ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

Security and Privacy Concerns in Cloud Computing

Ram Kumar Singh, Aniruddha Bhattacharjya

Abstract- Cloud computing emerges as one of the hottest topic in field of information technology. Strong security always consumes IT resource and increase difficult of use. In order not only to provide enough security, but also to mitigate the IT consumption and the difficult of use in cloud computing. 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. Using cloud computing, consumers can safe cost of hardware deployment, software licenses and system maintenance. This privacy review analyses the relevant laws, technological problems and literature on Software as a Service (SaaS). The advent of web applications within powerful web browsers has meant the consumer-oriented segment of the IT industry is evolving away from the server environment to an open field client environment. This paper aims to emphasize the main security issues existing in cloud computing environments. The security issues at various levels of cloud computing environment is identified in this paper and categorized based on cloud computing architecture.

Index Terms: **Cloud Computing, Security Issues, Security Concerns of Cloud Computing, Securing Data in the Cloud, Cloud Computing Security Issues**

I. INTRODUCTION

Cloud computing is a new term in the computing world and it signals the advent of a new computing. This new paradigm is quickly developing and attracts a number of customers and vendors alike. The quick development of cloud computing is being fuelled by the emerging computing technologies which allows for reasonably priced use of computing infrastructures and mass storage capabilities. Cloud computing provides greater flexibility and agility as new applications and services can be deployed in less time. These challenges need to be understood and managed before attempting to take advantage of what the cloud has to offer. In this paper, a cloud life cycle approach is introduced. Over the past years, the servers were shared with other businesses in shared service centers (SSC), while recently they have been outsourced to third parties. Cloud computing is the next central step in this evolution of IT, as depicted in Figure 1.

A. Background

Cloud computing can mean different things to different people, and obviously the privacy and security concerns will differ between a consumer using a public cloud application, a medium-sized enterprise using a customized suite of business applications on a cloud platform, and a government agency with a private cloud for internal database sharing (Whitten, 2010). The shift of each category of user to cloud systems brings a different package of benefits and risks. Cloud computing is becoming very popular computing paradigm for network applications. In essence, the idea is to host various application servers in a virtual network environment ("cloud") and offer their use through the concept of (Web) and other services.

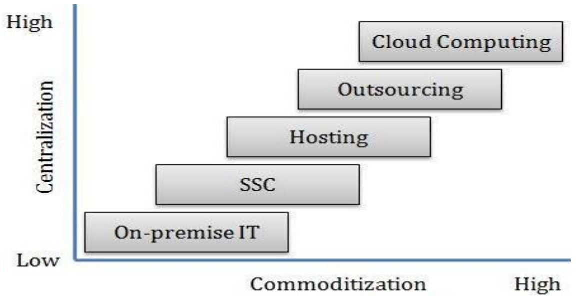

Fig 1: Paradigm shift in IT

Cloud computing is a model for enabling 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. This cloud model promotes availability and is composed of five essential characteristics**,** three service models, and four deployment models. There are still many open and interesting issues regarding cloud computing paradigm and standards are still evolving. But, it is a general opinion that security is indeed one of the most important issues. In the recent IDC report over 74% of users think that security is dominant issue for widespread use of cloud computing services:

Q: Rate the issues/challenge ascribed to the 'cloud'
(1=not significant, 5=very significant)

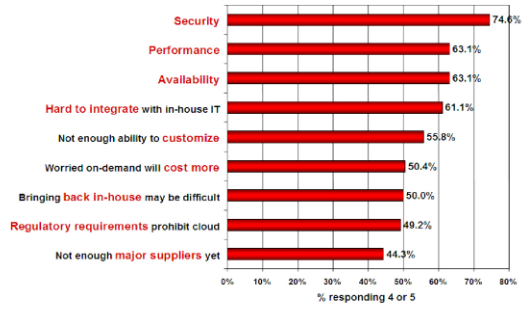

Fig 2: Importance of Security for Cloud Computing Environments

1. Causes of Problems Associated with Cloud Computing

A. Loss of control

- Data, applications, resources are located with provider
- User identity management is handled by the cloud
- User access control rules, security policies and enforcement are managed by the cloud provider
- Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

B. Lack of trust (mechanisms)

- A brief deviation from the talk
    - (But still related)
    - Trusting a third party requires taking risks
- Defining trust and risk
    - Opposite sides of the same coin (J. Camp)
    - People only trust when it pays (Economist's view)
    - Need for trust arises only in risky situations
- Defunct third party management schemes
    - Hard to balance trust and risk
    - e.g. Key Escrow (Clipper chip)
    - Is the cloud headed toward the same path?

C. Multi-tenancy

- Conflict between tenants‟ opposing goals
    - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
    - Can tenants get along together and „play nicely‟?
    - If they can't, can we isolate them?
- How to provide separation between tenants?
- Cloud Computing brings new threats
    - Multiple independent users share the same physical infrastructure
    - Thus an attacker can legitimately be in the same physical machine as the target

B.Cloud Computing Models

Cloud computing models can be broken into three basic designs, which are shown here and described below.

- Infrastructure-as-a-Service (IaaS): As the name implies, you are buying infrastructure. You own the software and are purchasing virtual power to execute as needed. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk. This model is similar to a utility company model, as you pay for what you use. An example is Amazon Web Services at http://aws. amazon.com/.

- Platform-as-a-Service (PaaS): In this model of cloud computing, the provider provides a platform for your use. Services provided by this model include all phases of the system development life cycle (SDLC) and can use application program interface (APIs), website portals, or gateway software. Buyers do need to look closely at specific solutions, because some providers do not allow software created by their customers to be moved off the provider's platform. An example of PaaS is GoogleApps.

- Software-as-a-Service (SaaS): This model is designed to provide everything and simply rent out the software to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a per use fee. Salesforce.com offers this type of service.

C. Security Concerns Of Cloud Computing

While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater level of security than the organization would have if the cloud were not used. Listed here are ten items to review when considering cloud computing.

A. Where's the data? Different countries have different requirements and controls placed on access. Because your data is in the cloud, you may not realize that the data must reside in a physical location. Your cloud provider should agree in writing to provide the level of security required for your customers.

B. Who has access? Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. If anyone doubts this, consider that in early 2009 an insider was accused of planting a logic bomb on Fanny Mae servers that, if launched, would have caused massive damage. Anyone considering using the cloud needs to look at who is managing their data and what types of controls are applied to these individuals.

C. What are your regulatory requirements? Organizations operating in the US, Canada, or the European Union have many regulatory requirements that they must abide by (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT). You must ensure that your cloud provider is able to meet these requirements and is willing to undergo certification, accreditation, and review.

D. Do you have the right to audit? This particular item is no small matter; the cloud provider should agree in writing to the terms of audit.

E. What type of training does the provider offer their employees? This is actually a rather important item, because people will always be the weakest link in security. Knowing how your provider trains their employees is an important item to review.

F. What type of data classification system does the provider use? Questions you should be concerned with here include: Is the data classified? How is your data separated from other users? Encryption should also be discussed. Is it being used while the data is at rest and in transit? You will also want to know what type of encryption is being used. As an example, there is a big difference between WEP and WPA2.

G. What are the service level agreement (SLA) terms? The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.

H. What is the long-term viability of the provider? How long has the cloud provider been in business and what is their track record. If they go out of business, what happens to your data? Will your data be returned, and if so, in what format? As an example, in 2007, online storage service MediaMax went out of business following a system administration error that deleted active customer data. The failed company left behind unhappy users and focused concerns on the reliability of cloud computing.

I. What happens if there is a security breach? If a security incident occurs, what support will you receive from the cloud provider? While many providers promote their services as being unhackable, cloud based services are an attractive target to hackers.

J. What is the disaster recovery/business continuity plan (DR/BCP)? While you may not know the physical location of your services, it is physically located somewhere. All physical locations face threats such as fire, storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising? As an example, in February 2009, Nokia's Contacts on Ovi servers crashed. The last reliable backup that Nokia could recover was dated January 23rd, meaning anything synced and stored by users between January 23rd and February 9th was lost completely.

2. Cloud Computing – Functional Architecture

This approach indicates that, in addition to various application servers, one distinctive service of a cloud is "Service Dispatcher", in this document called Applications Access Point (AAP) Server. AAP is service– level dispatcher, i.e. it distributes service requests into a cloud to individual application servers, based on types of requests and other processing parameters. Good analogy is a switch for bankcard payment transactions, distributing payment transactions to various banks in the background. In order to discover application services available in the cloud, those services must be published and must be discoverable. This is another cloud service in a cloud, in this document called Services Publishing and Dispatching (SPD) Server. This server is usually based on the standard concept of the UDDI Server, as specified by OASIS [7], i.e. it is the server used for publishing and discovery of cloud application services. AAP Server queries SPD Server to discover application services, conditions and rules of their access and invocation, and parameters that must be provided in service requests. Access to SDP and AAP servers is usually performed through Web service APIs. Clients may access cloud services through a variety of communication protocols, as shown in Figure 2. Usually, it used to be Internet and HTTP (Web access) protocol. But, with the recent advances of mobile and wireless technologies and networks the scope of communication protocols is much wider. Clients today may access a cloud using SMS messages, GPRS data channels, Wi–Fi, Bluetooth, RFID and even some proprietary communication protocols. Therefore, in order to be able to accept requests coming through different communication protocols, a cloud needs in front of it and facing various communication networks another service provider. This is communication services provider, in this document called Communication Access Point (CAP). So, simplified functional architecture of a cloud computing environment is shown in Figure 3. It includes front-end CAP, handling alternative communication protocols, after it is AAP, handling different application service requests, and distributing them to appropriate Application Servers located in a cloud and providing various application services.

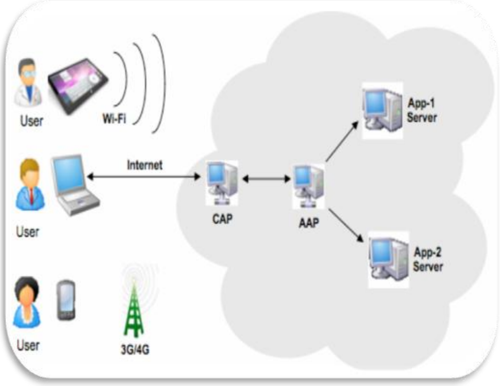

Fig 3: Simplified Functional Architecture for Cloud Computing Environments

3. Cloud Computing – Security Architecture

We designed and structured our security architecture for cloud computing based on the described functional architecture. The approach was to enhance the components of a functional architecture with additional components providing various security services. This is an extension of the SaaS concept, which is suitable for functional description of a cloud, to the new approach where cloud infrastructure is treated as a service – IaaS approach. The idea is to have several security components, which are common to all application servers and their services. Therefore, clients are provided security services by an infrastructure itself, not by individual servers. As all other components and services in a cloud, security components and services must also be transparent and generic. Transparent means that they are automatically applied, without too much of user intervention, and generic means that they are adjustable to individual users, requirements, applications, and required services. Based on those results, we have extended functional components and architecture of a could computing environment, shown in Figure 2, with the following additional security components and services:

A. Security Access Point

The first component that is needed as an extension of the functional architecture is **Security Access Point (SAP).** That is cloud server providing front-end security services. The first service, which is important before any access to a cloud is allowed, is authentication of users. Authentication must be based on open standards (for interoperability) and without any pre–arrangements (to be applicable in an open environment). We used challenge-response authentication protocol based on the FIPS 196 standard. The standard requires the use of public–key cryptography, therefore for the first, identification message in the FIPS 196 protocol, we use client's certificate. Public–key cryptographic operations on a client side are performed using PIV–compliant smart card, so client certificate is in fact stored in the card. The first component of the SAP is therefore Strong Authentication Server providing strong authentication service. Finally, after a client has been authenticated and SAML ticket has been issued, the final service before allowing him/her to access any Application Servers is authorization. SAP must verify that a client and his/her request are authorized to access internal cloud resources. Authorization is based on the XACML standard. The standard specifies two core components for enforcement of authorization policies: Policy Decision Point (PDP) and Policy Enforcement Point (PEP). Therefore, PEP Server and authorization enforcement is the final security service provided by the SAP server.

B. Security Infrastructure Servers

Three security servers are security infrastructure servers already mentioned in the previous section: IDMS Server, PDP Server, and CA Server. IDMS is X-500 compliant server that stores registration data for all local resources of a cloud. Data for users registered in the cloud may also be stored in that server. Alternatively, user registration data may be stored in IDMS servers located in users' home environments. In that case, those servers and security servers in the cloud must be federated. Federation may be accomplished as binding of X.500 directories, as Microsoft forest of domain servers (Active Directories), as distributed database, or using federation protocol for Web services. Since cloud should also support open access, even by users being registered in other clouds, binding between IDMS Servers located in cooperating clouds must be performed as a prerequisite for federated secure cloud architecture. Besides binding of IDMS servers, in case of multiple clouds, federation must also be established between authorization policies. In a single cloud PDP is the server maintaining XACML authorization policy and performing verification of access requests on behalf of a SAP server that acts as a PEP Server. So, in a federated environment, authorization policies maintained by individual PDP servers must be synchronized. Synchronization is performed using federation protocol and it covers both aspects syntactic (dictionaries) and semantic (rules) synchronization. Finally, CA is standard Certificate Authority Server. For the purpose of scaling, CA Server must be linked into a large–scale Public–Key Infrastructure (PKI). Therefore, security components and architecture for cloud computing environments are shown in the following Figure 4:

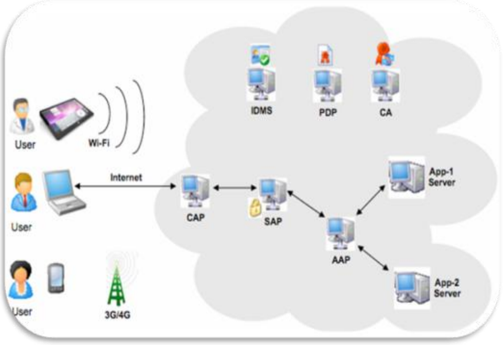

Fig 4: Security Components and Architecture for Cloud Computing Environments

C. Secure Client for Cloud Computing

The most important of them is ability to use smart cards. PIV cards are used for strong authentication to the cloud. Based on the scope of the FIPS 201 standard, PIV–compliant cards can only be used for local and strong remote authentication. PIV cards cannot support single–sign on protocol and also cannot support authorization services, since SAML token cannot be stored in a PIV applet. Since PIV applet is strictly standardized, it cannot be extended. Therefore, in order to store SAML ticket and some other security parameters, we use an additional – Security applet in our PIV card. Our cards are fully compliant to the FIPS 201 standard, since they contain standard PIV applet and support all standard PIV security services. Client performs strong authentication protocol with the SAP server by sending PIV authentication certificate to the server. That certificate is verified and if valid, further used to verify the identity of a user by consulting IDMS server. Certificate validity is verified either by using verification of signatures and expiration dates for all certificates in a certificate chain or by using On–Line Certificate Status Protocol (OCSP), depending on the configuration of the SAP server. After successful validation of the user's certificate and user's identification data, SAP performs strong authentication (challenge/response) protocol. In our system, all cryptographic responses by the client are performed by user's PIV card.

When strong authentication protocol is successfully completed, SAP server sends SAML authentication request to the PDP server. If user is authorized, PDP server will return SAML authentication response, i.e. SAML ticket. That ticket will be returned to the client. If user uses our extended PIV card, SAML ticket will be stored in the Security applet in the card. With this feature we provide mobility to users, as they can move from one station to another, accessing repetitively the cloud without performing repetitive authentication and authorization.

II .SECURING DATA IN THE CLOUD

A secure infrastructure ensures and builds confidence that the data stored is secure in providers‘side. Proper implementation of security measures is mandatory in cloud computing. The fact that application is launched over the internet makes it susceptible for security risks. Cloud providers should think beyond the customary security practices like restricted user access, password protection etc. Physical location of stored data is also vital and it‘s the responsibility of the provider to choose the right location of storage.

A. Installation and Maintenance of firewall**:** Installation of firewall and its maintenance is mandatory to ensure the protection. A firewall should be present in all external interfaces. A list of necessary port and services should be maintained. Assessment of firewall policies and rule sets and reconfiguration of router should be done in regular intervals. Build and deploy a firewall that denies access from untrusted sources or applications, and adequately logs these events. Build and deploy a firewall that restricts access from systems that have direct external connection and those which contain confidential data or configuration data.

B. Data Encryption: In public cloud the resources are shared by multiple cloud consumers and hence its providers responsibility to bestow data separation among their clients. Data encryption is one common approach the providers follow to safe guard their clients data but the question is whether the data is getting stored in encrypted format or not. Many providers follow private/public key encryption to ensure data security. To store crucial data organizations can think of private or hybrid cloud where the data will be in secure corporate firewall.

C. Data Sanitization: Data sanitization is essential for cloud security especially since the data is stored in a common platform. Sensitive data should be removed from storage devices when the particular device is moved to different location or when it‘s removed from a particular service. Data refinement is valid in case of backed up data also.

D. Certification and Auditing: Providers should allow the customers to determine the security measures followed data storage details so that the customers can ensure the data security policies of the providers. Data access to the cloud by the employees should be monitored and recorded so that the providers will be able to furnish the detailed report of who has accessed what data at a given point of time. Before moving any sensitive data to the cloud; consumers should ensure that the providers are _certified by external agencies and they follow the expected security standards and practices.

E. Backup and Recovery: In cloud computing data is stored in distributed location. The cloud customers will never be able to make out the exact storage location of their records and there comes the importance of data backup and recovery. Backup software should include public cloud APIs, enabling simple backup and recovery across major cloud storage vendors, such as Amazon S3, Nirvanix Storage Delivery Network, Rack space and others, and giving consumers flexibility in choosing a cloud storage vendor to host their data vault.

1. Security Enhancement for Cloud Computing

- Implement security practices at organizational level and make sure that the providers security plans are in alignment with the business.
- Employ and maintain secure Infrastructure in client side (secure VPN , changing default vendor provided passwords) and host side (firewalls , patch managements ,anti-virus updates)
- Ensure accurate user permissions and restricted access at both sides
- Data sanitizations at the right time

- Include clause regarding data ownership and protection of intellectual property in SLA agreement.
- Keep a log of Users who access data, time of event and event description.
- Regular auditing should be conducted
- Encryption /decryption key should be kept secured.
- Providers should verify the authenticity of their clients.
- Frequent data backup policy should be in place
- Penetration testing at regular intervals to ensure vulnerabilities is not in the cloud.

III. CLOUD COMPUTING SECURITY ISSUES

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 5 and 6 illustrate an example of an XML signature element wrapping attack.

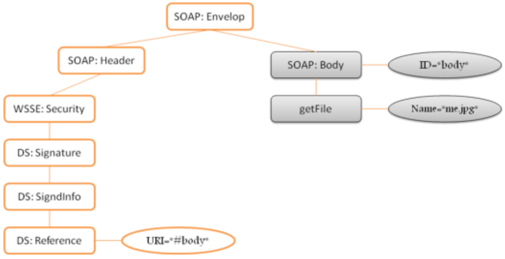

Fig 5: Proposed Model of SOAP Message with Signed SOAP Body

According to the figure 4, 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 5. 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. In 2008, Amzon's EC2, which is the public cloud computing system of Amazon, was discovered that it was vulnerable to XML signature element wrapping attack. The possible countermeasure would be using a combination of WS-Security with XML signature to sign particular element and digital certificated such as X.509 issued by trusted Certificate Authorities (CAs). Furthermore, the web service server side should create a list of elements that is used in the system and reject any message which contains unexpected messages from clients.

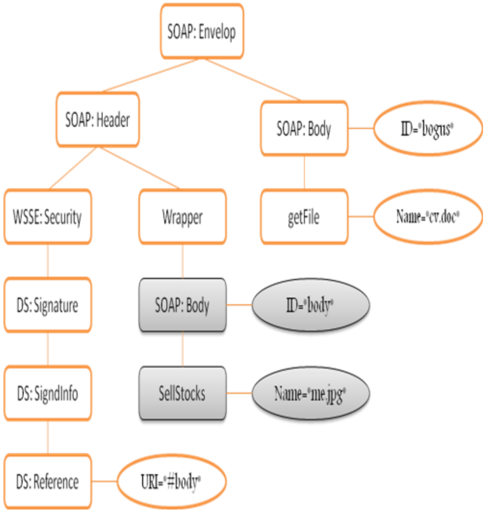

Fig 6: Proposed Model of SOAP Message with Signed SOAP Body

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 view, these days, 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.

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 IssA). 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 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. In terms of accounting point of view, DoS attack costs extra fees to the consumers. For instance, Amazon Elastic Compute Cloud (Amazon EC2) charges money to customers from the actual data transfer and resources usage. Once a service instance running on Amazon EC2 has been attacked by DoS, the extra computational resources have been used and also there are a lot of additional data transfer between the attacker and the service instance. The service instance owner has to pay extra money to Amazon for the unexpected situation. 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. Nonetheless, sometimes, IDS can mislead the administrator because it gives false alerts. It may consider normal requests as intrusive requests.

IV. CONCLUSION

There is reason to be optimistic about the gains to be had from a transition of many information services to cloud architecture. Cloud computing makes possible cost savings, scalability, and more efficient use of IT resources, among other things. However, the risks to privacy and security from cloud computing cannot be ignored. Not all these risks are new, and some of them can be mitigated through technology investment and due diligence from the client. But others are systematic in nature, and may not be solvable through unilateral innovation. In this paper, 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. The flexibility the cloud brings in has some disadvantages over privacy and security. If the providers and consumers follow the security measures discussed above cloud computing will be more secure. As and when the issues around security and privacy are elucidated cloud computing will be accepted widely.

REFERENCES

[1] Amazon Web Services. (2009) Amazon Elastic Compute Cloud (Amazon EC2). [Online]. Available: http://aws.amazon.com/ec2

[2] M. Jensen. et. al. (2009) "On Technical Security Issues in Cloud Computing" IEEE International Conference in Cloud Conouting, pp.109-116, Sep 2009.

[3] Cloud Computing Security. http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html

[4] Security in Cloud Computing Overview.http://www.halbheer.info/security/2010/01/30/cloud-security-paper-looking-for-feedback

[5] Security and Privacy in Cloud Computing, Dept. of CS at Johns Hopkins University. www.cs.jhu.edu/~ragib/sp10/cs412

[6] Acquisti, Alessandro, Allan Friedman and Rahul Teland. "Is There a Cost to Privacy Breaches? An Event Study," International Conference of Information Systems (ICIS), 2006.

[7] European Network and Information Security Agency (ENISA), "Cloud Computing: Benefits, Risks and Recommendations for Information Security," Report. November, 2009.

[8] Yared Keleta, J.H.P. Eloff, H.S. Venter, Proposing a Secure XACML Architecture Ensuring Privacy and Trust, Research in Progress Paper, University of Pretoria, 2005 <URL: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_Article.pdf>.

[9] Wayne Jansen, Timothy Grance, The NIST Guidance on security and privacy in public cloud computing, January 2011.

[10] P. Wainewright. Many Degrees of Multi-tenancy, ZDNET News and Blogs, June 16, 2008, http://blogs.zdnet.com/SAAS/?p=533

[11] S. Pearson, Taking Account of Privacy when Designing Cloud Computing Services, ICSE Workshop on Software Engineering Challenges of Cloud Computing, May 23, 2009, Vancouver, Canada

[12] Tim Mather, Subra Kumaraswamy, Shahed Latif "Cloud Security and Privacy", O'Reilly Media, 2009

[13] "Security and high availability in cloud computing environments" , IBM Global Technology Services Technical White Paper ,IBM ,June 2011