Scalable and Secure Network Storage in Cloud Computing

Muhib Ahmad Khan, M. Munwar Iqbal, Fahad Ubaid, Rashid Amin, Asima Ismail
Department of Computer Science, University of Engineering and Technology Taxila Pakistan

ABSTRACT

Cloud Computing is a newly born type of computation, which depends on the shared resources of the network. Cloud Computing term discovered from that time when the system can access the different types of applications as well as different types of services remotely. Cloud Computing is the unique, next generation of IT architecture, in which computation is done on the open network shared resources, which create a security risk. In comparison to the existing conventional infrastructure, The IT services come under the IT expert control. In a market there is a different type of service provider using cloud computing features offers many different services like virtualization, applications, servers, data sharing, and try to the reduce client-side computation overhead. Nevertheless, most of these services are outsourced to the third party, which creates the risk of data confidentiality as well as the data integrity. These days cloud computing, and its security is the hot topic for the research. In this paper, a new model proposed for storage data on the network for the secure data storage on the cloud server, which achieve the security, availability, confidentiality and integrity.

Keywords -- Cloud Computing, Data Integrity & Security, Data Confidentiality & Availability.

INTRODUCTION

The changing mode of technology and the rapid increase in these technologies had made the world a global village. The emergence of the new computing technologies has with certain types of benefits as well as challenges. Cloud computing is one of unique technology which emerge with a high amount of benefits. Cloud computing comes with the combination of the other core computing technologies [5]. Cloud-based computing is more than an IT shifted standard, it converts not only the IT sector, moreover every industry of the society. In simple language, Cloud Computing is a collection and combination of different computing applications and services from different servers on a network [1] [3]. Cloud Computing is the emerging field of computer science which required more research. Due to the miraculous success of the Internet, computing resources is now more abundantly available. The term "cloud" is used as a metaphor for the internet. The basic objective of cloud computing is secure data storage and for the internet computing devices [9] [6]. In cloud computing traditional service provider follow two different ways and these are infrastructure and service provider. In infrastructure, provider arranges cloud platform and lease resources according to the demand from the service provider. In service provider take the service from the infrastructure and sale it to the end users. Cloud computing is omnipresent. Basically it comes as new era technology which gives the facility of on-demand approach to the required network. Cloud computing comes with enormous benefits which all are available on one platform such as distributed computing, virtualization and much more [9]. All the advantages which come by

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

gaining the cloud computing methodology, in spite of all these features the sole of the cloud is not properly easy to implement. However, Cloud is in its initial phase, faces several risks, among all the issues of the cloud computing the most risk is security [3] [4]. The old conventional data security techniques are not satisfactory. The integrity of the data cannot be achieved by the old conventional methodologies. The user transfers their critical data to the scattered cloud environment [1] [6]. Thus, the cloud provider should enforce the appropriate security protocols to protect the essential integrity, authentication and authorization protocols of data.

Although cloud computing provides many facilities in term of data storage and online computation, there are also several issues which should be handled carefully. Traditionally Security measures are not adequate enough to keep the data safe according to the data security demands. To ensure the security factor in cloud computing, we need to define more security procedure in cloud computing as compared to the recent traditional procedures.

CLOUD SECURITY

Among besides all other problems in cloud computing, the security of the data is the core issue with respect to the business model tracked by privacy, integrity, and availability. Now the security of data is main interest among various services provider organizations, especially in a shared environment.

In the public or common cloud situation, its cloud service provider responsibility ensure the adequate security protocols to the critical data regarding authentication, integrity, and compliance. There are three different types of clouds available such as [2] [3]:

1. Software as a service (SaaS)
2. Platform as a service (PaaS)
3. Infrastructure as a service (IaaS)

The other types of cloud environment which are also used as services by a huge amount of users are as under:

A. Storage as a service
B. Database as a service
C. Information as a service
D. Process as a service
E. Integration as a service
F. Security as a service
G. Management/Governance as a service
H. Testing as a service

All these three clouds based services drives on different security problems. In IaaS, the basic resources processing and network utilization are offered by the service provider where user install and run the different applications. Moreover, in IaaS, the users have a superior hold on all over the security with respect to the other models. According to the PaaS, users are able to install their software on the cloud structure without the deployment of any other additional tools and the service providers dealing in PaaS also wishes to protect the platform software stack. SaaS users use the cloud service provider software with the help of web browser. In this model, the security of data is a chief challenge when the user utilizes SaaS based model of cloud.

In cloud computing environment, the data of the users are managed, and stored as plain or simple text and backup of data are also a serious concern.

ISSUES IN CLOUD

Cloud computing is a new era computing which makes it unique. Cloud computing emergence is very rapid. As the cloud is becoming popular, it also faces some issues which make it enhanced

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

for the stand alone in the market. These issue of the date are related to the data level. Cloud users move their sensitive data to the cloud to make it secure, but if cloud fails to provide better security to the data, which makes the cloud improper computing. The threats related to the data are [3]:

1. Malicious Insiders
2. Denial of Service
3. Data Loss or Data Leakage
4. Data Scavenging
5. Customer-data
6. Manipulation

DATA STORAGE IN CLOUD

The Cloud Service Providers offer two basic things one is computing and second is storage [3]. In cloud computing environment data is kept at the service provider location, and it is maintained by the further distributed vendors companies. Cloud computing changes the mode of the storage of the sensitive data on the cloud where you access it remotely rather than on the Hard Disk Drives of your personal computers. The trend of storing sensitive data in the cloud, the security measure shifts from as well and it needs more security parameters than local Hard Disk Drives. Different service providers of the Cloud own huge-sized data centers for data storage. So the user whether purchase or rent some of its portion for the storage of their critical data [3] [4]. A single data center contains hundreds of thousands of servers that are arranged in a rack of 20-40 servers each. The storage providers contain the hundreds of the datacenters linked with one another form a huge structure. Data is stored and maintained in the datacenter. Storage providers provide a huge number of services; these services are bitterly use by the special Application programming interface (API) through the network. These API are specially designed for the cloud and their users. The API of the cloud provides the whole image of the cloud. It describes the cloud performance as well as its security and much more [3]. To enhance the security of the cloud, we need to increase API efficiency and keep it update. As the cloud emerge, it proves itself more powerful, scalable, and more optimized than other available technologies [7]. Especially it has the strength or power to accommodate itself to new upcoming variations that based on the requirements, moreover the reduction of the huge amount of cost. There are different flaws in security parameters in cloud computing which make it unpopular. If it is unable to provide maximum security to the sensitive data, the all other benefits of the cloud have no value, and no one will agree to use it and make a compromise on security parameter [3].

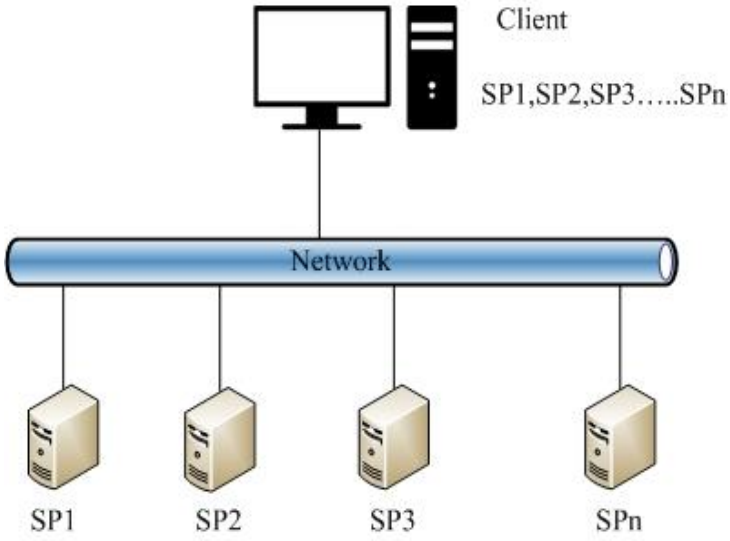

Figure 1.1: Data on different cloud services providers

The storage on the cloud offers security to the critical data by dividing the data into smaller chunks and store them in different places on the data center. If any particular chunks of the data are crashed in datacenter than remaining chunks, also sum up the data. The storing of the sensitive data as a plain text on the cloud providers location makes the data highly unsafe [3] [4] [5] [7]. The fame of storing data on the cloud is highly increasing by the reason of it can accessible from remote locations as well as it's not user concern to hold it all the time just as a reason of service provider accepts all the

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

accountability and all the concerns about the security.

In this paper, we suggest a more efficient way of more scalable as well as secure network storage architecture which contains different cloud storage providers for the improved storage of critical data. For better security, confidentiality, reliability and availability of the cloud, firstly the data of the user is encrypted and then divide the whole encrypted data into different chunks, then finally store it on to the different cloud services provider location. A cipher key is placed with every chunk of the data. Moreover, one of the special service providers contains whole encrypted data, but it does not contain the cipher key along with the data. If the data on any particular service provider is crashed, it can recover from this special service provider which contains all encrypted data by using the cipher key from the other service provider. For improved reliability and availability of data stored in the cloud, the Redundant Array of Inexpensive Disks model is implemented on the service provider side.

RELATED WORK

Fawaz in the related research [3] divide the data into a different number of chunks. These data distributions are places the on several different locations of clouds in such a way, that if any hacker or unauthorized person is able to gain access to a particular network. Then this unauthorized person is unable to extract the meaningful information because it is a small chunk of data and the other chunks of that critical data are stored in another different cloud locations. In other papers, the authors discussed the new advanced technology named RAID for the storage in the cloud. The Cryptographic technology is not so much mature. As the data increases in the cloud, then it is unable to provide the maximum security and privacy.

In this paper [3], the authors firstly apply the encryption mechanism on the critical data which user wishes to store in the cloud. After encryption, the author breaks the data into cipher chunks. Chunks of the encrypted data are now placed on the different cloud provider's locations named as SP1, SP2, and SP3. Figure 1.2 shows the initial image of the author proposed architecture, containing the host machine and the different service providers [3]. The author here introduces the parity bit to restore the encrypted data. For better availability and performance of the cloud he adopt the RAID technology and implement it on every server in the datacenter for improving availability and cloud performance. Our suggested model is somehow same to this methodology with little change in the distribution strategy. According to the paper authors [3] [5] [10], RAID 10 is more efficient than other RAID models. RAID 10 provides better availability as well as performance than other models of RAID.

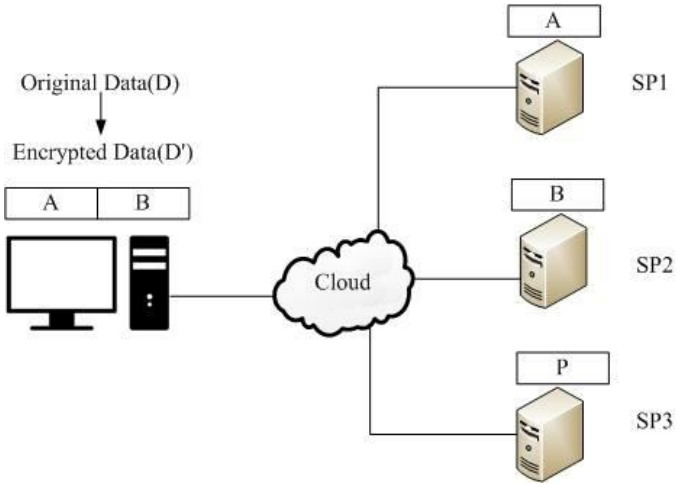

Figure1.2: Architecture of related Model

RAID 10 (1+0) gives various characteristics like, availability, redundancy of data and fault tolerance by the combination of characteristics of the mirroring and stripping [3].

PROPOSED MODEL

In this proposed model the "scalable and secure storage in cloud computing" is achieved by the number of different steps, every step involved in this architecture has its importance. Each step involved in this architecture is designed to provide maximum security to the sensitive data

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

which the user want to store on the cloud and not any unauthorized person or intruder gain the access of the whole data. Firstly, the critical data is divided into a different number of chunks depending upon the length of the data. After splitting the sensitive data into chunks, an encryption mechanism is applied on all these chunks [7]. Every particular chunk has its encryption key through which the encrypted data is retrieved into its original, meaningful form. As we stated earlier that every chunk of data has its encryption key so as the number of the data chunks increases, the number of keys also increases. The conversion of the plain critical data into numbers of encrypted cipher blocks is to provide maximum security to the data. RAID 10 model is implemented at data centers that are located on the clouds services provider side to provide better availability and performance [3] [10].

Suppose D is the original data of a user which is very secret from the user opinion. The user wants to move the data to the clouds service provider location. Firstly the original data D is split into a number of blocks A, B, C, D, E, F. and G. Then, after the splitting of data D, an encryption mechanism is applied on all these blocks of the data. Which convert the data blocks to the cipher blocks A', B', C', D', E', F' and G'. Every cipher block has its encryption key K (A), K (B), K (C), K (D), K (E), K (F) and K (G). Now the cipher blocks are placed on the different cloud provider's locations named as SP1, SP2, and SP3. For a while, the chunks of the encrypted data A' is placed on SP1. B' is placed on SP2, C' is placed on SP3, D' is placed on SP4, E' is placed on SP5, F' is placed on SP6 and G' is placed on SP7. It depends on the length as well as the number of chunks of the encrypted critical data, and the key of the encrypted cipher data is placed in such a way that a particular chunk contains the next two keys of the cipher block as shown in figure 1.3.

Original Data (D) -> Data Blocks (A, B, C, D, E, F & G) -> Encrypted Data Blocks (A', B', C', D', E', F' and G')

The figure 3 shows that the A' is on SP1 and contains the key of B. while C as K (B), K (C), B' is on SP2 and contains the key of C and D as K (C), K (D). C' is on SP3 and contains the key of D and E as K (D), K (E). D' is on SP4 and contains the key of E and F as K (E), K (F). E' is on SP5 and contains the key of F and G as K (F), K (G). F' is on SP6 and contains the key of G and A as K (G), K (A)and G' is on SP7 and contains the key of A and B as K (A), K (B). So the key on a particular cloud is determined by the piece of chunk on the number cloud services provider we placed:

D ((A'+1), (A'+2))

It gives the key of B' and C'. So we can find the key according to the piece of the block we placed on any particular cloud [3]. And the one cloud contains all the encrypted data without keys. Every chunk of data and its key is the division and mirrored affording to RAID 10 employment. A chunk of every data block is divided into two more pieces, and it's replica or copy is also stored on SP1, and the same procedure is also applied on all the cloud services provider sides.

SECURITY

Cloud computing became popular within a couple of years. Security emerges as a most important drawback in cloud computing which affects its popularity, and soon enough it realizes that it is the top most challenge of the cloud computing.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

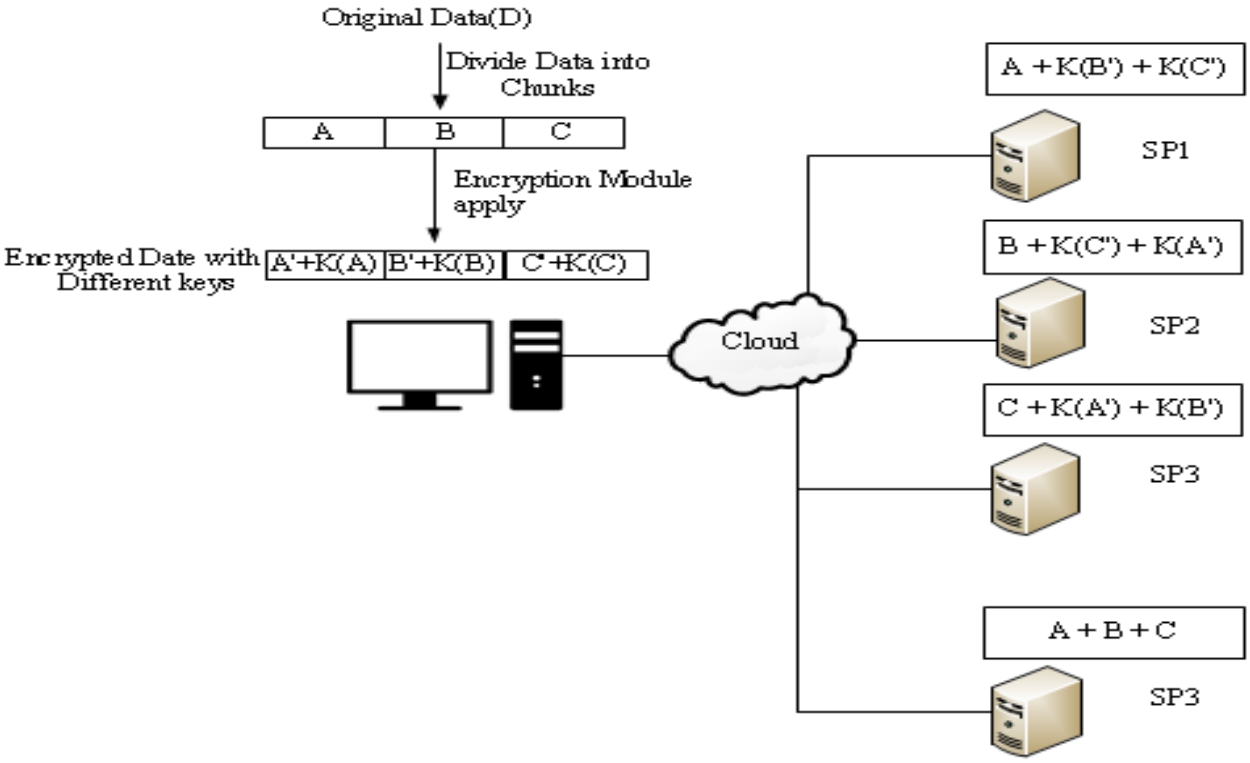

Figure 3: Detail proposed architecture

Besides cloud services provider there is also another scourge which is also a problem in cloud computing. Moreover, another threat of unauthorized access or intruder also affects the security of the cloud computing [3] [8]. Therefore, to ensure the security we firstly split the data and then offer encryption strategy in our proposed methodology. After this, distribute all the data on different clouds services provider location.

AVAILABILITY

The proposed model promises that the availability of the resources of the data at any time. The services provided by the cloud service provider contain a high level of risk, the risk of single degree of failure, which may destroy all the system. These failures rely upon numbers of factors software, hardware as well as a network failure. Our proposed model gives its solution by splitting and distributing the data on different clouds as compared to store the whole data on the single standalone cloud. If one cloud is down, we can recover the data from the other cloud with is also available on other clouds [10].

RELIABILITY

Through the key reliability of the offered model can be attained. The chunk of the data cannot be deciphered without a key. Moreover, the intruder did not get the whole data at once. If the particular chunk at the specific cloud is corrupted or lost, it can also be recover from another cloud as well.

CONCLUSION

The cloud computing became more general, more and more flaws emerge. Currently, the cloud computing is facing several problems, security, reliability and availability are the top most issue of the cloud computing. Security of the sensitive data is the top most priority of an organization. So according to the need, we proposed a better solution to provide more security to the data in the cloud computing. The client's critical data is more secure at the cloud service provider side and the user can access it at any time based on need. Our

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

model ensures better security, availability as well as reliability.

REFERENCES

[1]. Y. Singh, F. Kandah and W. Zhang,(2011) "A Secured cost effective multi-cloud storage in cloud computing," IEEE INFOCOM Workshop on Cloud Computing, pp. 619-624.

[2]. Qi Zhang, Lu Cheng, Raouf Boutaba (2010)" Cloud computing: state-of-the-art and research challenges" J Internet Serv Appl 1: 7–18.

[3]. Fawaz S. Al-Anzi, Jyoti (2014) et al., "Towards Robust, Scalable and Secure Network Storage in Cloud Computing".

[4]. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.Available: https://cloudsecurityalliance.org/ guidance/csaguide. /csaguide.v3.0.pdf.

[5]. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358.

[6]. X. Zhang, H. Du, J. Chen, Y. Lin, and L. Zeng,(2011) "Ensure Data Security in Cloud Storage," Proc. International Conference on Network Computing and Information Security (NCIS 11), IEEE Press, pp. 284-287.

[7]. P. F. Olivera, L. Lima J. Barros and M. Medard, (2010)" Trusted storage over untrusted networks," IEEE Global Telecommunication Conference, pp. 1-5.

[8]. W. Liu, (2012) "Research on cloud computing security problem and strategy," Proc. 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet 12), IEEE Press, pp. 1216-1219.

[9]. J. Sun and S.-S Yue, (2011) "The application of Cloud Storage Technology in SMEs," Proc. International Conference on E –Business and E –Government (ICEE 11), IEEE Press, pp. 1-5.

[10]. P. C. Chen, C. P. Freg, T W Hou and W G Teng,(2011) "Implementing RAID-3 on cloud storage for EMR System," IEEE International Computer Symposium, pp. 850-853.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500