ISSN: 2321-7782 (Online)
Volume 1, Issue 5, October 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Cloud Computing Security and Encryption

Varsha Alangar
Department of Computer Science Engineering
Meenakshi Sundararajan Engineering College (Affiliated to Anna University)
Chennai – India

Abstract: ***Cloud computing has been the talk of the town in the recent years. It has been suggested to everyone to store their data on a cloud. This has led to the birth of a new domain of research. As the cloud technology improves over time, so does the security threats. So, we need to solve the security issues in the cloud technology. In this paper, I have given a brief introduction on Cloud computing and touched some of the security issues related to a cloud. Having explained the problems in the cloud, I have also proposed some solutions to the same with the help of algorithms like the DES and RAS Algorithms.***

Keywords: Cloud, Security; Encryption algorithms; Security issues; RAS Algorithm.

I. INTRODUCTION

When we say the word "Cloud", our minds tend to wander towards the clouds in the sky, floating all alone, not disturbing anyone. However, this cloud has been redefined to suit the world of Information Technology. A cloud is no longer a mass of gases floating in the upper atmosphere. It is now an IT service. A cloud is nothing but a virtual space where a humongous amount of data can fit in. A cloud enables a user to store all his/her data in servers located in remote locations. These locations could be a remote island that is scarcely populated. A user, with the help of a cloud ID, can access these data from the comfort of their home. This not only helps the user easily access the data, but the user requires very less hardware resources to do so.

To generalize this concept, a cloud is a pool of virtual resources which could include both hardware and software resources. A user can access these resources on a pay-per-use basis. This means that the user would pay only for the resources he/she uses, not paying a penny more or a penny less. The user is given freedom to not only access the data but also to create new data or alter an existing one if given proper permission. Although the storage units for a cloud requires huge space and servers that has the capacity to hold the tremendous amount of data, the end user only requires a small, light device that can access these data via the internet.

We could say that a cloud is a pattern of interconnected web of virtual computers which uses remote services through a network using various resources. The main objective of a cloud is to give maximum with minimum hardware which means that with a minimum amount of hardware, the user can access a maximum amount of resources. A cloud is a set of parallel and distributed systems, all combined into a web of computers.

Fig 1: Virtual picture depicting the cloud concept

The cloud employs certain services like the PaaS, IaaS and the SaaS which respectively stand for Platform as a Service, Infrastructure as a Service and Software as a Service.

II. Cloud Computing Deployment Model

Depending on infrastructure ownership, there are four deployment models of cloud computing each with its merits and demerits. This is where the security issues start.

A. The Public Cloud

This is the traditional view of cloud computing in every day lingua. It is usually owned by a large organization (e.g. Amazon's EC2, Google's AppEngine and Microsoft's Azure). The owner-organisation makes its infrastructure available to the general public via a multi-tenant model on a self-service basis delivered over the Internet. This is the most cost-effective model leading to substantial savings for the user, albeit with attendant privacy and security issues since the physical location of the provider's infrastructure usually traverses numerous national boundaries.

B. The Private Cloud

Refers to cloud infrastructure in a single tenant environment, it defers from the traditional datacenter in its predominant use of virtualization. It may be managed by the tenant organization or by a third party within or outside the tenant premises. A private cloud costs more than the public cloud, but it leads to more cost savings when compared with a datacenter as evidenced by Concur Technologies (est. savings of $7million in 3 years from 2009) . The private cloud gives an organization greater control over its data and resources. As a result, the private cloud is more appealing to enterprises especially in mission and safety critical organizations.

C. The Community Cloud

According to NIST, the community cloud refers to a cloud infrastructure shared by several organizations within a specific community. It may be managed by any one of the organizations or a third party. A typical example is the Open Cirrus Cloud Computing Test bed, which is a collection of Federated data centers across six sites spanning from North America to Asia.

D. The Hybrid Cloud

Comprises of a combination of any two (or all) of the three models discussed above. Standardization of APIs has led to easier distribution of applications across different cloud models. This enables newer models such as "Surge Computing" in which workload spikes from the private cloud is offset to the public cloud.

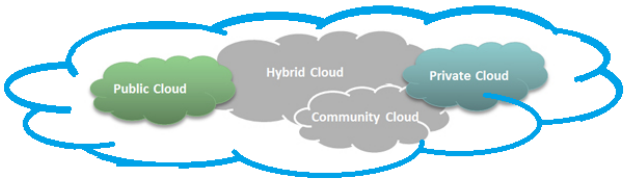

Fig 2: Various cloud models making up the entire cloud

III. Security Issue in Cloud Computing

Although cloud is one of the most sought out technologies nowadays, it is also the most recent technology. With cloud, like any other new technology, there has not been much research on the security a cloud provides its users. Due to this reason, a cloud suffers from serious security problems including:

1. Problems with data security
2. Problem of infection
3. Other security issues

1. *Problems with data security*

As mentioned earlier, there can be a very large amount of data on a cloud. With so much information, it becomes susceptible to losses. Data loss is a common problem with cloud storage where due to improper storage, the required information may be difficult to find later. This is considered as loss of data since the data cannot be found. However, in certain situations, a cloud service provider might try to reuse a service, might use someone else's server to provide service to the user instead of using their own servers. In these cases, data stealing can occur. Data stealing is a serious issue in a cloud. The actual owner of the server will have complete access to his/her server. When a service provider allocates the same server to a user, and the user places all the personal information into that server, the owner of the server could easily access this personal information.

2. *Problem of infection*

Since a user can access the data on a cloud, a mischievous user could upload a virus or any other application or software that could seriously harm another user's computer or hardware device when it is downloaded. To prevent such mishaps, a great deal of security measures must be implemented.

3. *Other Security issues*

The other kinds of security issues are not just exclusive to a cloud. These include some of the common security threats like hacking a user's cloud account to gather information. A sound password and a mechanism where tracing is impossible must be implemented.

IV. ENCRYPTION METHODS FOR DATA SECURITY IN CLOUD

Encryption is the mechanism of protecting the private data of a user. Public and private keys can be used to achieve encryption of the data but the effectiveness of the encryption depends on how well the keys are used.

A. *Implementing DES Algorithm in Cloud for Data Security*

DES is short for **Data Encryption Standard**. This Cipher Block Chaining system is to be secure for clients and server. Developed in the 1970s at IBM, this algorithm is highly influential in the world of cryptography.

The structure of the DES Algorithm is as follows:

There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa). IP and FP have no cryptographic significance, but were included in order to facilitate loading blocks in and out of mid-1970s 8-bit based hardware.

Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar processes — the only difference is that the subkeys are applied in the reverse order when decrypting. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as there is no need for separate encryption and decryption algorithms.

The ⊕ symbol denotes the exclusive-OR (XOR) operation. The F-function scrambles half a block together with some of the key. The output from the F-function is then combined with the other half of the block, and the halves are swapped before the next round. After the final round, the halves are swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes.

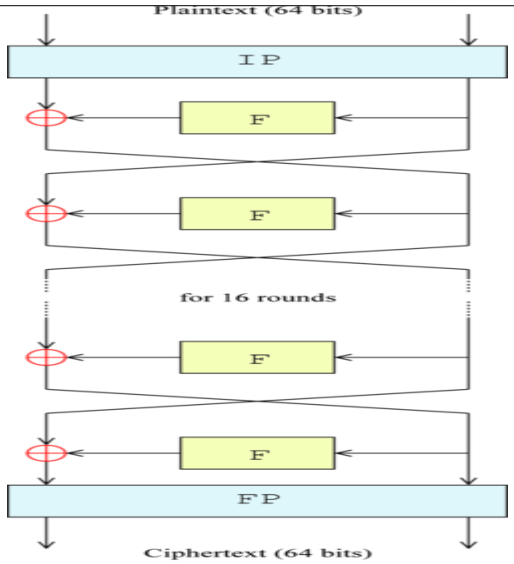

Fig 3: Structure of DES Algorithm

B. RSA Algorithm

RSA which stands for Ron Rivest, Adi Shamir and Leonard Adleman is an encryption algorithm where the data is encrypted in such a way that only the appropriate user can access it. The algorithm first encrypts the user data and then saves the data on the cloud. Public and private keys can be used to decrypt the data when the allowed user retrieves the data from the cloud. Public-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. The Cloud service provider encrypts the data and decryption is done by the Cloud user or consumer.

The steps involved in the RAS Algorithm are as follows:

1) **Select two large, unique prime numbers say, p and q.**
2) **Compute the value of n, where n is the product of p and q. i.e.; p*q**
3) **Compute the Euler's Totient w(n), by using the formula: w(n)=(p-1)*(q-1)**
4) **Choose the value of 'e', the encryption key, where e<w(n) and the GCD(e, w(n))=1**
5) **Find the value of'd'. d*e must be congruent to 1(mod w(n))**
6) **Determine the value of cypher text C using the M^e mod n formula.**
7) **Determine the value of plain text M using the C^d mod n formula to ensure that you obtain the already calculated value of d.**

We now try to explain the calculations with the help of an example:

1) Consider the two primes 11 and 17. Let p=11 and q=17.
2) Now, the value of n is 187 (n=11*17).
3) w(n) when calculated using the formula in step 3 gives the value 160.
4) At this point, we assume the value of e to be 23. Any other value can also be chosen with the condition in step 4 in mind.
5) The value of d is 7 since d*23 must be congruent to 161.
6) Now, we assume the value of M to be 2. As per step 6, 2^23 mod 187 yields the result 162.
7) Now, the value of M is recalculated as per step 7, 162^2 mod 187, to get back the value of M as 2.

a. Querying Encrypted Data

There are several methods that were proposed to handle Querying of Encrypted Data. In the proposed scheme, several cryptographic methods were used to encrypt the data in each cell of each table to be stored in the cloud. When a user needs to query this data, the query parameters are encrypted and checked against the stored data. No data decryption is done in the cloud, thus protecting the Authenticity and integrity of the information. When the results of the query is returned (in encrypted form) to the user, the user then decrypts the data and uses it. This scheme also has significant improvements for select queries over previous related schemes.

i. Key Management

Since encryption is the main method used to ensure data security, naturally we would be faced with the problem of key management. The encryption keys cannot be stored on the cloud; therefore the customer must manage and control a key management system for any cryptographic method used. For simple encryption schemas, there might not be a problem since a single encryption and decryption key can be used for the entire system. However, almost any real database requires a more complex system. This simple system to manage keys might even have to take the form of a small database which would have to be a secure local database; which again, may defeat the purpose of moving the original database to the cloud.

Clearly Key Management is a real problem for cloud systems using encryption, and recent research has been done on using two-level encryption which allows the Key Management system to be stored in the cloud. This scheme is efficient, and may be the solution to the Key Management problems cloud systems faces; however, it hasn't yet been applied specifically to database encryption.

ii. Data Splitting

Some methods have been developed that serve as alternatives to encryption. These methods are generally faster than encryption but have their own drawbacks. The idea is to split the data over multiple hosts that cannot communicate with each other; only the owner who can access both hosts can collect and combine the separate datasets to recreate the original. This method is extremely fast compared to encryption but it requires at least two separate, but homogeneous service providers**.**

iii. multi-clouds Database Model (MCDB)

This is a method of Data Splitting which uses multiple clouds and several other techniques to ensure data is split in across clouds in a manner that preserves the data Confidentiality, Integrity and ensures Availability. MCDB provides cloud with database storage in multi-clouds. MCDB model does not preserve security in a single cloud; rather security and privacy of data will be preserved by applying multi-shares technique on multi-clouds. By doing so, it avoids the negative effects of single cloud, reduces the security risks from malicious insiders in cloud computing environment and reduces the negative impact of encryption techniques.

MCDB preserves security and privacy of user's data by replicating data among several clouds, using a secret sharing approach that uses Shamir's secret sharing algorithm, and using a triple modular redundancy (TMR) technique with the sequential method. It deals with the cloud manager to manage and control operations between the clients and the multi-clouds inside super cloud service provider.

iv. Multi Tenancy

Cloud systems share computational resources, storage, services between multiple customer applications (tenants) in order to achieve efficient utilization of resources while decreasing cost, this is referred to as multi-tenancy. However, this sharing of resources violates the confidentiality of tenants' IT Assets. This implies that unless there's a degree of isolation between these tenants, it is very difficult to keep an eye on the data flowing between different realms which make the multi-tenancy model insecure for adoption. Some multi-tenancy issues are:

1. Virtual Machine Attacks

Typically, in a cloud, business data and applications are stored and ran within virtual machines. These virtual machines are usually running on a server with other virtual machines, some of which can be malicious. Research has shown that attacks against, with and between virtual machines are possible.

If one of the virtual machines on a server hosts a malicious application that breaches legal or operational barriers; this may lead legal authorities, the service provider or other authorities to shutting down and blocking access the entire server. This would greatly affect the users of the other Virtual Machines on the server.

2. Shared Resources

Assuming the cloud system isn't running on a virtual machine, the hardware is now an issue. Research has shown that it is possible for information to flow between processor cores, meaning that an application running on one core of a processor can get access to information of another application running on another core. Applications can also pass data between cores. Multicore processors often have complex and large caches. With these hardware resources, if data is decrypted in the cloud, if even for a moment for comparison, it would then exist unencrypted in the memory of some one of the cloud machines. The problem is that we don't know what other application is running on these machines. Other malicious cloud users or the service provider can me monitoring the machine memory and be able to read our data. However, the likelihood of these hardware attacks is very. If one of the applications on a server hosts is malicious, this may lead to the service provider or some other authority shutting down and blocking access the entire server in order to investigate and determine the malicious application. This would greatly affect the users of the other applications on the server.

V. CONCLUSION

Cloud computing has become the future of computing and it helps to have a good security backup for the ever growing cloud to secure private data from being tapped by hackers or malicious viruses. The algorithms proposed in this paper could be implemented in the cloud network to prevent its data loss or corruption.

References

1. Virtualization Overview. White Paper. Vmware. Retrieved April 6, 2011, available at: http://www.vmware.com/pdf/virtualization.pdf
2. Web Search For A Planet: The Google Cluster Architecture. Retrieved April 6, 2011, available at: http://labs.google.com/papers/googlecluster-ieee.pdf
3. What is Cloud. Retrieved April 6, 2011, available at: http://www.rackspace.co.uk/cloud-hosting/learn-more/whatis- cloud/
4. What is Cloud Computing. Retrieved April 6, 2011, available at: http://www.microsoft.com/business/engb/ solutions/Pages/Cloud.aspx
5. What is Cloud Computing. Retrieved April 6, 2011, available at: http://www.ibm.com/developerworks/cloud/newto.html#W HATIS
6. Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.
7. Cloud computing methodology, systems and applications lizhe wang, rajiv ranjan.http://www.unitiv.com.
8. C.N. Höfer and G. Karagiannis, "Cloud computing services: taxonomy and comparison", Internet Serv Appl (2011)
9. F.A.Alvi, B.S.Choudary, N.Jaferry,"Review on cloud computing security issues & challenges", iaesjournal.com, vol (2) (2012).
10. Furht,B., and Escalante,A. (2010). Handbook of Cloud Computing. New York: Springer http://searchcloudcomputing.techtarget.com/definition /private-cloud

AUTHOR(S) PROFILE

Varsha Alangar, is currently pursuing her B.E in Computer Science Engineering at Meenakshi Sundararajan Engineering College which is affiliated to the Anna University of Chennai, Tamil Nadu, India. She has presented several papers on Cloud computing and Green cloud computing along with other networking papers including "Resource allocation in Wireless Mesh networks" and other papers related to Operating systems.

