INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 2)
Available online at: www.ijariit.com

A three-layer privacy scheme for storing data using fog computing along with cloud computing

M. Sai Poojitha
poojithasai.2199@gmail.com
Andhra University College of Engineering for Women, Visakhapatnam, Andhra Pradesh

P. Jyothsna Vani
painjvani999@gmail.com
Andhra University College of Engineering for Women, Visakhapatnam, Andhra Pradesh

K. Yaseswini
yashuyash9825@gmail.com
Andhra University College of Engineering for Women, Visakhapatnam, Andhra Pradesh

L. Tejaswini
tejaswinilaveti123@gmail.com
Andhra University College of Engineering for Women, Visakhapatnam, Andhra Pradesh

ABSTRACT

Now-A-Days, we often listen to the word of cloud computing. In our technological world we care a lot about our privacy, so we use cloud computing to achieve it. For the time being, there are many people who are interested in others life and are always try to get others data. Recently, we came to know that this cloud computing storage system also beesn crashed. In order to decrease the risk of losing data we introduced a new technology called as Fog computing. In this new storage system, we have used a theory of Hash-Solomon code of algorithm which helps in dividing data into three parts. And fog computing we use is to store the three parts of data into cloud, fog and in secondary storage or main memory of the device/system. The composition of data that divided into is 95%, 4% and 1% respectively. As it is dived into three parts it'll be difficult for the hacker to crash into fog server and get the data stored in it. We all know about cloud storage is secured externally whereas fog server is secured both in and out of it. That means, fog storage system is secured both internally and externally. Here Hash-Solomon ensures the data to be encoded first before dividing the data and even encodes each part after division of data. For retrieving this data when the owner needed then it is decoded by Hash-Solomon itself, if we use another algorithm it will only do encode or decode but not both. So, we use this algorithm for flexibility, compatibility and also for better efficiency. So, we can say that this increases the privacy protection.

Keywords— *Cloud computing, Fog computing, cloud storage, fog server, privacy protection, Hash-Solomon algorithm*

1. INTRODUCTION

Before 21st century, every user used the main memory or secondary storage to store their data. It no longer gives the security to their data. Because of firewall crashing whole data is in the hands of the hacker and is very easy to commit crimes with that data. To reduce these cybercrimes a special storage system came into use in early years of 21st century. That is Cloud storage, it is also called as cloud server which is very strong storage system. It protects the privacy of the user. With this storage system our firewall will be in out of danger. So, it was accepted by all streams of industries and even individuals too.

In this cloud computing system data in a local machine or main memory of system is sent into cloud server. Here in cloud server the data is kept safe so that no outsider can take this data out of the user's hand.

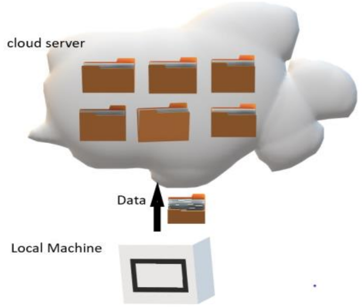


Fig. 1: Storage process in Cloud Server Provider (CSP)

In the above figure 1 it is clearly shown that the files that are stored in local disk are stored in cloud server provider. Here the CSP only concentrated on the external guarding and restricting the attacker but neglected the internal attacks. This is called as the Traditional data storage provider.

We proposed a Three Layer Security (TLS) system using fog computation. Because in fog computation mathematical calculations are done by default. So, we use the algorithm called Hash-Solomon. Hash-Solomon algorithm is based on the Reed Solomon algorithm. It is more efficient algorithm than other algorithms for encryption and decryption. Because, here we need both encryption and decryption for the user.

Fog server is more secure than Cloud Server Provider (CSP). It is secured inside the server and protects the data in it. In addition to this server, we have Hash-Solomon algorithm which is responsible for generating signature keys to encrypt the data inside the three parts of data in cloud, fog and local machine. Regarding this we have explained in following sections like related works, results, proposed system and the conclusion.

2. RELATED WORKS

The cloud storage system has been the growing technology for the exponential increase of data. With this, the attention and also the significance of security for the cloud storage has also increased. There have been researches looking out to secure the cloud storage.

One of those researches provide the security to the image content by using the CBIR for encryption and watermarking scheme which will prohibit the unauthorised image retrieval or modification by deteriorating the image specifications. In the conventional system, the data in the cloud is stored using CSP. Even though the CSP is valid, the system can be exploited by taking the control over storage management node. For this there is an extra level of user authentication with server using an asymmetric response system.

In order to secure the cloud storage, a virtual protection system was introduced which uses SSL framework and deploys Daoli for transferring of data. The data being transferred is encrypted before the data is written on the disk which dodges a huge burden on the server.

There have been different researches and approaches which provide high privacy to the data stored in the cloud in different aspects but there is a common defect which is lacking of internal security. So, we propose a new security system for cloud storage which divides and combines the data into different servers based on fog computing and Hash-Solomon code algorithm for higher order privacy of the cloud.

The cloud storage aids in the problem of increasing content of data but has a lot of security problems as the data storage attracts the attackers for exploitation. To suppress this problem, we suggest a TLS framework which works on fog computing model using Hash-Solomon code algorithm. On analysing, the system is practicable which divides the data in an appropriate ratio onto different servers assures privacy as the integrity of the data depreciates. If an attacker acquires the data in the cloud, it is worthless of actual data. Also hacking the encryption matrix is very difficult. The experiment test reveals that the scheme is completely efficient in providing the security to a cloud system irrespective of the cloud storage capacity.

3. PROPOSED MODEL

As mentioned earlier we propose a security model using fog computing based on data being stored in distributed environment. This model preserves data privacy and data integrity of the users and it also takes the advantage of cloud computing model and those are access restrictions and encryption techniques. This model protects data not only from external attacks but also from internal attacks.

Let us get into the more detail, this model involves a three-layer architecture. The top-most layer is the cloud computing layer which has large storage capacity and certain computational capability. The next layer is fog computing layer which serves as a middle layer. This layer has a limited storage capacity and fast computing capability based on computational intelligence. The bottom layer is user's local machine.

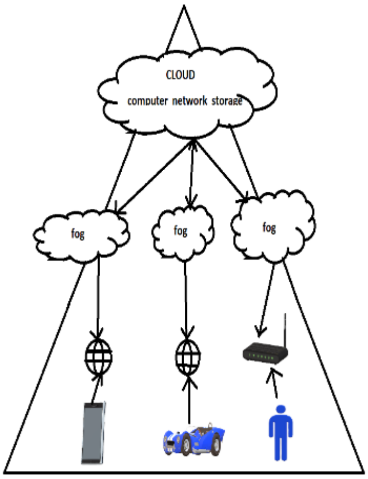


Fig. 2: Architecture of fog computing

The above figure depicts the generalized architecture of fog computing model. This model uses Hash-Solomon Algorithm which encodes the user data and it computes the amounts of data that need to be stored across different layers. Firstly Hash-Solomon algorithm encodes the entire data and 1% data and encoding information is stored in the local machine and sends the remaining data (99%) is sent to fog layer. Again, the fog layer encodes the remaining data and it stores 4% data and encoding information in the fog layer and sends remaining data (95%) to cloud layer. It is explained in the Fig 3. The same process takes place in the cloud layer.

It divides the entire data into '*k*' blocks and produces '*m*' redundant blocks after encoding the data. So that we store less than *k-1* blocks in any layer so that if any attacker get data of any of the three layers, He won't recover the entire data.

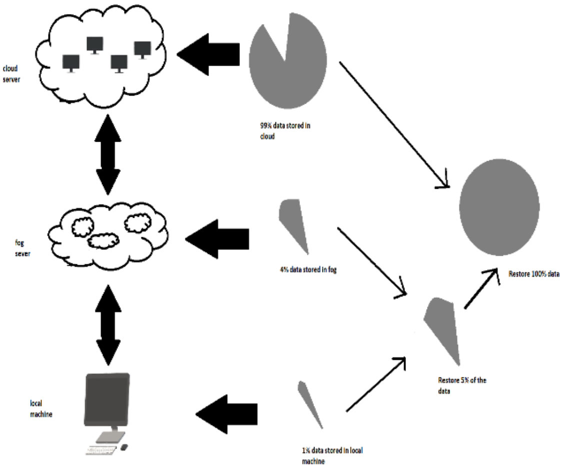


Fig. 3: Three Layer Storage Framework Using Fog Computing

In order to avoid the upper server recovers entire data, the values of *k*,*m*,*r* must satisfy the below relation,

$$\frac{m}{k+m} \leq \frac{(k+m)*r}{k}$$

Where,
k=Total no of data blocks,
m=No of redundant blocks,
r=Storage ratio across servers.

The algorithm actually involves matrix computation. Initially, we apply mapping transformation on the file that needs to be stored.

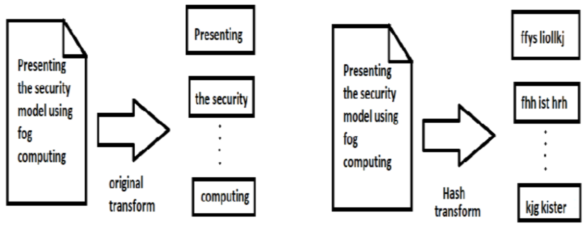
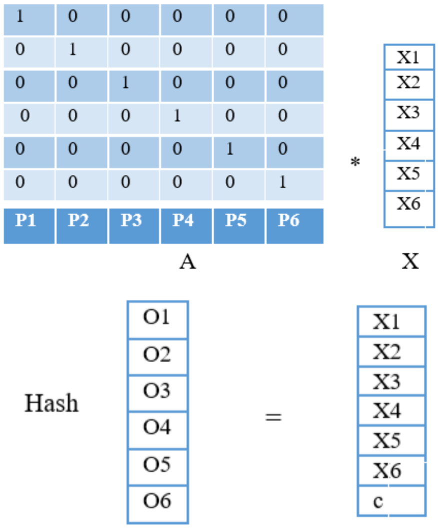

Presenting the security model using fog computing
original transform
Presenting
the security
computing
Presenting the security model using fog computing
Hash transform
ffys liollkj
fhh ist hrh
kjg kister

Fig. 4: Difference between original and hash transform

It results in a matrix named 'O', we apply hash transform on that matrix so that it results in matrix 'X', This matrix is multiplied with encoding matrix 'A', This generate certain no of data blocks and redundant data blocks. The importance of hash transform is explained in fig4. Based on our assumption, less than total no of datablocks will be stored on higher server, Here the encoding matrix is Cauchy or vandermonde matrix, Even the attacker acquires the complete data, as it is hashed, It would be hard to crack the encoded information. The above process is explained using figure 5.



1	0	0	0	0	0
0	1	0	0	0	0
0	0	1	0	0	0
0	0	0	1	0	0
0	0	0	0	1	0
0	0	0	0	0	1
P1	P2	P3	P4	P5	P6

Fig. 5: Data Encoding and Data Division

With increase in the no of data blocks, the speed of encoding and decoding will be reduced. For an application, it is necessary To work efficiently. Higher the efficiency, Greater we can save the storage capacity. Therefore, We can achieve privacy through and hashing and redundant blocks.

4. EXPERIMENTAL WORK

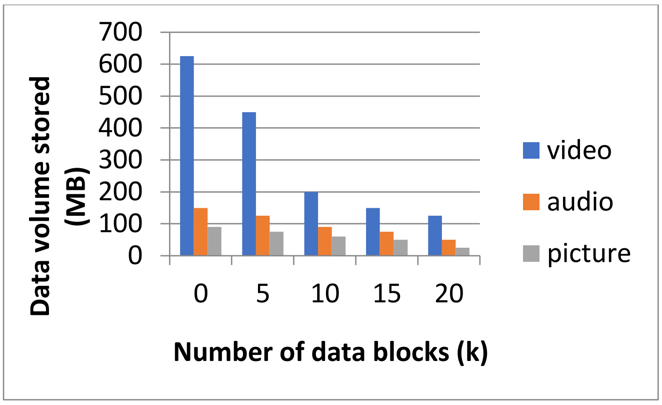
By some series of tests like encoding, decoding we can calculate the performance of the TLS framework based on fog computing model.

4.1 Experimental Environment

In the experiments shown below, lower server save m+1 data blocks and leave the remaining data blocks to the higher server to save the privacy of data and the pressure of the lower server to storage data can also be reduced.

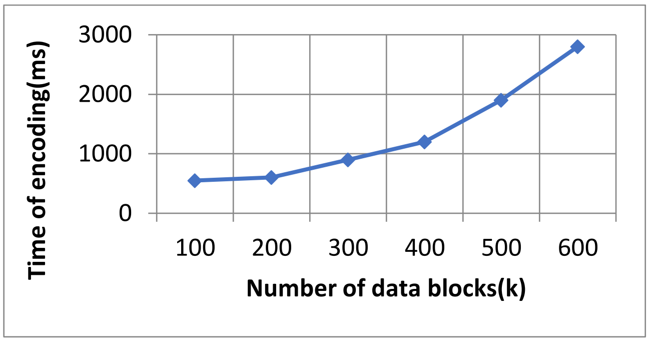
4.2 Experiment Results

While using different kinds of data the relationship between data storage in the user's machine and the number of data blocks is evaluated which is represented in below graph.



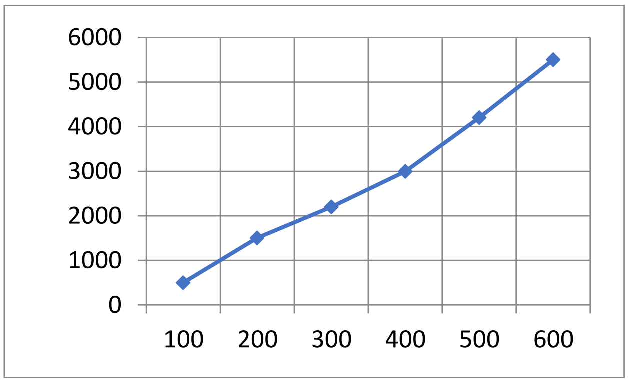
Graph 1: Relation between data storage and number of data blocks

K is number of data blocks and m is number of redundant data blocks. Here m is taken as value 2. From the chart we can conclude that, increasing the number of data blocks results in smaller volume stored in user's local machine. The below graph2 shows the relationship between time of decoding and number of blocks. The encoding time increases exponentially with the increase in number of data blocks (K). Here also value of m is considered as 2.



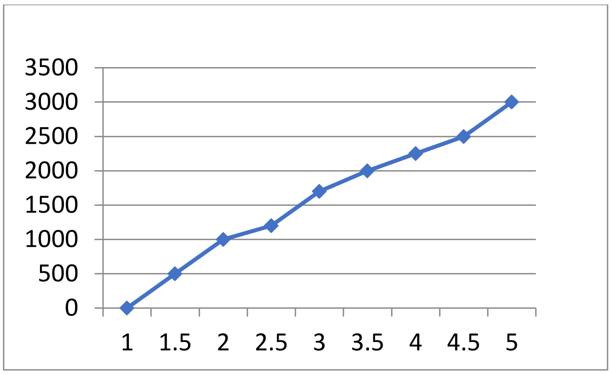
Graph 2: Relationship between time of encoding and number of blocks

In Graph 3, the relationship between decoding time and number of data blocks is represented. With increase in the number of data blocks there is a increase in time of decoding. Decoding takes more times than encoding.



Graph 3: Relationship between time of decoding and number of blocks

The relationship between the decoding time and number of removed data is shown in Graph 4. Here the value of K is taken as 100 and m is taken as 5. The ratio of m and k should be small. To avoid error reporting the number of removed data should be smaller than m. By increasing in number of removed data we can increase the decoding time.



Graph 4: Relationship between time of decoding and number of removed blocks

5. CONCLUSION

Cloud computing is very popular for not letting an attacker from outside. But, recently in 2014 we have seen a case tells icloud has been attacked by a hacker to get the data of a celebrity. It caused a huge fuss in that year. To reduce the attacks like this and prevent the theft we proposed a Three Layer Storage framework there the data to be stored in three different layers that are cloud, fog and localmachine or main memory. Here we used an algorithm called Hash-Solomon which is efficient in dividing the data into three parts and even encrypting and decrypting the data. This is used because this is of more reliable and compatible for our storage system. So, we want the users to use this Three Layer storage using cloud and fog computing for better and speed performance. And even for secured both in and outside the server.

6. REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50-50, 2009.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587-1611, 2013.

[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, “Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments,” in Proc.IEEEInt.Conf.Commun.,2014, pp. 2969-2974.

[4] H. Li, W. Sun, F. Li, and B. Wang, “Secure and privacy-preserving data storage service in public cloud,” J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397-1409,2014.