Available Online at http://www.recentscientific.com

ISSN: 0976-3031

International Journal of Recent Scientific Research
Vol. 5, Issue, 1, pp.128-132, January, 2014

International Journal of Recent Scientific Research

RESEARCH ARTICLE

ENHANCING SECURITY IN CLOUD COMPUTING STRUCTURE BY HYBRID ENCRYPTION

Aparjita Sidhu* **and Rajiv Mahajan**

Department of Computer Science GIMET, Amritsar, India

ARTICLE INFO

Article History:

Received 16th, December, 2013
Received in revised form 26th, December, 2013
Accepted 15th, January, 2014
Published online 28th, January, 2014

Key words:

Message Digest, Advanced Encryption Standard, Distributed environment, cloud computing, data security

ABSTRACT

Modern communication is containing different types of networks depending on the behavior of users. Cloud network and services are one of the mostly used networks. Security in the cloud service architecture is always a big concern for the vendor as well as users. In this paper distributed cloud service architecture is considered which is used as network detection system for outer attacks to the cloud architecture. Outer attacks can be prevented by security services such as McAfee, Imperva etc. but insider attacks are very difficult to detect and to avoid them, different resources consuming processes are considered. So to provide solution for security without spending many resources, encryption of messages is a good option. Hash function encryption is easy and light encryption process which will challenge the odds and can be suitable for cloud computing structures.

INTRODUCTION

At the present world of networking system Cloud computing is one the most important and developing concept for both the developers and the users. Therefore in recent days providing security in cloud has become a major challenging issue in cloud computing. Cloud computing is primarily based on virtualization which enables multi tenancy and on-demand use of scalable shared resources by all tenants [3][4]. Cloud computing provides the facility to access shared resources and common infrastructure which offers the services on demand over the network to perform operations that meet changing business needs. The location of physical resources and the devices which are being accessed are not known to the end user. It also provides facilities for users to develop deploy and manage their applications on the cloud which entails virtualization of resources that maintains and manages itself. Overlay networks have also received much attention in recent years. Overlay networks were first used in the deployment of the Internet over telephone networks [1]. By definition, they are virtual networks built on top of physical networks. They consist of virtual nodes connected via virtual links and aim to offer additional functionalities which are not available in the underlying physical network [2].Because overlay networks are also based on virtualized nodes for implementing network services both techniques are combined to reap the benefits of each. This is particularly useful for deploying new transparent network security services over existing networks to enhance their protection [5].

In the area of cloud computing different security models and algorithms are applied at present. But these models have failed to solve most of the security threats. Moreover for E-commerce and different types of online businesses high capacity security models are implied in cloud computing fields. Security models that are developed and currently used in the cloud computing environments are mainly used for providing security for a file and not for the communication system. Moreover present security models are sometimes uses secured channel for communication. But this is not cost effective process. Some models attempt on discussing about all of these but are completely dependent on user approach. The models usually fail to use machine intelligence for generating key and newer proposed model. Some models have proposed about hardware encryption system for secured communication system. The idea is usually straightforward but the implementation is relatively difficult. Hardware encryption is helpful only for the database system not for other security issues. Authenticated user detection technique is currently very important for ensuring security in cloud computing. A network-based IDS (NIDS) passively monitors traffic traversing a given network for malicious payloads. NIDS sensors sniff and capture this traffic. The NIDS analyzes the collected data to detect malicious activities and responds to or generates reports based on the detection. It also examines the content of the network and the transport layer packet headers and analyzes the packet sequence as well as how these packets will affect applications at the customer endpoints. Security is broadly categorized as two types protecting the asset and protecting the data. In this research encryption process is performed for cloud architecture and machines act as network intrusion detction system and send encrypted messages to servers in the network.

Various algorithms have been used to provide message security. It is good practice to encrypt the actual message to be transmitted using a Symmetric key algorithm with better computational speed for cloud environment. Firstly Advanced Encrption Standard is used in which keys are generated randomly by the system. AES is a block cipher with a block length of 128 bits and also allows for three different key lengths 128, 192 or 256 bits. AES has different rounds which are performed for each block. Except for the last round in each case all other rounds are identical. In the processing steps used in single round 128-bit block is divided into 4 by 4 matrixes of bytes. The 4 by 4 matrix of bytes is referred to as the state array. The steps performed for each block are same for encryption and decryption but the order in which they are performed is different. Secondly message digest hash function is

* Corresponding author: **Aparjita Sidhu**
Department of Computer Science GIMET, Amritsar, India

used which is a cryptographic hash function with a 128-bit hash value.This hash function is expressed as a 32-digit hexadecimal number. This algorithm outputs a particular length string which can be used in password handling. for example the message content is hello how are you. Now each word is calculated and its digest is produced. Lets its digest is 89 so 89 is send during the communication. Message digest operates with following steps:

- Append Padding Bits
- Append Length
- Initialize MD buffer
- Process message in 16-word blocks
- Output

The main purpose of message digest hashing algorithm is that this method is a one way system and unbreakable. Therefore it will be difficult for an unauthorized or unknown party to retrieve the password for a selected user even if gained access to the system.

Related Concepts about Cloud

Deployment Cloud Models

- ❖ Public cloud: This type of cloud infrastructure is available to the general public or a large industry group with an internet connection.
- ❖ Private cloud: A private cloud is established for a specific group or organization and limits access to just that group.
- ❖ Community cloud: This type of cloud infrastructure is shared among two or more organizations that have similar cloud requirements like security requirements, policy, and compliance considerations.
- ❖ Hybrid cloud: This cloud infrastructure is a combination of at least two clouds where the clouds included are a mixture of public, private, or community

Service Models

Cloud computing can be classified based on the services it offers.

- ➢ Infrastructure as a service: In infrastructure as service storage, computation and network resources are the major components that are provided as a service to the customer. Customers run their choice of operating system and other software on the infrastructure provided by the cloud provider.
- ➢ Platform as s service: In Platform as a service model the cloud provider provides a platform for developing and running the web based applications. This platform provides all the facilities to support the complete life cycle of building and delivering the applications to end users.
- ➢ Software as a service: Software as a Service is the model in which an application is hosted as a service to customers who access it through the internet. When the software is hosted off-site the customer does not have to maintain it or support it.

Cloud Characteristics

- On demand service: Cloud is a large resource and service pool from where the service or resource can be utilized whenever needed by paying the amount for the service being used.
- Ubiquitous network access: Cloud provides services everywhere through standard terminal like mobile phones, laptops and personal digital assistants.
- Easy use: The most cloud providers' offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services.
- Business model: Cloud is a business model because it is pay per use of service or resource.
- Location independent resource pooling: The providers computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand

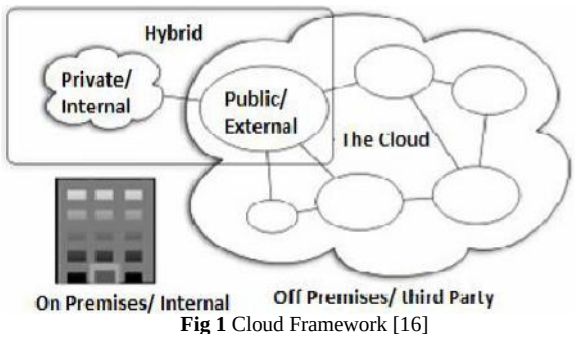

Fig 1 Cloud Framework [16]

Related Work

Cloud computing offers on-demand use of third party IT infrastructures on a pay-per-use basis. Khaled Salah in 2008 discussed that cloud computing reduces customers need for hardware while improving the elasticity of computational resources allowing them to adapt to business requirements. Therefore businesses are finding it attractive to adopt the cloud computing paradigm. Hassan Takabi explains that Cloud computing is an evolving paradigm with tremendous momentum but its unique aspects exacerbate security and privacy challenges. This explores the roadblocks and solutions to providing a trustworthy cloud computing environment. Jianyong Chen proposed an architecture that differentiates security according to service-specific characteristics avoids an unnecessary drain on IT resources by protecting a variety of cloud computing services.
Lori M. Kaufman explained that Software as a service (SaaS) is a well-established cost-effective means to deliver traditional software applications without investing in infrastructure and qualified personnel. A natural extension of cloud services is to extend platform independence via virtualization to a security model. This paradigm allows for the distributed provisioning of common security services. This model and its application demonstrate the viability of security as a service for cloud computing. Security as a service can enable cloud customers to implement and maintain the protection they need in an efficient, cost-effective manner that can be tailored to meet their risk profile.

Volker Fusenig proposed that the cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance. Kawser Wazed Nafi proposed new security architecture for cloud computing platform. This ensures the secure communication system and hiding information from others. AES based file encryption system and the asynchronous key system for exchanging information or data is included here. This structure can be easily applied with main cloud computing features like PaaS, SaaS and IaaS. Maha Tebaa proposed an application of a method to execute operations on encrypted data without

decrypting them which will provide same results after calculations as if work is directly done on the raw data. Homomorphic encryption is a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out with respect of the data confidentiality. Abhishek Patial briefly discussed that data security is becoming a core problem in cloud computing and to secure data from unauthorized access the Method of data security is RSA algorithm for providing data security by encrypting the given data based on the KEY combinations. And this data then can only be decrypted by authorized person by using his private key.

Proposed Work

At present ensuring security in cloud computing platform has become one of the most significant concerns. These problems have been considered to provide some solution correlated with security. The Cloud computing environment discussed earlier implements the security layers having IDS, IPS, AV, Anti-spam with firewall to provide protection to all endpoints connected to it. But they do not provide protection to the messages that transfer between the VM sensor, SEM and CSM in cloud structure while communicating to each other. The messages which are to be transferred are in the format of IDMEF called Intrusion Detection Message Exchange Format (IDMEF) which are very much the backbone for integrity of the network communication and synchronization process. This information is stored on and retrieved from a security event manager (SEM). CSM is a cloud-management unit which gathers information from other sensors and processes it from a global perspective. In this research the message digest hash function is considered for encryption purposes.

To achieve this secure communication is provided for transfer of Intrusion Detection Message Exchange (IDME) by encrypting the messages by Message Digest Hash function. A log file has been taken for demonstration of the proposed work. A log file is a record of cookies. Information from log file has been processed under encryption and decryption. NIDS sensor encrypts the message with symmetric digest function and sends data to Central Security Manger. CSM can encrypt or decrypt data with symmetric hash function. Same process of encrypting and decrypting has been taken place between central security manager and security event manger. This work provides the guarantee of secure communication between all nodes present in the network. Proposed solution has been implemented with five personal computers connected to each other in a distributed environment and running on same network. Due to the distributed environment the data is made available in all the PCs simultaneously. All the PCs are in real time synchronization with each other. The proposed work is shown in figure 1. Development of message digest algorithm has been done in Java language.

AES and MD5 is the Hybrid approach that is proposed here with the idea of the whitened Text. The Proposed algorithm starts with having a plain text file and converting the content of the plain text file to the Whitened text. This plain text file contains the message that needs to be encrypted. The whitened text conversion takes place by converting the message to the Hex Decimal form and then performing XOR with the Key that will be used for the encryption.
For Example: Message is: Hello world, here is some sample text.

Whitened Text:-
>[xU^U]GYB_U¬YSEW_@E_UUATZBY\B\MG

The Second step of the proposed algorithm comes with the AES (Advance Encryption Standard) Algorithm. The basic difference between the AES and the proposed one is that the numbers of the rounds are limited to 5 which are basically 10, 12 and 14 for 128,192 and 256 bit blocks. Along with this the encryption of the AES is provided not with only one key but with two keys so that if breaching takes place in between then one is able to know one of the key the block encrypted with and the other keys are saved.

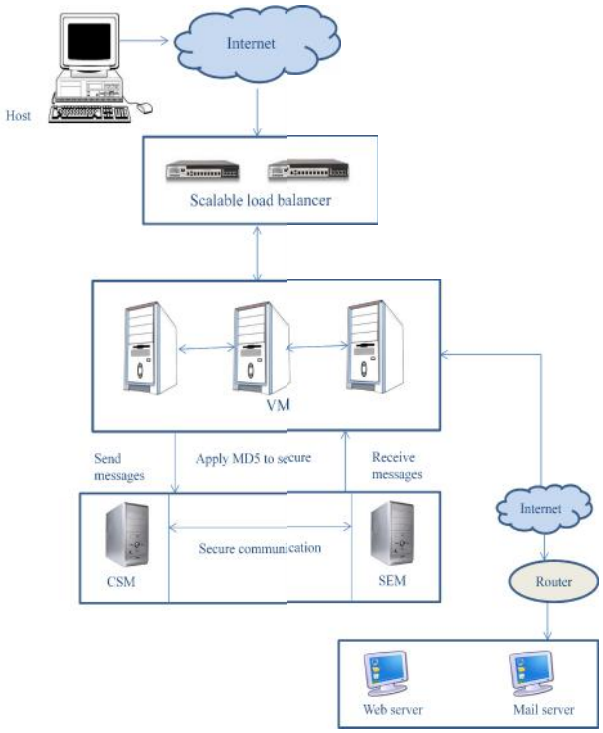

Fig 2 proposed cloud computing environment

The algorithm starts with giving its whitened text as the input to the AES .Now this algorithm again encrypt the encrypted text. The numbers of steps that are processed on each block are basically:

1. Convert to State Array
2. Transformations (and their inverses)
   - ❖ Add Rounds Keys: each byte of the state is combined with the round key using bitwise xor.
   - ❖ Substitute Byte: a non-linear substitution step where each byte is replaced with another according to a lookup table.
   - ❖ Shift Row: transposition step where each row of the state is shifted cyclically a certain number of steps.
   - ❖ Mix Column: a mixing operation which operates on the columns of the state combining the four bytes in each column.

Key Expansion

The transformation is performed at each round on each block of the data. The given input is firstly divided into the block of the fixed size values and then keys are applied to this.
Example now Input is:
[xU^U]GYB_U¬YSEW_@E_UUATZBY\B\MG
AES encryption is: [È´t¤mÍw,N/m#¾ñÀšÿ"çíƒ Ü ˆÆØc;

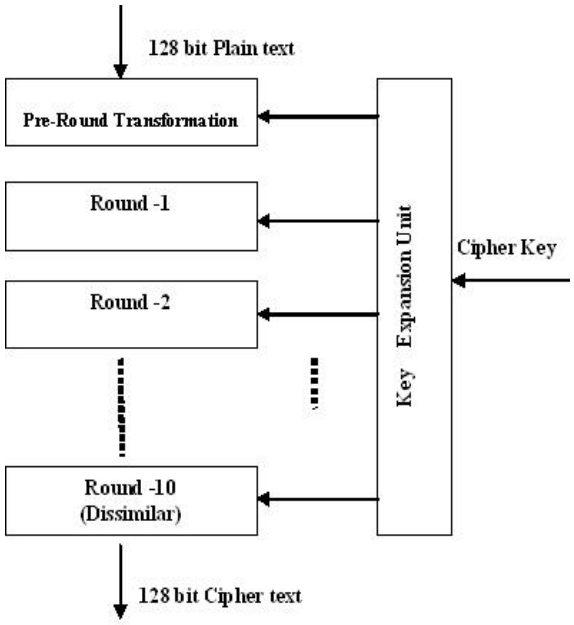

Fig 3 AES algorithm [7]

Now the final step of the algorithm will take place. The AES encrypted text is given as the input to the RC4.The algorithm process the data in the form of the stream. RC4 generates a pseudorandom stream of bits as with any stream cipher. These can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way prepared stream. To generate the key stream the cipher makes use of a secret internal state which consists of two parts:

1. A permutation of all 256 possible bytes (denoted "S").
2. Two 8-bit index-pointers (denoted "i" and "j").

The permutation is initialized with a variable length key typically between 40 and 256 bits.

Experimentation

For experimentation following steps are followed:

- We developed a cloud computing environment by using 5 machines with minimum dual core processor and 2 gigabytes of random access memory.
- These machines are connected to each other and are loosely coupled to each other for synchronization process.
- MacAfee security solutions are used for prevention of attacks on every machine.
- Development is done in JAVA language with IDE Eclipse or Net beans.
- In this we have used MD5 encryption mechanism for secure communication. With this we have used AES-Advanced Encryption Standard.
- Along with this hybrid approach of MD5 and AES we used RC4 algorithm.
- Encrypted messages are sent from one machine to other and are further decrypted by concerned machine with appropriate rights.
- Each machine is having encrypted data and can be decrypted according to need and with proper decryption process.
- Developed interface for encryption and decryption process is installed on every machine for demonstration.
- Finally encrypted data is sent to central server (CSM).

Basic parameters used for experimentation in Java platform. Some of the experimentation done for checking the behaviour of Cloud architecture under encryption hashing functions is given below:

Table 1 Parameters used for experimentation

Parameters	Value
Simulation	JAVA
Simulation tool	Net beans
No of machines	4
Communication	Wireless Communication through IP addresses
Traffic Model	FTP (Web log)
Architecture	Client Server (loosely synchronized)
Speed	100 mps

RESULTS

Our work has yielded results that ful fill the objectives. We were able to provide better security to the messages that were exchanged between different connecting nodes. We were able to establish an encryption based system for protecting our messages by encrypting them while they were transferred to other machine and decrypt them while receiving on other virtual machine. We have created an application where different algorithms have been used for the encryption and decryption process.

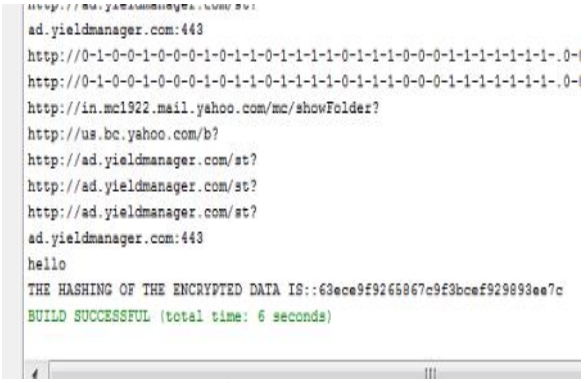

Figure 4 Hashing functionality in the proposed work

Results obtained for cloud architecture equipped with hashing algorithm is been implemented in Java language in well known IDE Net Beans. Loosely synchronized client server architecture has been implemented as discussed in related study in which network intrusion detection clients will send the web log information to servers. Same methodology has been implemented in the current research. Messages in the previous study are moving in plain text without any encryption or hashing which could give rise to insider attacks.

Figure 5 Server configuration after receiving hashed data message

To save message from been attacked a well known hashing algorithm Message Digest level 5 is used for hashing along with advanced encryption standard for the web log messages. The performance of network is judged on the basis of variation of web log queries with respect to CPU utilization. Hash function shown in figure 5 shows successful hashed functioned data messages. Below is the server configuration received from clients in encrypted form. The graph shown compares all the ciphers based on their throughput. Again RC4 tops as it do encryption of maximum data in minimum time. The hybrid approach is better than all other ciphers.

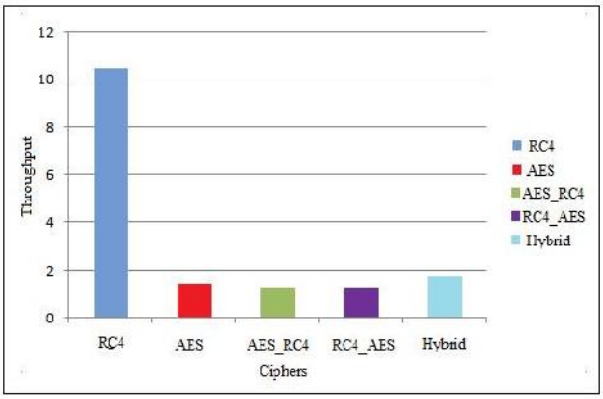

Figure 6 comparison of all ciphers

CONCLUSION AND FUTURE WORK

In this work the security of the cloud architecture was the focused part. To provide better security in cloud architecture encryption in form of hashing function is provided to the messages which are been transferred from various client machine to server machines in the cloud infrastructure. The useful concept of hashing has been done for preventing the inside attacks in cloud service architecture. In future it is very interesting to test various other encryption techniques such as Rivest cipher, DES etc for better security concerns for cloud architecture. Further we can also compare security features under various attacks in cloud services.

References

1. Khaled Salah, Jose M. Alcaraz, Sherali Zeadally, Sameera Al-Mulla and Mohammed Alzaabi, "Using Cloud Computing to Implement a Security Overlay Network", security & privacy IEEE, vol. 11, Issue: 1, pages: 44 – 53, Jan.-Feb. 2013.
2. Hassan Takabi and James B.D. Joshi -University of Pittsburgh and Gail-Joon Ahn -Arizona State University," Security and Privacy Challenges in Cloud Computing Environments", Security & Privacy, IEEE,Vol 8, Issue:6 Pages: 24 - 31 ,2012.
3. Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker Siemens," Understanding Cloud Computing Vulnerabilities", Security & Privacy, IEEE, Vol : 9 , Issue: 2, Pages: 50 – 57, March-April 2011.
4. Jianyong Chen, Yang Wang, and Xiaomin Wang, "On-Demand Security Architecture for Cloud Computing", Computer IEEE, Shenzhen University, China, vol.45 , Issue: 7, Pages: 73 – 78, july 2012.
5. Lori M. Kaufman, Bruce Potter, BAE Systems, "Can a Trusted Environment Provide Security?", Security & Privacy, IEEE, Vol : 8 , Issue: 1,Pages: 50 – 52, Jan.-Feb. 2010.
6. Volker Fusenig and Ayush Sharma, "Security Architecture for Cloud Networking", Computing, Networking and Communications (ICNC), 2012 International Conference on, Pages: 45 – 49, Jan. 30 2012-Feb. 2 2012.
7. M.Sudha, M.Monica,"Enhanced Security Framework to ensure data security in cloud computing using Cryptography", Advances in computer science and its applications, March 2012.
8. Hamdi, M., "Security of Cloud Computing, Storage, and Networking", Collaboration Technologies and Systems (CTS), 2012 International Conference IEEE Pages 1-5, 21-25May2012.
9. Uma Somani, Kanika Lakhani and Manish Mundra,"Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing", Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on, Pages: 211 – 216, 28-30 Oct. 2010.
10. Lakshmi Subramanian, "Security as a Service in Cloud for Smartphones", MS dissertation, Fraunhfer Institute for Secure Information Technology, Munich, Germany, 28th June 2011.
11. Tata Communication, "Moving from Legacy Systems to Cloud Computing", A Tata Communications White Paper, October 2010.
12. Michael Miller, "Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online", 800 East 96th Street, pp. 66-69, Vol.9, Issue. 3, May 2010.
13. Kawser Wazed Nafi, Tonny Shekha kar, Sayed Anisul Hoque, Dr. M.M.A. Hashem, "A Newer User Authentication, File Encryption and Distributed Server Based Cloud Computing Security Architecture", International Journal of Advanced Computer Science and Applications(IJACSA), 2012.
14. Abhishek Patial, Sunny Behal, "RSA Algorithm achievement with Federal information processing Signature for Data protection in Cloud Computing" International Journal of Computers and Technology, 2012.
15. Lewis, Grace. Cloud Computing: Finding the Silver Lining, Not the Silver Bullet.
16. Anurag Porwal, Rohit Maheshwari, B.L. Pal, Gaurav Kakhani, "An Approach for Secure Data Transmission in Private Cloud",International Journal of Soft Computing and Engineering (IJSCE), March 2012.

****