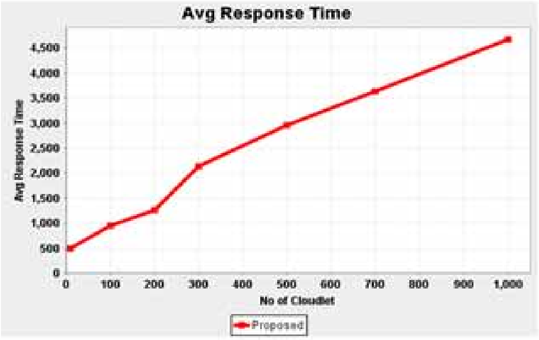
Figure 13. *packet delivery ratio*



4.3.7 Average Response Time

Response time refers to the amount of time it takes for the Application Server to return the user the results of a request. Factors such as network bandwidth, number of users, number and type of requests sent, and average think-time influence the response time, thus it illustrates the Figure 14.

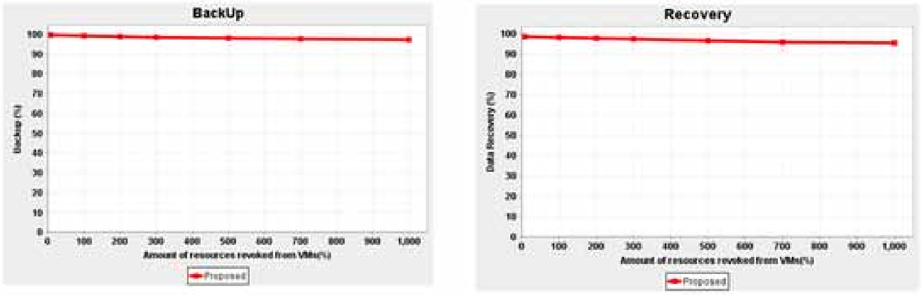
Figure 14. *Average response time*



4.3.8 Backup and Recovery Analysis

Backup and recovery refer to the process of data backup in the event of loss and system setup that allows data recovery due to data loss. Data backup requires computer data copying and archiving so that data can be accessed in the event of data deletion or corruption. The performance of backup and recovery is described in Figure 15.

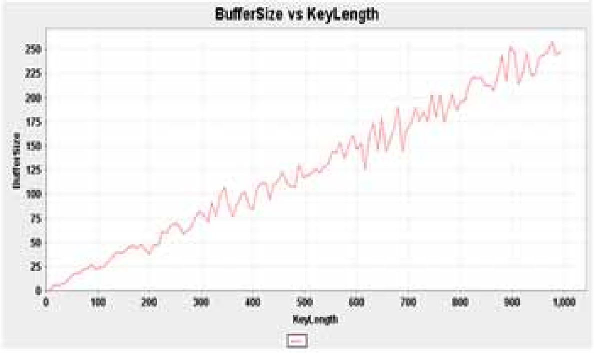
Figure 15. *backup and recovery analysis*



4.3.9 Buffer Size

The optimum buffer size depends on several network environment variables including switch and device types, recognition timing, error rates, the topology of the network, memory capacity, and data transfer size. In Figure 16 shown the illustration of buffer size based on key length.

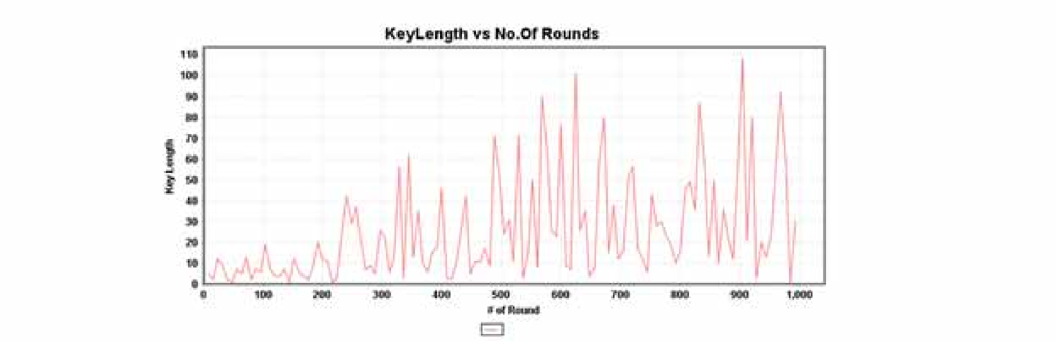
Figure 16. *Buffer size based on key length*



4.3.10 Key Length

In cryptography, the key size or key length is the number of bits that a cryptographic algorithm uses in a key. Key length defines the upper bound on the safety of an algorithm therefore Figure 17 illustrates the proficiency of the proposed security algorithm.

Figure 17. *key length based on the number of rounds*



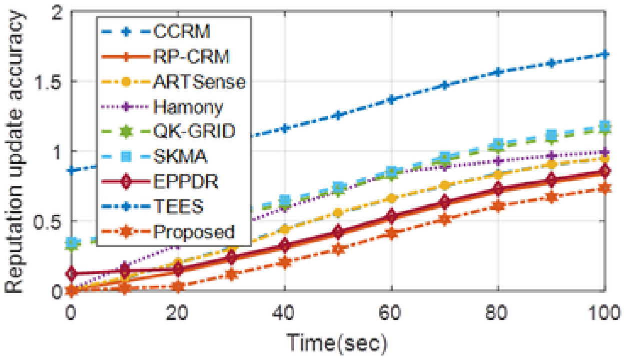
4.4 Comparison Result

In the comparison results, Reputation and its update accuracy, Effective recommendation rate (ERR), malicious user detection rate (MDR), time elapsed for the key generation and throughput for the proposed method is compared with the various existing methods such as CCRM (Lin et al., 2017), harmony (Shen & Liu, 2014), RP-CRM (Lin et al., 2014), ARTSense (Wang et al., 2013), QK-GRID (Arul et al., 2019), SKMA (Ghosh, 2019), EPPDR (Treacy & McCaffery, 2016), and TEES (Sowjanya et al., 2019). The comparative results are shown in the following figures.

4.4.1 Reputation and its Update Accuracy

Figure 18, shows the comparison of the proposed method Reputation update accuracy with the existing method such as CCRM, PR-CRM, ARTSense, Harmony, QK-GRID, SKMA, EPPDR, and TEES respectively. Here, the proposed method took lesser time and drop the other eight mechanisms. Initially, for 0.0207 it took only 10sec and for 0.7357 it took 100sec which is lesser than the other existing method.

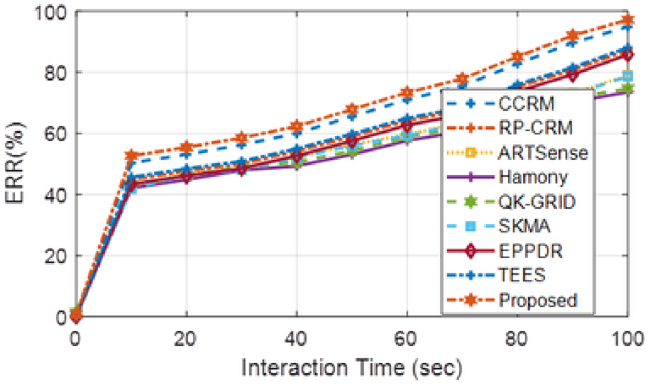
Figure 18. comparison of Reputation update accuracy



4.4.2 Effective Recommendation Rate (ERR)

Figure 19, shows the comparison of the proposed method Effective recommendation rate with the existing method such as CCRM, PR-CRM, ARTSense, Harmony, QK-GRID, SKMA, EPPDR, and TEES respectively. This evaluated the effectiveness and reliability of the nine mechanisms by comparing their ERR performances. The result shows that the ERR performance is very close. The ERRs of ARTSense and Harmony decrease by 15% and 30%, respectively, and the ERRs of RP-CRM and CCRM decrease by 10% and 20%, respectively. The ERR of the proposed method is higher than the other eight existing methods.

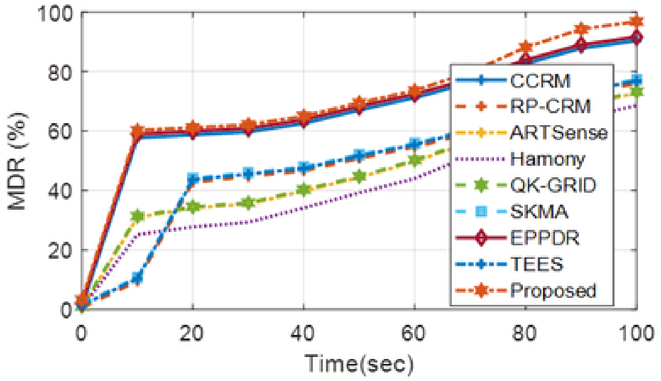
Figure 19. comparison of Effective recommendation rate



4.4.3 Malicious User Detection Rate (MDR)

Figure 20, shows the comparison of the proposed method malicious user detection rate with the existing method such as CCRM, PR-CRM, ARTSense, Harmony, QK-GRID, SKMA, EPPDR, and TEES respectively. MDR decreases with time and increases the percentage of strong authentication. It is observed that the MDR of the proposed method is highest among the other existing methods. This finding is observed because the integrated combination of the data category, context sensing, and security relevance scheme improves the accuracy, efficiency, and reliability of the user authentication and thus enhances the MDR.

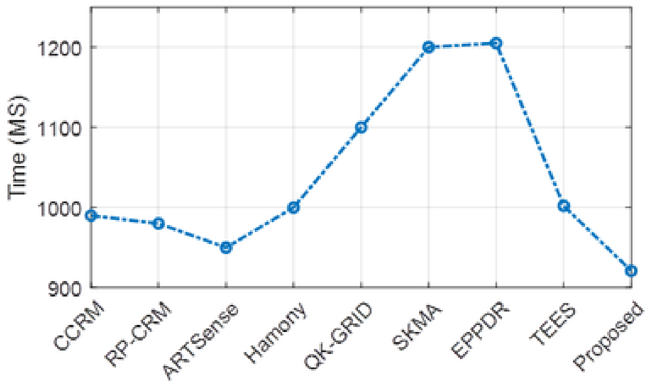
Figure 20. comparison of malicious user detection rate



4.4.4 Time Elapsed for Key Generation

The time elapsed for key generation is defined as securely generating and distributing the secret keys. In Figure 21 described the proposed performance of time taken for a key generation with existing techniques. Here existing QK-GRID technique taken time for key generation is 1251.4milli seconds, and SKMA is 1145.789milli seconds. Finally, the proposed system taken for key generation time is 998.756milli second.

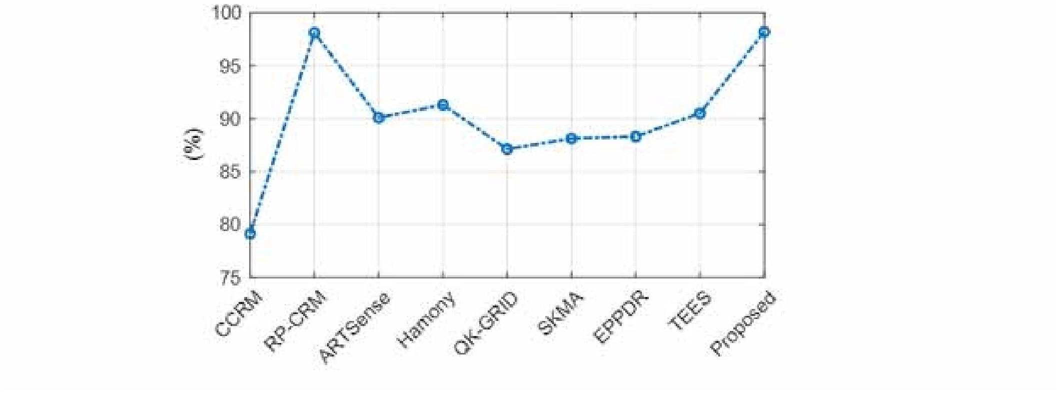
Figure 21. *comparison of time elapsed of key generation*



4.4.5 Throughput

The overall system throughput is compared with existing techniques in Figure 22. Thus it described the existing technique perform a very low percentage of throughput such as EPPDR throughput is 92.47% and TEES is 94.59% then the proposed system throughput is 98.75%.

Figure 22. *Comparison of throughput*



Thus from the above comparison result, the proposed work has efficiently attained greater output than the existing method. Reputation and its update accuracy, Effective recommendation rate (ERR), malicious user detection (MDR), Time elapsed for key generation and throughput is taken for comparison with the existing methods such as CCRM, PR-CRM, ARTSense, Harmony, QK-GRID, SKMA, EPPDR, and TEES. Time taken for the reputation update accuracy is lesser compare to the existing method and the ERR performance is also higher for the proposed work. The MDR of the proposed method is highest among the other existing methods and the finding is observed because the integrated combination of the data category, context sensing, and security relevance scheme improves the accuracy, efficiency, and reliability of the user authentication and thus enhances the MDR. The proposed method has only taken 998.756milli a second time for the key generation while previous methods such as QK-GRID, and SKMA has taken 1251.4milli seconds, and 1145.789milli seconds for the key generation which is so far. Also, throughput for the proposed method has achieved 98.75% which is higher than the existing method as EPPDR 92.47% and TEES is 94.59% respectively. The performance of the proposed method is shown under a different scenario with a comparison of the existing methods.

5. CONCLUSION

Mobile cloud computing has become a very active study subject over the previous few years and has therefore attracted a lot of researcher's attention. For security concerns in MCC, this paper proposed a novel Trefoil Congruity framework, which efficiently offers tri-level security in mobile cloud computing. Initially, the Quantum Key Fibo Privacy Approach (QKFPA) is introduced along with quantum computation which performed the key generation in an effectual time manner and offered great security to transmit/upload the user data. Also, High-Security Distribution and Rake Systems are enhanced to search for data manipulation or destruction by the attacker and ensure the recovery of data without failure. Finally, the research introduces the Emperor-Imperial technique which enhanced the data confidentiality to ensure robust authentication with less time of connection establishments between user and cloudlet. The proposed method has achieved a high throughput value of 98.75% and the elapsed time for generating key is 998.756ms which takes less time compared to the prior methodologies. Also, it attains 96% and 97% of backup and recovery of stored data than the previous methods. The ERR and MDR performance is also higher than the other respective existing methods. Hence it provides strong authentication and security to access data only for the authorized user and effectually achieve better results for data backup and recovery. In the future, the analysis of bandwidth and energy efficiency when transferring/storing the data in cloud computing will be the main consideration.

REFERENCES

Ahmed, E., Naveed, A., Gani, A., Ab Hamid, S. H., Imran, M., & Guizani, M. (2019). Process state synchronization-based application execution management for mobile edge/cloud computing. *Future Generation Computer Systems*, *91*, 579–589. doi:10.1016/j.future.2018.09.018

Annane, B., Ghazali, O., & Alti, A. (2019). A new secure proxy-based distributed virtual machines management in mobile cloud computing. *International Journal of Advanced Computer Research*, *9*(43), 222–231. doi:10.19101/IJACR.PID10

Arul, R., Raja, G., Almagrabi, A.O., Alkatheiri, M.S., Chauhdary, S.H., & Bashir, A.K. (2019). A Quantum-Safe Key Hierarchy and Dynamic Security Association for LTE/SAE in 5G Scenario. *IEEE Transactions on Industrial Informatics*.

Bellini, E., Marcolla, C., & Murru, N. (2020). *On the decoding of 1-Fibonacci error-correcting codes.* arXiv preprint arXiv:2003.12991.

Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., Perrenoud, M., Gras, G., Bussières, F., Li, M. J., Nolan, D., Martin, A., & Zbinden, H. (2018). Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters*, *121*(19), 190502. doi:10.1103/PhysRevLett.121.190502 PMID:30468607

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*, 24–41. doi:10.1016/j.future.2015.09.031

Chaudhry, S. A., Kim, I. L., Rho, S., Farash, M. S., & Shon, T. (2019). An improved anonymous authentication scheme for distributed mobile cloud computing services. *Cluster Computing*, *22*(1), 1595–1609. doi:10.1007/s10586-017-1088-9

Gharajeh, M. S. (2015). *The Significant Concepts of Cloud Computing: Technology, Architecture, Applications, and Security*. CreateSpace Independent Publishing Platform.

Gharajeh, M. S. (2017). Security Issues and Privacy Challenges of NoSQL Databases. In G. C. Deka (Ed.), *NoSQL: Database for Storage and Retrieval of Data in Cloud* (pp. 271–290). Chapman and Hall/CRC. doi:10.1201/9781315155579-15

Ghosh, S. (2019). A Quantum-based Signcryption for Supervisory Control and Data Acquisition (SCADA). *Networks*.

Ghudayyer, M. B., Javed, Y., & Alenezi, M. (2017). A Security Perspective on Adoption and Migration to Mobile Cloud Technology. *JOIV: International Journal on Informatics Visualization*, *1*(4), 143–149. doi:10.30630/joiv.1.4.54

Gupta, B. B., & Badve, O. P. (2017). Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. *Neural Computing & Applications*, *28*(12), 3655–3682. doi:10.1007/s00521-016-2317-5

Han, D., Yan, Y., & Shu, T. 2015, December. Context-aware distributed storage in mobile cloud computing. In 2015 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

Han, Z., Yang, L., Wang, S., Mu, S., & Liu, Q. (2018). An efficient multifactor two-server authenticated scheme under mobile cloud computing. *Wireless Communications and Mobile Computing*, *2018*, 2018. doi:10.1155/2018/9149730

Huang, X., Liu, J. K., Tang, S., Xiang, Y., Liang, K., Xu, L., & Zhou, J. (2014). Cost-effective authentic and anonymous data sharing with forwarding security. *IEEE Transactions on Computers*, *64*(4), 971–983. doi:10.1109/TC.2014.2315619

Kim, H. W., & Jeong, Y. S. (2018). Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain. *Human-centric Computing and Information Sciences*, *8*(1), 11. doi:10.1186/s13673-018-0136-7

Lin, H., Hu, J., Tian, Y., Yang, L., & Xu, L. (2017). Toward better data veracity in mobile cloud computing: A context-aware and incentive-based reputation mechanism. *Information Sciences*, *387*, 238–253. doi:10.1016/j.ins.2016.12.031

Lin, H., Xu, L., Mu, Y., & Wu, W. (2014). A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing. *Future Generation Computer Systems*, *52*, 125–136. doi:10.1016/j.future.2014.10.032

Ma, R., Li, J., Guan, H., Xia, M., & Liu, X. (2015). EnDAS: Efficient encrypted data search as a mobile cloud service. *IEEE Transactions on Emerging Topics in Computing*, *3*(3), 372–383. doi:10.1109/TETC.2015.2445101

Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications*, *84*, 38–54. doi:10.1016/j.jnca.2017.02.001

Mordor Intelligence Industry Report. (2018). *Mobile Cloud Market*. https://www.mordorintelligence.com/industry-reports/global-mobile-cloud-market-industry

Nayak, A., & Bansode, R. (2016). Analysis of knowledge-based authentication system using persuasive cued click points. *Procedia Computer Science*, *79*, 553–560. doi:10.1016/j.procs.2016.03.070

Oludele, A., & Oluwabukola, O. (2016). A survey of mobile cloud computing applications: perspectives and challenges. In International multi-conference on complexity, informatics, and cybernetics. Academic Press.

Pandian, A. P., & Smys, S. (2020). Effective Fragmentation Minimization by Cloud-Enabled Back Up Storage. *Journal of Ubiquitous Computing and Communication Technologies*, *2*(01), 1–9. doi:10.36548/jucct.2020.1.001

Shen, H., & Liu, G. (2014). An efficient and trustworthy resource sharing platform for collaborative cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, *25*(4), 862–875. doi:10.1109/TPDS.2013.106

Sood, S. K. (2019). Mobile fog based secure cloud-IoT framework for enterprise multimedia security. *Multimedia Tools and Applications*, 1–16. doi:10.1007/s11042-019-08573-2

Sowjanya, P. I., Sudhakar, P., & Narayana, D. V. S. (2019). Application of an Encrypted Data search across Mobile Clouds. *International Journal for Innovative Engineering & Management Research*, *8*(05). Advance online publication. doi:10.2139/ssrn.3395106

Treacy, C., & McCaffery, F. (2016). Data security overview for medical mobile apps assuring the confidentiality, integrity, and availability of data in transmission. *International Journal on Advances in Security*, *9*(3 & 4), 146–157.

Tsai, J. L., & Lo, N. W. (2015). A privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE Systems Journal*, *9*(3), 805–815. doi:10.1109/JSYST.2014.2322973

Wang, C., Ren, K., & Wang, J. (2015). Secure optimization computation outsourcing in cloud computing: A case study of linear programming. *IEEE Transactions on Computers*, *65*(1), 216–229. doi:10.1109/TC.2015.2417542

Wang, X., Cheng, W., & Mohapatra, P. (2013). Artsense: anonymous reputation and trust in participatory sensing. *The 2013 IEEE Proceedings of INFOCOM*, 2517–2525.

Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X., & Ren, K. (2016). A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*, *11*(11), 2594–2608. doi:10.1109/TIFS.2016.2590944

APPENDIX A. ADDITIONAL DATA

With the rise in the challenges of mobile cloud computing during data transmission, User authentication plays a vital role in tackling these issues with the aid of cryptographic solutions as well as storage and recovery have become a serious issue that has been widely faced daily in our lives nowadays. To tackle these issues, This paper proposes an efficient Trefoil Congruity framework, Which includes Quantum Key Fibo Privacy Approach (QKFPA) ensures robust safety and HSDRT attains the lossless backup and recovery of the data then Emperor-Imperial technique offers the strong authentication for data access which is more indispensable in mobile cloud computing.