IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Efficient Cloud Security Method for Preventing Insider Attacks in Cloud Computing Platforms

Bhushan Rathod[1], Prashant Yelmar[2]

Research Scholar, Department of Information Technology, MIT-COE, Pune, India[1]

Professor, Department of Information Technology, MIT-COE, Pune, India[2]

Abstract: Different types of organizations based on requirements commonly and widely used cloud-computing frameworks. Many companies are sharing very important data on daily basis over the different cloud server. Hence it is required to have efficient data confidentiality and security method to protect against different security threats like insider attacks. The recent works proposed on cloud computing security has mainly worked either on cloud computing platform protection from malicious users or cloud client's protection from each other's unwanted activities. However, the issues of cloud client's protection from the other malicious cloud client's attacks (this attack is called insider attacks are still remaining research problem. In this project, a novel approach is presenting in order to ensure the client data confidentiality and integrity during computation over the cloud platform. The goal of proposed approach is to ensure that cloud user private data not be exposed to other internal cloud users like other cloud clients and administrator. The proposed designed method makes use of remote attestation and late launch based method called Flicker in order to verify the integrity of the cloud platform. This is a practical approach designing for securing the confidentiality and integrity of client data and computation from cloud clients and from the Infrastructure-as-a-Service (IaaS) based cloud system administrator himself. For data security, we are using newly designed hybrid cryptography method to deliver the best efficiency performance.

Keywords: Cloud Computing, Cloud Security, Security threats, Risk analysis, Data Protection, Privacy.

I. INTRODUCTION

With recent technical advancement in data storage and access, Cloud computing is getting more popularity day by day in a computing environment. Cloud computing is helping small and medium scaled businesses to move their data and application to the cloud for easy access, with benefits ranging from pools of computing resources such as the network to storage, and infrastructure with a pay-per-use facility.

Three basic types of Cloud Computing service models are:

1. Software as a Service (SaaS): SaaS provides a capability to use to run the application on a cloud without dealing with an underlying structure like operating system, platform, network, servers famous SaaS services are Google Apps, Microsoft Office 365.
2. Platform as a Service (PaaS): PaaS model enables a user to decrease cost and complexity of purchasing and maintaining software and hardware components. Users can directly deploy their application on cloud. Some of the famous PaaS services are Force.com, Google App Engine.
3. Infrastructure as a Service (IaaS): The efficiency provided to the consumer is processing of data, storage of data, networks, and other basic computing resources where the consumer is able to deploy and run the software. Services like Amazon EC2, Windows Azure are some widely used IaaS services.

There are different categories of threat actors, with each of them represents a significant threat to an organization:

1. Compromised actors: Insiders with access credentials or computing devices that has been compromised by an outside threat actor.
2. Negligent actors: Insiders who expose data accidentally such as an employee who accesses company data through public WiFi without the knowledge that it is unsecured. A large number of data breach incidents result from employee negligence towards security measures, policies, and practices.
3. Malicious insiders: Insiders who steal data or destroy company networks intentionally such as a former employee.
4. Tech savvy actors: Person having in-depth knowledge of network and who knows the backdoor and loophole in the system.

II. RELATED WORK

In paper [1] author is mainly focusing on malicious insider attack in a cloud environment. According to an author, in

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

most of the previous work only considered the perspective of MI (malicious Insider) attack from tenant side in public cloud.

Malicious Attacks by Cloud Vendor.

1. Memory Dumping
2. Template Poisoning
3. Snapshot Cracking

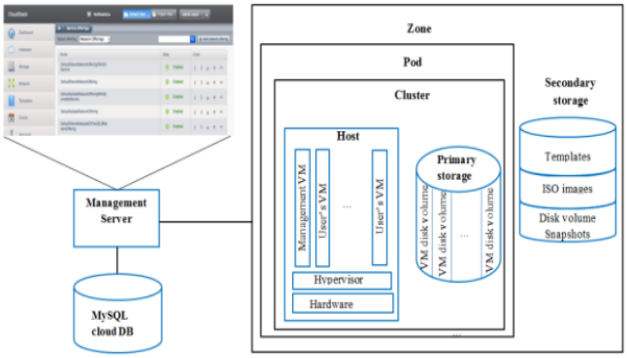


Figure 1 Cloud Environment Architecture. [1]

In paper [2] author has provided a comprehensive study of cloud computing security and privacy concerns. Author has identified cloud vulnerabilities, classify known security threats and attacks, and present the practices to control the vulnerabilities, neutralize the threats, and calibrate the attacks. Additionally, Author has investigated and identified the limitations of the current solutions and provides different security perspectives. Along with it, an author has provided a cloud security framework in which he presents the various lines of defense and identifies the dependency levels among them.

Network category related issues are biggest security challenges in clouds since cloud computing is more prone to network related attacks compared to the traditional computing paradigms. In addition, cloud operations are tightly coupled and highly dependent upon networking. Therefore, cloud network security issues receive more attention compared to the other security categories.

Author [2] has gone through problem background with following points:

1. Trusted Computing.
2. Remote Attestation.
3. Virtualization.
4. Late Launch.
5. Sealed Storage.
6. Flicker.
7. Protocol Verification.

In this paper [3] author has discussed several types of attacks on a cloud. All the attacks are focused on a particular layer of cloud architecture. Cloud computing architecture composed of three layers Infrastructure as a service (IaaS), platform as a service (PaaS) and Application as a service (AaaS). If IaaS is vulnerable, then all above layers can't be secure. The principal concern of security in IaaS is Virtualization. There are several attacks on virtualization in IaaS layer like an attack on VM image sharing. VM isolation violation, insecure VM migration, and VM escape. In this paper, all such attacks are studied and the solutions were discussed.

Author has described the six security issues customer should aware of while giving data to cloud provider:

1. Privileged User Access.
2. Regulatory Compliance.
3. Data Location.
4. Data Segregation.
5. Recovery.
6. Investigative Support.

This paper [4] represents an investigative survey of sequence mining algorithms that was utilized for detecting Insider attack. The sequence mining algorithms was classified into mainly four ways, viz, apriority-inspired algorithm, pattern matching and pattern growth, pruning and last but not lease the combination any of these. In this survey, author [4] has checked each category of these to find suitability of algorithms for detection of the Insider attack, which can be

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

detected with help of abnormal patterns in daily routines of the cloud uses. As per current status of the state of art in this area, we have found that combination of pattern growth with freshness factors are best suited for identification of insider attack in the cloud.

This paper [5] presents an Insider Threat Detection Model that was used to detect suspicious insider activities. Insider threats are some of the growing security concerns that are hindering the adoption of the cloud. Cloud providers are faced with a challenge of monitoring usage patterns of users to ensure that malicious insiders do not compromise the security of customer data and applications. Solutions are still in need to ensure that the data stored in the cloud is secure from malicious insiders of the cloud service provider. An experimental system was designed to implement this model. This system uses sequential rule mining to detect malicious users by comparing incoming events against user profiles.

III.PROPOSED SYSTEM

1. Problem Definition.

As we know, cloud technology is becoming promising and growth paradigm, which provides end users to outsource the computational and storage resources as per the demands. Based on a recent survey among different IT companies, it is noted that 75 % IT companies are using the cloud computing based services. As public clouds are becoming the origin of novel and rice range of IT solutions starting from massive online collaborative content storage to healthcare functionality management systems, companies are using the cloud based IT solutions. However, increasing use of cloud computing services is badly suffering from the problem of data confidentiality and security while data sharing, storage, and monitoring process from the different attacks especially from insider attacks. Therefore, it is necessary to have a mechanism for data security and confidentiality in cloud computing systems. There are a number of security methods designed based on cryptography algorithms since from last decade, but suffering from the scalability, efficiency and robustness problems. Very recently, the novel approach introduced to ensure the confidentiality and integrity of client data and computation on the cloud platform efficiently. Infrastructure as a Service (IaaS) based cloud model designed in this method. The problem with this approach is that it depends on basic cryptography method AES (Advance Encryption Standard) which may be lead to scalability issues.

2. System Architecture.

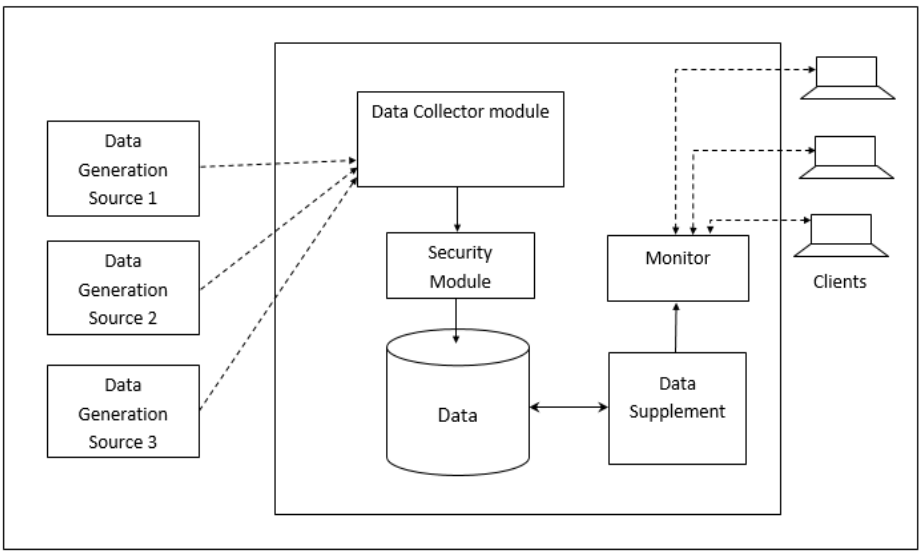


Figure 2. System Architecture

System Architecture consists of three phases:

2.1. Data Generation Module.

Data Generation Module used to collect the raw data from various resources segregated in a different cluster, activity, Keyword Configured. Data generation module will have three sub modules as follows:

A. Domain Selection, Cluster, Activity, Keyword Configuration

The system will have a feature for selecting a domain of choice to generate leads in. for ex: Education, Business. The system will have a feature for selecting a cluster of choice to generate data in. Keywords for a particular domain will be set.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

B. Manual Data Upload

This system provides uploading conventional data files. Conventional data can be added to the system using different files.

C. Generating data from the Internet.

Websites and Forums in a particular domain will be home to many comments from the public. These comments will be analyzed through NLP and only desirable data from users will be acquired. These would be potential information for business.

Procedure for generating data from the internet:

1. Selecting the Cluster. (For which domain result should be generated.)
2. Selecting the Activity. (For which activity the result should be filtered.)
3. Selecting the Sub-cluster.
4. Displaying the preconfigure keywords according to selected cluster.
5. Selecting the forum for generating data according to keywords.
6. Storing the filtered generated data into a database for a particular cluster.

HTML/XML parser is used to parse HTML pages from the internet. A parser constructor takes an XML or HTML document in the form of a string. It parses the document and creates a corresponding data structure in memory. After creating a parse tree by parsing HTML document, we can filter the data according to keywords to find out possible results out of completely raw data.

2.2. Data Management Module.

Data Management module is used to handle and manage all the information generated from the internet or uploaded manually. Data Management module will also help to generate data pattern. These data patterns will be given to forecasting model for prediction analysis.

2.3. Security Module.

Security module applied to the whole system to protect data from different attacks specially intended from inside of the system like a cloud provider, authorized system administrator.

Algorithm: Digital Watermarking based Algorithm [2]

Notation:

I: Data to be watermarked; $\bar{I}$: Watermarked Data;
K: Session key; A: Watermarking algorithm;
P_{kl} : Private key of person P1;
p_{kl}: Public key of peron P1;
P_{kp}; Private Key of P cloud application.
p_{kp}: Public Key of P cloud application.

Pseudo code:

M ← (Data) //Generate Watermark
$\bar{I}$ ← encode (I, K, M) //Embed a watermark
$\bar{\imath}$ ← P_{kl} (hash ($\bar{I}$)) //For non-repudiation and integrity check.
Sec ← p_{kp} (K) // Encrypt K with P public key
Person $\xrightarrow{\bar{I},sec,\bar{\imath}}$ Cloud Application

P Cloud application:

P verifies signature and applies integrity check using$\bar{I}$, $\bar{\imath}$, p_{kl}
Flicker ($\bar{I}$, sec) // P initiated flicker session
K ← P_{kp} (sec) //Gets session key K to decode $\bar{I}$
M ← decode ($\bar{I}$, K) //Gets embedded watermark M
Get Data //Original Data

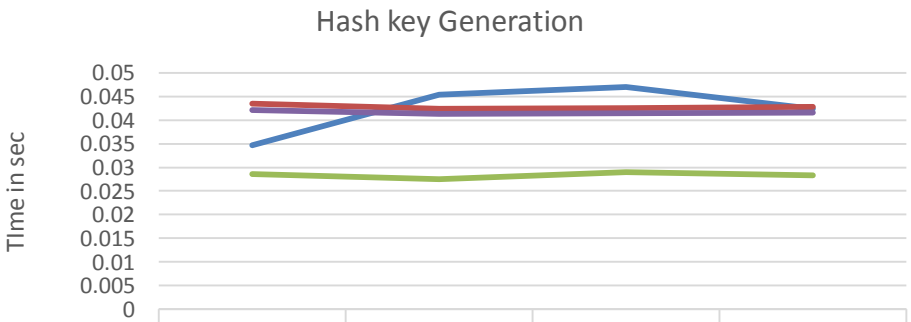
IV. RESULT AND ANALYSIS

The Proposed system has successfully generated data from different resources. The system has also successfully gathered the data, which was uploaded manually by a user. The data has generated without applying any security parameters to it. The generated data can be easily monitored with Data management module.

IJARCCE

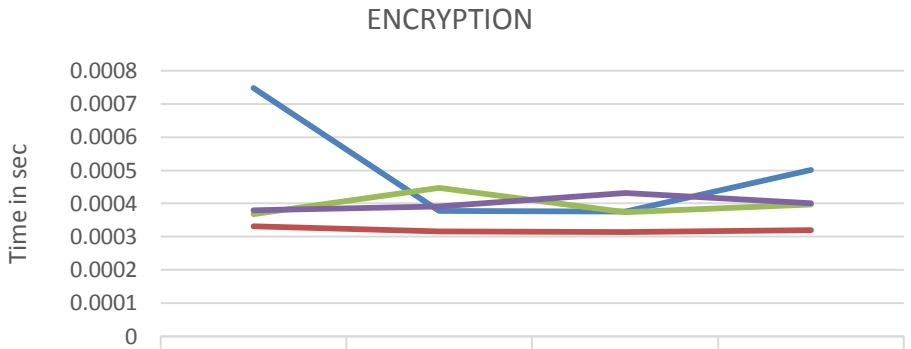
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017



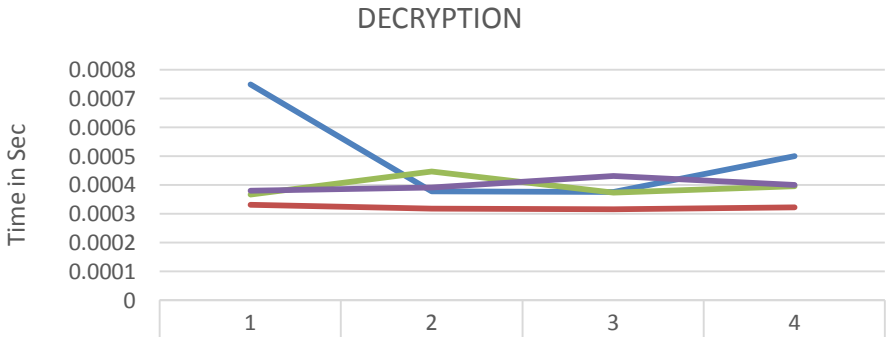
	1	2	3	4
MD5	0.034685148	0.045432661	0.047026915	0.042381575
SHA1	0.043495021	0.042432526	0.042565467	0.042831005
SHA256	0.028669377	0.027515519	0.029064091	0.028416329
SHA512	0.042155867	0.041337696	0.041485008	0.041659523

Graph 1. Hash Key Generation. Iteration=10000, length=32



	1	2	3	4
MD5	0.000747852	0.000376749	0.000375209	0.000499937
SHA1	0.00033068	0.000317015	0.000314822	0.000320839
SHA256	0.000368023	0.000446236	0.000373669	0.000395976
SHA512	0.000379316	0.000390094	0.000432148	0.000400519

Graph 2. Encryption Timing



	1	2	3	4
MD5	0.000747852	0.000376749	0.000375209	0.000499937
SHA1	0.00033068	0.000317015	0.000314822	0.000320839
SHA256	0.000368023	0.000446236	0.000373669	0.000395976
SHA512	0.000379316	0.000390094	0.000432148	0.000400519

Graph 3. Decryption Timing.

DOI10.17148/IJARCCE.2017.66101

The Proposed system is designed using different hashing technics with AES encryption to check the best suitability according to end application. The end system designed by us was used to store corporate data, which had moderate security level. The proposed system can modified to handle more secure data according to end system. The following graphs are derived by comparing the system developed with secure hashing algorithm for hashing with AES for encryption.

V. CONCLUSION

With above graphs, we can see that depend upon iteration cycle, the hash key generation varies in time. Even though SHA256 takes less time to create hash digest, but encryption and decryption time is comparatively more than SHA1. Hence choosing a best combination is totally depends upon the type of data that we will be storing, along with the sensitivity of data. In last, Cloud computing is an emerging paradigm that involves all the basic components of computing such as end-user machines (PCs), communication networks, access management systems and cloud infrastructures. To achieve comprehensive cloud security, Data and cloud infrastructure must be protected against known/unknown attacks across all cloud components. In proposed work, a system has successfully collected data from different resources.The proposed system will have support for endeavors to provide preventive measures as well as proactive tools in defending the clouds from different threats. This project will contribute providing security to the data stored in the cloud, by encrypting the data before uploading into the cloud. As encryption consumes more processing overhead, many cloud service providers will have basic encryption applied only on few data fields. To keep the cost low and maintain high sensitive data, it would be better to encrypt the data before uploading.

ACKNOWLEDGMENT

I, **Bhushan Rathod** would like to thank **Prof. Prashant Yelmar** for his valuable advice and immense support. Also, my sincere gratitude towards Creocis Technology Pvt. Ltd. for providing all required resources and valuable advice. I would like to thank **Prof. Bharati Dixit** and other staff from MITCOE, Pune for their guidance and support.

REFERENCES

[1] Minh-Duong Nguyen, Ngoc-Tu Chau, Seungwook Jung, and Souhwan Jung ,“A Demonstration of Malicious Insider Attacks inside”, IJIET, Vol. 4, No. 6, December 2014.
[2] Imran Khan, Zahid Anwar, Behzad Bordbar, Eike Ritter, and Habib-ur Rehman ,“A Protocol for Preventing Insider Attacks in Untrusted Infrastructure-as-a-Service Clouds”, IEEE TRANSACTIONS ON CLOUD COMPUTING-10.1109/TCC.2016.2560161, 2016
[3] Geetanjali Nenvani, Huma Gupta, “A Survey on Attack Detection on Cloud using Supervised Learning Techniques”, Symposium on Colossal Data Analysis and Networking (CDAN),IEEE-2016.
[4] Er. Paramjit Singh, Er. Jasmeet Singh Gurm,“Utility Survey of Sequence Mining for Insider Attack”, International Journal of Computer and IT, Vol. 4, , April-2016.
[5] Lucky Nkosi, Paul Tarwireyi and Matthew O Adigun,“Insider Threat Detection Model for the Cloud”,National Research Foundation of South Africa(2012-2014).
[6] Raju M., Lanitha B., ,“Survey about Cloud Computing Threats”, International Journal of Computer Science and Information Technology (IJCSIT), Vol. 5, 2014
[7] Shipla D., Nagashree C., Divya C., Spurthi G. S. ,“Survey on Security Attacks and Solutions in Cloud Infrastructure”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 8, Aug-2014.
[8] M. Naehrig, K. Lauter, and V. Vaikuntanathan. “Can homomorphic encryption be practical?” In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pp. 113-124, New York, USA, 2011.
[9] P. Tysowski and M. Hasan. “Hybrid Attribute- and Re-EncryptionBased Key Management for Secure and Scalable Mobile Applications in Clouds”. IEEE Transactions on Cloud Computing, Volume 1, Issue 2, pp. 172-186, 2013.
[10] A. Baldwin, C. Dalton, S. Shiu, K. Kostienko, and Q. Rajpoot. “Providing secure services for a virtual infrastructure”. Operating Systems Review-ACM Special Interest Group on Operating Systems, Volume 43, Issue 1, PP. 44-51, 2009.