Journal of Engineering and Applied Sciences 12 (Special Issue 12): 9400-9404, 2017
ISSN: 1816-949X

Building a Dynamic Virtual Machines Using KBR Agent for Data Security in Hybrid Cloud

[1]R.G. Suresh Kumar and [2]T. Nalini
[1]Vels University, Pallavaram, Chennai, Tamil Nadu, India
[2]Bharath University, Chennai, Tamil Nadu, India

Abstract: Cloud computing plays a key role towards the world for data sharing. In order to outsource the data in a secure manner the encryption scheme plays an important role in the cloud because sensitive information present in the cloud potentially causes privacy problems. Most of the encryption techniques will split the file in different hunk then the file is encrypted and store on multiple cloud where rather storing complete file on single cloud system. But if any one of the sliced file is corrupted it's difficult to rearrange the original file format. The proposed KBR agent will store the keys and data with high security in DVM with low budget for the client requirement. The proposed model KBR agent is creating Dynamic Virtual Machines (DVM) based on the Threshold keys and storing those secret keys in the DVMs which perform the high security on keys data and the integrity is maintained by storing the encrypted data in CSP (Cloud Service Provider).

Key words: Cloud computing, encryption, security, DVM, secret keys, CSP

INTRODUCTION

Cloud computing is a type of computing which supports on sharing the computing resources in network rather than storing those resources in local servers. Cloud computing is similar to grid computing where all computers unused processing cycles in a network are attached to solve problems too intensive for any stand-alone machine.

The objective of cloud computing is to make use of the, high-performance computing or supercomputing power to perform millions or trillions of computations per second in applications to afford data storage or to power large, immersive online computer games.

Cloud computing is an internet-based computing which provides different type of services and those services are delivered to all computers through the internet. Figure 1 explains cloud computing utilize large groups of servers which is running in low-cost technology with dedicated connections to share the data among servers. This shared computing infrastructure has large group of systems which are linked together. Often, the techniques called virtualization is used to make best use of power in cloud computing.

Security issues in cloud computing: The main issue for the IT executives is when the data is moves to cloud computing are preserve the security and privacy. But the cloud environment is a multi domain environment where the different types of resources are shared. But when sharing the data and hardware is highly risk factor. Any illegal users can hack easily either accidently or due to malevolent attack. So, the data storage will be a major security violation. In view of the security issues in 2008 and 2009 the two surveys were conceded by IDC. The surveys observations are analyzed and presented here.

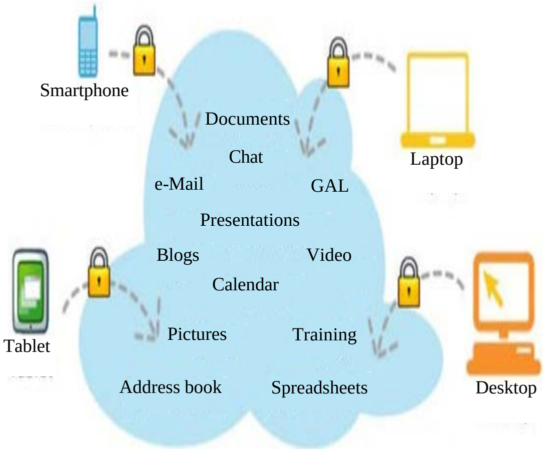

Fig. 1: Overview of cloud computing

The survey is conducted for 244 IT executives, CIOs and with the business colleagues about their views about companies use of IT cloud services and about their rating for the challenges and issues legitimate to the cloud or

Corresponding Author: R.G. Suresh Kumar, Vels University, Pallavaram, Chennai, Tamil Nadu, India

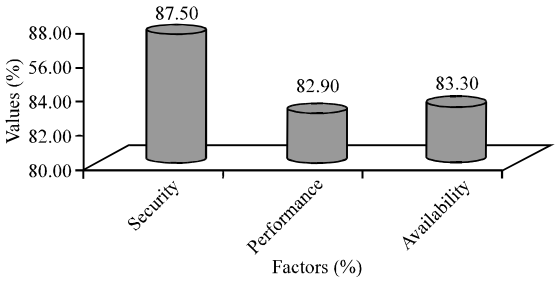

Fig. 2: Rate of challenges/issues with the cloud/on demand model in 2009 (Balasubramanian and Aramudhan, 2012)

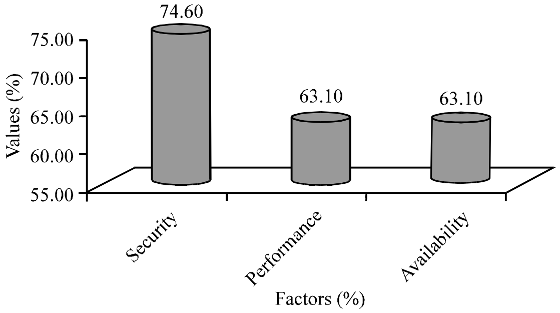

Fig. 3: Rate of challenges/issues with the cloud/on demand model in 2008 (Balasubramanian and Aramudhan, 2012)

on-demand model. By comparing these two surveys, we observe from the Fig. 2 and 3, that security challenges seem to be the top. The rate of all the three challenges was increased where as in 2008 performance and availability were tied. From their survey we understand that the cloud providers should take much more care for security of data stored in cloud (Balasubramanian and Aramudhan, 2012).

Public cloud: There is an ongoing dispute between IT sectors and professionals whether the private clouds are really more secure or not, further how the private clouds are more secure when comparing with some attributes and properties of public clouds (Balasubramanian and Aramudhan, 2012). In public cloud there is a larger target for the hackers when compare with the private clouds. When cloud service is best then there will have millions and trillions of customers depends on that service provider. But the provider would be definitely careful about whom they hire. In nowadays, the public cloud providers like Amazon, Facebook and Google are using the latest security mechanism which is much simpler than a private company (Balasubramanian and Aramudhan, 2012).

Private cloud: It is built on their own software and hardware and also know as corporate or internal cloud, similar like public clouds the private clouds are also having the same security issues. The companies protecting their data in private cloud have converses about the new security issues and the following are suggested by them for making some changes in private cloud and they are hypervisors are placed to ensure the security in private cloud, security and integrity of discussed also considered, configuration and patch management also be considered (Balasubramanian and Aramudhan, 2012).

The consulting group of Gabriel recently conducted the survey regarding the security issues in private cloud. But the report says that 38% organizations are using private cloud, 40% organizations say they need improvement in security and 8% say that security is very weak. In response 40% organizations who are building the private cloud are trust on that security is very strong (Balasubramanian and Aramudhan, 2012).

Hybrid cloud: Recently, the survey is conducted by Trend Micro company and analyzed that there is failure in public cloud services to congregate with IT and business organizations. But the hybrid cloud environment can assist needs of IT and business organizations. About 30% of survey says that CSP are not met their IT requirements, 38% claimed that CSP are not meeting their business needs, 40% indicated that how to secure the data in cloud which increased the thought of adopting cloud. The companies realizing that using of hybrid cloud expands the deployment of more application in cloud (Balasubramanian and Aramudhan, 2012). The following are approaches to address the security issues (Thinakaran and Chitra, 2016):

- Prevention of placement risk by shared infrastructure
- Physical isolation for cloud customers as per the service agreement, so, to save the cost and computation
- Minimizing the shared infrastructure by removing the hypervisor but still containing the virtualization
- The trusted cloud computing enables the IaaS providers and determines the security in service before uploading into cloud. A privilege is needed to unable the access of customers memory

Virtualization technology: Virtualization allows you to create a virtual computer on a physical computer. Fundamentally virtualization is what allows a computer operator to divide up the component parts of a computer into separate resource pools and allocate them to virtual machines (computers). Therefore, from one single computer, you could create many more virtual computers thus, allowing the users of virtual computers to share all the resources of the single physical computer. These virtual computers are most commonly known as Virtual Machines (VMs). This in itself would still not normally be classified as cloud computing as it's broadly accepted that cloud computing needs to extend the virtualization layer across multiple computers, akin to "grid computing" or multiple computers all acting together, distributing the workloads of multiple virtual machines across multiple physical machines.

Literature review: Prakash *et al*. (2014) introduced an efficient data encryption and decryption algorithm to protect the outsourced privacy data in cloud computing. By using data encryption, the file splitting technique is used to reduce the storage and also overheads on computational and for authorized users verification to access the data from cloud server, third party is introduced. The drawback of this approach is there is no data integrity and security when the file is spit and third party handles taking the ownership.

Mirajkar and Biradar (2014) proposed a multi-cloud architecture which will maintain the integrity of data even one cloud fails but the disadvantage is the budget will be more for the client to define the architecture.

Waghmare and Patil (2014) proposed a secured cost-effective multi-cloud storage model which clutch's an economical distribution of data in the cloud service provider in the market and provide the security and advanced data availability for customer. But security is not preserved when the data is distributing in multiple service providers. Gupta and Priyanka (2013) proposed hybrid encryption scheme encryption and decryption of files at cloud server is done using blowfish and modified version of RSA but the complexity of the model will affect performance of the data processing.

Muhil *et al*. (2015) proposed algorithm for secret sharing keys in multi cloud to address the security risks using Shamir's algorithm for secret sharing. But security level will low when the keys are stored in CSP (Cloud Service Provider). Dable and Mishra (2014) define the data splitter over the multiple cloud drive as a hunk of file with encryption. But no data integrity is maintained while storing a hunk of file in the multiple clouds.

Bessani *et al*. (2013) define the DEPSKY Model to improve the availability of resource in the cloud. But the confidentiality will not be maintained when the resources are shared in multiple clouds.

MATERIALS AND METHODS

Proposed work: Storage in cloud is an area of concern for confidential information. The existing scenarios flows with cloud provider encrypting the files by using encryption algorithm with the key and those files and keys are split and stored in different clouds. The objective of the research is to share the data in a secure way and also storing the shared keys with high security and the low cost.

The drawbacks of the existing data sharing mechanism have been overcome by the proposed KBR agent. The architecture aims at fulfilling dynamicity, security, integrity and low budget to provide complete secure data sharing in hybrid cloud.

The agent includes the mechanism Hadoop which is used to provide a generalized and extensible framework created to upgrade from one server to thousands of machines, each contribute the local computation and storage. In the proposed work Hadoop is used to create DVM to store the keys. The DVM are created based on size of the file uploaded in the proposed model. Shamir's secret key algorithm is used for storing the secret keys in different virtual machines and RSA algorithm for file encryption and decryption. Linear congruential generator method is used to generate OTID (One Time Identification) to verify the valid used for uploading and downloading files.

In the proposed model a users can register themselves and then share their data in the cloud. The users joining the group have to register themselves with their information with the private cloud (Fig. 4). The One Time Identification Number (OTID) is dynamically generated to verifies whether the valid user to upload the file. Once the file is uploaded, KBR Agent encrypt the file using AES (Advanced Encryption Standard) and stored in the cloud (without splitting the file), simultaneously the Shamir's secret key algorithm generates the secret keys for the encrypted file based on the file size, secret keys are created dynamically and stores those secret keys in the DVM.

RESULT AND DISCUSSION

Design and implementation: For the purpose of implementing the proposed model (Fig. 4) three techniques are used LCG (Linear ongruential Generator) for the user's identity by Generating OTID (One Time Identification Number), LCG is an algorithm which generates randomized numbers calculated with a linear equation. It is one of the oldest pseudorandom number generator algorithms and also it is relatively easy to understand and they are fast and easily implemented.

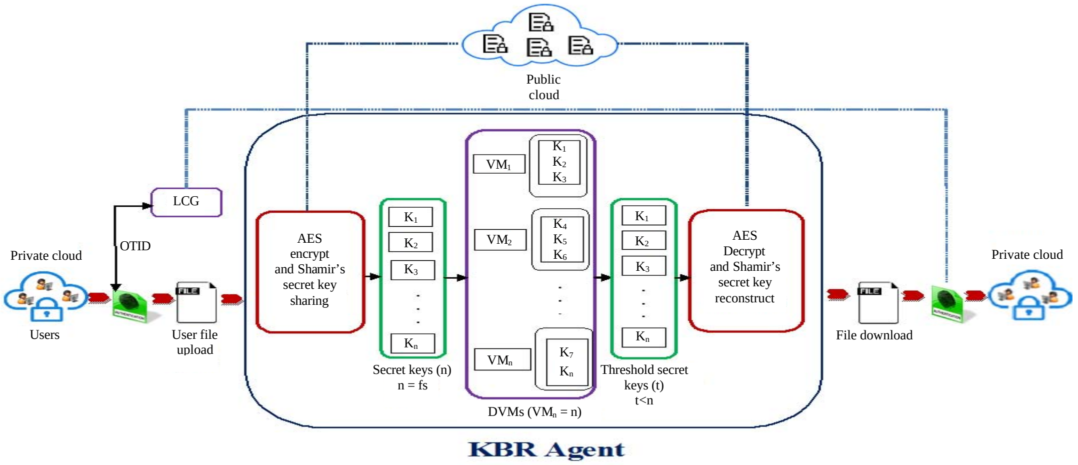

Fig. 4: Proposed KBR architecture

Shamir's secret key sharing algorithm is used for secret key generation, securing the data is an essential in the cloud environment. Therefore, to secure the hybrid cloud data, Shamir algorithm is used to store the key in more than one place and AES algorithm is used to encrypt the private data and stored in any CSP (Cloud Service Provider) in the market. The goal of the algorithm is to divide the keys into n pieces. The secret keys are divided based on the size of the file to be uploaded.

The objective is to divide the secret keys Sk in to n pieces Sk_1, Sk_2, ..., Sk_n and store it in different virtual machines. When:

$$(Sk, n)<t$$

Where:

t = The no. of threshold key count
Sk = The Secret Key and n is the no of shares

$$n = fs/P$$

Where:

fs = The file size
P = Prime number

where, P>fs and n>0. Figure 4 describes the process flow of the KBR agent and the step by step process is explained as follows.

Uploading phase:

- Step 1: users register their details are stored in the private cloud
- Step 2: LCG generator the OTID (One Time Identity) for the user and copy of OTID is stored in the private cloud
- Step 3: the generated OTID is verified with the OTID in private cloud
- Step 4: once OTID is verified the user can upload the file
- Step 5: when uploading the file KBR Agent encrypt the file and store the copy in the public cloud
- Step 6: the secret keys and DVM are dynamically generated based on the size of the file (n = fs)
- Step 7: the generated secret keys are stored in the generated dynamic virtual machines

Downloading phase:

- Step 1: the registered user verifies their OTID authentication for downloading the file
- Step 2: after OTID authentication is passed the file can be downloaded
- Step 3: KBR agent receives the user requested file and retrieves the threshold keys (t<n) from the DVM
- Step 4: the user requested file will be downloaded when matching of secret keys from DVM is successful
- Step 6: after downloading the file the secret keys in the DVM and OTID will be deleted

The benefit of using the VM for storing the secret key is the VMs are generated dynamically, so that, the security is maintained where the keys are stored and the keys can be cracked are hacked are not possible from the virtual machines.

The file is uploaded with different sizes in existing and proposed system and the result (Fig. 5) is compared with performance of file uploading in milliseconds with the same configuration of the system.

Hadoop: Hadoop is a framework developed in Java programming and it is the product of Apache. The eco system consists of HDFS, Apache Hive, Zookeeper and

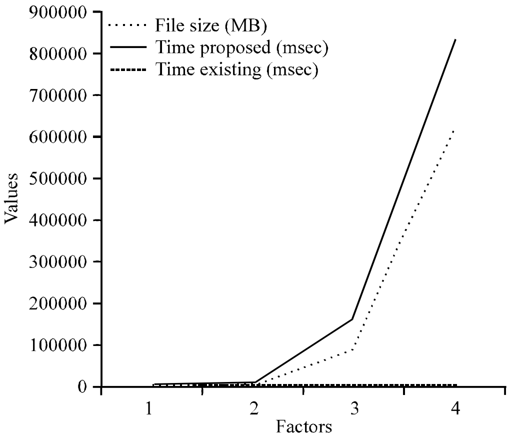

Fig. 5: Performance comparison of KBR agent with exsisting

MapReduce. Hadoop supports the processing of large collection of data in a distributed computing environment uses a master/slave structure (Bessani *et al*., 2013). The collection of data sets can be processed among a group of servers and applications running on thousands of nodes involving thousands of terabytes by using Hadoop. In Hadoop file system the data transfer fast rate is high which allows the system to maintain their normal operation even the node is failures which reduce the threat of a whole system failure. Hadoop allows a computing solution that is cost effective, scalable and flexible and fault tolerant. Hadoop framework is used by popular companies in world. The sub projects of Hadoop have two types one is map reduce and another one is Hadoop Distributed File System (HDFS) (Bhosale and Gadekar, 2014).

Hadoop Distributed File System (HDFS): HDFS is the component of Hadoop exclusively used for the file system. In file system HDFS stores the application data and metadata separately. The file system in HDFS stores metadata in the server called NameNode and stores the application data in the server called DataNode. But both the servers are communicated and connected with them by using the protocol TCP. Hadoop distributed file system framework is designed for storing large data and flow the data with high bandwidth to user application (Bhosale and Gadekar, 2014).

CONCLUSION

The proposed KBR Agent uses OTID, cryptography and virtualization technology to ensure the shared data privacy, user identity and dynamicity. The agent is flexible to allocate VMs Dynamically (DVM) for storing the secret keys instead of storing in multiple clouds which will provide the confidentiality for the keys and integrity for the data stored in public clouds. The agent can be implemented with low cost when comparing with existing architecture models. The proposed agent is simple and efficient to use for data security and privacy in the hybrid cloud.

REFERENCES

Balasubramanian, R. and M. Aramudhan, 2012. Security issues: Public vs private vs hybrid cloud computing. Intl. J. Comput. Appl., 55: 35-41.

Bessani, A., M. Correia, B. Quaresma, F. Andre and P. Sousa, 2013. DepSky: Dependable and secure storage in a cloud-of-clouds. ACM. Trans. Storage, Vol. 9, 10.1145/2535929

Bhosale, H.S. and D.P. Gadekar, 2014. A review paper on big data and hadoop. Intl. J. Sci. Res. Publ., 4: 1-7.

Dable, N.D. and N. Mishra, 2014. Enhanced file security using encryption and splitting technique over multi-cloud environment. Intl. J. Adv. Comput. Theor. Eng., 3: 6-10.

Gupta, R. and T. Priyanka, 2013. Enhanced security for cloud storage using hybrid encryption. Intl. J. Adv. Res. Comput. Commun. Eng., 2: 2710-2713.

Mirajkar, S. and S.K. Biradar, 2014. Using secret sharing algorithm for improving security in cloud computing. Intl. J. Adv. Res. Comput. Sci. Technol., 2: 395-398.

Muhil, M., U.H. Krishna, R.K. Kumar and E.M. Anita, 2015. Securing multi-cloud using secret sharing algorithm. Procedia Comput. Sci., 50: 421-426.

Prakash, G.L., M. Prateek and I. Singh, 2014. Data encryption and decryption algorithms using key rotations for data security in cloud system. Proceedings of the 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT.), July 12-13, 2014, IEEE, New York, USA., ISBN:978-1-4799-3140-8, pp: 624-629.

Thinakaran, P. and S. Chitra, 2016. Examining the security and privacy practices in cloud computing. Asian J. Inf. Technol., 15: 1199-1206.

Waghmare, A. and R. Patil, 2014. Data storage in secured multi-cloud storage in cloud computing. Intl. J. Comput. Eng. Res., 4: 66-69.