RESEARCH ARTICLE OPEN ACCESS

Information Leakage Prevention In Cloud Computing

Raziqa Masood*, Dr. Nitin Pandey **
*(Department of Information Technology, Amity University,Noida)
** (Department of Information Technology, Amity University, Noida)

ABSTRACT
The cloud computing is still in it infancy.this is an emerging technology which will bring about innovations in terms of businessmodels and applications.the widespread penetration of smartphones will be a major factor in driving the adoption of cloude computing.however, cloud computing faces challenges related to privacy and security. Due to varied degree of security features and management schemes within the cloud entities security in the cloud is challenging. Security issues ranging from system misconfiguration, lack of proper updates, or unwise user behaviour from remote data storage that can expose user‗s private data and information to unwanted access can plague a Cloud Computing. The intent of this paper is to investigate the security related issues and challenges in Cloud computing environment . We also proposed a security scheme for protecting services keeping in view the issues and challenges faced by cloud computing.

***Keywords* -**Cloud Computing, Data Protection,Security, Application Program Interface, Average Revenue

I. INTRODUCTION

Privacy in this report ,refers to the right to self determination ,that is the right of individuals to “know what is known about them” be aware of stored information about them,control how that information is communicated and prevent its abuse. In cloud computing the recourses are shared via internet. Cloud computing provides the fast, quick and convenient data storage and other computing services via internet.

The cloud computing system is like your virtual computer that is a virtual location of your resources.The user can access their resources those are placed on a cloud as on their real system resources. The user can install applications, store data etc. and can access through internet anywhere. The user do not need to buy or install any hardware to upgrade his machine. They can do it via internet. In future we may need only notebook PC or a mobile phone to access our powerful computer and our resources anywhere.Security aspects of cloud computing are gaininginterests of researchers as there are still numerous unresolved issues which needed to be addressed before large scale exploitation take place. Cloud computing is not something that suddenly appeared overnight;in some form it may trace back to a time when computer systems remotely time –red comuting resources And applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications [2]

II. PRIVACY ISSUES IN CLOUD COMPUTING

Security issues are the most concerned challengesin cloud computing [3]. Cloud is expected to offer the capabilities like encryption strategies to ensure safe data storage environment, strict access control, secure and stable backup of user data. However, cloud allows users to achieve the power of computing which beats their own physical domain. It leads to many security problems. We will discuss the major security concerns in the following:

2.1. Identification and Authentication
:The multitenancy in cloud computing allows a single instance of the software to be accessed by more than one users [3].This will cause identification and authentication problem because different users use different tokens and protocols , that may cause interpretability problems.

2.2. Access control:
Confidential data can be illegally accessed due to lenient access control.If adequate security mechanisms are not applied then unauthorizedaccess may exist. As data exists for a long time in a cloud, the higher the risk of illegal access [3].

2.3. Data Seizure:The company providing service may violate the law. There is a risk of data seizure by the some foreign government.

2.4.Coding/ Decoding:There is an issue of the

Encryption/ Decryption key that are provided. The keys should be provided by the customer itself.

2.5.Policy Integration : Different cloud servers can use different tools to ensure the security of client data.So Integration policy is one of the major concerns of security.

2.6.Audit : In cloud computing the Cloud Service Provider (CSP)controls the data being processed. CSP may use data while being processed [3]. So the process must be audited. The all user activities must be traceable. The amount of data in Cloud Computing may be very large. So it is not possible to audit everything.

2.7.Availability: Availability is the major concern in the cloud computing. When the client data is virtualized, clients have no control on the physical data [3]. If in the cloud, the data or service is not available, it is rigid to fetch the data.

III. Proposed Privacy Model :

The global dimension of cloud computing requires standardized methodologies and technical solutions to enable stake holders to asses privacy risks and established adequate protection level. In this section we proposed a security scheme taking regarding issues and challenges keeping in mind. Our aim is to design and develop a security proposal that would be accurate, secure data in shared pool, secure for unexpected intrusions, adaptive and be of real time. The proposed secure model provides the security of cloud services by challenging these privacy issues:

1. Complexity of risk assessment in a cloud environment.
2. Emergence of new business models and their implication for consumer privacy.
3. Achieving regulatory compliance.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks.so this is necessary to protect the priate information and maintain the priacy for any organisation ,that is why we developed a cryptographic scheme for protection the information.

Whenever a sender will send the data over a cloud then following priacy techniques or model will work :

Break the complete information in form of two tables : static and dynamic.

We would be able to communicate the private information on cloud if we devide it in data tables or messages by using cryptographic techniques,in which a sender will keep a private or secure key to unlock the half part of message and to disclose the complete message the reciever will combined both the tables and decrypted by sender's key.

This can be done by splitting the tables. The part of the tables which is dependent on the key is sent to the client and the other part of the tables which is not dependent on the key is stored on the client's device. When we want to update the key, only part of the tables needs to be sent to the client. Therefore, less data needs to be transmitted. The tables that are sent by the server to the client can be updated and are called the dynamic tables. The tables that are stored on a clients's device cannot be updated and are called the static tables. If an attacker taps the ciphertext plus part of the tables, he is not able to decrypt the ciphertext, because he also needs the other tables.

The following needs to be considered:

- It is important that each client receives different static tables to ensure that each client uses a unique combination of static and dynamic tables. If this is not ensured,then someone could tap the dynamic tables which were sent to another client and use these dynamic tables in combination with his own static tables to decrypt the content.
- It is important that the static tables cannot be copied. Otherwise a client could publish his static tables and his dynamic tables which together could be used for decrypting content. This can be done by locking the static tables on the device(nodelocking).

However, the question remains which tables need to be transmitted and which tables can be stored.

There are five types of tables: type Ia, II, III, IV, and Ib. The tables that are dependent on the key are the type II and the type Ib tables. We want to be able to update this key, therefore these tables cannot be fixed on the client's device. The least amount of data a server needs to send are the tables which are dependent on the keys and those are the type II and type Ib tables.

There are several possibilities for partitioning the set of tables into a set of dynamic tables and a set of static tables:

1. Dynamic tables: II, Ib (208 KB) Static tables: Ia, III, IV(544 KB)
2. Dynamic tables: Ia, II, Ib (272 KB) Static tables: III, IV (480 KB)
3. Dynamic tables: II, III, Ib (352 KB) Static tables: Ia, IV (400 KB)
4. Dynamic tables: II, IV, Ib (544 KB) Static tables: Ia, III (208 KB)
5. Dynamic tables: Ia, II, III, Ib (416 KB) Static tables: IV (336 KB)
6. Dynamic tables: II, III, IV, Ib (688 KB) Static tables: Ia (64 KB)

7. Dynamic tables: Ia, II, IV, Ib (608 KB) Static tables: III (144 KB)
8. Dynamic tables: Ia, II, III, IV, Ib (752 KB) Static tables: -

Partition 8 is the original situation in which all the tables are sent to the client. If an attacker has access to all the tables, the attack can be executed. Therefore, it is not recommended to transmit all the tables over the line.The server wants to send the least amount of data. Therefore, the server only wants to send tables which it wants to update, like the tables which are dependent on the key or the tables which represent the external encodings. Two partitions remain:

- Dynamic tables: II, Ib (208 KB) Static tables: Ia, ,III, IV (544 KB)

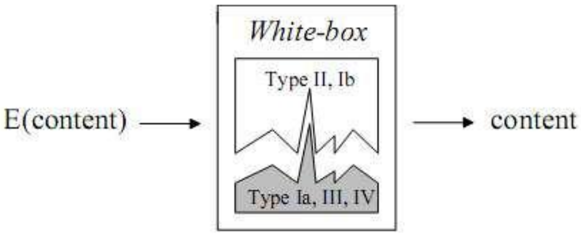

Fig .1

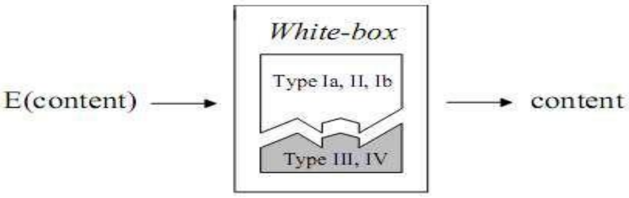

Fig 2

IV. Cloud security controls

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management.[7] The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:[7]

4.1 Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. [Some consider them a subset of preventive controls.]

4.2 Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

4.3 Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[7] System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

4.4 Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

V. Conclusion

I propose a safer path down Cloud adoption, especially for Government agencies
, which is founded upon thorough and exhaustive Risk assessments.These assessments are of critical importance and must be undertaken especially in light of the risks and relative deficiencies of currently existing methods and strategies for ensuring data security.This project is important because it has drawn together research from several fields and sources, analyzing them to arrive at this conclusion. Furthermore, I also conclude that a complete elimination of the risks to personal information is highly unlikely; especially given the complexity of the multi-layered infrastructure, technological limitations, and the human factor.Only through the utilisation of the identified risk mitigation tools and strategies, “due diligence” on the part of the organisation will have been met.

The proposed secure model has to ensure security of each service by applying the various security schemes on each cloud architectural component. While most of the risk against security in Cloud computing are caused by the involvement of computing in different plate forms. For defending the threats, developing the secure system that will be efficient is a great research challenge. Again, ensuring each component secure is a major research issue. Many of today‘s security schemes based on specific component mode but there is a lack of combined effort to take a common model to ensure security of each architectural component, in future though the security mechanism become well - established for each individual component, combining all the mechanism together for making them work in collaboration with each other will incur a hard research challenge.

References

[1] P.F. da Silva and C.B. Westp hall, ―Improvements in the Model for Interoperability of Intrusion Detection Responses Compatible with the IDWG Model‖ Int‘l J. Network Management, vol. 17, no. 4, 2011, pp. 287–294.

[2] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong , ―Characteristics of cloud computing‖ , 39th International Conference on Parallel Processing Workshops ,2012

[3] ZiyuanWang , ―Security and privacy issues within the Cloud Computing‖ ,International Conference on Computational and Information Sciences , 2011

[4] Shuai Zhang, ShufenZhang, Xuebin Chen and XiuzhenHuo , ―The Comparison Between Cloud Computing and Grid Computing‖ , International Conference on Computer Application and System Modeling (ICCASM 2010),2010

[5] Siani Pearson and AzzedineBenameur , ―Privacy , Security and Trust Issues Arising from Cloud Computing‖,2nd IEEE International Conference on Cloud Computing Technology and Science

[6] ZhidongShen and QiangTong ,―The Security of Cloud Computing System enabled by Trusted Computing Technology‖, 2nd International Conference on Signal Processing Systems (ICSPS) , 2010

[7] Shuai Zhang , Shufen Zhang , Xuebin Chen and XiuzhenHuo , ―Cloud Computing Research and Development Trend‖ , Second International Conference on Future Networks , 2010

[8] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, ―The Eucalyptus open source cloud-computing system‖ in Proceedings of the 9thIEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID 09), May 2011, pp. 124–131.

[9] Q. Wang, K. Ren, W. Lou, and Y. Zhang, ―Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance‖ Proc. of IEEE INFOCOM, 2010.

[10] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, ―Hey , you, get off of my cloud: exploring information leakage in third-party compute clouds,‖ in CCS 09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2011, pp. 199–212.

[11] K.hamlin, M. Kantarcioglu, L. Khan and B. Thuraisingham "Security Issues for Cloud Computing" Journal of Information Security and Privacy,vol. 4, no. 2, pp. 39–51, April-June 2010.