RESEARCH ARTICLE OPEN ACCESS

A Survey on Cloud Computing Security and Solutions

N. Sugavaneswaran, D.Saravanan
Assistant Professor
Department of Computer Science
Srimad Andavan Arts and Science College (Autonomous), Trichy-5
TamilNadu – India

ABSTRACT
Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, thus infecting the entire cloud and affects many customers who are sharing the infected cloud. This paper firstly lists the parameters that affect the security of the cloud then it explores the cloud security issues and problems faced by cloud service provider and cloud service consumer such as data, privacy, and infected application and security issues. It also discuss some tips for tackling these issues and problems.
Keywords:—Data Security, Data Correctness, Data Integrity, Threats.

I. INTRODUCTION

Key to the definition of cloud computing is the "cloud" itself. For our purposes, the cloud is a large group of interconnected computers. These computers can be personal computers or network servers; they can be public or private. Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels.

Many companies developing and offering cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. In fact, many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as AMAZON, Google, IBM, Salesforce, ZOHO, rack space, MICROSOFT. It also shares necessary software's and on-demand tools for various IT Industries. Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises.

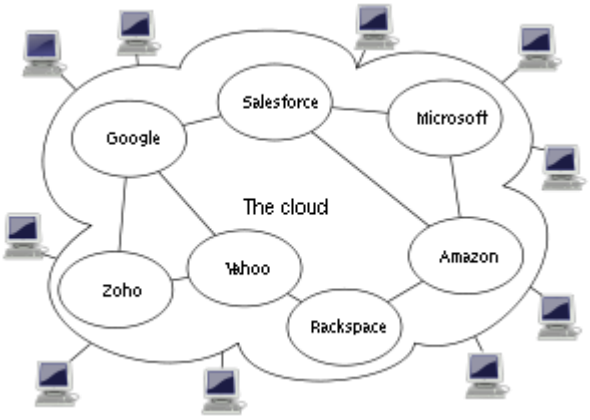

Fig. 1 Cloud computing Conceptual diagram

Clouds are primarily driven by economics- the pay-per use pricing model. While the pay-per-use pricing model is very appealing for both service providers and consumers.

II. CLOUD DEPLOYMENT MODELS

A cloud deployment model specifies how resources within the cloud are shared. There are four primary cloud deployment models.

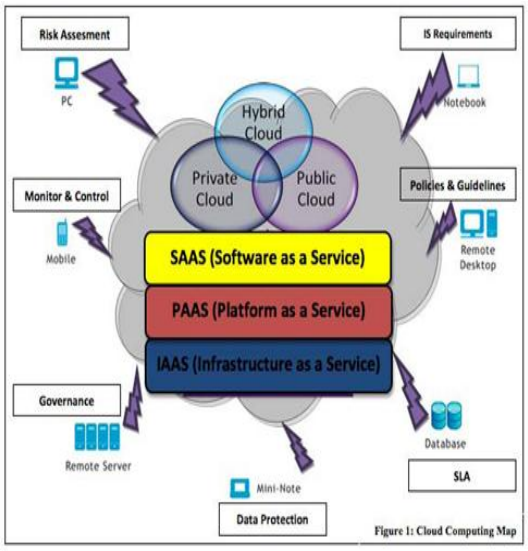

Fig 2. Cloud Depoyment Model

.Private cloud: Owned by a specific entity and normally used only by that entity or one of its customers. The underlying technology may reside on-or off-site. A private cloud offers increased security at a greater cost.

.Public cloud: Available for use by the general public. May be owned by a large organization or company offering cloud services. Because of its openness, the cloud may be less secure. A public cloud is usually the least expensive solution. .Community cloud: The cloud is shared by two or more organizations, typically with shared concerns.

.Hybrid cloud: A cloud that consists of two or more private, public, or community clouds.

3.SECURITY IN THE SPI MODEL

The cloud model provides three types of services:

•Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

•Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.

•Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

III. CLOUD SECURITY PILLERS

A. Confidentiality

The confidentiality of a system is guaranteed providing it prevents unauthorized gathering of information. In data secure systems, the "confidentiality" characteristic requires authorizations and checks to be defined, to ensure that information cannot be accessed by subjects who do not have corresponding rights. This comprises both access to stored data authorized by users and data transferred via a network. It must be possible to assign and withdraw the rights that are necessary to process this data, and checks must be implemented to enforce compliance. Cryptographic techniques and access controls based on strong authentication are normally used to protect confidentiality.

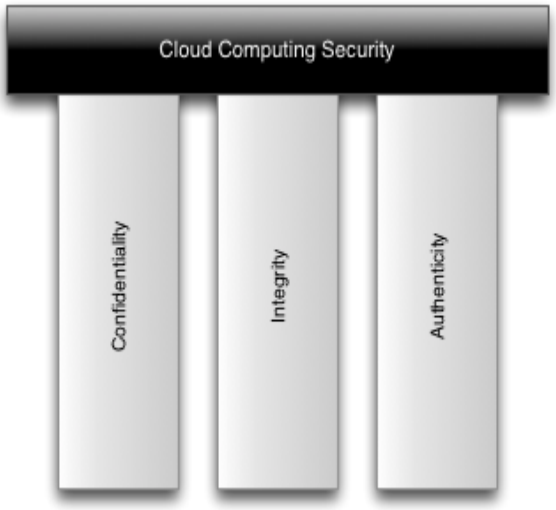

Fig 3. Pillars of Cloud Computing Security

B. Integrity

A system guarantees data integrity if it is impossible for subjects to manipulate the protected data unnoticed or in an unauthorized way. Data, messages, and information are considered to have integrity if they are trustworthy and cannot be tampered with. A cloud computing system assures the integrity of the protected data if this information cannot be modified by third parties. Data that is stored on a virtual hard drive, for instance, must be protected against unauthorized manipulation either by other participating systems used to process the information or by external attackers.

C. Authenticity

The authenticity of a subject or object is defined as its genuineness and credibility; these can be verified on the basis of its unique identity and characteristic features. Information is authentic if it can be reliably assigned to the sender, and if it can be proved that this information has not been changed since it was created and distributed. A secure technique for identifying the communication partners and mechanisms for ensuring authenticity are essential here. These mechanisms must be capable of confirming or disproving the authenticity of the protected information. Digital signatures, security tokens, or passwords, which enable the signatory of a message or the creator of a signature to be identified, are normally used to verify authenticity in a cloud computing system.

IV. ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. There are four types of issues raise while discussing security of a cloud.

A. Data Issues

B. Privacy issues

C. Infected Application

D. Security issues

A. Data Issues: sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing. Secondly, data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server. Thirdly, Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accesses able to users. Fourthly, data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

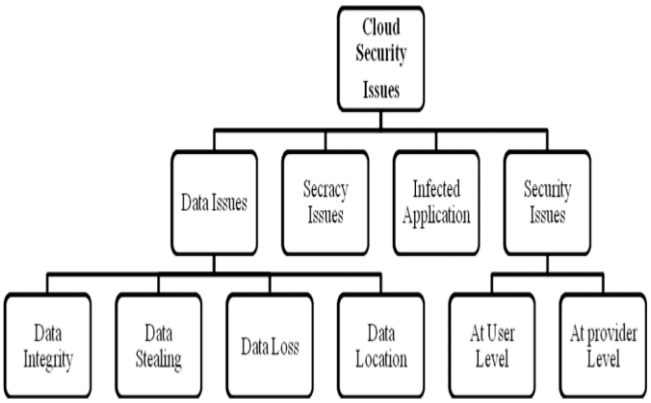

Fig 4. Cloud Security Issues

B. Privacy Issues: The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

C. Infected Application: cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

D. Security issues: cloud computing security must be done on two levels. One is on provider level and another is on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

V. CLOUD COMPUTING THREATS

Cloud computing faces just as much security threats that are currently found in the existing computing platforms,

networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms. The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the flowing seven major threats:

- 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

VI. CLOUD SECURITY BEST PRACTICES

The following are cloud security best practices to mitigate risks to cloud services:

Architect for security-as-a-service – Application deployments in the cloud involve orchestration of multiple services including automation of DNS, load balancer, network QoS, etc. Security automation falls in the same category which includes automation of firewall policies between cloud security zones, provisioning of certificates (for SSL), virtual machine system configuration, privileged accounts and log configuration. Application deployment processes that depend on security processes such as firewall policy creation, certificate provisioning, key distribution and application pen testing should be migrated to a self-service model. This approach will eliminate human touch points and will enable a security as a service scenario. Ultimately this will mitigate threats due to human errors, improve operational efficiency and embed security controls into the cloud applications.

Implement sound identity, access management architecture and practice – Scalable cloud bursting and elastic architecture will rely less on network based access controls and warrant strong user access management architecture. Cloud access control architecture should address all aspects of user and access management lifecycles for both end users and privileged users – user provisioning & deprovisioning, authentication, federation, authorization and auditing. A sound architecture will enable reusability of identity and access services for all use cases in public, private and hybrid cloud models. It is good practice to employ secure token services along with proper user and entitlement provisioning with audit trails.

Leverage APIs to automate safeguards – Any new security services should be deployed with an API (REST/SOAP) to enable automation. APIs can help automate firewall policies, configuration hardening, and access control at the time of application deployment. This can be implemented using open source tools such as puppet in conjunction with the API supplied by cloud service provider.

Digital signatures -we proposes to secure data using digital signature with RSA algorithm while data is being transferred over the Internet.

Always encrypt or mask sensitive data –Encryption techniques have been used for long time to secure sensitive data. Sending or storing encrypted data in the cloud will ensure that data is secure. However, it is true assuming that the encryption algorithms are strong. There are some well-known encryption schemes such as AES (Advanced Encryption Standard). Also, SSL technology can be used to protect data while it is in transit.

Do not rely on an IP address for authentication services – IP addresses in clouds are ephemeral in nature so you cannot solely rely on them for enforcing network access control. Employ certificates (self-signed or from a trusted CA) to enable SSL between services deployed on cloud.

Log, Log, Log – Applications should centrally log all security events that will help create an end-to-end transaction view with non-repudiation characteristics. In the event of a security incident, logs and audit trails are the only reliable data leveraged by forensic engineers to investigate and understand how an application was exploited. Clouds are elastic and logs are ephemeral hence it is critical to periodically migrate log files to a different cloud or to the enterprise data center.

Continuously monitor cloud services – Monitoring is an important function given that prevention controls may not meet all the enterprise standards. Security monitoring should leverage logs produced by cloud services, APIs and hosted cloud applications to perform security event correlation. Cloud audit (cloudaudit.org) from CSA can be leveraged towards this mission.

Verify the access controls - Set up data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by cloud service consumer. To implement access control methods for consumer side, the cloud service provider must describe and ensure that the only authorized users can access the user or consumer's data.

Control the consumer access devices - Be sure the consumer's access devices or points such as Personal Computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. The loss of an endpoint access device or access to the device by an unauthorized user can cancel even the best security protocols in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features.

Monitor the Data Access - cloud service providers have to assure about whom, when and what data is being accessed for what purpose. For example many website or server had a security complaint regarding snooping activities by many people such as listening to voice calls, reading emails and personal data etc.

Share demanded records and Verify the data deletion- If the user or consumer needs to report its compliance, then the cloud service provider will share diagrams or any other information or provide audit records to the consumer or user. Also verify the proper deletion of data from shared or reused devices. Many providers do not provide for the proper degaussing of data from drives each time the drive space is abandoned. Insist on a secure deletion process and have that process written into the contract.

Security check events - Ensure that the cloud service provider gives enough details about fulfilment of promises, break remediation and reporting contingency. These security events will describe responsibility, promises and actions of the cloud computing service provider.

VI. CONCLUSIONS

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. Also, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines. Also, some current solutions were listed in order to mitigate these threats. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

REFERENCES

[1] http://searchvirtualdatacentre.techtarget.co.uk/news/1510117/Community-cloud-Benefits-and-drawbacks.

[2] Michael glas and paul Andres, “An Oracle white paper in enterprise architecture-achieving the cloud computing vision”, CA-U.S.A, Oct 2010.

[3] Harjit Singh Lamba and Gurdev Singh, “Cloud Computing-Future Framework for e-management of NGO's”, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[4] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, “CM-Measurement Facets for Cloud Performance”, IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[5] Joachim Schaper, 2010, “Cloud Services”, 4th IEEE International Conference on DEST,Germany.

[6] A. Kundu, C. D. Banerjee, P. Saha, “ Introducing New
Services in Cloud Computing Environment ”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[7] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008,ISBN: 978-0-7695-3352-0.

[8] R. L Grossman, “The Case for Cloud Computing,” IT Professional, vol. 11(2), pp. 23-27, 2009,ISSN: 1520-9202.

[9] B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[10] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon,“On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.