Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

A Survey of Cloud Computing with its Security Concerns

[1]AmalRedge. G and [2]Pavithra. D.N,
[1]Assistant Professor, [2]Student,
[1,2]Department of Computer Science, St. Joseph's College of Arts and Science for Women, Hosur, Tamilnadu, India

Abstract-The cloud has come forward as a successful computing exemplar allowing users and organizations to rely on external providers for storing and processing their data and making them available to others. This survey presents an overview of cloud computing with its components, service models, deployment models and security concepts. Cloud computing has a lot of security issues that are gaining great attention now a days, including the data protection, network security, virtualization security, application integrity and identity management. Many techniques are suggested for data protection in cloud computing but there are still a lot of challenges in this subject. In this paper we present an overview of Cloud computing framework and its security issues related to storage, management and processing of data.

Keywords: *Cloud Computing, Virtualization, Cloud Security, Service Model, Deployment Model*

I. INTRODUCTION

Cloud computing is abroad and diverse observable fact. Users are allowed to store huge amount of data on cloud storage for future use. Anytime, anywhere access to virtualized IT resources delivered dynamically as a service. In cloud computing, the computers need not to be in the same physical locations.

The practice of using a network of remote servers hosted on the internet to store, manage and process data rather than a local server or a personal computer.

Most of the cloud service provider stores the data in plaintext format and user need to use their own encryption algorithm to secure their data if required. The data needs to be decrypted whenever it is to be processed. The data is stored in DynamoDB of Amazon Web Service (AWS) public cloud. User's computation is performed on encrypted data in public cloud. When results are required they can be downloaded on client machine. In this scenario users data is never stored in plaintext on public cloud.

Cloud computing was defined by the US National Institute of Standards and technology (NIST) (Mell & Grance, 2011). They defined a cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg: network, servers, storage, application and services) that can be rapidly provisioned and released with minimal management effort of service provider interaction (Mell & Grance, 2009).

Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. The cloud computing provides rich benefits to the cloud clients such as costless services, elasticity of resources, easy access through internet, etc. from small to large enterprises moving towards cloud computing to increase their business and tie-ups with other enterprises. Main corporations including Google, Amazon, Cisco, IBM, Sun, Dell and HP have invested in cloud computing and propose a range of cloud-based solutions to individuals and businesses.

There are different types and models in cloud computing regarding the different provided services. So, the cloud computing involve public cloud, private cloud, hybrid cloud and community cloud. Cloud computing could be usually classified by two ways: by cloud computing location, and by the offered types of services.

The following Figure. 1 shows the schematic definition of cloud computing (Khorshed, Ali, & Wasimi, 2012):

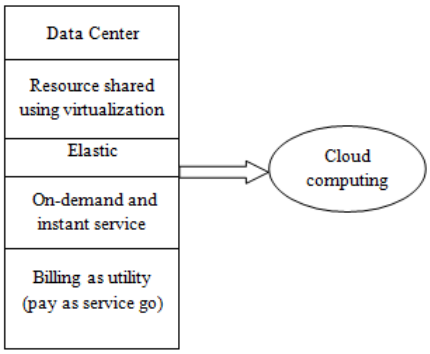

Figure 1: Schematic Definition of Cloud Computing

In this technology users outsource their data to a server outside their premises, which is run by a cloud provider (Zhou & Huang, 2012). In addition memory, processor, bandwidth and storage are visualized and can be accessed by a client using the internet (Kumar & Lu, 2010). Cloud computing provides highly efficient data retrieval and availability. Cloud providers are taking the delicacy of resource optimization.

II. CHARACTERISTICS OF CLOUD COMPUTING

There are five characteristics of cloud computing. They are:

A. On-demand Self Service

The first one is on-demand self-service, where a consumer of services is provided the needed resources without human intervention and interaction with cloud provider. A consumer can unilaterally provision computing capabilities, such as server time and network storage as needed automatically without requiring human interaction with each service provider.

B. Broad Network Access

The second characteristics is broad network access, which means resources can be accessed from anywhere through a standard mechanism by thin or thick client platforms such mobile phone, laptop, and desktop computer.

C. Resource Pooling

Another characteristic is resource pooling, which means the resources are pooled in order for multi-tenants to share the resources. In the multi-tenant model, resources are assigned dynamically to a consumer and after the consumer finishes it, it can be assigned to another one to respond to high resource demand. Even if consumers are assigned to resources on

demand, they do not know the location of theseassigned resources. Sometimes they know the location at a high-level abstraction, such as country, state and data center. Storage, processing, memory and network are the kind of resources that are assigned. In short, the providers computing resources are pooled to serve multile consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned to consumer demand.

D. Rapid Elasticity

Rapid elasticity is also one of the cloud computing characteristics, which means that resources are dynamically increased when needed and decreased when there is no need. Capabilities can be elastically provisioned and released, in some cases automatically to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimeted and can be appropriated in any quantity at any time.

E. Measured Service

Measured service in order to know how much is consumed. Also, it is needed by the cloud provider in order to know how much the consumer has used in order to bill him or her. Cloud syatems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service(eg., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilized service.

III. FRAMEWORK OF CLOUD COMPUTING

The following Figure.2 shows the framework of cloud computing, which consists of service models available in cloud, deployed models of cloud, basic components of cloud and the security concepts in cloud.

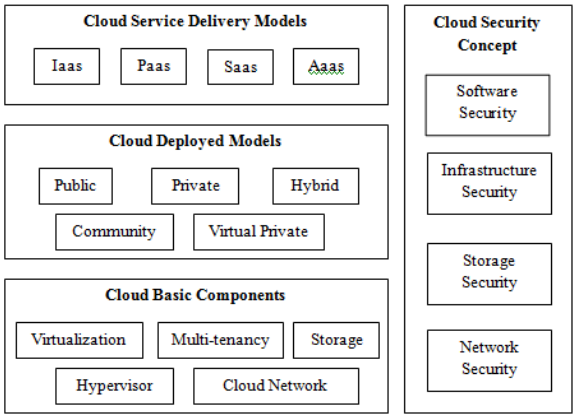

Figure 2: Cloud Computing Frame work

IV. SERVICE MODELS

There are four models. Those models differ in the capabilities that are offered to the consumer (Mell & Grance, 2011). It can be a software, platform or infrastructure.

A. Software as a Service (SaaS)

It is a collection of remote computing services (Fan, Haolong, & Hussain, 2015). The cloud service provider provides software and the cloud infrastructure to the clients so they can use this software on the cloud infrastructure for their application. The cloud service provider is responsible and is the only one who is in charge of controlling underlying physical setting without client intervention.The cliet can access this software as a thin client through a web browser.

B. Platform as a Service (PaaS)

It is in middleware of service model and delivers the services in the form of development tools (Sun, Dawei, & Chang, 2011). This service is similar to SaaS in that the infrastructure is controlled by the cloud service provider but is different in that the users can deploy their software. Physical setting are controlled and restricted by the cloud service provider and application settings are given to each user to control them.

C. Infrastructure as a Service (IaaS)

This service is belongs to the bottom of the model (Madjid, Kifayat, & Kashif, 2013). Computing resources such as processing storage and networks can be provisioned. The client of IaaS can install and use any arbitrary operating system. The clients can deploy their application on the operating system. The elasticity of allocating physical or virtual resources helps providing the infrastructure in an abstract manner. It also provides scalability and provisions issues of infrastructure without the need of spending huge amount of funds and time.

D. Anything as a Service (AaaS)

It is a collective term which combines a number of things as X as a service. X may be anything or everything as a service. This service becomes interchangable in cloud land. The cloud system are able to support the large resource to specific, personal and coarse requirements using Monitor as a Service(MaaS), Data as a Service(DaaS), Communication as a Service(CaaS), Security as a Service(SecaaS), Routing as a Service(RaaS) (Ali, Mazhar, & Khan, 2015).

V. DEPLOYMENT MODELS

Cloud computing generally depends on shared resources by local servers or individual devices. Therefore it is able to achieve consistency by taking the benefit of resource sharing. Deployed model tells what is the purpose and nature of the cloud. The following are the deployed models in cloud: (Aguiar, Zhang, & Blanton, 2014) (Mohamed, Abdelkader, & El-Etriby, 2012) (Gul & al, 2011) (Ramgovind, Eloff, & Smith, 2011)

A. Private Cloud :

The cloud provider provides cloud infrastructure to a single organisation that has many consumers. This infrastructure is to be used exclusively for their use and need. In other words, Cloud computing operates and manages within the data center of an organization is called private cloud. In private cloud it is much easier to identify the customer and vendor connection because the infrastructure owned and operated by the same group. Therefore, security risks are easier to detect.

B. Public Cloud :

This model differs from the previous model on that it is open for the public; it is not private and not exclusively for community. A public cloud can be provisioned for public to use it to satisfy their needs. It is the true representation of cloud hosting where the customer and provider have a strong service level agreement (SLA) to maintain the trust between them. This creates many issues, as we don't know where the resources are located or who owns them, which rising the difficulty of protecting them from attack.

C. Community Cloud :

The cloud provider provides cloud infrastructure to many organisations that forms community that share mission, security requirements, compliance consideration or policy. Cloud infrastructure of the organizations shared concerns of consumers a special provision has been made for exclusive use by the community model. It is owned, managed by a third party or some combination of them is driven by one or more and that may be presenton or off campus. A community cloud being shared and controlled by multiple organizations.

D. Hybrid Cloud :

This model comprises two or more deployment models (private, community or public). The cloud infrastructure can be combination of those models. A cloud can be considered hybrid if the data moves from a data center to a private cloud or public cloud or vice versa. The data and application are bounded together by standarized and respectability technology. Hybrid cloud offers the advantages of different clouds deployment models. However, it is well planned and more secure than public cloud while accessing the entities over the internet.

E. Virtual Private Cloud :

It is a semi private cloud, which is less resources and it consists of Virtual Private Network(VPN). It is on require configurable pool of shared resources allocated with in the cloud upbringing.

VI. CLOUD COMPUTING BASIC COMPONETS

These components consist of a wide range of services that we can use all over the internet.

A. *Virtualization* :

It plays an vital role in deploying the cloud. It is the strategic componet in the cloud, which allows the physical resources by multiple consumers (Subashini, Kavitha, & Veeraruna, 2011). It creates the virtual occurrence of resource or device such as operating system, servers, network resources and storage devices where in the framework utilize the resources into more than one execution environment.

B. *Muti-tenancy* :

Multi-tenant environment can have mutiple customers or users who does not see or share each others data but can share resource or function in an execution environment even if they may not fit in to the same organization. Multi-tenancy results the most favorable consumption of hardware and data storage mechanism.

C. *Storage* :

It is a component, which maintained, managed and backed up vaguely and it made availabe over the network where the users can access the data.

D. *Hypervisor* :

The virtual machine monitor or manager is a key module of virtualiztion. It allows multiple virtual machines to run on a single hardware host. It manages and monitors the various operating systems, which run in a shared physical system.

E. Network :

It can operate more than one predictable data centers. A typical data center contains hundreds or thousands of servers. To proficiently construct and manage the storages, the cloud requires an internet connection and similar with a virtual private network which enables the user to securely access printers, applications, files etc.

VII. CLOUD SECURITY CONCEPT

When the data transfer to the cloud services, the requirements of security should be the most important. There are many security issues in cloud computing such as infection on confidential document, loss of governance, malicious insider and insecure incomplete data. And also unauthorised apps discovered in an organization. So the very challenging role is how to build an effective cloud application security architecture which provides control, visibility and remediation. The following section briefly introduce about the major security concerns of cloud computing:

A. *Software Security* :

It provides basic idea of software security come from the engineering software department that it continues to function correctly under the cruel behavior. To build a cloud environment a central and critical problem is software security problem. It defects with security including implementation bugs, buffer overflow, designed flaws, error handling promises and etc.

B. *Infrastructure Security* :

The most common and fundamental challenges is to demonstrate that the virtual physical infrastructure of the cloud can be trusted. The verification of the third party is not enough for the organization to be able to verify bussiness requirements that the primary infrastructure is secure.

C. *Storage Security* :

In cloud storage system, end user stores the data in the cloud and no longer owns the data and where it is stored. This always has been an important aspect of quality of service. Storage security concerns about data sanitization, cryptography, data leakage, snooping of data availability and malware.

D. *Network Security* :

In cloud computing, communication is via the internet and it is the strength of the cloud environment. Network security concerns about both internal and external attacks. These attacks in the network can either occur in the virtual or physical network.

VIII. CLOUD SECURITY ISSUES AND CHALLENGES

Despite of all advantages, the lack of security is the major concern in cloud environment. The goal of this paper is to provide the major and important security concerns in a very efficient way. It also includes some public and private cloud authorities and their security concerns.

The following Figure.3 shows the classification of cloud security issues:

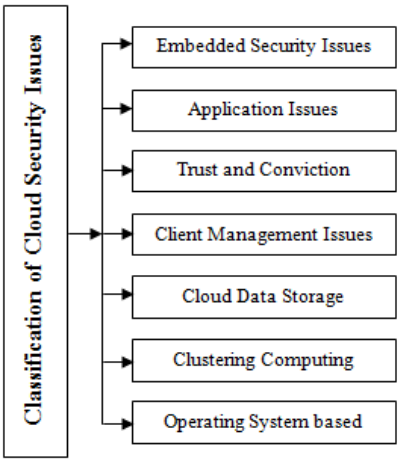

Figure 3: Classification of Cloud Security Issues

A. Embedded Security Issues

Security in cloud computing environment is a essential concern in these days. The security in embedded systems has several challenges that caused by the unique feature of these systems. The simple way to debug an embedded device is to connect it to a local network. The main security issues for cloud computing in embedded systems are caused by virtualizations (Zissis, Dimitrio, & Lekka, 2012). Different areas of security issues in embedded systems are as follows:

- Virtual Machine Isolation
- Virtual Machine Monitoring
- Programmability
- Electronic Access controlSystem
- Simple Network Management Protocol (SNMP) Server

B. Application Issues

Security in a software application is the most susceptible area. Most of theapplications have a front end, back end, different types of platforms, frameworks, parallelism. The basic security issue in a software application is that it has a million lines of programming code. Different programmers in a different language write the software and many of the programming languages have vulnerabilities. The following are the different varieties of application issues in cloud computing:

- User Frontend
- User backend
- Platform
- Framework
- License
- Service Availability
- Parallel Application

C. Trust and Conviction

We measured it as the faith that utilizes the experience of the employer, which gives contribution in the trust worthy decision. In addition to cloud stakeholders, storage, hardware, virtualization, web-based access, the computational algorithm related to trust. (Chen, Zhao, & Deyan, 2012) In security transparancy the next limit presented the TCP concepts, which aim to ensure the privacy and integrity of data under taken by the service provider. Security program in TCP detects whether data has been altered or tampered or not. The following are the issues related to trust in cloud computing:

- Humal Factor
- Forensic Value
- Reputation
- Governance
- Trusted Third party
- Lack of consumer trust

D. Client Management Issues

In cloud computing the management of client is one of the major concern for the security point of view (Attas, Batra, & Omar, 2011). The following are the security issues related to client management in cloud computing:

- Client Experience
- Client Authentication
- Client Centric Privacy
- Service level management

E. Cloud Data Storage

Data storage is also one of the most important components of cloud computing. As the growing of many online application and internet services, the storage of data and its security over the distributed computing is the big issue. The security issues regarding cloud storage are as follows:

- Location of the Data Warehouses
- Anonymization
- Availability
- Integrity Management
- Data Loss and Leakage
- Cryptography
- Unreliable Data
- Sanitization
- Maintenance
- Location protection of metadata

F. Clustering Computing

Clustering computing utilizes many computers, virtual machine, servers and they set to be loosely or tightly connected that work together that they can view as a single system is called computer cluster. The basic use of clustering in the cloud is for implementing the parallel processing application in enterprises (Kim & Jin-Mook, 2013). But it brings many confront while increasing the nodes per cluster for the system administrator. The following are the cluster security issues in cloud computing:

- Physical Cluster
- Virtual Cluster
- Multi Cluster
- Hierarchical Cluster

G. Operating System based Issues

Cloud computing utilizes many virtual machines, different kind of servers in a different inter and intra network, different kind of operating system working together brought many security challenges (Artem, Volokyta, & Igor, 2012). The following are the different security issue and vulnerability on different operating systems used in cloud computing:

- Desktop Operating System
- Server Operating System
- Network Operating System
- Smart Phone Operating System

CONCLUSION

The cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. With the rapid growth of cloud computing platforms and services, cloud security is becoming a key priority for all players. In this paper we presented an overview of essential characteristics of cloud computing, its service delivery and deployment models, basic components of cloud and security issues related to cloud.

ACKNOWLEDGEMENT

First of all, I am glad to thank THE LORD ALMIGHTY for giving me the spirit in completing this paper. I would thank my family for the constant support they provided throughout my preparation.

References

[1]Aguiar, E., Zhang, Y., & Blanton, M. (2014). An overview of issues and recent developments in cloud computing and storage security. Springer , 3-33.

[2]Ali, Mazhar, & Khan. (2015). Security in cloud computing: Opportunities and challenges. Inf.Sci.305 , 357-383.

[3]Artem, Volokyta, & Igor. (2012). Secure Virtualization in Cloud Computing.

[4]Attas, Batra, & Omar. (2011). Efficient Integrity checking technique for securing client data in Cloud computing. Intt. J. Electr. Comput. Sci. 11, 6105 .

[5]Chen, Zhao, & Deyan. (2012). Data security and privacy protection issues in cloud computing. Proceedings of 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE). I. 1, pp. 647-651. IEEE.

[6]Fan, Haolong, & Hussain. (2015). An integrated personalization framework for SaaS-based cloud services. 157-173.

[7]Gul, I., & al, M. I. (2011). Cloud computing security auditing. Next Generation Information Technology (ICNIT), (pp. 143-148). The 2nd International Conference on IEEE.

[8]Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. 28, 833 – 851.

[9]Kim, & Jin-Mook. (2013). An Effective Resource Management for Cloud Services using Clustering Schemes.

[10]Kumar, K., & Lu, Y.-H. (2010). Cloud computing for mobile users: Can offloading computation save energy? Computer , 51–56.

[11]Madjid, Kifayat, & Kashif. (2013). Detecting Intrusions in the Cloud Environment. 14th Annual Post graduate Symposium on Convergence of Telecommunications, Networking and Broadcasting.

[12]Mell, P., & Grance, T. (2009). The NIST Definition of Cloud Computing.

[13]Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012). Enhanced ata security model for cloud computing. Informatics and Systems (INFOS) , CC-12.

[14]Ramgovind, S., Eloff, M. M., & Smith, E. (2011). The management of security in cloud computing. nformation Security for South Africa (ISSA) , 1-7.

[15]Subashini, Kavitha, & Veeraruna. (2011). A survey on security issues in service delivery models of cloud computing. . Netw. Comput. Appl. 34 (1) , 1-11.

[16]Sun, Dawei, & Chang. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments., (pp. 2852-2856).

[17]Zhou, Z., & Huang, D. (2012). Efficient and secure data storage operations for mobile cloud computing. Proceedings of the 8th International Conerence on Network and Service Management (pp. 37–45). International Federation for Information Processing.

[18]Zissis, Dimitrio, & Lekka. (2012). Addressing cloud computing security issues. Future Gener. Comput. Syst. 28 (3) , 583-592.