SURVEY ON CLOUD COMPUTING SECURITY TECHNIQUES

Archana T A[1], V Jeyakrishnan[2]

[1, 2]*Computer Science and Engineering Department, Karunya University, Coimbatore, India*

Abstract

Cloud computing is one of the emerging technology in computer science field. It provides various services and resources, still enterprises are disinclined to invest their business in cloud computing. It is because of security issues it has. There are different service models in cloud computing and threats to security also have different. The characteristics that are must be ensured while thinking about data security in cloud computing are integrity, availability and confidentiality. In this paper we are surveying some of the Intrusion Detection and Prevention Systems (IDPS) and comparing them regarding their ability to provide data security.

Keywords— *Cloud Security, cloud computing, data security, IDPS*

---***---

1. INTRODUCTION

Cloud computing is one of the important area in computer science in which researches are still going on. A cloud has virtualized group of services or resources that are needed in computing. Users can request the resources or services and they can make benefit of them even though they don't have them in their hand. Cloud computing provides resources on demand. That is it provides services or resources when the user/client requesting them and it is based on some service level agreement between the user/client and cloud service provider.

There are 3 cloud service models

1. Software as a Service (SaaS)-It provides software that run in your PC behind firewall
2. Platform as a Service (PaaS)-It provides the developmental environment as a service.
3. Infrastructure as a Service (IaaS)-It will provide the infrastructure as a service. For example server, software.

Cloud computing is the future of IT but only reason for its slow growth is absence of a secure environment. In Cloud computing resources are shared. That is one of the major issues. Another thing is services are provided through a network, mainly internet. Internet is vulnerable to threats. If there are multiple users in a system we cannot assure that all of them are trustworthy.

Following are the major characteristics of cloud computing

- On demand resource allocation
- Elasticity and flexibility of system
- Pay per use services
- Shared resource pooling
- Broad network access

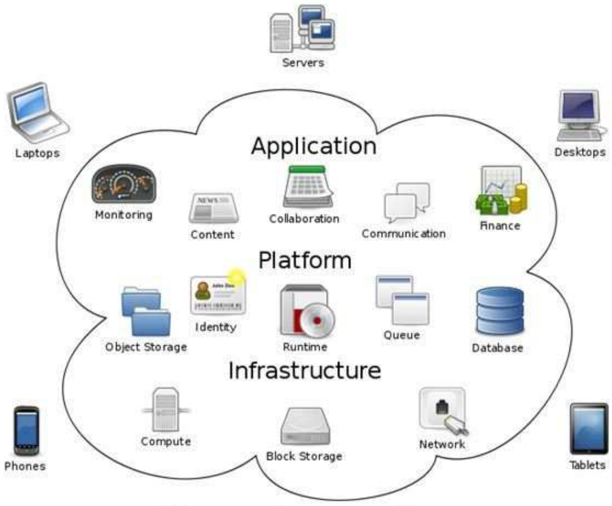

Fig 1 Cloud Computing

2. CLOUD COMPUTING SECURITY

2.1 Deployment Models

There are three deployment models for cloud computing. They are Public Cloud, Private Cloud and Hybrid Cloud mainly. Features of each deployment models are described below.

2.1.1 Public Cloud

In Public cloud, customers will access services over the web. Each client has his/her own resources that are provided by the cloud service provider. These cloud service provider serves multiple clients and provide the infrastructure for them. Client will not be aware about the infrastructure. The problem with this type of deployment is not at all secured.

2.1.2 Private Cloud

In private cloud client is managing their data. Client will decide where the data should reside and what level of security is needed. Also the data is more secured assuming that all the users are trusted.

2.1.3 Hybrid Cloud

Hybrid Cloud is mixture of public and private cloud within the same network. Clients can store sensitive data on their private cloud and use the public cloud for storing high volume of data.

2.2 Different Types of Threats

To provide secure environment for cloud computing should ensure confidentiality and integrity. Confidentiality means the data should not be available to any user who is not authorised. By providing integrity we are ensuring that data will not change or delete by a unauthorised user. Types of threats in cloud computing is given below.

Table 1 Type of Threats

Threat	Description
Malicious Insiders	Cloud service provider misuse the user’s data or resource
Man in the Middle attacks	Third party tries to access the data in transmit or inject the faulty data
Denial of Service Attacks	Denying the services to authorised user
Data Loss	Deleting or updating the sensitive data in unauthorised way

2.3 Detection Methodologies

Various threat detection methodologies are there. We can categorize them depending on the methodology used. First is signature based threat detection. In this methodology they will monitor behavior of the client and if known pattern of unauthorized behavior is found take it as threat. But it will not detect the new attacks which are not defined yet. Next is anomaly detection, in which any unexpected behavior is taken as a threat and it will help to find out the new attacks. But the number of false alarms may be high comparing with the signature based threat detection methodology.

Another broad category is hybrid threat detection methodology. Here uses the combination of the signature based detection methodology and anomaly detection methodology.

2.4 Different Detection Techniques

Juels et al. (2007) proposed a POR (Proof of Retrievability) model to check whether the file to be retrieved is correct or not.POR has a Cryptographic sum and in this technique needed to check this cryptographic sum to verify the integrity of the data. This checksum does not depend on the size of the file. One advantage of using this technique is the user can check the integrity without downloading the file. Author proposed this particular technique for large files.

Shacham and Waters (2008) built on this model and constructed a random linear function based Homomorphic Authenticator.. The central challenge is, it should be possible to extract the user's data from cloud service provider that passes a verification check. In this paper, gives the first proof-of-retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski. First scheme, based on BLS signatures, has the shortest query and response of any proof-of-retrievability with public verifiability. Second scheme, which is based on pseudorandom functions, has the shortest response of any proof-of-retrievability scheme with private verifiability.

Bowers et al. (2008a) proposes a theoretical framework for the design of PORs. It improves the previously proposed POR constructions of Juels-Kaliski and Shacham-Waters. It supports a fully Byzantine adversarial model, possessing only the restriction- fundamental to all PORs-that the adversary’s error rate be bounded when the client seeks to extract F. This techniques support efficient protocols across the full possible range of Ɛ, up to non-negligibly close to 1. Proposes a new variant on the Juels-Kaliski protocol.

Bowers et al.(2008b) introduced HAIL (High-Availability and Integrity Layer). It is a distributed cryptographic system that allows a set of servers to prove to a client the integrity of a file. Proofs in HAIL are efficiently computable by servers and highly compact. HAIL cryptographically verifies and reactively reallocates file shares. It is resistant against the entity one that may progressively corrupt the full set of servers. It manages file integrity and availability across a collection of servers or independent storage services.

Kamara and Lauter (2010) worked over public cloud infrastructure and proposed a model. This technique is purely based on cryptographic storage services. In proposed procedure, when a user wants to send data to other user, they first generate a master key that encrypts their message. The secret key for decryption is stored on receivers’ system for decrypting the same message. They use the concept of index encryption and tokens are generated with the knowledge of secret key.
The comparison table is given below

Table 2 Comparison Table

Reference	Advantage	Disadvantage
Juels et al. (2007)	Neither the prover nor the verifier need actually have knowledge of File	Limited number of queries only
Shacham and Waters (2008)	Support unlimited number of queries It can tolerate any adversarial error rate Ɛ <1	Derandomizing he query in this scheme is the major problem
Bowers et al. (2008a)	Lower storage overhead,Colerates higher error rates	Problems of designing efficient POR that support file updates, as well as publicly verifiable PORs
Bowers et al.(2008b)	Strong file-intactness assurance,Low overhead	HAIL only provide assurance for static files
Kamara and Lauter (2010)	Well suited for preserving integrity with the help of cryptography	The searching method is not very efficient for encrypted data

CONCLUSIONS

This paper presented a comparative study on some threats and threat detection techniques used in cloud computing. Specific concentration given to the threat detection techniques. In the future, we plan to develop threat detection technique which is based on these concepts and their advantages.

REFERENCES

[1] Bowers KD, Juels A, Oprea A. Proofs of retrievability: theory and implementation, Cryptology e-Print Archive. Report 2008/175; 2008a.

[2] Bowers KD, Juels A, Oprea A. HAIL: a high-availability and integrity layer for cloud storage, Cryptology e-Print Archive. Report 2008/489, 2008b.

[3] Juels A, Burton J, Kaliski S. PORs: proofs of retrievability for large files. Proceedings of CCS ’07, p. 584–597, 2007.

[4] Kamara S, Lauter K. Cryptographic cloud storage. Lecture Notes in Computer Science 2010;6054:136–49.

[5] Shacham H, Waters B. Compact Proofs of Retrievability, Proceedings of Asiacrypt’08, 5350, p. 90–107, 2008.