A Framework based on Security Issues in Cloud Computing

N.Suganya
PG Scholar
Department of Computer Science and Engineering
Coimbatore Institute of Engineering and Technology,
Coimbatore, India

N.Boopal
Assistant Professor
Department of Computer Science and Engineering
Coimbatore Institute of Engineering and Technology
Coimbatore, India

S.Gunasekaran, Ph.D
Professor and Head
Department of Computer Science and Engineering
Coimbatore Institute of Engineering and Technology
Coimbatore, India

ABSTRACT

Resource sharing is the vital notion of cloud computing. Everything that is available in cloud can be accessed as a service. The users can move the data to the cloud environment because of the accessing flexibility. While moving the data to the cloud ,the infrastructure can pose severe security and privacy issues. There is a chance that the attacker can easily spoof an authorized user's data. This study explains an overview of the possible threats and attacks that occurs in cloud computing and provides certain solution to overcome those threats and attacks.

Keywords:
cloud computing, threats and attacks

1. INTRODUCTION

Cloud computing change the waypeople using the computer and the internet.Cloud computing is a subscription-based service where the users can obtain networked storage space and computer resources .The Cloud makes it possible to access the information from anywhere at any time. The cloud provides many facilities to the computer users and the large as well as small businesses. The resources are provided as a service to the user in different service models. The models are Software-as-a-service, Platform-as-a-service and Infrastructure-as-a-service. Each service can be built upon the layer of other services.

2. BENEFITS OF CLOUD

2.1 Less Expenditure cost

Cloud computing reduces the capital investment in large and small organizations. Since everything will be accessed from the cloud

2.2 Scalability

At peak time, the capabilities that are available in the cloud can be expanded to handle the workloads[8]. Depending on the user needs its capabilities are handled.

2.3 Security

In cloud,the data storage must take place only in the server. So there is less chance that the data stolen occur in the client side.

2.4 Less Power Consumption

The cloud capabilities can be mostly accessed by the thin client. The thin client consumes less amount of power because it does not have hard drive [8].

3. SERVICE MODELS

Based on the requirements,the cloud environment service models are categorized.The service models are as follows:

3.1 Private cloud

The private cloud is preserved by a specific society and they have the control over it. The private clouds are more secure than the public cloud because only the members of the specific society can contact the cloud.

3.2 Public cloud

The public clouds are operated and used by general public.They can be an organization or an enterprise or government bodies or any combination of them.The capabilities are provided to multiple customers with more massive storage,hardware and infrastructures.

3.3Hybrid cloud

Hybrid cloud is a variation of both public cloud and private cloud. Public cloud can be used for large amount of data are processing and with private cloud the information's are stored securely.

3.4 Community cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns whether managed internally or by third-party.

4. PROBLEM STATEMENT

Although cloud computing is an emerging technology, the recent increased use of cloud services require current insights into necessary security requirements and its solutions.

The objective of this paper is to convey the types of security issues in cloud and gives a structuredoverview ofthe security issues investigated and the proposed solutions to deal with the issues. This paper therefore informs fellow researchers on what is better-known in discovered empirical studies concerning security needs in cloud computing. It moreover helps cloud developers with a detailed overview to quickly discover and address gaps in cloud security issues.

5. SECURITY ISSUES IN CLOUD COMPUTING

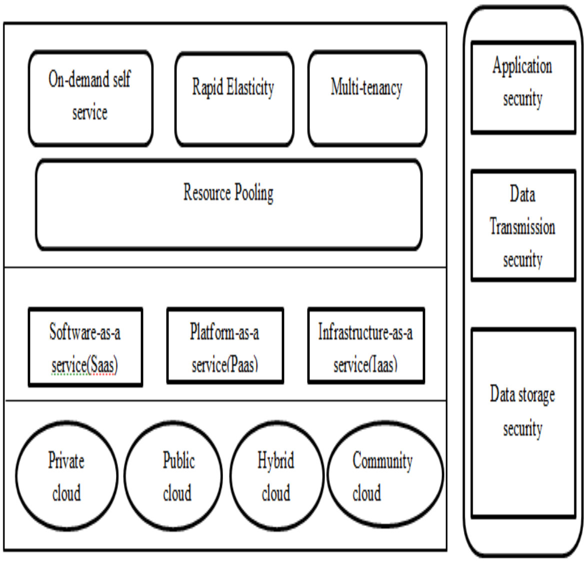

Figure:1 Complexity of security in cloud computing

Cloud computing has come with not only benefits but also have some disadvantages. The users can store their data in cloud and by knowingly giveup direct control of their data.

Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are [1]:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders.
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile

6. LITERATURE REVIEW

The literature identifies different security issues in cloud computing:

6.1 Cloudcomputing security auditing-2010[6]gives a survey report on the most important challenges that exist in cloud environment and security is the top most issue. The issues are resolved by implementing auditing mechanisms and set of frameworks.The auditing mechanism introduces public preserving audit protocol where four algorithms are used and the auditor has zero knowledge about the user's data. DDOS[1](Distributed Denial of Service) is an attack where unauthorized users trying to steal the user's data which could be prevented by IDAAS (Identity and access management as a service) where the users of the organization are provided with the resources based on their role. In future, a tool is to be developed to identify the integrity without compromising the data privacy in cloud which should be automated.

6.2 Security challenges and solutions in cloud computing-2011[4]gives an overview of the service models and the security issues.Even though firewalls,access control and authentication mechanism exists in cloud there are still vulnerabilities available. Software security measures such as virtualization technology,operating system and data encryption methodologies are implemented to prevent from attacks.For physical security,data backup with continuous data protection and the location of the servers are protected.The vendorlock-in becomes a major problem in the near future.If a user wants to change the cloud provider the information stored in the previous providers environment will be formatted.

6.3 Security based model for cloud computing-2011[9]describes the evolution of cloud computing from distributed and grid computing and gives anopen security architecture.They evaluate cloud security with the measures such as confidentiality,integrity,Access control,Non-repudiation and authentication.Some of the security solutions are provided. They are backup, firewall, and Investigation support. Before getting an agreement with cloud providers some security management models should be ensured by users.They are security image testing,risk management,risk assessment,security governance,application security and data security.Bandwidth and capacity improvements are to be done in the future.

6.4 A home healthcare system in the cloud-addressing security and privacy challenges--2011[7]deals with the data security and privacy of the patients. The patients can store their own medical data and only authorized persons can access the data. Depending on the kind of information, the patients datum are segregated and stored in the corresponding data store. Encryption techniques such as digital rights management and RSA algorithms are implemented to provide more security to the data. TClouds are an advanced cloud infrastructure that wasdeveloped to deliver computing and storage that achieves a new level of security and privacy . Cryptographic techniques are not sufficient to protect the patient'sdata.

6.5 Ensuring Data Storage Security in Cloud Computing-2011[3] discussesdata storage correctness which is an important quality of service parameter. The storage correctness under dynamic data updates need to be ensured which is of more importance. Erasure-correcting code is used for the file distribution preparation which provides redundancies and guarantees data dependability. Misbehaving servers are identified by the homomorphic token and erasure-code. The Third-Party auditor progress the user's data to ensure the storage correctness. The main goal is to ensure storage correctness, fast localization of data error, dynamic data support, Dependability and lightweight. Token computation function is used to preserve homomorphic properties. File retrieval and error recovery could be used for file distribution preparation,challenge token precomputation,correctness verification& error localization, File retrieval &error recover. Data storage correctness is an important issue and is resolved in the future with the help of public verifiability and storage correctness assurance.

6.6 A security aspects in cloud computing-2012 [5]deals with the most suspicious attacks in cloud such as DDOS [1](Distributed Denial Of service) and explains that what could happen if misconfiguration of SSL occurs. Different security measures for provider, infrastructure and end-user are explained.Service provider utilizes the security-Identity and Access Management,providing protocols such as SSL/TLS,Audit and compliance,user identity techniques are used.Infrastructure security could be enabled by encryption techniques,virtual server and application .Likewise, for end-user security-browser security,authentication and the Cloud Service Providers (CSP) can give security-as-a-service are discussed. The challenging task i is to identify andmanage the risk involved in the cloud which and must be resolved in the future.

6.7 Research on cloud computing security problem and strategy-2012[10]discusses the data privacy and service availability issues. The frequently used cloud computing systems and their operations are discussed. Techniques such as encryption, security authentication mechanisms and access control policies are used to enforce the data privacy.The encryption includes asymmetric and symmetric key encryption system. Security authentication mechanisms include PKI technology,x.509& x.500 certificate standards .Access control policy ensures that the network resources are not illegal. Monitoring and auditing is a serious problem in cloud computing.Viruses and worms must be controlled in the network of cloud.The abnormal action of the system and cloud must be controlled.The disaster recovery mechanism includes backup plans and the network data transmission security is controlled by data encryption and VPN technology. The cloud provider needs to have several measures to protect the security in the future.

6.8 An analysis of cloud computing security issues-2012[2]describes the security issues in the cloud service models.The issues such as multi-tenancy,elasticity,availability of information,secure information management,information integrity and privacy,cloud secure federation are noticed. Multi-tenancy implies sharing of the application resources by more than one user's.Lack of confidentiality occurs due to multi-tenancy. Isolation is a technique to overcome the confidentiality issue. Elasticity is a characteristic of cloud computing in which the resources are scaled up and down based on requirements. The placement engines are used in which it contains the list of available resources and eliminate the users request for resource on the same physical or logical server.Availability of informationdeals with the maximum time for which the resources may not be available for use to the customer. Unavailability of the resource can be solved with the help of backup plan.In secure information management set of policies and security requirements are derived from multi-user organizations.Information integrity and privacy deals with authentication and confidentiality issues, which can be resolved by RSA certificates and key management. The cloud federation issues are resolved by single sign on, authentication and authorization. The stack holder's requirements are gathered and a standard is developed based on that requirement in the near future.

7. CONCLUSION AND FUTURE WORK

We accept as true that facts and figures in Cloud Computing, an area full of trials and of paramount importance, is still in its infancy now, and many study troubles are yet to be recognized. From this reconsider, different modes of algorithms are utilized for security anxiety. Even encryption is implemented, there exists a difficulty. More advanced encryption methodologies are utilized to prevent the threats. In future,e encryption needs to be applied at the client environment before transmitting the data.

REFERENCES

[1] "Security Guidance for Critical Areas of Focus in Cloud Computing", April 2009, presented by Cloud Security Alliance (CSA).

[2] Ayesha Malik, Muhammad MohsinNazir "Security Framework for Cloud Computing Environment: A Review"Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 3, March 2012.

[3] Cong Wang, Qian Wang, and KuiRen and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing"-IEEE Transaction on Parallel and Distributed Systems, Vol. 22, No. 5, May 2011.

[4] EysteinMathisen "Security Challenges and Solutions in Cloud Computing" 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 31 May -3 June 2011, Daejeon, Korea.

[5] GurudattKulkarni&JayantGambhir, TejswiniPatil, AmrutaDongare (2012) "A security aspect in cloud computing" 3rd IEEE International Conference on Software Engineering and Service Science (ICSESS).

[6] IrfanGul, AtiqurRehman and M Hasan Islam (2011) "Cloud computing security Auditing", 2nd International Conference on Next Generation Information Technology (ICNIT).

[7] Mina Deng, Milan Petkovi, Marco Nalin and IlariaBaroni "A home healthcare system in the cloud – addressing security and privacy challenges" -IEEE 4th International Conference on Cloud Computing,2011.

[8] RajnishChoubey, RajshreeDubey, Joy Bhattacharjee "A Survey on Cloud Computing Security,Challenges and Threats"-International Journal on Computer Science and Engineering (IJCSE) ,Vol. 3 No. 3 Mar 2011.

[9] Sameera and Chan, "Cloud Computing Security Management",Second International Conference on Engineering Systems Management and Its Applications (ICESMA), 30 March, 2010.

[10] ShivlalMewada , Umeshkumar Singh and Pradeep Sharma "Security Based Model for Cloud Computing", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1, December 2011.

[11] Wentao Liu (2012) "Research on Cloud Computing Security Problem and strategy" 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).