International Journal of Advanced Science and Technology
Vol. 29, No. 8, (2020), pp. 5520 - 5533

`

A Fog-Centric Quantum Security for Cloud Storage Scheme with Enhanced Multipath Routing Architecture

B. Shireesha,
M.Tech Student, Dept of Computer Science And Engineering, JNTUA College of Engineering, Pulivendula-516390, Andhra Pradesh, India

Dr.G. Murali
Assistant Professor and Head of the Department, Dept of Computer Science And Engineering, JNTUA College of Engineering, Pulivendula-516390, Andhra Pradesh, India

Abstract

Now a days the cloud computing has been widely used in day to day life. Confidentiality, Integrity, and Availability are basic goals of security architecture. To ensure CIA, many authentication scheme has been introduced in several years. Every type of data is stored in the cloud and it can be easily accessed at any time and any place. But, while coming to the privacy in the cloud computing it steps behind due to location awareness. Cloud computing uses a fog-centric secure scheme to protect data against unauthorized access, modification, and destruction. To prevent the illegitimate access, the scheme employs a new technique Xor-Combination to conceal data. Moreover, Block-Management outsources the outcomes of Xor-Combination to prevent malicious retrieval and to ensure better recoverability in case of data loss. The current system uses hash algorithm for detection with higher probability. But the current algorithm does not providing better efficiency and security. The Proposed work is a different approach when compare with existing system for securing data in the cloud using segment technology and faster multipath routing. Proposed approach will be providing the better efficiency and security for the cloud storage. To enhance the efficiency of fog based cloud storage service, multi path file transmission has been used, in which a file will be divided into many parts and transmit to cloud servers via various fog servers. Currently deployment of Public Key Infrastructure (PKI) is a most significant solution. PKI involving exchange key using certificates via a public channel to a authenticate users in the cloud infrastructure. However, there is a certain issue pertaining to the PKI authentication where the public key cryptography only provide computational security because PKI is based on Asymmetric Key Cryptography. It is exposed to widespread security threats such as eavesdropping, man in the middle attack, masquerade et al. This paper aims to look into basic security architecture in place currently and further it tries to introduce a new proposed security architecture, which makes use of the knowledge of Quantum Mechanics and current advances in research in Quantum Computing, to provide a more secure architecture.

Keywords: *Fog Security, Quantum Computing, Multipath Routing.*

I. INTRODUCTION

Legacy Cloud networks are frequently designed to function with easy single-direction routing, like shortest-course, which is understood to be throughput suboptimal. On the alternative hand, previously proposed throughput premiere guidelines (i.e., backpressure) require every tool in the community to make dynamic routing choices. In this painting, I study an overlay structure for dynamic routing such that simplest a subset of devices (overlay nodes) want to make dynamic routing selections. I determine the crucial series of nodes that should bifurcate visitors for accomplishing the maximum multi

ISSN: 2005-4238 IJAST

commodity network throughput. We apply our choicest node placement algorithm to several graphs and the effects display that a minimum fraction of overlay nodes is enough for attaining maximum throughput. Finally, we suggest a heuristic coverage, which dynamically controls site visitors' bifurcations at overlay nodes. In all studied simulation situations, OBP now not simplest achieves full throughput, however additionally reduces delay in evaluation to the throughput choicest backpressure routing. Multipath Switching systems (MPS) play a pivotal function in fabricating latest high overall performance core routers. A famous paradigm is the deployment of Benes multistage switches in Cisco CRS-1. Other examples consist of the Varese transfer chip family implementing the Parallel Packet Switch (PPS), and the Load-balanced Birkhoff- von Neumann (LBVN) switches. In general, MPS is constructed by aggregating several decrease velocity SWI. In previous solutions cannot gracefully deal with the weight-balancing problem in MPS to satisfy the 3 goals outlined above. In this paper, I broaden a brand new scheme known as Flow Slice (FS) that achieves our load balancing goals perfectly. Based on the observations on tens of widely located Internet lines, I discover that the interflow packet durations are often, say in 40-50 percent, larger than the delay upper certain at MPS which can be calculated statistically. If I cut off each float at every c programming language larger than a reducing threshold set to this certain and balance the weight on the generated waft slices, all three objectives are met concurrently: Flow slices exhibit small common size, mild-tailed size distribution, and large in general variety; consequently, the common load balancing of FS, measured by using common packet delay and loss rate, is only fairly degraded from the most appropriate load balancing. In our simulations, FS gets nearly the same loss fee because the most excellent even underneath load charge of 0.95. The assignment also depicts the average IF underneath FS. It suggests that the burden-balancing uniformity improves fast closer to the ultimate price as timescale increases.

As the cutting threshold is about to the statistical delay upper bound at MPS, the interflow packet order is saved intact as they come. Exceptions simplest arise in negligible possibility (under 10_6) [5]. Hence, there is no want to use luxurious sequencing mechanisms. Throughout the paper, except otherwise referred to, the statistical postpone (top) sure is described as a minimal price t that greater than 99.9999 percent packet delays thru MPS are smaller than t. Through lay-apart Buffer Management module, all packets are really queued on the output according to the float group and the priority class in a hierarchical way. The output scheduler fetches packets to the output line the use of information provided with the aid of. Packets within the identical drift will bevirtually buffered within the same queue and scheduled in subject. In this challenge a singular load-balancing scheme, specifically, Flow Slice, based totally at the truth that the intraflow packet c language is often, large than the. Due to a few advantageous properties of waft slice, our scheme achieves properly load-balancing uniformity with little hardware overhead and timing complexity. By calculating put off bounds at three famous, I display that when the reducing threshold is ready to the smallest admissible value at, the FS scheme can reap ultimate performance while retaining the intraflow packet out-of-order possibility negligible given an inner speedup up to 2. Our outcomes are also proven via hint-pushed prototype simulations beneath visitor's styles.

ISSN: 2005-4238 IJAST

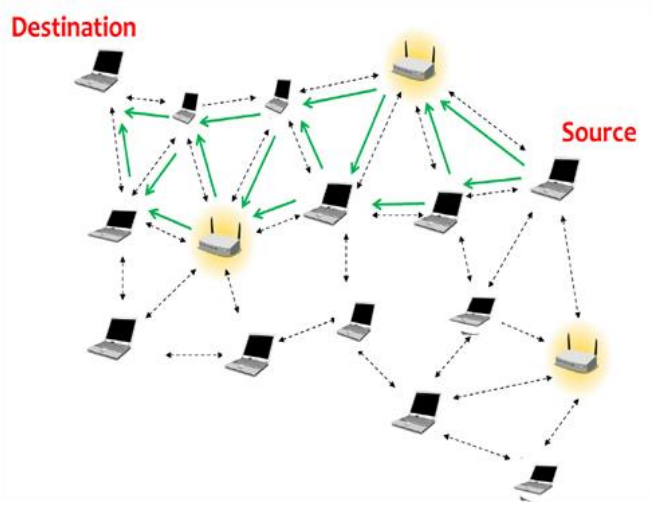


Fig 1: Multi Path Routing

In Internet communication network that can operate without existing infrastructure and support a number of mobile users. It is one of the general scopes of multi-hop networking. Such networking paradigm originated from the needs in emergency operations, battlefield communications, search and rescue, and disaster relief operations. The main challenges in this area of research include end-to-end data forwarding, communication link access control, network security and providing support for real-time multimedia streaming. Centralized control and management or fixed network infrastructure such as base stations or access points are not essential in ad-hoc networks. Quick and inexpensive set up can be done for it, as needed. In a network contains an autonomous group of mobile users that communicate over reasonably network links. Due to the mobility of nodes, many rapid and unpredictable changes may be done over the time. In such network, the mobile nodes maintain all the network activities like route discovery and message delivery, so that such network is decentralized. In this paper, we propose a lightweight proactive source routing protocol to facilitate opportunistic data forwarding in Cloud Networks. The information is periodically exchanged among neighbouring nodes for updated network topology information to all other nodes in the network. This allows it to support both source routing and conventional IP forwarding. When doing this, we try to reduce the routing overhead as much as we can. The results of simulation denote that our methodology has only a fraction of overhead of OLSR, DSDV, and DSR but still offers a similar or better data transportation capability compared with these protocols.

Confidentiality is a basic for strong confidentiality security in all online computing sides, but confidentiality alone is not satisfies. Companies and customers are ready to use online computing only if they have the belief that their data will stay confidential and safe. Thus to produce a trusted surrounding for customers, we need to create a software, assist and works with confidentiality in mind. The location of physical assets and accessories being allowed in general doesn't known to the particular user. It also affords services for user to form up, use and maintain their data in the applications on the cloud, which maintains and manages the virtualization of assets by itself. Cloud memory is a method of networked online memory in which the data is stored in virtual group of stash that is generally being introduced by the third person. Cloud memory makes data stored remotely to be limitedly cached on mobiles, PC or other Internet connected devices. Confidentiality and cost are the barriers in this field, depending on the dealers. Although the first achievement and identification of the cloud model and the broad availability of producers and tools, a number of trials and prospects are intuitive to this new design of computing.

ISSN: 2005-4238 IJAST

II. LITERATURE SURVEY

Denture and Bad ache [4] proposed security mechanism is essential which keeps document of node's public and private key. While a node forwards a packet to the following node inside the path it generates a random range and encrypts it with the public key of node. Once the two hops lost node obtained this packet it decrypts and send the equal random huge variety as an acknowledgement. Acknowledgement is authenticated with the aid of the node's public key and some encryption method.But the node does not obtained acknowledgment by hops left node and it indict the only hop away node as selfish. The 2 ACK receivers, video display units the hyperlink periodically via retaining the information approximately the no of statistics packets dispatched and the no of facts packets does no longer stated inside the duration. Samreen and Narasimha [1] explained 2ACK technique detects the misbehaving link but can't decide the related node wherein nodes are misbehaving for that reason, PFC tracking as to stumble on the misbehaving nodes as soon as the misbehaving hyperlink is detected. Hernandez-Oral [3] delivered Watchdogs to discover egocentric nodes in computer networks. A watchdog is the collaborative method. The analytical model is comparing the detection time and value of this collaborative approach. Watchdog can appreciably reduce the overhead and decrease common detection time. Also improve the accuracy. Hernandez-Oral et al [7] proposed CCW (Collaborative Contact-based Watchdog) approach is a collaborative based absolutely at the diffusion of nearby selfish nodes alertness consequently that statistics approximately egocentric nodes is rapidly propagated.This approach reduces the time and increases the accuracy even as detecting egocentric nodes. Hussein et al [6] proposed egocentric node detection which includes two major considerations. First, it makes a specialty of the elements that result in suitable nodes to act self-interestedly. Second, it proposed a barely mild-weight mechanism in phrases of low power intake.

This approach includes three fundamental modules such as tracking, records collection and detection. Tarannum and Payday [11] explained detecting and eliminating the misbehaving node in addition have to improve the performance of the machine by means of reentering the fake detected node in community. This scheme consists of Data Gathering and Processing, Decision Making, and Response Operation. Gathering and Processing Module of the device collect information in approaches; first it regionally runs a tracking manner to get the behavior data of neighbor nodes and secondly it exchanges this statistics with different nodes monitored statistics. This module is used as a statistics processing unit. Manchikalapudi et al [8] proposed that every node within the network monitors the sports of its neighbors and if any irregular action is detected it invokes set of rules to conclude whether the assumed node is without a doubt egocentric. This mechanism builds trust in the network with the aid of communications among a few protection components. The additives at each node are manager, aggregator, accept as true with calculator and disseminator. Supervisor module video display units pals through passively concentrate to their communiqué. This module makes use of Passive Acknowledgement (PACK) mechanism that tests whether or not the buddies genuinely ahead the packets or drops them. Aggregator module collects all the details of the verbal exchange that can be used to estimate the wide variety of packets dropped. Trust calculator is determined by the share of packet dropped. The percentage is dealt with as fuzzy enter variable and the output of the set of rules is agree with level of a node. Muthumalathi and Raseen [9] introduced that each node can approximate the diploma of selfishness supposed for all of its connected nodes based at the Credit Risk (CR) score. CR is calculated based totally on the common of credit score hazard and predicted fee. Selfish functions are categories including Node precise and Query processing specific. Node-precise functions represent the scale of shared memory area and the range of shared information objects may be used to symbolize the diploma of selfishness. The question processing-specific characteristic can constitute the anticipated risk of a node. Every node has its own threshold cost. The measured CR while exceeds the edge node may be detected as a selfish node. Kargl et al [5] defined an algorithm which may be labeled

ISSN: 2005-4238 IJAST

into two predominant classes; the first is detection and exclusion while detection is to locate the selfish nodes and isolate them from community and the second is motivational this is perceive egocentric nodes and set off them to cooperate in network. MIMO (Multi-Input and Multi-Output) became proposed by means of Rachedi and Baddish [10]. It allows the display node to keep away from the collision during the tracking manner with the aid of adjusting the antennas weights with the intention to invalidate the signal coming from other nodes than the monitored one. Sundararajan and Shanmugam [12] proposed strength saving is the most effective motive assumed for a node is egocentric. Hence the node is performing selfishness based on residual electricity. While the node has highest electricity, the node is successful to deliver extra cooperation as well as greater packet transport ratio. Suit and Pinkie [13] proposed the egocentric node detection and punishment could be very important problem and makes the nodes cooperative in nature in case of transferring records. Replica allocation approach is very efficient for co-running the selfish node to different nodes. It is used to make the egocentric node cooperative to different nodes. The network is disrupted such that the nodes aren't dependable for forwarding packets. This method is applicable for all nodes which might be having facts items of other nodes. When the record transmits from one node to other nodes, allocation of reminiscence area of each node is responsible for conversation. If one node is selfish inside the network the memory area of selfish node would not take the records items of other neighbor. In desire of forwarding packets through the selfish nodes replica the records gadgets of neighbor nodes into the memory area of selfish node explicitly and make the selfish node cooperative to different nodes. Reputation based and Credit based technique for detection of selfish node in MANETs becomes proposed by means of Dipole and Supriya [14]. 2ACK system uses the Reputation based totally technique to perceive and diminish the effect of misbehaving nodes in MANET. As well as laborious the egocentric nodes and cheering the cooperating nodes there may be 2nd alternative for the nodes are dropped a packet reluctantly. This method made the node to be a egocentric node and punished. Thus cooperation coefficient is improved then it modifications its conduct.

III. APPLICATIONS

Secure Cloud Computing

With the success of Internet, there has been a rapid and significant success in the development of data processing and data storage technologies. These advancements in storage techniques alongside SaaS techniques have enabled a different computing model – Cloud Computing. Examples of such service providers include big players like Google, Microsoft, Apple, Amazon et al. Since the data transfer for such an application occurs through the classical network, storage on the same server for many users where resource allocation and scheduling is provided by the cloud service provider and with the breakthrough in malicious programs, cloud security becomes an important issue. Every day hackers are trying to hack into some cloud or the other and recently with the security of giants like Apple and Dropbox being compromised, With the success of Internet, there has been a rapid and significant success in the development of data processing and data storage technologies. These advancements in storage techniques alongside SaaS techniques have enabled a different computing model – Cloud Computing. Examples of such service providers include big players like Google, Microsoft, Apple, Amazon et al. Since the data transfer for such an application occurs through the classical network, storage on the same server for many users where resource allocation and scheduling is provided by the cloud service provider and with the breakthrough in malicious programs, cloud security becomes an important issue. Every day hackers are trying to hack into some cloud or the other and recently with the security of giants like Apple and Dropbox being compromised, 10 cloud security has become a hot topic. Here, I'm trying to propose a new hybrid security architecture for the cloud which uses benefits of current protocols like Kerberos and security benefits of Quantum Cryptography

ISSN: 2005-4238 IJAST

IV. PROPOSED SYSTEM

Techniques to offer throughput-most advantageous multipath routing have been explored in numerous contexts. The work within the current machine considers the trouble of placing hyperlink weights provided to the Open Shortest Path First routing protocol such that, when coupled with bifurcating traffic equally among shortest paths, the network achieves through- put equal to the premiere multi commodity drift. The authors of the existing machine use an entropy maximization framework to increase a new throughput-most desirable hyperlink kingdom routing protocol where each router intelligently bifurcates site visitors for each vacation spot amongst its outgoing links. These existing techniques all require centralized control, time-honored adoption by all community nodes, or both; thus none of these strategies could offer incremental deployment of throughput most fulfilling routing to cloud networks. Moreover, those techniques cannot be used alongside throughput foremost dynamic manipulate schemes, such as backpressure. In the proposed system, the system implemented overlay architecture for dynamic routing such that only a subset of devices need to make dynamic routing decisions.

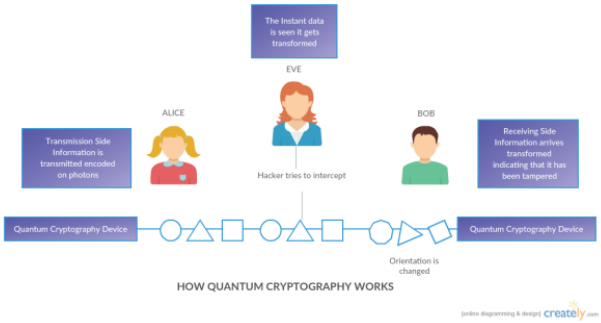
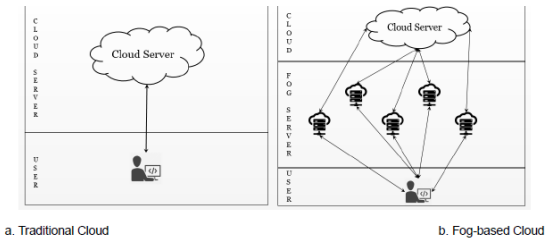


Figure 1: The working of Quantum Cryptography

Fig 1: Three Cloud Architecture with Quantum Cryptography



a. Traditional Cloud b. Fog-based Cloud

Fig. 1. Comparative computing architecture

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the

ISSN: 2005-4238 IJAST

hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal.

CIA triad – Confidentiality, Integrity, and Availability are basic goals of security architecture. To ensure CIA, many authentication scheme has been introduced in several years. Currently deployment of Public Key Infrastructure (PKI) is a most significant solution. PKI involving exchange key using certificates via a public channel to a authenticate users in the cloud infrastructure. However, there is a certain issue pertaining to the PKI authentication where the public key cryptography only provide computational security because PKI is based on Asymmetric Key Cryptography. It is exposed to widespread security threats such as eavesdropping, man in the middle attack, masquerade et al. This paper aims to look into basic security architecture in place currently and further it tries to introduce a new proposed security architecture, which makes use of the knowledge of Quantum Mechanics and current advances in research in Quantum Computing, to provide a more secure architecture.

In a classical computing system, a bit would have to be in one state or the other. However in a quantum computing system, quantum mechanics allows the qubit to be in a superposition of both states at the same time. In quantum computing, a qubit or quantum bit (sometimes qbit) is a unit of quantum information—the quantum analogue of the classical bit. A qubit is a two-state quantum-mechanical system, such as the polarization of a single photon: here the two states are vertical polarization and horizontal polarization

Algorithm

In 1994, Shor proposed an algorithm for period finding and then subsequently integer factorization problem. Later, Shor also proposed an efficient quantum algorithm for the discrete logarithm problem. Shor's algorithm consists of Classical Part and Quantum Part. Quantum part of the algorithm, uses quantum Fourier transform to find the period of a certain function, which is infeasible with classical computers, but in 2001 a group at IBM, who factored 15 into 3 × 5, using an NMR implementation of a quantum computer with 7 qubits. Shor mathematically showed that the quantum part runs in time O ((log n) 2 (log log n)(log log log n)) on a quantum computer. Next, it must perform O (log n) steps of post processing on a classical computer to execute the continued fraction algorithm. Factorizations and discrete logarithm problem are two of the most difficult problems arising in the breaking of current cryptographic algorithms. If the Shor's algorithm is implemented on Quantum Computers, no application using this algorithm will be able to withstand the attackers. Quantum Cryptography The uncertainty principle, possible of indivisible quanta and the quantum entanglement forms the basis of the quantum cryptography. The no-cloning theorem, presented by Wootters and Zurek in 1982, forms another basis of Quantum Cryptography. As a direct application of no cloning theorem – Eavesdropper cannot interpret the unknown qubits i.e. the unknown quantum states, which makes the use of qubits in key transmission for asymmetric cryptography resistant to man in the middle attack. Hence, it is attracting considerable attention as a replacement for other contemporary cryptographic methods, which are based on computational security. Quantum Cryptography doesn't reinvent the wheel as a whole. Internally, it works just like a traditional asymmetric cryptographic system. But while cryptographic methods like RSA, use computational difficulty in breaking the key, Quantum Cryptographic system that uses quantum physics for key transmission. Quantum cryptographic transmission encrypts the 0s and 1s of a digital signal on individual particles of light - photons. Each type of a photon's spin represents one piece of information - usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 01101000 01101001 could correspond with "hi". Now, a binary code can be assigned to each photon -- for example, a photon that

ISSN: 2005-4238 IJAST

has a vertical spin (|) can be assigned a 1 and a photon with a horizontal spin, can be assigned 0. Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive. Now, even if eve detects (eavesdrops on) the signal, the information on the photons is suddenly transformed, meaning both that it is immediately noticeable that eavesdropping has appeared and that the third party is not able to decrypt the information.

Quantum Key Distribution (QKD)

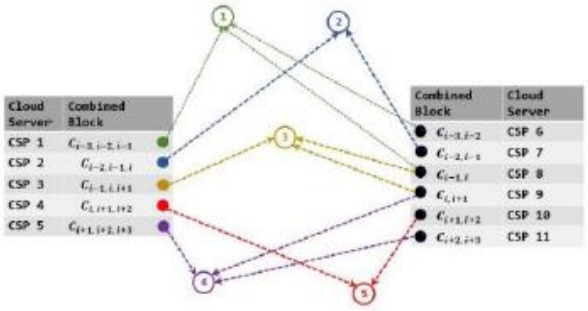
Quantum Key Distribution is the most famous application of Quantum Cryptography. Before understanding the basics of QKD, let's see current encryption standards. Currently, in public key cryptography, before transferring data, both Alice and Bob agrees upon a shared secret key. Alice uses the public key of Bob to transfer the shared secret key to Bob and that encrypted key can be decrypted only by Bob's private key. Now, Bob uses his private key to decrypt the shared key and then using that shared secret key, Bob can decrypt all the encrypted messages that Alice sends. This type of system is susceptible to Man in the Middle attack since the assumption used for transmission of shared key is that decrypting it without the key is, computationally infeasible. But with Shor's algorithm, even this isn't computationally infeasible anymore. This is where QKD walks in. The Quantum Key Distribution is a method used in the framework of quantum cryptography in order to produce a perfectly random key which is shared by a sender and a receiver while making sure that nobody else has a chance to learn about the key, e.g. by capturing the communication channel used during the process. The best known and popular scheme of quantum key distribution is based on the Bennet– Brassard protocol (i.e. BB84). It depends on the no-cloning theorem for non-orthogonal quantum states. The basic principle of the Quantum Key Distribution (QKD) using the BB84 protocol, involves sending decryption keys as quantum particles. Thanks to the quantum properties of these particles, sender, and the receiver can surely identify if their communication was subjected to man in the middle attack. To detect the intruders, the photons can be randomly sampled for different properties. Now, since the measurement in one property results in uncertainty in the measurement of other property, Alice and Bob independently chooses to measure each proton for different properties, say polarization or spin. They then exchange which property they measured on each photon, and examine whether the values are the same on photons that they measured are same or not. If there is a large difference, it is likely the signal was intercepted, and the communication should be dropped. If results are similar, then the values can be stored as binary data; for instance, left spin = 0, right spin = 1. This is the shared key. Once both Alice and Bob have agreed upon the shared secret key, they use the normal channel to transfer the data encrypted with the shared key.

Steps:

- First the Cloud Service Provider generates random Quantum base and shares it with KDC.
- When a Client logs in, it first sends the request containing Client Name et al. to the KDC encrypted with its own password using the classical channel.
- Client → KDC: EPASSWORD-CLIENT (Client Address) || IDCLIENT.
- Authentication Server inside the KDC authenticates the client and sends it the ticket-granting ticket (TGT).
- KDC → Client: EPASSWORD-CLIENT (TGT).
- When a client wants to access the cloud, it generates the random quantum base and sends it to the KDC along with TGT encrypted with its own password via the classical channel.
- Client → KDC: EPASSWORD-CLIENT (QBCLIENT || TGT) || IDCLIENT.

ISSN: 2005-4238 IJAST

- KDC generates a session key by comparing the quantum bases of the cloud service provider and client and stores the session key in the global database.
- After KDC generates the session key, it communicates the base to the client via quantum channel, due to which client can compute the session key itself using the it's base.
- KDC → Client: EPASSWORD-CLIENT (QBCLOUD-SERVICE-PROVIDER).
- Once, the client computes the session key, it uses that session key to encrypt and send data to the server via a quantum channel. The client doesn't encrypt its
- Client ID since server uses the client ID to find the session key to decrypt the data.
- Client → Service Provider: ESESSION-KEY (FILE) || IDCLIENT.



Data Block Technique

Given the rule-of-thumb of multipath technique to maximize recoverability, every 6th 3-block-combination is
to be stored in the same cloud server and every 7th multipath technique is to be stored in the same cloud server, we preserve the combined blocks in 11 different cloud servers as shown in Fig. From Fig., Multipath Technqiue Bi can be retrieved using $combined\ blocks\ Ci{-}1{,}i{,}i{+}1$, $Ci{-}1{,}i$ and $Ci{,}i{+}1$ which are preserved in CSP 3, CSP 8 and CSP 9 respectively. Even if other CSPs hide or loss data, data block Bi can be recovered. In the same manner, despite disasters in any of the cloud server, entire data can be reconstructed.

System Module:

In traditional cloud computing realm, cloud server supports the user with computation, storage, and networking facilities. In this scenario, user directly uploads their data either for safe keeping or for processing with scalable computing/storage resources which is illustrated in Fig. 1(a). However, outsourcing data to the cloud may breach the privacy of the data. Furthermore, there are situations where large amount of data gets accumulated from a particular location and is processed in real time to generate some result. Sending data to a centralized infrastructure (i.e. cloud server) may cause transmission delays. Fog computing can resolve this issue. Fog computing is smaller version of cloud computing that is placed between cloud server and the user. Fig. 1(b) shows the scenario of fog-based cloud storage system. As user needs a trustworthy storage to save data, the proposed scheme considers an architecture where user has full control over fog devices. Users can rely on fog computing/storage devices for the management of their data.

User Module:
User is the owner of data. Privacy, disaster recoverability, modification detection of user's data is ultimate goal of this paper.

ISSN: 2005-4238 IJAST

Fog Server:

Fog server is trusted to user. User relies on fog server with his data. Close proximity of fog devices to the user, robust physical security, proper authentication, secure communication, intrusion detection ensures fog server's reliability to the user.

Cloud Server

Cloud server is considered as huge storage sever. This means that cloud server follows the Service Level Agreement (SLA) properly, but has an intention to analyse user's data. Conversely, cloud server may pretend to be good but acts as a potential.

V.RESULTS

A set of experiments carried out on stress analysis data obtained from facebook on the social media users. The performance evaluation of the system is performing using this dataset. This section lays down experimental comparison of the proposed scheme with prior work of Wang et al. [13]. In order to make the logical comparison, we tried to align different aspects of environment such as block size, communication speed and so on.

Data Processing

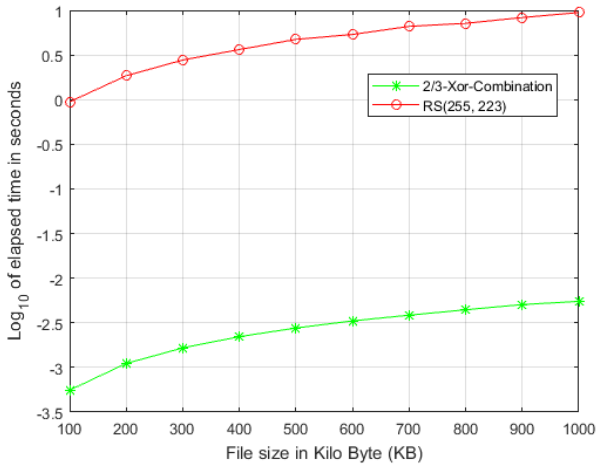
We selected files with size of 100KB to 1MB at increment of 100KB at each step, pad sufficiently and processed using 2/3-Xor-Combination and a popular Reed-Solomon code RS(255, 223). Splitting operation is same for both schemes, therefore, splitting is kept out of comparison in our experiment. The experiment takes each data block, processes it using respective algorithms and writes down the execution time. Data block technique populates Meta data into fog server's database and cloud servers' database tables as shown in Table 1 and Table 2 correspondingly.

Data/Document ID	Block Tag	Cloud Server	File Sie
1093	B14	Drivehq	100
1094	B14	Drivehq	200
1095	B14	Drivehq	399
1096	B14	Drivehq	599

Data Block Transmission

The result is shown in Fig. 1.

ISSN: 2005-4238 IJAST



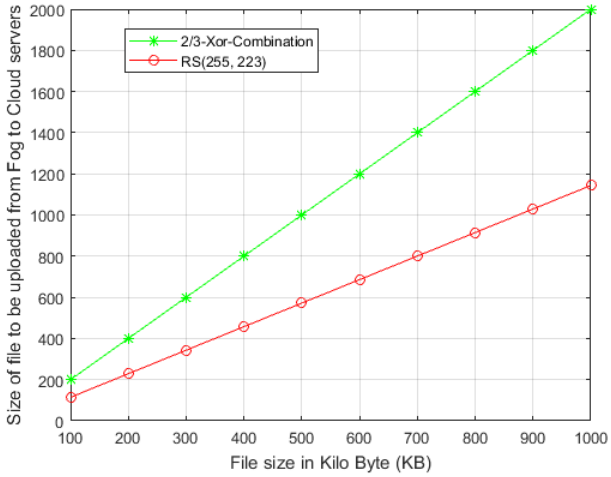
Xor Combination with Multi Path Routing

Data/Document ID	Cloud Server	Download Time	Upload Time
1093	Drivehq	100	100
1094	Drivehq	200	200
1095	Drivehq	399	399
1096	Drivehq	599	599

Table Showing Upload and download Time

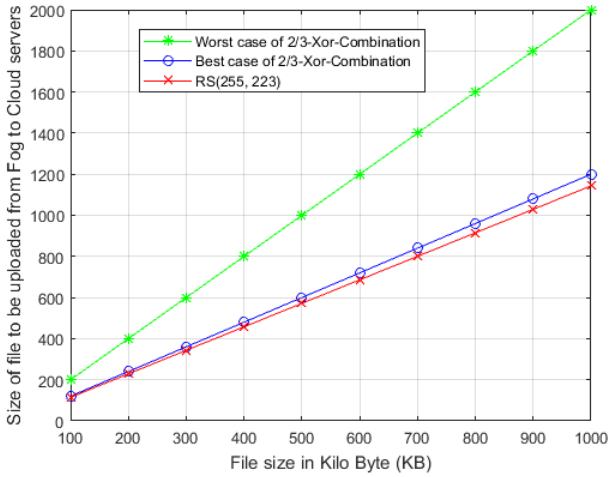
Fig. 1 demonstrates Log of elapsed time to encode different size of blocks using $Xor-Combination$ and Reed-Solomon code, namely, RS(255, 223). It shows that, $Xor-Combination$ is three dimensional and faster than RS(255, 223). It can be attributed to the fact that, $Xor-Combination$ requires only Xor operation where the processor computes it directly inside its circuitry. Conversely, Reed-Solomon codes in software require Galois Field arithmetic operation and general purpose processor does not support it directly. For example, to implement a Galois field multiply in software, requires a test for 0, two log table look-ups, modulo add and anti-log table look-up.

ISSN: 2005-4238 IJAST



Uploading time comparison using payload size

In case of downloading a file from cloud server to fog server, proposed scheme has some advantages in a special case. For example, in best case scenario when no malicious modification and/or data loss occur, only then a fraction of all combined blocks need to be downloaded from clouds to fog server. However, in case of malicious modification or data loss, fog server may need to incrementally download all the combined blocks of a file. Fig. 11 demonstrates the facts. In the best case of technique, cloud server needs to download only 1.2 times the size of the original file and in the worst



Downloading time comparison using payload size In case of downloading a file from cloud server to fog server, proposed scheme has some advantages in a special case. For example, in best case scenario when no malicious modification and/or data loss occur, only then a fraction of all combined blocks need to be downloaded from clouds to fog server.

VI.CONCLUSION

In a nutshell, this paper has introduced a new security architecture for Cloud Computing. This new

ISSN: 2005-4238 IJAST

method builds on top of the pre-existing architecture of using Kerberos for Single Sign-On authentication for flexibility and scalability but gives a workaround for the limitation of classical cryptographic algorithms by using QKD inside the KDC for key distribution and using Quantum Channel for transmission. This paper introduced a new cloud computing environment, which suggested integrates and uses ease and simplicity of Classical Cryptography models and secure benefits of QKD as a new hybrid technique.

Compared to current models, my attempt is better than existing models in following ways:

1. Gives the flexibility and the scalability of an ideal Kerberos-based solution
2. QKD based method for sharing keys is more secure than existing cloud computing architecture deployed upon AES and/or PKI.
3. Since, there's less computation included compared to PKI or AES for key generation, it's faster than existing models. I suggest a unique load-balancing scheme, particularly, As QS provisioning is also important in transfer designs, certainly one of our destiny works might be studying FS overall performance beneath QS situations.

REFERENCES

[1] Nathaniel M. Jones; Georgiou S. Pasco's ; Brooke Shrader ; Eytan Modiano, "An Overlay Architecture for Throughput Optimal Multipath Routing" Computer IEEE, 2017.

[2] C.S. Chang, D.S. Lee, and Y.S. joy, "Load Balanced Birkhoff-von Neumann Switches, Part I: One-Stage Buffering," Computer Comm., vol. 25, pp. 611-622, 2002.

[3] C.S. Chang, D.S. Lee, and Y.J. Shih, "Mailbox Switch: A Scalable Two-Stage Switch Architecture for Conflict Resolution of Ordered Packets," Proc. IEEE INFOCOM, 2004.

[4] C.S. Chang, D.S. Lee, and C.Y. Yew, "Providing Guaranteed Rate Services in the Load Balanced Birkhoff-von Neumann Switches," IEEE/ACM Trans. Networking, vol. 14, no. 3, pp. 644-656, June 2006.

[5] H.J. Chao, P. Jinsoo, S. Artan, S. Jiang, and G. Zhang, "True Way: A Highly Scalable Multi-Plane Multi-Stage Buffered Packet Switch," Proc. IEEE Workshop High Performance Switching and Routing (HPSR), 2005.

[6] F.M. Chassis, D.A. Khotimsky, and S. Krishnan, "Generalized Inverse Multiplexing of Switched ATM Connections," Proc. IEEE Conf. Global Comm. (GLOBECOM), pp. 3134-3140, 1998.

[7] G. Dittmann and A. Herkersdorf, "Network Processor Load Balancing for High-Speed Links," Proc. Int'l Symp. Performance Evaluation of Computer and Telecomm. Systems (SPECTS), 2002.

[8] A.B. Downey, "Evidence for Long-Tailed Distributions in the Internet," Proc. ACM SIGCOMM Workshop Internet Measurement (IMW), 2001.

[9] M. Henrion, "Sequencing System for a Switching Node," US Patent, 5,127,000, June 1992.

[10] S. Iyer, A. Awadallah, and N. McKeown, "Analysis of a Packet Switch with Memories Running Slower than the Line Rate," Proc. IEEE INFOCOM, pp. 529-537, 2000.

[11] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[12] T. M. Cover and A. A. E. Gamal, "Capacity Theorems for the Relay Channel," IEEE Transactions on Information Theory, vol. 25, no. 5, pp. 572–584, September 1979.

[13] T. Wang, J. Zhou, X. Chen, G. Wang, A. Liu, and Y. Liu, "A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 3-12, 2018. [14] S. Biswas and R. Morris, "ExOR: Opportunistic Multi-Hop Routing for Networks," in Proceedings of ACM Conference of the Special Interest Group on Data Communication (SIGCOMM), Philadelphia, PA, USA, August 2005, pp. 133–144.

[15] P. Larsson, "Selection Diversity Forwarding in a Multihop Packet Radio Network With Fading Channel and Capture," ACM Mobile Computing and Communications Review, vol. 5, no. 4, pp. 47–54, October 2001.
[16] E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "Simple Opportunistic Routing Protocol for Networks," in Proceedings of the 2nd IEEE Workshop on Networks (WiMesh), Sep. 2006, pp. 48–54.
[17] M. Kurth, A. Zubow, and J.-P. Redlich, "Cooperative Opportunistic Routing Using Transmit Diversity in Networks," in Proceedings of the 27th IEEE International Conference on Computer Communication (INFOCOM), Apr. 2008, pp. 1310–1318.

ISSN: 2005-4238 IJAST