ISSN 2277-3061

ADVANCED FILE BASED SECURITY MECHANISM IN CLOUD COMPUTING: A REVIEW

Nisha [1], Naseeb Singh [2]
[1] Research Scholar, Department of Computer Science Engineering, AIET, Faridkot
nisha.nikhanj@gmail.com
[2] Assistant Professor, Department of Computer Science Engineering, AIET, Faridkot
naseebdhillon@hotmail.com

ABSTRACT

Cloud computing is a broad solution that delivers IT as a service. Cloud computing uses the internet and the central remote servers to support different data and applications. It is an internet based technology. It permits the users to approach their personal files at any computer with internet access. The cloud computing flexibility is a function of the allocation of resources on authority's request. It represents all the complexities of the network which may include everything from cables, routers, servers, data centers and all such other devices. Cloud based systems saves data off multiple organizations on shared hardware systems. In this paper the attempt to secure data from unauthorized access. The Method of data security is AES algorithm for providing data security by encrypting the given data based on the AES. It is based on a design principle known as a substitution-permutation network, and is fast in both Software and Hardware. The algorithms used in AES are so simple that they can be easily implemented using heap processors and a minimum amount of memory and this data then can only be decrypted by authorized person by using his private key.

Keywords

Cloud Computing, Cloud Security, Virtual Machine, AES, XOR Operation.

INTRODUCTION

Cloud Computing is one of the biggest technology advancement in recent times. It has taken computing in initial to the next level. Cloud computing is a broad solution that delivers IT as a service. Cloud computing uses the internet and the central remote servers to support different data and applications. It is an internet based technology. It permits the users to approach their personal files at any computer with internet access. The cloud computing flexibility is a function of the allocation of resources on authority's request. Cloud computing provides the act of uniting. Cloud computing is that emerging technology which is used for providing various computing and storage services over the Internet. In the cloud computing, the internet is viewed as a cloud. By the use of cloud computing, the capital and operational costs can be cut. The new developments in the field of information technology offered the people enjoyment, comforts and convenience. Cloud computing is one of the latest developments in the IT industry also known as on-demand computing. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. It is the application provided in the form of service over the internet and system hardware in the data centres that gives these services. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash-strapped IT departments that are wanted to deliver better services under pressure. When this cloud is made available for the general customer on pay per use basis then it is called public cloud. When customer develops their own applications and run their own internal infrastructure then is called private cloud. Integration and consolidation of public and private cloud is called hybrid cloud. But having many advantages for IT organizations cloud has some issues that must be consider during its deployment.

A. SECURITY CONCERNS IN CLOUD COMPUTING

As the next generation, Cloud Computing has visional architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under physical, logical and personnel controls. Current cloud service is grant access to web browser or host install application directly. Cloud storage space moves the users data to large data centers database, on which user does not have any management to manage data. The commercial achievement of Cloud Computing and up to date developments in Grid Computing has been create platform virtualization technology deal with high performance computing by both enterprises and individuals with high service-level requirements. Data security has grow to be predicament of cloud computing like file system, data security, host security. Security is a secure mode practical Internet based on the cloud computing. These are security and trust issue forth, users data has been liberating to the Cloud and safety measures sphere of the data owner. The data is physically not available to the user the cloud shall provide a way for the user to check if the integrity of his data is maintain.

In this section we first introduce some major security concern-

• **Network Availability** The value of cloud computing [2] can only be realized when our network connectivity and bandwidth meet our minimum needs: The cloud must be available whenever we need it. If it is not, then the consequences are no different than a denial-of-service situation.

• **Cloud Provider Viability** Since cloud providers are relatively new to the business, there are questions about provider viability and commitment. This concern deepens when a provider requires tenants to use proprietary interfaces, thus leading to tenant lock-in.

• **Disaster Recovery and Business Continuity** Tenants and users require confidence that their operations and services will continue if the cloud provider's production environment is subject to a disaster.

• **Security Incidents** Tenants and users[3] need to be appropriately informed by the provider when an incident occurs. Tenants or users may require provider support to respond to audit or assessment findings. Also, a provider may not offer sufficient support to tenants or users for resolving investigations.

• **Transparency** When a cloud provider does not expose details of their internal policy or technology implementation, tenants or users must trust the cloud provider's security claims. Even so, tenants and users require some transparency by providers as to provider cloud security, privacy, and how incidents are managed.

B. RELATED WORK

• **Xueli Huang, Xiaojiang Du** (2013): discuss about the security in cloud computing. Cloud computing is fast growing area in computing research. The author propose a novel scheme to achieve the above goals. They test their scheme in real network environments (including Amazon EC2). We also propose a novel algorithm to process private image data. Our experimental results show that: Our algorithm achieves data privacy but only takes about 1/1,000 the time of the AES algorithm. The delay of our hybrid cloud approach (including the private and public cloud communications) is only 3% - 5% more compared to the traditional public-cloud-only approach.

• **Amanpreet kaur**, et.al, (March2013): In this paper there is a analysis of feasibility of attacks on cloud i.e "Extrusion" to detect and prevent attacks caused by unauthorized users. In this paper author discuss about the cloud computing. As, the computer networks are still in their infancy, but they grow up and become sophisticated. Cloud computing is emerging as a new paradigm of large scale distributed computing. In this paper, author discuss about the various scheduling problems. One of the challenging scheduling problems in Cloud datacenters is to take the allocation and migration of reconfigurable virtual machines into consideration as well as the integrated features of hosting physical machines.

• **Vishwa gupta**, et.al, (January 2012): In this paper author discuss about the enhancement of data security. Not only this makes researchers to make some modifications in the existing cloud structure, invent new model cloud computing and much more but also there are some extensible features of cloud computing that make him a super power.

• **Eman M.Mohamed, Sherif El-Etriby** (May 2012): discuss that today's world relies on cloud computing to store their public as well as some personal information which is needed by the user itself or some other persons .We present an evaluation for selected eight modern encryption techniques namely: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish at two independent platforms namely; desktop computer and Amazon EC2 Micro Instance cloud computing environment. The evaluation has performed for those encryption algorithms according to randomness testing by using NIST statistical testing in the cloud computing environment. This evaluation uses Pseudo Random Number Generator (PRNG) to determine the most suitable technique and analysis the performance of selected modern encryption techniques.

• **OP Verma , Ritu Agarwal** et.al, (2011): In this paper author discuss about the performance comparison between four of the most commonly used encryption algorithms: DES(Data Encryption Standard), 3DES(Triple DES), BLOWFISH and AES (Rijndael).The comparison has been conducted by running several setting to process different sizes of data blocks to evaluate the algorithms encryption and decryption speed. Based on the performance analysis of these algorithms under different hardware and software platform, it has been concluded that the Blowfish is the best performing algorithm among the algorithms under the security against unauthorized attack and the speed is taken into consideration.

• **Sk. Subidh Ali** et.al,(2011): In this paper, the review of existing security on cloud methods is given. In keeping-in mind, the current and future security trends, a new Extrusion based methodology has been proposed a DFA on AES-128 key schedule which requires only one single byte fault and a brute- force search of 28 keys, showing that a DFA on AES key schedule is equally dangerous as a fault analysis when the fault is injected in the intermediate state of AES. We proposed an improved differential fault attack on AES-128 key schedule.

• **Deguange Le, Jinyi Chang**, et.al, (2010): describes that the Cloud computing is emerging field because of its performance, high availability, least cost . we studied the technologies of GPU parallel computing and its optimized design for cryptography. Then, we proposed a new algorithm for AES parallel encryption, and designed and implemented a fast data encryption system based on GPU. The test proves that our approach can accelerate the speed of AES encryption significantly.

• **Chong Hee KIM** (2010): Discuss about the security in cloud computing. Cloud computing is fast growing area in computing research. Due to the longer key size and the characteristic of AES key schedule, we need subtle caution in attacking AES-192 and AES-256. We propose new DFA against AES with 192 and 256-bit key. We could retrieve AES-192 key with two pairs of correct and faulty ciphertexts. Normally the attacker can get faulty ciphertexts by giving an external impact on the device with voltage variation, glitch, laser, etc.

• **Laurie Genelle, Christophe Giraud** (2009): discuss that today's world relies on cloud computing to store their public as well as some personal information which is needed by the user itself or some other persons . Fault Attack (FA) is a powerful technique which enables to break unprotected cryptographic schemes very efficiently. In this paper author present a fault attack detection scheme for the AES using digest values. They are deduced from the mathematical description of each AES individual transformation. The security of our countermeasure is proved in a realistic Fault Model. Moreover we show that it can be combined with data masking to thwart efficiently both FA and DPA.

• **Md. Nazrul Islam**, et.al,(2008): Describes that the Cloud computing is emerging field because of its performance, high availability, least cost . The Advanced Encryption Standard (AES,) that uses 128 bit block size as well as 128 bits key size was introduced by NIST. In this paper, They showed the effect in security increment through AES methodology. To do this, we propose an algorithm which is higher secure than Rijndael algorithm (by comparing the key size) but less efficient than that.

C. CLOUD TYPES

Depending on infrastructure ownership, there are four deployment models of cloud computing [6].

1) Public Cloud: - Public cloud [4] allows users to access the cloud publicly. It is access by interfaces using internet browsers. Users pay only for that time duration in which they use the service, i.e., pay-per-use.

2) Private Cloud: - A private clouds [5] operation is with in an organization's internal enterprise data center. The main advantage here is that it is very easier to manage security in public cloud. Example of private cloud in our daily life is intranet.

3) Community Cloud:-When cloud infrastructure construct by many organizations jointly, such cloud model is called as a community cloud. The cloud infrastructure could be hosted by a third-party provider or within one of the organizations in the community.

4) Hybrid Cloud: - It is a combination of public cloud [7] and private cloud. It provide more secure way to control all data and applications. It allows the party to access information over the internet. It allows the organization to serve its needs in the private cloud and if some occasional need occurs it asks the public cloud for some computing resources.

D. SERVICE MODELS

There are different types of services are provides by cloud models like: Software as a Service(SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [6] which are deployed as public cloud, private cloud, community cloud and hybrid clouds.

1) Software as a Service (SaaS):- The capability provided to the consumer is to use the some applications which is running on a cloud infrastructure. The applications are accessible from many devices through an interface such as a web browser (e.g., web-based email). The consumer does not control the cloud infrastructure which includes network, and servers, all operating systems, and provides storages.

2) Platform as a Service (PaaS):- PaaS [5] provides all the resources that are required for implementation of applications and all services completely from the Internet. In this no downloading or installing is required of any software. The capability provided to the consumer is to deploy onto the cloud infrastructure .Consumer uses all the applications by using different programming languages and tools which are provide by the provider. Any consumer has not any control on cloud infrastructure including all networks, servers and operating systems, but has control over the applications which they deployed.

3) Infrastructure as a Service (IaaS):- The capability provided to the consumer is to access all the processing, storage , networks and other many fundamental computing resources . Consumer [5] [6] is able to deploy arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage ,deployed application ,and possibly limited control of select networking components.

RESEARCH MOTIVATION

It becomes necessary to find appropriate protection as the data may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. So in the recent world, security is a prime important issue. Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. Malicious activity monitoring is a tough task in cloud system as logging data might be spread over multiple hosts and data centres. Restricting user to his own virtual partition only will not allow logs to be dispersed allowing access to logs for monitoring easily. User access is another major concern in restricting user access is a major challenge in cloud based storage system. Use of virtual partition and enhanced user access control in cloud system will allow us to improve data security. Enhanced Cloud system will be compared with existing secure cloud systems. We will compare enhanced system against security, performance & ease of use.

we will attempt to secure data from unauthorized access, Method of data security is “Enhancement of AES ALGORITHM” with AES Algorithm for providing the secure data in cloud computing. .

- The AES is very large in size. Hence the complexity of the system is increased.
- AES Consumes more CPU time and power thus increasing the time.
- To reduce the System Complexity, We Enhance the AES ALGORITHM to reduce the Rounds of AES. It helps to make the cloud computer more efficient than the existing one.
- The Enhanced AES Algorithm is used to provide the security to the system and it also helps in the management of the information.

OBJECTIVES

- To enhance the security in cloud computing of AES Algorithm.
- To enhance the integrity of data. Hardware cost is decreased because lesser operations will be applied.
- To reduce the complexity in security modules.
- To provide prevention from active and passive attacks

METHODOLOGY

- We are going to use file based encryption through Enhanced AES algorithm in cloud computing.
- In the first step we will make a virtual cloud for saving the files and this virtual cloud is made with the help of development tool i.e. Cloud Sim.
- Inside the cloud DataCenter, we are having the Storage as a service (SAAS) for storing the files received from the client.
- The cloud server has number of files like a1.txt, a1.mp3, a1.mdf, a1.jpg.
- User has sent the request to server to send a file(KEY) for encryption.

- Server randomly choose any file from its inventory and send it to client.
- Client receives the file and generate the row no & column no, length randomly.
- Client fetches the corresponding data from the file.
- Client applies the Shift Row Operation of AES algorithm on the key data.
- Then again apply the XOR OPERATION on the key and the original data.

Data is encrypted which is send to the cloud server then same operation is performed for decrypted the data

CLOUD SIM

Cloud service providers charge users depending upon the space or service provided. In R&D [16], it is not always possible to have the actual cloud infrastructure for performing experiments. For any research scholar, academician or scientist, it is not feasible to hire cloud services every time and then execute their algorithms or implementations. For the purpose of research, development and testing, open source libraries are available, which give the feel of cloud services. Nowadays, in the research market, cloud simulators are widely used by research scholars and practitioners, without the need to pay any amount to a cloud service provider.

The following tasks can be performed with the help of cloud simulators:

• Modelling and simulation of large scale cloud computing data centres.

• Modelling and simulation of virtualised server hosts, with customisable policies for provisioning host resources to VMs.

• Modelling and simulation of energy-aware computational resources.

• Modelling and simulation of data centre [18] network topologies and message-passing applications.

• Modelling and simulation of federated clouds.

• Dynamic insertion of simulation elements, stopping and resuming simulation.

• User-defned policies for allocation of hosts to VMs, and policies for allotting host resources to VMs.

CONCLUSION

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks, as well as the destruction of infrastructure and services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. Cloud Computing is gaining popularity, but with the widespread usage of cloud the issue of cloud security is also surfacing. But to solve the existing issues becomes utmost urgency. To protect against the compromise of the compliance integrity and security of their applications and data, firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of thei r competitors. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. To advance cloud computing, the community must take proactive measures to ensure security.

REFERENCES

[1] Xueli Huang. “Efficiently Secure Data Privacy On Hybrid Cloud” IEEE ICC 2013-Communication and Information System Security Symposium.

[2] Vishwa gupta. “Advance Cryptography Algorithm for improving Data security”, International Journal Of Advanced Reserch in Computer Science and Software Engineering volume 2, Issue 1, January 2012 ISSN:2277 128X.www.ijarcsse.com

[3] Deguang Le. et.al, “Parallel AES Algorithm for fast Data Encryption on GPU” School of Computer Science & Engineering 978-1-4244-6349-7/10/$26.00 2010 IEEE.

[4] Eman M.Mohamed et.al, “Randomness Testing of Modern Encryption Techniques in Cloud Environment” 8th International Conference on INFOrmatics and system (INFOS2012)-14-16 may.

[5] OP Verma et.al, “Performance Analysis Of Data Encryption algorithm” Information Technology 978-1-4244-8679-3/11/$26.00 2011 IEEE.

[6] Amanpreet Kaur et.al, “Secure Broker Cloud Computing Paradigm Using AES And Selective AES Algorithm” International Journal Of Advanced Reserch in Computer Science and Software Engineering volume 3, Issue 3, March 2013 ISSN:2277 128X.www.ijarcsse.com.

[7] Chong Hee KIM " Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults" Information Security Group , Universite Catholique de Louvain , 978-0-7695-4169-3/10/$26.00 2010 IEEE. DOI 10.1109/FDTC.2010.10.

[8] Sk.Subidh Ali , et.al, " Differential Fault Analysis on AES Key Schedule using Single Fault" Dept. of Computer Science and Engineering, 978-0-7695-4526-4/11/$26.00 2011 IEEE. DOI 10.1109/FDTC.2011.10.

[9] Md. Nazrul Islam, et.al, "Effect Of Security Increment To Symmetric Data Encryption Through AES Methodology" Dept. of Computer Science and Engineering, 978-0-7695-3263-9/08/$25.00 2008 IEEE. DOI 10.1109/SNP.2008.101.