ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURITY ISSUES IN CLOUD COMPUTING AND THEIR COUNTERMEASURES

Arwa Saifuddin. Ainewala*, Prajakta P.Chapke

*Final Year Student, Department of Computer Science & Engineering, H.V.P. Mandal's College of Engineering and Technology, Amravati, Maharashtra 444605 India

Assistant Professor, Department of Computer Science & Engineering, H.V.P. Mandal's College of Engineering and Technology, Amravati, Maharashtra 444605 India

ABSTRACT

Cloud computing technology is a new concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. Consumers can typically requests cloud services via a web browser or web service. Cloud computing is model which uses combine concept of "software-as-a-service" and "utility computing", provide convenient and on-demand services to requested end users. 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. This paper introduces the parameters that affect the security of the cloud then it explores the cloud security issues such as data, privacy, Infected application and security Issues. There are four cloud security problems, which are XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and also give the possible countermeasures. This also describes the security challenges in Software as a Service (SaaS) model of cloud computing.

KEYWORDS: Cloud Computing, Cloud issues, Software as a Service, Security issues and their countermeasures.

INTRODUCTION

Cloud computing is a new concept of computing technology that uses the internet and remote servers in order to maintain data and applications. Users can typically connect to clouds via web browsers or web services. Although cloud computing offers many advantages to the consumers, it also has several security issues. Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts. 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. The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to cloud it is more focused upon the frontend and the back end. The front end is the User who requires the data, whereas the backend is the numerous data storage device, server which makes the Cloud. There are three types of cloud according to their usage. They are private cloud, public cloud and hybrid cloud. There are three different delivery models that are utilized within a particular deployment model. These delivery models are the SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). These models form the core of the cloud and they exhibit certain key characteristics like on demand self-service, broad network access, resource pooling, measured service and rapid elasticity. In this paper the main area of concern is the Software as a service (SaaS) model. The Organization of the paper is as follows:

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Background and related technologies in section 2.List of parameters affecting cloud security in section 3.Security Issues in SaaS in section 4.Issues of Security and their solutions.

BACKGROUND AND RELATED TECHNOLOGIES

A. Web Service

A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It can be a user request a service from a web service or another web service request a service from the web service. Web service can be interacted using SOAP messages. The SOAP messages are generally transmitted through HTTP protocol with an XML format. In general usage, a web service provides services to clients. On the other end, a client requests a service via a particular application communicating directly to the web service or a web browser connecting to the web service via AJAX (Asynchronous JavaScript and XML). In order to protect SOAP messages from unauthorized parties to view or alter the messages, OASIS (Advancing open Standards for the information society) released a standard for web service called Web Services Security (WS-Security). WS-Security is the security mechanism for web service working in message level. It relies on digital signature and encryption techniques to ensure that messages are secured during in transit. Digital signature provides data integrity or to proof authenticity to the communications by using hash algorithm whereas encryption process offers data confidentiality to the messages. In WS-Security case, encryption method can be implemented by either symmetric or asymmetric method.

B. Cloud Computing

Cloud computing is a model for enabling on-demand network access in order to share computing resources such as network bandwidth, storage, applications, etc , that is able to be rapidly scalable with minimal service provider management. National Institute of Standard and Technology (NIST) describes cloud computing with five characteristics, three service models and four deployment models.

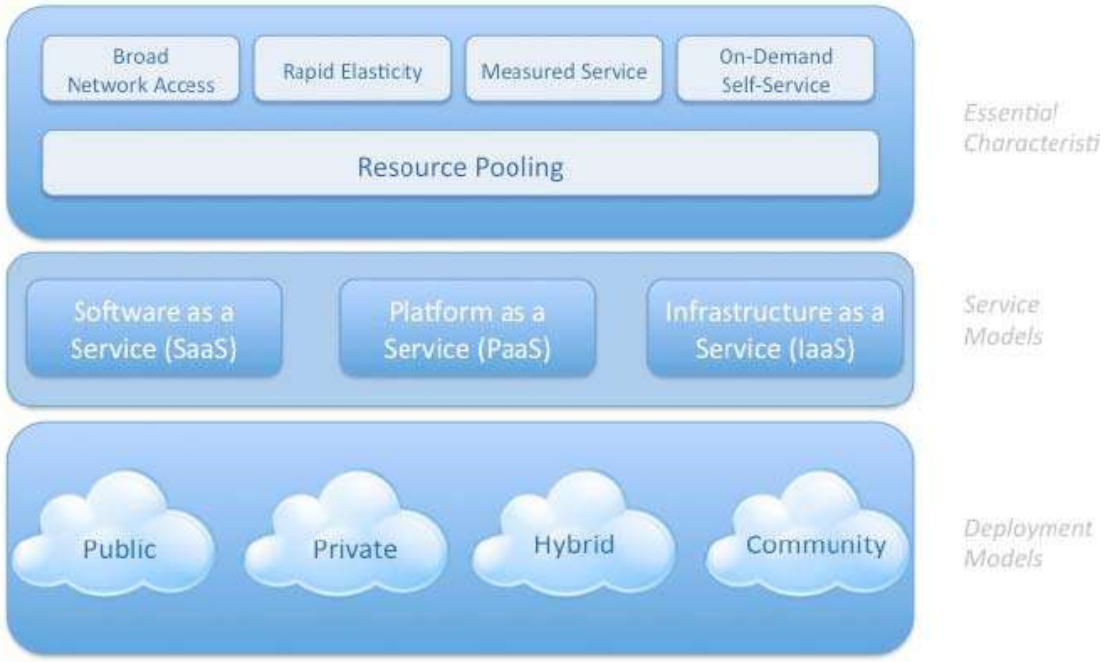

Figure 1: NIST visual model of cloud computing definition.

Five characteristics of cloud computing consist of on demand self service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self service provides automatic computing capability management to systems, without requiring human interaction. Broad network access allows heterogeneous clients, such as mobile phones, laptops, to connect to cloud systems over the network. Resource pooling in cloud systems is available as pooling resources for multiple consumers

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

which is able to dynamically assign and reassign according to consumer demand. Rapid elasticity offers rapidly and elastically provision of capabilities. It can quickly scale out and dramatically release to quickly scale in automatically in order to support consumer's systems. Measure service provides monitoring, controlling and reporting of resource usage. Three cloud service models refer to software, platform and infrastructure models. Cloud Software as a Service (SaaS) is the model of providing the capability for consumers in order to use the provider's application running on a cloud infrastructure. The applications can be accessed from a client interface such as a web browser or web service. An example of this model is "Google Apps". Cloud Platform as a Service (PaaS) allows consumers to deploy their own infrastructures or applications using programming languages and tools supported by the provider. Cloud Infrastructure as a Service (IaaS) provides processing, storage network bandwidth and other fundamental computing resources which allow customers to deploy and run operating systems or applications. Four cloud deployment models, public, private community and hybrid, are divides by considering by requirements. Public cloud is operated for the general public. The cloud system owner sells cloud services to consumers. Private cloud is made to a single organization. It can be managed by either the organization or a third party. Community cloud is the cloud infrastructure that is shared by several organizations and supports a specific community. Hybrid cloud is the composition of two or more cloud infrastructures that are bound together.

C. Denial of Service (DoS) Attack

DoS attack is the form of attack that an attacker aims to prevent legitimate users from accessing information or Services. The common type of DoS attack occurs when an attacker floods a network with excessive requests to the target server until the server is unable to provide services to normal users. There are many methods to perform a DoS attack such as SYN flood. A SYN flood exploits the TCP 3-way handshake by initialing request connections to the target server and ignoring the acknowledge (ACK) from the server. This makes the server to wait for the ACK from the attacker, wasting time and resources. Eventually, the server does not have enough resources to provide services to clients.

PARAMETERS AFFECTING CLOUD SECURITY

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling ,transaction management, load balancing, concurrency control and memory management.

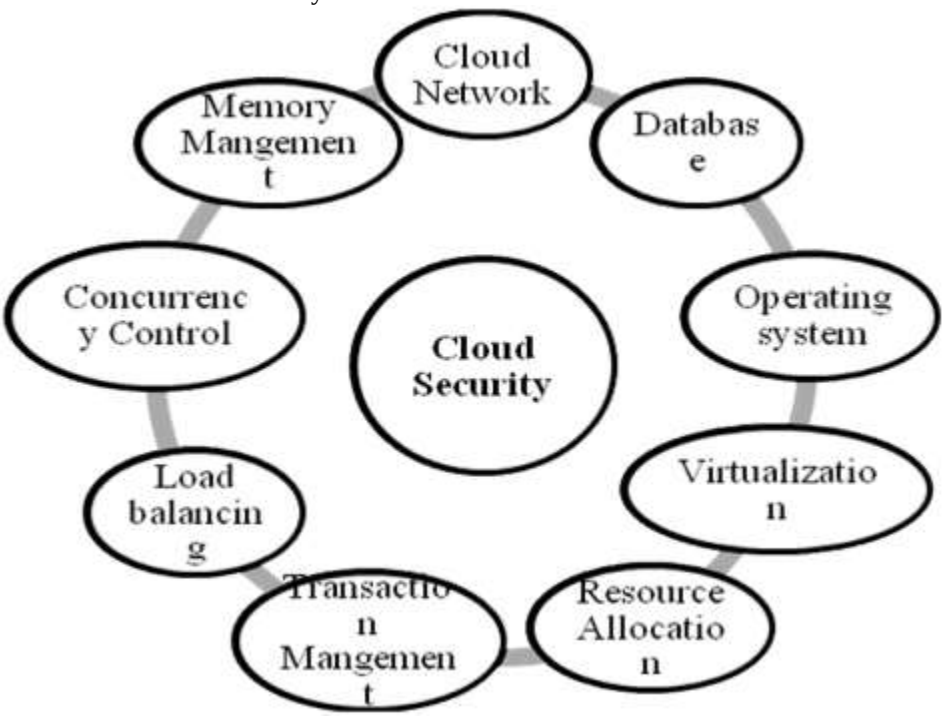

Figure 2: Parameter that affects cloud security

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

SECURITY ISSUES FACED BY 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.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues

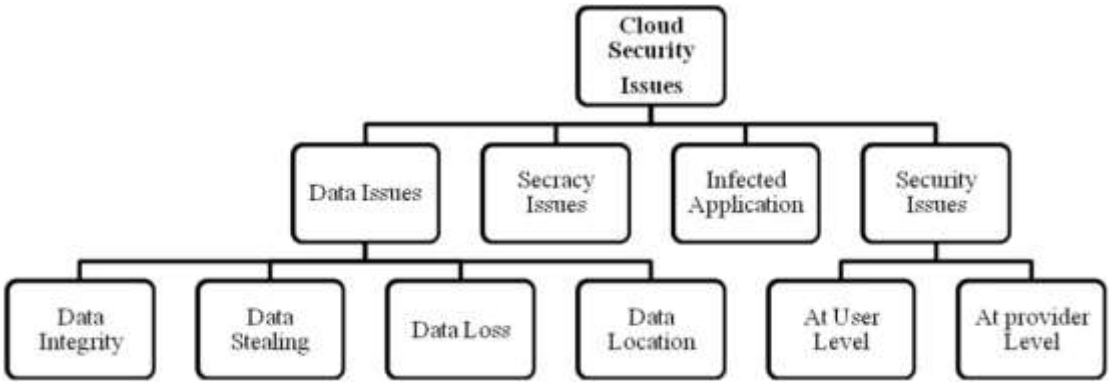

Figure 3: Cloud Security Issues

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.

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.

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

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

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.

SOLUTIONS AND TIPS TO CLOUD SECURITY ISSUES

There is need for advanced and extended technologies, concepts and methods that provide secure server which leads to a secure cloud. For this a layered framework is available that assured security in cloud computing environment. It consists of four layers as shown in figure

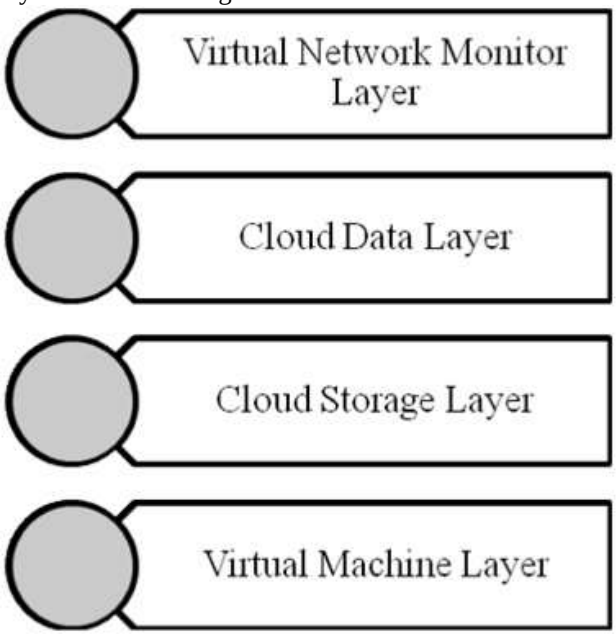

Figure 4: Layered Framework for Cloud Security

First layer is secure virtual machine layer. Second layer is cloud storage layer. This layer has a storage infrastructure which integrates resources from multiple cloud service providers to build a massive virtual storage system. Fourth layer is virtual network monitor layer. This layer combining both hardware and software solutions in virtual machines to handle problems. However, there are several groups working and interested in developing standards and security for clouds.

There are some tips and tricks that cloud security solution providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution.

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.

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

SECURITY ISSUES IN SAAS

In Software as a Service (SaaS) model, the client has to depend on the service provider for proper security

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

measures. The provider must ensure that the multiple users don't get to see each other's data. So, it becomes important to the user to ensure that right security measures are in place and also difficult to get an assurance that the application will be available when needed. While using SaaS model, the cloud customer will, by definition, be substituting new software applications for old ones. Therefore, the focus is not upon portability of applications, but on preserving or enhancing the security functionality provided by the legacy application and achieving a successful data migration. The SaaS software vendor may host the application on his own private server or deploy it on a cloud computing infrastructure service provided by a third-party provider (e.g. Amazon, Google, etc.). In the SaaS model, enterprise data is stored at the SaaS provider's data center, along with the data of other enterprises. Moreover, if the SaaS provider is leveraging a public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications. In the following section, the SaaS security issues have been categorized as traditional and new cloud specific security challenges, for sake of convenience.

Traditional Security Challenges

Although the security concerns in traditional communication systems also apply to the cloud, the use of cloud computing introduces new attack vectors that will make attacks either possible or simply easier to carry out. Some of the traditional security issues which also affect the SaaS model have been described below:

Authentication and authorization

Security is the most prioritized aspect for any form of computing, making it an obvious expectation that security issues are crucial for cloud environment as well as the cloud computing approach could be associated with having users sensitive data stored both at clients end as well as in cloud servers, identity management and authentication are very crucial in cloud computing. Verification of eligible users' credentials and protecting such credentials are part of main security issues in the cloud. A possible authentication scenario for a cloud infrastructure is illustrated in figure.

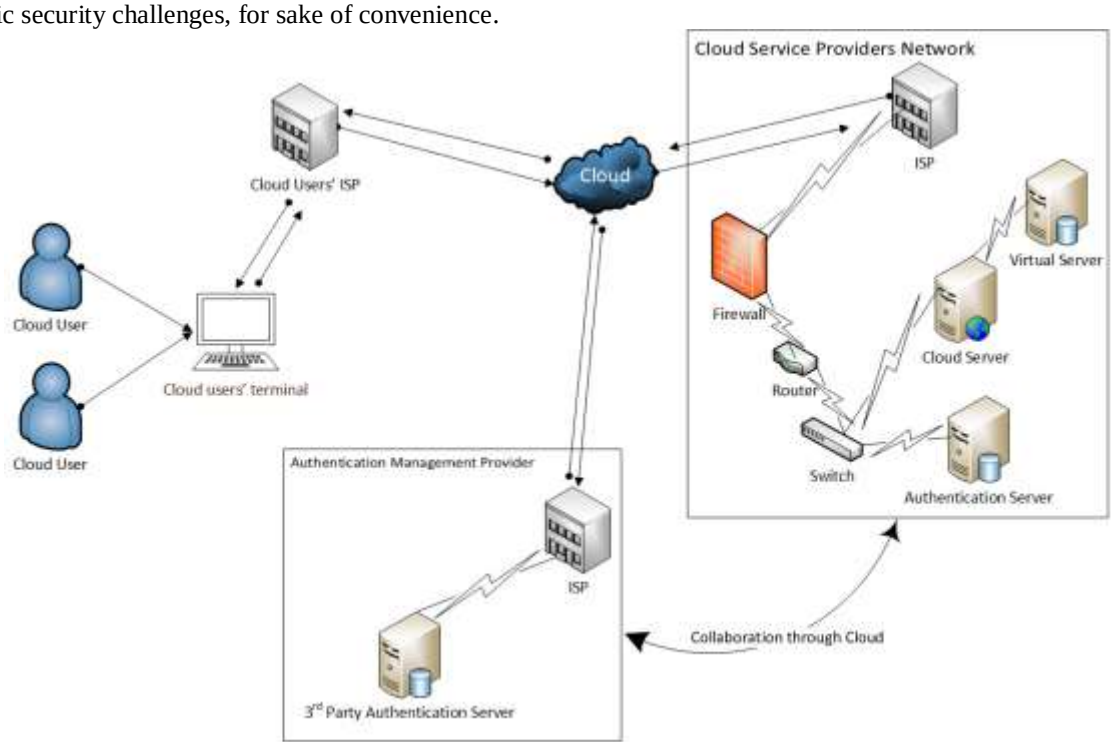

Figure 5: Authentication in the Cloud

The authentication for the cloud users can be done either by the cloud service provider or the service provider can outsource the identity management and authentication service to third party specialists. The cloud service provider is required to have collaboration with the third party authentication specialist – the collaboration between the cloud service provider and the third party authentication specialist during the authentication process of cloud users is done essentially through cloud. This feature

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

adds performance overheads and security issues to the cloud context as the message passing between third party authentication management authority and the cloud service provider as part of collaboration might essentially be done through cloud infrastructure.

Availability

The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. As its web-native nature, Cloud Computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the Cloud Computing systems. Two strategies, say hardening and redundancy, are mainly used to enhance the availability of the Cloud system or applications hosted on it. The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability of cloud service providers is also a big concern, since if the cloud service is disrupted; it affects more customers than in the traditional model. The SaaS application providers are required to ensure that the systems are running properly when needed and enterprises are provided with services around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability.

Confidentiality

Confidentiality means keeping users data secret in the Cloud systems. Cloud computing system offerings (e.g. applications and its infrastructures) are essentially public networks .Therefore, keeping all confidential data of users' secret in the Cloud is a fundamental requirement which will attract even more users consequently. Traditionally, there are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality, encrypting data before placing it in a Cloud may be even more secure than unencrypted data in a local data center.

Confidentiality in cloud system is related to the areas of intellectual property rights,

Covert channels, traffic analysis, encryption, and inference. Cloud computing involves the sharing or storage of information on remote servers owned or operated by others, while accessing through the Internet or any other connections. The entire contents of a user's storage device may be stored with a single cloud provider or with multiple cloud providers.

Cloud Specific Security Challenges

Information Security

In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, the enterprise data is stored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendor must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data.

Resource Locality

In a SaaS model of a cloud environment, the end-users use the services provided by the cloud providers without knowing exactly where the resources for such services are located, possibly in other legislative domains. This poses a potential problem when disputes happen, which is sometimes beyond the control of cloud providers. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in much enterprise architecture.

Cloud standards

To achieve interoperability among clouds and to increase their stability and security, cloud standards are needed across different standard developing organizations. For example, the current storage services by a cloud provider may be incompatible with those of other provider. In order to keep their customers, cloud providers may introduce so called ''sticky services'' which create difficulty for the users if they want to migrate from one provider to the other, e.g., Amazon's S3 is incompatible with IBM's Blue Cloud or Google storage.

Data Segregation

Multi-tenancy is one of the major characteristics of cloud computing. As a result of multitenancy, multiple users can store their data using the applications provided by SaaS. In such a situation, data of various users will reside at the same location. Intrusion of data of one user by another becomes possible in this environment. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system. A client can write a masked code and inject into the application. If the application executes this code without verification, then there is a high potential of intrusion into other's data. A SaaS model should therefore ensure a clear boundary for each

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

user's data. The boundary must be ensured not only at the physical level but also at the application level. The service should be intelligent enough to segregate the data from different users. A malicious user can use application vulnerabilities to hand- craft parameters that bypass security checks and access sensitive data of other tenants.

Data Access

Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. This organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations, wherein, some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization. The model must also be able to provide organizational boundary within the cloud because multiple organization will be deploying their business processes within a single cloud environment.

Web application security

SaaS is software deployed over the internet and/or is deployed to run behind a firewall in local area network or personal computer. The key characteristics include Network-based access to, and management of, commercially available software and managing activities from central locations rather than at each customer's site, enabling customers to access application remotely via the Web. SaaS application development may use various types of software components and frameworks. These tools can reduce time-to-market and the cost of converting a traditional on premise software product or building and deploying a new SaaS solution.

Data breaches

Since data from various users and business organizations lie together in a cloud environment, breaching into the cloud environment will potentially attack the data of all the users. Thus, the cloud becomes a high value target.

Backup

The traditional backup methods used with earlier applications and data centers that were primarily designed for web and consumer applications, are not optimally designed for the applications running in the cloud. The SaaS vendor needs to ensure that all sensitive enterprise data is regularly backed up to facilitate quick recovery in case of disasters. Also the use of strong encryption schemes to protect the backup data is recommended to prevent accidental leakage of sensitive information.

Identity management and sign-on process

Identity management (IdM) or ID management is an area that deals with identifying individuals in a system and controlling the access to the resources in that system by placing restrictions on the established identities. This area is considered as one of the biggest challenges in information security. When a SaaS provider has to know how to control who has access to what systems within the enterprise it becomes all the more challenging task. In such scenarios the provisioning and de-provisioning of the users in the cloud becomes very crucial.

THE CLOUD COMPUTING ISSUES AND THEIR COUNTERMEASURES

A. XML Signature Element Wrapping

Due to the fact that clients are typically able to connect to cloud computing via a web browser or web service, web service attacks also affect cloud computing. XML signature element wrapping is the well-known attack for web service. Although WS-Security uses XML signature in order to protect an element's name, attributes and value from unauthorized parties, it is unable to protect the positions in the document. An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value the attacker would like and moving the original element to somewhere else on the SOAP message. This technique can trick the web service to process the malicious message created by the attack. Figures 6 and 7 illustrate an example of an XML signature element wrapping attack.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

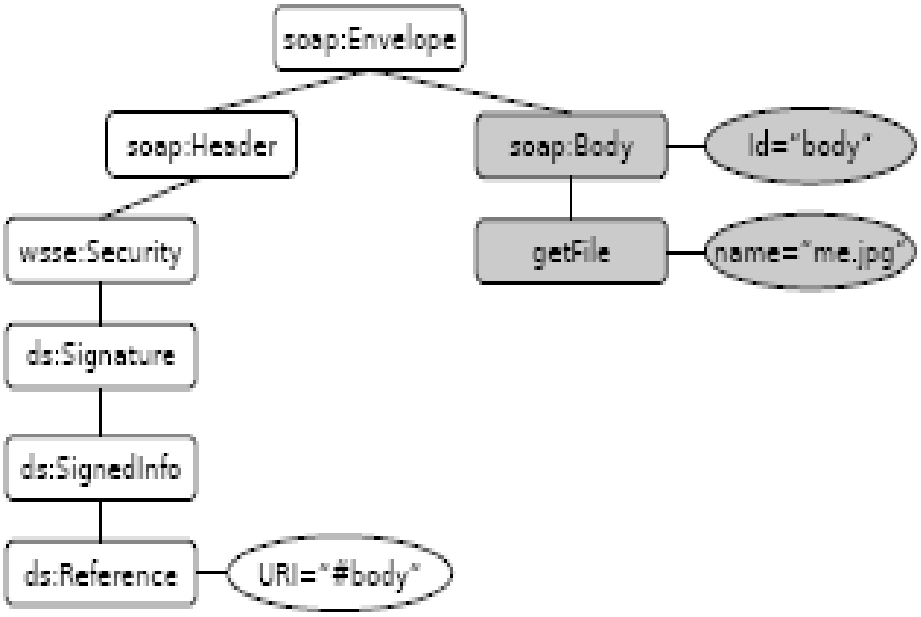

Figure 6: SOAP message with signed SOAP body.

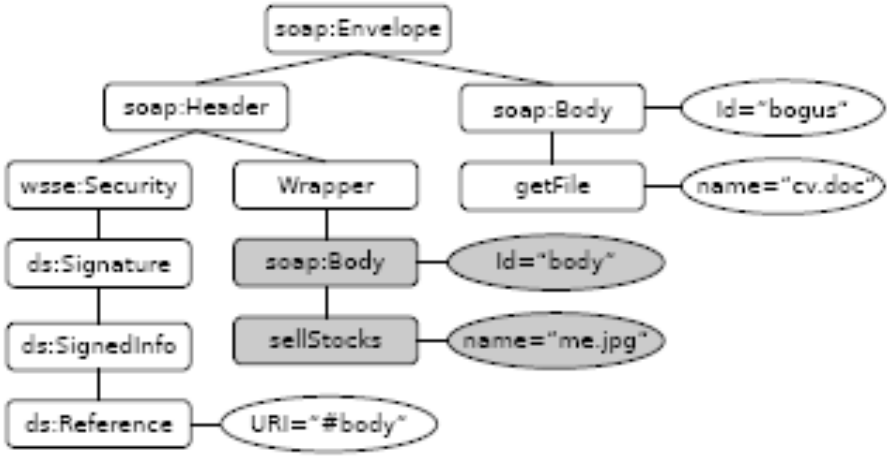

Figure 7

According to the figure 6, the client requests a picture called "me.jpg". However, if the attacker intercepts and alters the SOAP message by inserting the same element as the client but the attackers requests a document called "cv.doc" instead of the picture shown as the figure 7. After the web service receives the message, the web service will send the CV document back to the client. Another potential scenario attack may be in the case of the e-mail web service application. If an attacker intercepts the SOAP message and changes the receiver's e-mail address to the attacker's e-mail address, the web service will forward the e-mail to the attacker.

B. Browser Security

In a cloud computing system, the computational processes are completed in the cloud server whereas the client side just send a request and wait for the result. Web browser is a common method to connect to the cloud systems. Before a client can request for services on the cloud system, the client is required to authenticate himself whether he has an authority to use the cloud system or not. In the security point of

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

view, web browsers rely heavily upon SSL/TLS process. They are not able to apply WS-Security concept (XML Signature and XML Encryption) to the authentication process. As a consequence, when a web browser requests a service from the web service in a cloud system, it cannot use XML Signature to sign the client's credentials (e.g. username and password) in order to authenticate the user and XML Encryption to encrypt the SOAP message in order to protect data from unauthorized parties. The web browser has to use SSL/TLS to encrypt the credential and use SSL/TLS 4-way handshake process in order to authenticate the client. Nevertheless, SSL/TLS only supports point-to-point communications, meaning that if there is a middle tier between the client and the cloud server, such as a proxy server or firewall, the data has to be decrypted on the intermediary host. If there is an attacker sniffing packages on that host, the attacker may gain the credentials and use the credentials in order to log in to the cloud system as a valid user. In addition, SSL/TLS has been broken by Marlinspike in July 2009. Marlinspike used the technique called "Null Prefix Attack" in order to perform undetected man-in-the middle- attack attacks against SSL/TLS implementation. As a result of this, attackers are able to perform this technique in order to requests services from cloud systems without a valid authentication. It seems that SSL/TLS is still limited in its capacities as an authentication for cloud computing. The potential countermeasure for this is that the vendors that create web browsers apply WS-Security concept within their web browsers. The reason why WS-Security appears to be more suitable than SSL/TLS is WS-Security works in message level. As a result of this, web browsers are able to use XML Encryption in order to provide end-to-end encryption in SOAP messages. Unlike point-to-point encryption, end-to-end encryption does not have to be decrypted at intermediary hosts. Consequently, attackers are unable to sniff and gain plain text of SOAP messages at the intermediary hosts illustrated.

C. Cloud Malware Injection Attack

Cloud malware injection is the attack that attempts to inject a malicious service, application or even virtual machine into the cloud system depending on the cloud service models (SaaS, PaaS and IaaS). In order to perform this attack, an intruder is required to create his own malicious application, service or virtual machine instance and then the intruder has to add it to the cloud system. Once the malicious software has been added to the cloud system, the attacker had to trick the cloud system to treat the malicious software as a valid instance. If it is successful, normal users are able to request the malicious service instance, and then the malicious is executed. Another scenario of this attack might be an attacker try to upload a virus or Trojan program to the cloud system. Once the cloud system treats it as a valid service, the virus program is automatically executed and the cloud system infects the virus which can cause damage to the cloud system. In the case of the virus damages the hardware of the cloud system, other cloud instances running on the same hardware may affect to the virus program because they share the same hardware. In addition, the attacker may aim to use a virus program to attack other users on the cloud system. Once a client requests the malicious program instance, the cloud system sends the virus over to the internet to the client and then executes on the client's machine. The client's computer then is infected by the virus. The possible countermeasure for this type of attack could be performing a service instance integrity check for incoming requests. A hash value can be used to store on the original service instance's image file and compare this value with the hash values of all new service instance images. As a result of using the hash values, an attacker is required to create a valid hash value comparison in order to trick the cloud system and inject a malicious instance into the cloud system.

D. Flooding Attacks

Although data transmission between a client and the server may secure, attackers might choose to attack the cloud environment directly. One of the common characteristics of the cloud system is to provide dynamically scalable resources. It offers a benefit for variability in usage. Once there are more requests from clients, cloud system automatically scale up by starting up new service instances in order to support the clients' requirements. On the other hand, this also can be a severe vulnerability of flooding attack such as DoS, which, basically, is an action of sending a large number of nonsense requests to a certain service. When an attacker performs a DoS attack to a particular service in a cloud system, cloud computing operating system realizes the extra requests. It begins to provide more service instances in order to deal with the workload. If the attacker sends more requests, the cloud system will try to work against the requests by providing more computational resources. Eventually, the system might consume all of the resources on the cloud system and be not able to provide services to normal requests from users. Indirectly, the other service instances running on the same cloud hardware server of the target service

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

instance may also suffer from the workload caused by the DoS attack. Once the resources of the server are almost or completely depleted, there are no resources available for other services on the same server. As a consequence, the other services also might not be able to provide their services to normal users. Even though it is difficult to completely prevent DoS attacks, installing a firewall or intrusion detection system (IDS) is able to filter malicious requests from attacking the server.

CONCLUSION

Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. In this paper an overview of cloud computing service delivery model, SaaS along with the security challenges , including both the traditional and cloud specific security challenges ,associated with the model has been presented . A number of new challenges that is inherently connected to the new cloud paradigm have also been deliberated in the paper. Though there are numerous advantages in using a cloud-based system, there are yet many practical issues which have to be sorted. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency. A selection of issues of cloud computing security, XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and its potential countermeasures are introduced. It appears that the security systems of cloud computing requires an in-depth analysis because attackers may choose to exploit cloud systems via various vulnerabilities. An attacker may choose to manipulate a client's request during data transit from the client to the cloud system. This leads the attacker to gain unauthorized access to the cloud system. The attacker might try to add malicious service to the cloud system for a particular purpose which costs damage to other clients or even the could system itself. On the other hand, the attacker could attempt to stop the services on the cloud system; leading clients are unable to request services from the cloud system and the service owner has to pay extra fees to the cloud system provider for the extra requests from the attack.

REFERENCES

1. Rashmi, Dr.G.Sahoo, Dr.S.Mehfuz, "securing software as a service model of cloud computing: issues and solutions", IJCCSA ,[1,2]Birla Institute of Technology, Mesra, Ranchi, Jharkhand, India [3]Jamia Milia Islamia,Delhi,India,Vol.3, No.4, August 2013.

2. Danish Jamil and Hassan Zaki, "Security issues in cloud Computing and countermeasures", IJEST, ISSN: 0975-5462, Department of Computer Engineering, Sir Syed University of Engineering & Technology, Pakistan.

3. Prince Jain, "Security Issues and their Solution in Cloud Computing", ISSN (Online): 2229-6166, Malwa Polytechnic College Faridkot, Punjab, India.

4. Monjur Ahmed[1] and Mohammad Ashraf Hossain[2] , "cloud computing and security issues in the cloud",IJNSA, Vol.6, No.1, January 2014, [1] Senior Lecturer, Daffodil Institute of IT, Dhaka, Bangladesh.[2]Freelance IT Consultant, Dhaka, Bangladesh.