INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 25 ISSUE 1 – JULY 2017 - ISSN: 2349 – 9303

Sensitive Data Protection in Cloud Computing Using QR Code

Sandha[1]
St.Michael College of Engineering andTechnology,
Department of Computer Application,
yazhini98@gmail.com

M.Ganaga Durga[2]
Government Arts College for Women,
Department of Computer Science,
mgdurga@yahoo.com

Abstract – Data stored and shared in cloud environment .Integrity of outsourced data is challenging task in cloud computing. Client or auditor need to check the integrity of outsourced data. For this purpose several mechanisms have been developed to allow client and verifier to effectively audit the integrity of data without download entire data. Public auditing on the integrity of data with these existing technique have problem in storage space and in cloud environment searching process for authentication causes high network bandwidth, congestion and delay. This paper suggests QR code , a two dimensional code can be used for secure authentication between client and server at the time of storage and auditing .Which is used for reduce the storage space of HARS in server and achieve the fast retrieval of data from the server in cloud computing environment.

Index Terms— Cloud computing, privacy preserving, Oruta, QR Code

1.INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it. The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter .Cloud Computing has been defined as the new state of the art technique that is capable of providing a flexible IT infrastructure, such that users need not own the infrastructure supporting these services. This integrates features supporting high scalability and multi tenancy. Moreover, cloud computing minimizes the capital expenditure.

Cloud Service Provider offers cost effective approaches with low marginal cost. Cloud service users share data with the group members due to the hardware or software failure data may easily corrupted or lost. Therefore the Integrity of data should be monitored. The traditional approach for check data is ,retrieve entire data from cloud and verify data integrity by checking correctness using RSA or MD5.The size of the cloud data is large in general. The entire data downloaded and verified by the user or auditor. Cost and the amount of communication and computation resources of users will waste if the data corrupted .

Recently many approaches have been offered the effective auditing process for the data owner and verifier to check their data integrity without download entire data from cloud. The public auditing approach [9] proposed the technique, Data is divided into separate small blocks, each block is signed independently by the owner and stored in to the cloud . The auditor check a random combination of all the blocks instead entire blocks. Public verifier May be a data user or use owners data via cloud or may be Third Party Auditor. Problem of above approach is Content of the private data belonging to a personal user is considered as any public verifier. Public auditing solutions only focuses on personal data in the cloud

2. QR Code

Authentication is a important process in cloud computing. Data security is very big problem in public storage. In order to prevent this a proper effective authentication system must be implemented which prevents data leakage or loss a new technique called QR code.

A Quick Response code is a 2 dimensional bar code Which was developed by Densa-Wave. Basic of this technology is tracking the information. Two types of QR codes are there Static QR code and dynamic QR code. It can store and digitally present much more data than other barcode. Data is aligned in vertical and horizontal direction. Information is retrieved by photograph of the code using QR code Reader with camera. QR can be read from any position. QR code scanner decode the image through three squares present in the corner of the image.

A. QR Code Structure

Figure. 1

The three large squares highlighted in green are the Finder pattern. These enable the decoded software and to recognize the QR Code and determine the correct orientation. The smaller brown square is an alignment marker it will added more if the code size increased. Separators used to separate Finder pattern from the actual data . Timing pattern contained alternate red & yellow module.

format information is 15 bit data next to separators it contained about error correction level. Pink color squares are used to encode the version data. Blue color Data part is in 8 bit size.

B.Types

The 4 different types of QR codes differ in the view and features. QR code model 1 and model 2 are the first type of QR code. Up to 1167 numerals can be stored in Largest version of model 1 and Up to 7089 numerals can be stored in Largest version of model 2. The next type is micro QR code. It differs from regular QR model by position detection pattern and size. iQR Code is next type. The same size of IQR Code as an existing QR Code can hold 80% more information than the latter. SQR Code is used to store private information there is no difference from regular code in appearance. The next type is logoQR it incorporate high level of design features.

Recently, much of growing interest has been pursued in the context of remotely stored data security David Pintor Maestre et al.[4] consider secure authentication using QR code in their defined "A Improved secure authentication method using QR codes" develop an authentication method using 2 factor authentication.. In their scheme, they utilize IMEI number of smart phone with random number of QR code for secure authentication, thus private data security is achieved. The problem here is the server must have a copy of the user's private key in order to generate the same pincode.

Thiyagarajan M, Dinesh Kumar K et al.[2] consider authentication of consumer product can be done with QR codes . they achieve the security by QR code along with the public key encryption algorithm. But the normal QR code can be easily retrieved using any smart phone. They do not consider security of QR code. Suraj kumar sahu et al. [5] describe a " Encryption in QR code using stegnograpy" where cover image and QR data is embed and encrypted. Dong-sik oh et al. [6] consider creating 3 set of QR code by converting the single information into 3 versions of QR code and stored in distributed server system.

3.POSSIBLE APPROACHES

The signature for the block is created using the private key of any one person from the group members. so the verifier cannot determine the particular person. If the given ring signature is one among the group of users. the verifier cannot identify the signer identity. It is used to protect the signer identity from a verifier.

B wang H- li "privacy preserving public auditing for shared cloud data supporting group dynamics"-2013 B Wang & S Chow "storing shared data on the cloud via security mediator.Security of this concept is preserve the identify of the signature.They share the global public key among the group members.problem of this concept is if any user compromised or leaving from the group , new global key must be generated.

Another possible approach is trusted proxy model. It achieve identity privacy here all the data collected signed and uploaded to the cloud by the proxy. Verifier cannot learn the identity of group member

Approach	Identity privacy	Block less verifiability	Support dynamic	Reduce signature storage	Fast retrieval
Global public key	Yes	No	No	No	No
Trusted proxy	Yes	No	No	No	No
Group signature	Yes	No	No	No	No
Ring signature	Yes	No	No	No	No
HARS	Yes	Yes	Yes	No	No

Table 1

D.Boneh proposed the concept of group signature, data is divided in to multiple blocks and signed by the user. Signature combined in to set then it will stored in to the server as a random combination signature. Data is verified by the verifier without download all the data. They satisfied if the random combination of aggregate signature is correct. identity privacy preserved by this concept.

4.RELATED WORK

A.Support dynamic operations:

The ring signature is created using any one group members private key and all current members public key. So the recomputation of ring signature is needed for the dynamic group.Any one of the member can be revoked from the group or any new member can be added if it is a dynamic group. Recomputation is needed for the ring signature. Indices of blocks will changed after modification [9]"provable data possession at untrusted stores" need recomputation of signature even though content of blocks are not modified. Hash table is utilized for indexing each block based on its hash value [15]" dynamic audit services for integrity verification of outsourced storages in clouds".

B.Homomorphic:

It supports the blockless verifiability. Homomorphic authenticator based on signature should also satisfy the blockers verifiability and non malleability the verifier can audit the integrity and correctness of data in cloud server using blockless verifiability which is a special block. That is linear combination of all # blocks on data. The integrity of the combined block is proven by the verifier. So the entire data is correct.

C. HARS in oruta:

Randomly pick the private key of any one among the group they belongs to particular block. It will be the public key for the group.Ring signature is created,using the private key,public key of the group and block id.verifier can using the ring signature with the help of public key ,block and its id. The size of the storage used for ring signature is huge.

If the group is static that is group is predefined and membership created, the original user decide the group people before outsources shared data to the cloud. In oruta they used attribute based

encryption for protect the private data in the cloud.If the group is dynamic, re computation is needed for the ring signature.

5. PROPOSED SYSTEM

Let M_1,M_2 and M_T are multiplicative cyclic group of order count, $m_1$and m_2 be the generators of $M_1$and M_2 respectively.Let $f:M_1XM_2 \rightarrow M_T$ be a bilinear map and $e:M_2XM_1$ be a computable isomorphism with $\psi(M_2)=M_1$ the total number of users in the group is count

Key generation

For a user x_i he randomly picks $pr_i \rightarrow Z_{count}$ and computes $pu_i=m_2^{pr}{}_{i\in} M_2$. user x_i 's public key is pu_i and private key is pr_i

Ring signature

Given all the count users public keys (pu_i.....pu_{count}) , a block $B \in Z_{count}$,identifier of the this block id and the private key ($pr_{i.....}pr_{count}$),for some s user x_s chosses $\beta_i \in Z_{count}$ for all $i \neq s$ where $i \in [1, count]$ $\alpha_i=m_1^{\beta}{}_i$ then $\gamma=h(id)\ m_1^{bi}$ compute the ring signature α_s the ring signature of the block B (α_1....α_{count}).

Ring verify

$f(\gamma,m_2)=\prod_{i=1}^{count} f(\alpha_i,pu_i)$

Here the storage of ring signature occupy lot of storage space. In order to avoid this problem ,our proposed system convert ring signature in to QR and then stored in cloud storage.

From the above concept, the proposed system involved to reduce the storage of ring signature and searching bit ratio when we access the data from the server. Also maintain the identity privacy and traceability of user.

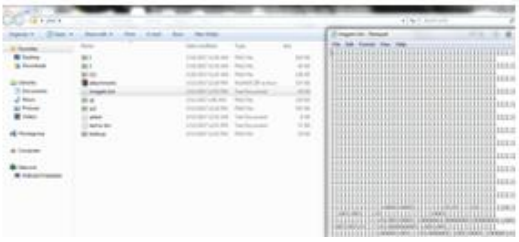

Figure .2

For that text is converted in to QR using Qr code generator. Got static QR code and then converted in to binary format.size of the binary file is 10kb

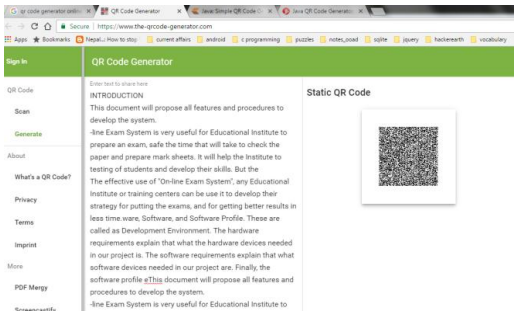

Figure-3

The size of the binary file is 71kb if the text is converted in to binary format directly.

We can scan the QR code using scanner present in the mobile or QR code Reader coding.

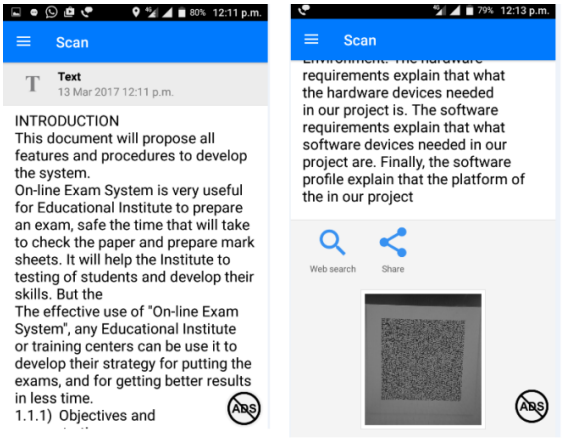

Figure-4

SIMULATED WORK

NetBeans IDE is introduced in june 2000 by sun micro system. It is the best tool for developing java desktop, mobile and web application quick and easy manner. NetBeans contain special features such as batch analyzes, converters and matching patterns. Large applications can be managed easy and efficient way of approaches. Missing feature in NetBeans IDE can be plug in by us.

1.CLOUD ACCESS

For implement this work we purchased three web domain which is considered as a three different public server. We can used this for storing file.

Before enter in to the secure cloud storage system client should register their detail to confirm the authenticated user. The authentication of client can be done with the email id as user id and password is given by the user. Unique random number is assigned for every user and is sent to the registered mail id. The key which is sent to the client is a authentication message for downloading file. The uploaded file encrypted by Ring signature authentication and converted as a QR code. It will stored in to the cloud server which is purchased by us. Key is getting from the user at the time of download. If the is key is correct then the data is downloaded from servers .

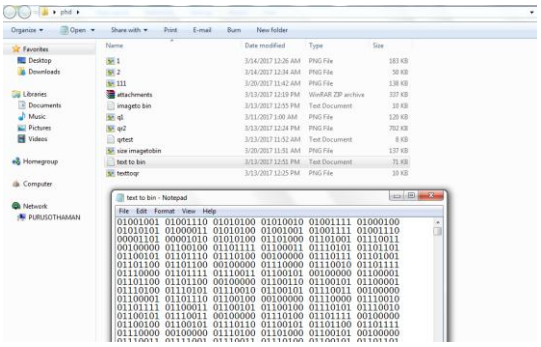

Figure-5

The pseudo code for our proposed system is Shown below

```
// Module for upload the data
 upload()
{
 If(user authentication success)
{
Encode+convert qr;
Distributed in to server
}
Else
 Return authentication failed;
}
// Module for download the data
 Download()
{
If (key is ok)
{
Collect from the server;
Decrypt the file;
}
Else
Failed;
}
```

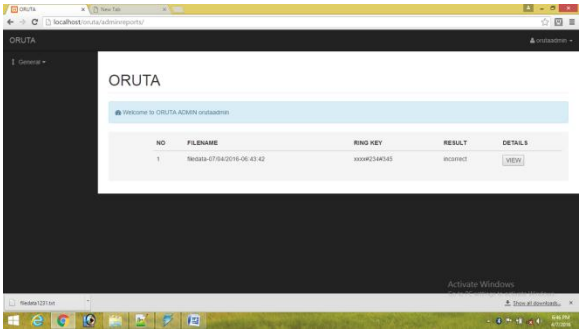

Figure-6

Compression Ratio is the ratio between the size of the compressed file and the size of the source file.
size before compression/compression Ratio size after compression

Compression Factor is the inverse of the compression ratio. That is the ratio between the size of the source file and the size of the compressed file.
size after compression/compression Ratio size before compression

Saving Percentage calculates the shrinkage of the source file as a percentage.
size before compression-saving percentage size before compression/ size after compression

All the above methods evaluate the effectiveness of compression algorithms using file sizes. There are some other methods to evaluate the performance of compression algorithms. Compression time, computational complexity and probability distribution are also used to measure the effectiveness.

S.N	Algorithm	File size	compressed	Compression ratio	Saving percentage
1	Run Length Encoding	78,144	68,931	88	11.79
2	L Z W	78,144	24,204	30	69.03
3	Adaptive Huffman	78,144	44,908	57	42.53
4	Huffman Encoding	78,144	45,367	58	41.94
5	Shannon Fano	78,144	46,242	59	40.82
6	QR optimization	71,000	10,000	14	85.9

Table-2

QR compression technique is compared with Six lossless compression algorithms are tested for text files .The sizes of the original text files are 78,144 bytes and 71,000 bytes.
The performances of the selected algorithms vary according to the measurements, while one algorithm gives a higher saving percentage it may need higher processing time. Therefore, all these factors are considered for comparison in order to identify the best solution. An algorithm which gives an acceptable saving percentage within a reasonable time period is considered as the best algorithm.

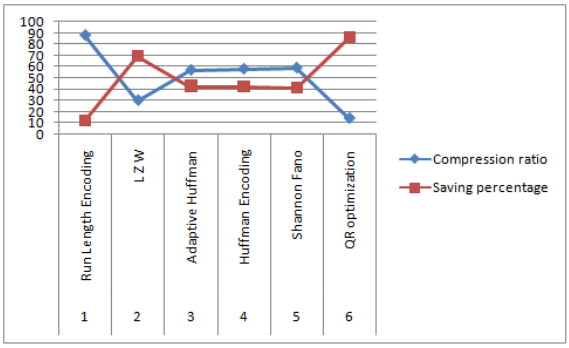

Chart-1

QR compression methodology is compared with Compression algorithm Run Length encoding, LZW, Adaptive Huffman, Huffman Encoding and Shannon Fano Algorithm. Compressed size of file using QR methodology lower than all other algorithms.

Compression ratio of QR is less than others based on our results. Saving percentage of QR is higher than other algorithms

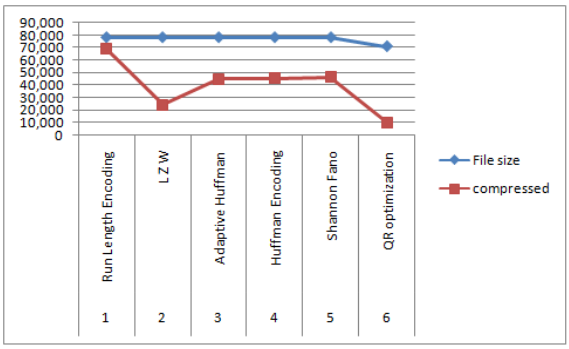

Chart-2

6.CONCLUSION

We thus conclude this proposed system saying that it will be a best data compression model can be implemented in cloud environment to avoid the cloud storage problem. Future enhancement of this work is compare this algorithm with other algorithm using Decompression , time and cost parameters

7.REFERENCES

[1] S.R.Kodituwakku, U.S.AmaraSinghe "Comparison Of Lossless Data Compression Algorithms for Text Data " Indian journal of computer science and engineering,

[2] Thiyagarajan M, Dinesh Kumar K" Qr code authentication for product using cloud computing"journal of global research in computer science, Volume 3, No. 2, February 2012

Information Intelligence Research "Encryption in QR Code Using Stegnography" 2013

[10]. Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, SebastianSchrittwieser, Mayank Sinha, Edgar Weippl: "QR-Code Security". SBA Research, 2010

[11]G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song. Remote data checking using provable data possession. ACM Trans. Info. & System Security 14(1), May 2011.

[12]. C. Wang, Q. Wang, K. Ren and W. Lou, &ldquo,Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,&rdquo, *Proc. IEEE INFOCOM ',10,* Mar. 2010.

[13].sandha,Dr.M.Ganaga Durga, " Study on Data Security Mechanism in Cloud Computing" 2014 ,IEEE digital Library

[14] sandha,Dr.M.Ganaga Durga, "Effective Data Security Mechanism in Cloud Computing Using QR Code" 2015.