Providing Data Security in Cloud Computing Using Quantum Search in Black box Approach

J. Velmurugan*, S.K. Manigandan, P. Vinothkumar, Mohammad K Saifullah Basha, S. abhilash kumar
Department of information technology, Vel tech high tech Dr.rangarajan Dr.sakunthala Engg College
Avadi, chennai-62
***Corresponding author: E-Mail: vel.jme@gmail.com**

ABSTRACT

Cloud computing is a technology which is used in the current market. It helps to share resources to provide on-demand services to the user. Cloud computing reduce operational and capital costs and more important help IT departments to focus on futures projects instead of keeping database centers running. It is a platform in which the resources can be shared as per the user needs. Cloud computing reduces the operational and capital costs and more importantly it helps the Information Technology departments to focus on future projects instead of keeping database centers running. This project deals with the issues of security occur during the cryptographic functions namely the encryption and the decryption process, during the search of the data in the cloud. This project puts light on the usage of the Grover Algorithm. The Grover Algorithm uses Quantum Bits to search the data in the cloud. The Grover Algorithm uses the high probability unique inputs and also uses the superposition methods. The security of the entire process is maintained since it is performed in a Black-Box Approach and after processing it searches the required data from the Cloud storage.

KEY WORDS: Cloud Computing, Network, Grover Algorihtm, Quantum Bits, Data Owner, Privacy.

1. INRODUCTION

Cloud computing is the growing technology. It provides on demand services to user and also provides access to shared resources. The cloud model is composed of five Essential Characteristics, three service models and three Deployments models. Cloud provides various services such as IaaS, PaaS and SaaS. It can be deployed at different level i.e. at public, private, hybrid, community (Fig.1). With the technology and services ease new security issues arises. Data on cloud are stored on various physical machines which are unknown from user. Thus their data are at risk many security attacks have been developed to acquire knowledge of data. So, some security measures need to be taken to protect user's data. Third party auditing is also done for data protection. The markets are expanding and many vendors are coming up with the similar functionalities. The users are concerned with their data storage location and by whom their data can be accessed. The user cannot easily trust the cloud service provider. Therefore trust management is the important factor which arises in this field.

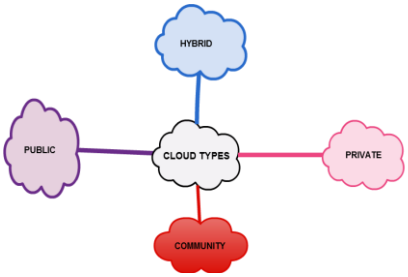

Figure.1. Cloud computing type

In this the system presents an Cloud Computing (CC) is an innovative technological paradigm that provides simple and user convenient data manipulation and access of resources that can be rapidly provide Infrastructure as a Service through Arm node. At the client sides, one can use the internet to request for Web Services that will store this big data format into Cloud system. The cloud provide three type of services IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (software as a Service) (Fig.2). The benefits of this system include basic computing hardware and reasonable storage capacities making it suitable for any smart device which can monitor real-time information from anywhere and reduce the cost of infrastructure. The customers can fully access our cloud service using devices that have internet capabilities.

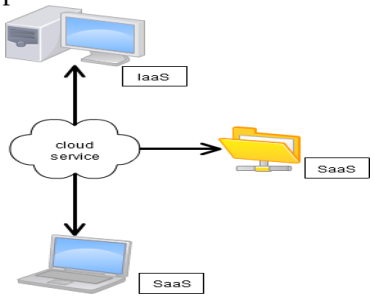

Figure.2. Cloud type services

It provides the data security not only at the storage and access mediums but also during the search of the data by using the Quantum search strategy with the aid of the Grover Algorithm. The Grover Algorithm searches the encrypted data in the cloud or any data storage medium. Cloud is a new consumption and delivers model for many IT based service.

2. EXISTING WORK

The paper about cloud computing and network security is provided with OPE method.In this paper the data which is stored in cloud has to provide with some privacy and by usingDeterministic OPE, the ciphertext will reveal the distribution of relevance scores (Ke Li, 2015). In this method Deterministic OPE was used for encryption and decryption. Then they introduce improvised method called as one-to-many OPE. In this system consist the ciper texts will share exactly the same distribution as its pain counter part by which the server can specify the keywords. In this plain text ma relevance score the one-to-many OPE first employs for m and then randomly chooses a value in the bucket for m and then randomly choose a value from the bucket as the cipertext. This bucket consists of unique id which helps to combine with the plain text with inverted index method for encryption. The bucket consists of plain text and it is encrypted with cipertext which is use hyper geometric probability (HGD) by one-to-many OPE Mapping. In encryption of sensitive data obstacles occur to the processing of the data. Information retrieval becomes difficult in the encrypted domain because the amount of outsourcing files can be very large and regular search patterns cannot be deployed to ciphertext retrieval directly. Users need to have all the data, decrypt it all, and then search keywords like plaintext retrieval. To overcome this, Searchable Encryption (SE) was proposed to make query in the encrypted domain possible while still preserving users 'Privacy. There are several problems in searchable encryption: fuzzy search, ranked search, multi-keyword search and so on. Proposed a search scheme only supporting single Boolean keyword search. After that plenty of searchable encryption methods arose to improve efficiency and reduce communication overhead. In initial study of OPE schemes in which they defined the security of proposed a provably secure OPE scheme. However, the security definition and the constructions of OPE in are based on the assumption that OPE is a deterministic encryption scheme which means that a given plaintext will always be encrypted as a fixed cipher text. However, deterministic encryption leaks the distribution of the plaintexts, so it cannot ensure data privacy in most applications. In the OPE scheme of, the range R is divided into some non-overlapping interval buckets with random sizes. The random-sized bucket is determined by a binary search based on a random HGD sampler. In the procedure of binary search is described as Algorithm 1, where Tape Genis a random coin generator.

Algorithm 1: Binary Search
Input: {K, D, R, m}
1: M ←length(D); N ←length(R)
2: d ←min(D) − 1; r ←min(R) − 1
3: y ←r + ceil(N/2)
4: coin R ←− TapeGen(K, (D,R, y||0))
5: x R ←− d + HGD(coin, M, N, y − r)
6: x = d + f
7: if m ≤ x then
8: D ← {d + 1, . . . , x}
9: R ← {r + 1, . . . , y}
10: else
11: D ← {x + 1, . . . , d + M}
12: R ← {y + 1, . . . , r + N}
13: end if
Output: {D,R}

Noted that, in applications of Privacy-preserving keyword search, if a deterministic OPE is used to encrypt relevance scores, the ciphertexts will share exactly the same distribution as its plain counterpart ,by which the server can specify the keywords. Therefore, Modified the original OPE to a probabilistic one, called "One-to-Many OPE". For a given plaintext *m*, i.e., a relevance score, the "One-to-Many OPE "first employs Algorithm 1 to select a bucket for*m*, and then randomly chooses a value in the bucket as the ciphertext. The randomly choosing procedure in the bucket is seeded by the unique file IDs together with the plaintext *m*, and thus the same relevance score in the Inverted Index will been crypted as different ciphertexts. The encryption process of "One-to-Many OPE" is described in Algorithm.2

Algorithm 2:
One-to-Many OPE
Input: {K,D,R,m, id(F)}
while |D|! = 1 do
{D,R} = binary search(K,D,R,m)

end while
coin R ← − TapeGen (K, (D,R, 1||m, id(F)))
c ←co−i−n R
c = round(coin)
Output: c
Proposed Method: In One-to-Many OPE using two Algorithms one is binary search algorithm and another one is One-to-Many OPE algorithm. In future work itself they mention that "*we will elaborate these ideas to design secure methods of probabilistic OPE and schemes for search in encrypted data*". So we try to introduce a method by which we can increase the security of data stored in cloud.

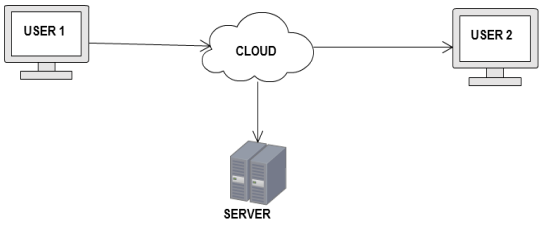

Figure.3. Cloud Communication

In fact, although the ciphertexts of One-to-Many OPE conceals the distribution of the plaintexts, an adversary may estimate the distribution from the differences of the ciphertexts. So in this paper, we propose a differential attack on the One-to-Many OPE. Our experimental results show that, when applying this attack to the secure keyword search scheme of the cloud server can get an estimation of the distribution of the relevance scores, and furthermore accurately reveal the encrypted keywords .The rest of this paper is organized as follows. The basic OPE, One-to-Many OPE, and privacy requirement in cloud computing are briefly reviewed. We elaborate on differential attack on One-to-Many OPE [Fig.3] and further attack with background information of outsourced data respectively. In our method we are going to try Grover's algorithm.

The steps of Grover's algorithm are as follows:

- Initialize the system to the state |a= \frac{1}{\sqrt{N}} \sum_x |x
- Perform the following "Grover iteration" *r(N)* times. The function *r(N)* is described below.
- Apply the operator $V\omega$
- Apply the operator $Ua = 2|a\rangle le\langle les| - I$.
- Perform the measurement λω. The measurement result will be Ω with probability approaching 1 for N>>1. From λω, ω may be obtained.

Grover algorithm:

- $a\rangle=1/N—\sqrt{\sum_{k=0}^{n-1}}(x)$.
- $U_a = 2|a\rangle\langle a|-I$.
- Apply $V\omega$ and Ua.

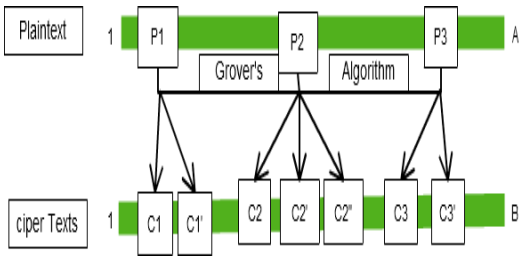

Figure.4. Grover's algorithm

Grover's algorithm uses quantum algorithm that finds the high probability the unique input to black box function that produce a particular output value (Fig.4). Quantum algorithm which run on realistic of quantum computation. It uses quantum bits. The data flow from user to server as given (Fig.5).
m = [(5A + 3) / 3] → Grover's final equation
A =denote the integer closest to the real number *x.*
m =Marked state.

Figure.5. Flow of data

The quantum bits have few similarities to a binary bit but are overall very different. There are two possible outcomes for the measurements of qubits- usually 0 and 1 like a bit.

The main application of this algorithm is that it may help to encrypt the data in unknown and in random order.

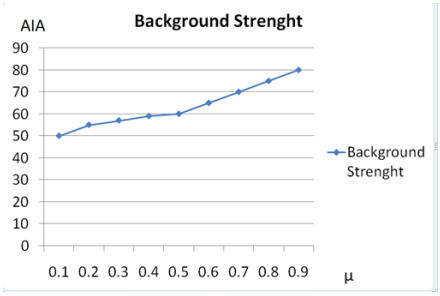

Figure.6. AIA for different background strength μ AIA - Average identifying accuracy

We use μ as a parameter to describe the similarity of the background acquired by the cloud server to the outsourced document collection (Fig.6). We μ call the background strength. There are 32 students in a class whose sequence number is from 0-31. The searched targets are the students whose sequence number satisfies m = [(5A + 3) / 3], where m= 0, 1..,.18; denote the integer closest to the real number x, where by convention we rounded down half (Table.1). The target numbers and marked states are shown in Table.1. In present example, B = 32, C=19, using 5 qubits can store all sequence numbers. As C/A=19 / 32 > 0.5, the general Grover algorithm is invalidated.

Table.1. Target serial numbers and marked states

K	Serial Number	Marked State	K	Serial Number	Marked State
0	1	1	10	18	10010
1	3	11	11	19	10011
2	4	100	12	21	10101
3	6	110	13	23	10111
4	8	1000	14	24	11000
5	9	1001	15	26	11010
6	11	1011	16	28	11100
7	13	1101	17	29	11101
8	14	1110	18	30	11111
9	16	10000			

3. CONCLUSION

The study suggested that trust is very crucial factor in the development of cloud computing technology. We successfully achieved our objective to store the data securely in the cloud by giving its indexing search function through the Grover Algorithm. Also we have proposed an approach that ensures the security principles such as confidentiality and integrity of data in cloud. The major analysis made in this paper is that, how to secure the data from an unauthorized access. By our proposal system, we are expected to get data security relatively higher than the earlier developed systems. And since our proposed system is functioning behind the Black Box the security is also enhanced drastically.

REFERENCES

Ala'Darabseh, Mahmoud Al-Ayyoub, Yaser Jararweh, Elhadj Benkhelifa, Mladen Vouk, and Andy Rindos, SD Storage, A Software Defined Storage Experimental Framework, 2015.

Christina Delimitrou and Christos Kozyrakis, Security Implications of Data Mining in Cloud Scheduling, IEEE, 15 (2), 2016.

Hao Yan, Jiguo Li, Jinguang Han, and Yichen Zhang, A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage, IEEE, 12 (1), 2017.

Longge Wang, Tao Song, An improved digital signature algorithm and authentication protocols in cloud platform, IEEE, 2016.

Ming Liu and Tao Li, Optimizing Virtual Machine Consolidation Performance on NUMA Server Architecture for Cloud Workloads, IEEE, 2014.

Ke Li, Weiming Zhang, Ce Yang, and Nenghai Yu, Security Analysis on One-to-Many Order Preserving Encryption-Based Cloud Data Search, IEEE, 2015.

Sathishkumar Easwaramoorthy, Sankar Thamburasa, Guru Samy, Bharath Bhushan S, Karrothu Aravind, Digital Forensic Evidence Collection of Cloud Storage Data for Investigation, IEEE, 2016.