ISSN:0975-9646

G.S.Raghavendra et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1156-1159

Security Issues and Trends in Cloud Computing

Asst prof.**G.S.Raghavendra**[1], Asst prof.**D.R.N.S.Lakshmi**[2], Prof .**S.Venkateswarlu**[3]

[1]*Department of Computer Science and Engineering, R.V.R & J.C College of Engineering, Guntur*
[2]*Department of Computer Science and Engineering, R.V.R & J.C College of Engineering, Guntur*
[3]*Department of Computer Science and Engineering, K.L.University, Guntur*

***Abstract*- Cloud computing is an emerging technological solution that provides a robust and scalable information technology infrastructure to enable business agility. Cloud computing offers, continuous availability, and low cost services as major benefits, but as with most new technologies, it introduces new risks and vulnerabilities too. There are different vulnerabilities in cloud computing and various threats to cloud computing. The main obstacle which was stopping the growth of this Technology is security. In this paper importance of cloud and various types of security attacks, solutions that providers developed, cases studies and cloud computing trends in 2015-16 are presented.**

***Key words*-cloud computing security, security case studies, Algorithms**

I.INTRODUCTION

Cloud computing has become the newest technology in the computing industry. Its ability to save business cost by eliminating the need to purchase huge amounts of software licenses for every employee, reducing the need for advanced hardware, eliminating the need for companies to rent physical space to store servers and databases, and shifting the workload from local computers that has appealed to cloud computing providers such as Amazon, Google, IBM, Yahoo, Microsoft, etc.

Cloud has three advantages- it is sold on demand (typically by the minute or hour), it is scalable (a user can have as much or as little of a service as needed at any given time), and the service is fully managed by the provider. These services are categorized as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)[1] .Infrastructure as a Service provides low-level services which can be booted with a user-defined hard disk image such as Amazon EC2. In Platform as a Service, the cloud provider offers an API which can be used by an application developer to create applications on the provider's platform. Examples of PaaS include Force.com, Google Apps, etc. With Software as a Service, the vendor supplies the software product and interacts with users through a front-end portal; web-based office applications like Google Docs or Calendar are examples of SaaS[1]. Data security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data. In a traditional application deployment model, the important data of each organization continues to reside within the organization boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, the organization data is stored outside the organization boundary, at the SaaS service provider end. Therefore the service provider has to use techniques such as encryption, strong user authentication and back up for providing data security.

A. Challenges

1. Protect Data Privacy

Data privacy protection has always been an important aspect of a service level agreement for cloud storage services. Thus, the implementation of a public auditing protocol should not violate the owner's data privacy. In other words a tpa should be able to efficiently audit the cloud data storage without demanding a local copy of data or even learning the data content.

2. Support

Data Dynamics as a cloud storage service is not just a data warehouse; owners are subject to dynamically updating their data via various application purposes. The design of auditing protocol should incorporate this important feature of data dynamics in cloud computing.

II. ENVIRONMENT OF CLOUD COMPUTING

When software companies decide to migrate to cloud computing, security is a main consideration. Cloud computing consists of client and provider sides. The client side is the end users who use the cloud for their work. It provides the users with the ability to choose cloud. It is the interface that users see after they enter valid user credentials and have the ability to use the services provided by the cloud. The user side may consist of different users, laptops, tablets, cell phones, various computers.

The provider side of cloud computing is the service providers which consists of application servers and data centers etc. An application server can be Web Sphere Application Server that is a Java EJB supported technology-based application platform[2]. A data center can provide voluminous sorage for users to store data. Figure 1 is an example that shows the over view structure of Cloud Computing. The Cloud Security Alliance (CSA) give certification to cloud providers that meet the above criteria. The CSA's Trusted Cloud Initiative program was developed to help cloud providers. Cloud providers must keep users' privacy and assure the information stored on the cloud is always secure [3]. The Service-Level Agreement (SLA) between cloud providers and a customer specifies information and protocols of the service.

Figure 1.Cloud Overview Diagram

III. CASE STUDIES

They are several real-world cases where cloud computing were compromised. For each case the attack type will be briefly described.

A. XML Signature Wrapping Attack

Wrapping attacks inject fake information into the message so that a valid signature covers the unmodified element while the faked one is processed by the application logic. As a result, an attacker can perform an random Web Service request while authenticating as a legitimate user[4].

In 2011, researchers lead by Dr. Jorg Schwenk from Ruhr-University Bochum found a cryptographic hole in Amazon's EC2 and S3 services. The flaw was located in the web services security protocol and enabled attackers to trick servers into authorizing digitally signed SOAP messages that have been altered. The attackers

hijacked control interfaces used to manage cloud computing resources, which would allow attackers to create, modify, and delete machine images, and change administrative passwords and setting messages that have been altered. The attackers hijacked control interfaces used to manage cloud computing resources, which would allow attackers to create, modify, and delete machine images, and change administrative passwords and settings [4].

B. Malware Injection

In a malware-injection attack an adversary attempts to inject malicious code in to a system. This attack can appear in the form of code, scripts, active content.. When an instance of a legal user is ready to run in the cloud server, the respective service accepts the instance for computation in the cloud. The only checking done is to determine if the instance matches a legal existing service. However, the integrity of the instance is not checked. By penetrating the instance and duplicating it as if it is a valid service, the malware activity succeeds in the cloud.

Case one occurred in May 2009. The United States Treasury Department moved four public websites offline for the Bureau of Engraving and Printing after discovering malicious code was added to the parent side . The third party cloud service provider hosting the company's website was victim to an intrusion attack. As a result numerous websites (BEP and non-BEP) were affected. Roger Thompson, chief research officer for Anti-Virus Guard (AVG) Technologies, discovered malicious code was injected into the affected pages. Hackers added a tiny snippet of a virtually undetectable iFrame HTML code that redirected visitors to a Ukrainian website. IFrame (Inline Frame) is an HTML document embedded inside another HTML document on a website. From there, a variety of web-based attacks were launched using an easy-to-purchase malicious toolkit called the Eleonore Exploit Pack [6].

C. Account Hijacking

Account hijacking is usually carried out with stolen credentials. Using the stolen credentials, attackers can access sensitive information and compromise the confidentiality, integrity, and availability of the services offered. Examples of such attacks include: eavesdropping on transactions/sensitive activities, manipulation of data, returning falsified information, and redirection to illegitimate sites.

In July 2012, the hacker group, UGNazi, exploited a major flaw in Google's gmail password recovery process and AT&T's voicemail system which in turned allowed the group to access the CEO of Cloud Fare's personal gmail account. The hacker deceived AT&T'S system into redirecting the victim's cell phone to a fraudulent voicemail box. The hacker visited gmail and initiated the account recovery feature for the victim's personal email address. A voicemail message was recorded on the compromised voicemail box to sound like someone was answering the phone. A call was placed to the victim from Google, but the victim did not recognize the number and let the call go to voicemail. Google's system was tricked by the fraudulent voicemail and a temporary PIN was left (which allowed the password to be reset) in the voicemail. The hacker logged into the victim's gmail account and added his email address to the 'account recovery control' feature. The victim's linked Cloud fare account received an email informing him that the recent password was changed[5].

The victim initiated the account recovery process changed the password back. An email is sent to the hacker informing him that the victim changed passwords, but immediately the hacker changed the password. Both users continue going back and forth to get control over the account. Soon, the hacker is able to remove the victim's mobile phone and email addresses authorized for account recovery preventing the victim from\ resetting the gmail password. The team at Cloud Fare is called to investigate the situation.

A flaw in Google's account recovery system allowed two-factor authentication setup on the victim's Cloud fare account to be bypassed and the hacker now had access to the account. The victim's administrative privileges were used by the hacker to change passwords on other administrative accounts. Cloud fare's operations team suspended the victim's account, reset all Cloud Fare employee email passwords, and cleared all web mail sessions, which terminated the hacker's access to the email system [6].

Another case occurred in July 2012. Drop box, the cloud storage service, confirmed that hackers used usernames and

passwords stolen from third-party sites to access Drop box users' accounts. It was altered after users complained about Spam they were receiving to email address used only for the Drop box accounts. One stolen password was used to access an employee account that contains a file that included user email addressed. The company believed users who use the same password on multiple websites make it easier for hackers to access their accounts on other websites.

D. *Wireless Local Area Network Attack*

An authorized user's wireless local area network to perform attacks such as man-in-the-middle, accidental association, identify theft, denial of service, network injection attacks, etc.

In January 2011, German security researcher Thomas Roth used cloud computing to crack wireless networks that relied on pre-shared passphrases, such as those found in homes and small businesses. The results of the attack revealed that wireless computing that relies on the pre-shared key (WPA-PSK) system for protection is fundamentally insecure. Roth's program was run on Amazon's Elastic Cloud Computing (EC2) system. Using the massive power of Amazon's cloud the program was able to run through 400,000 possible passwords per second. It would typically cost tens of thousands of dollars to purchase the computers to run the program, but Roth claims that a typical password can be guessed by EC2 and his software in about six minutes[6] The type of EC2 computers used in the attack costs $.28 cents per minute, so $1.68 is all it took to hack into a wireless network.

IV. Fujitsu's Access control in Cloud

The most outstanding feature of a Cloud-computing platform is across-the-board virtualization. The virtualization of each system level leads to flexible system construction and operation essential to Cloud computing. In Fujitsu's Cloud services platform called the "Trusted Service Platform," the network, operating-system, and data layers feature a logical separation of computing environments through advanced virtualization technology established, for example, by METI's secure platform project. This logical separation by virtualization achieves the same level of security as physical separation of computing environments. To ensure sufficient reliability, especially in the virtual-server layer, which is the focus of virtualization, source-code reviews of the virtualization software are conducted within Fujitsu. Moreover, through the combination of virtualization and more robust authentication of Cloud-computing clients and the addition of key functions such as ones for visualizing access activities, it has become possible to detect and prevent access-control problems and attack schemes and to create more effective security measures.

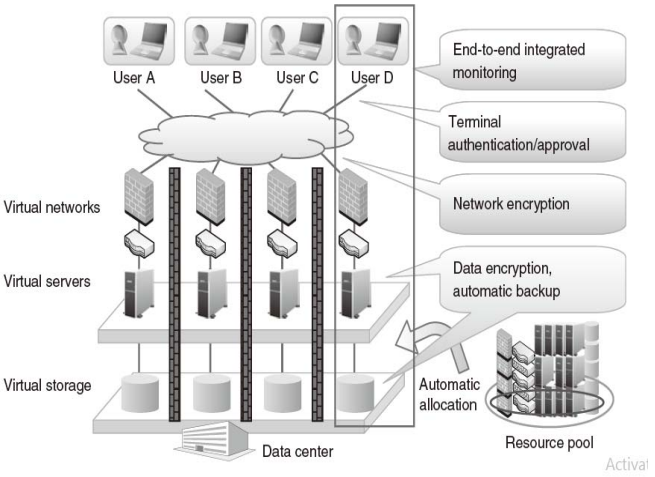

Fig 2: Access Control in Cloud

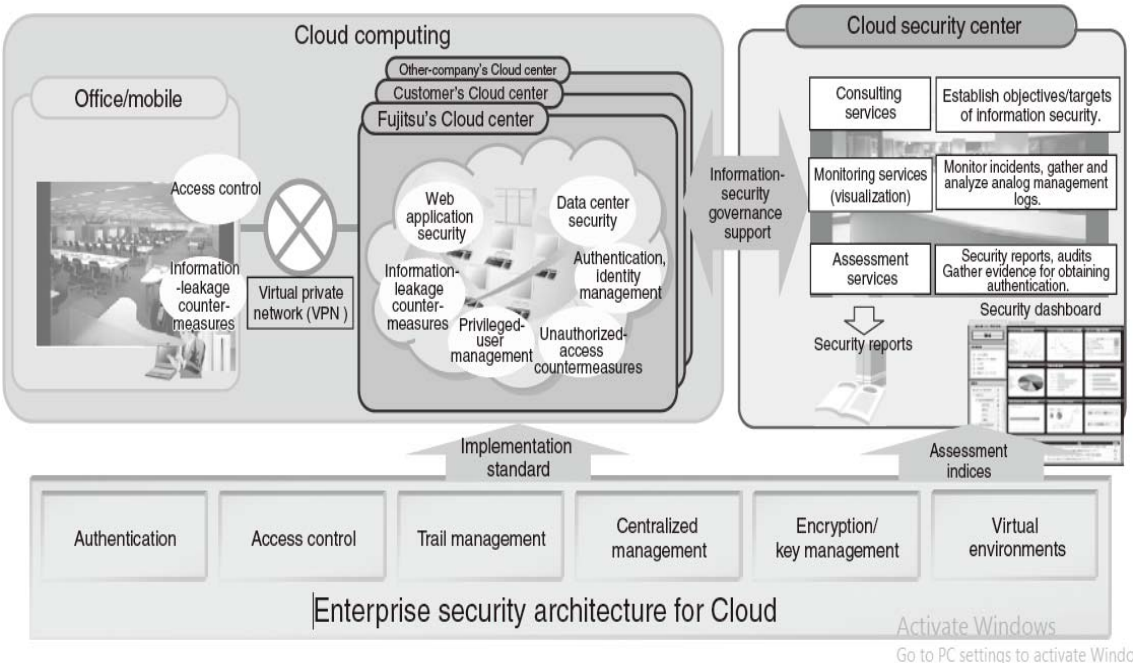

Fig 3: Enterprise Security in Cloud

V.SECURITY ALGORITHM: BLOW FISH-128 BIT

This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64 bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption.In this paper we changed block cipher from 64-bit to 128-bit for very fast processing.

Algorithm:

Divide X in to two 64-bit halves:$X_{L,}X_R$

For i=1 to i=32:

$X_L=X_L$ XOR P_i

$X_R=F(X_{L)}$ XOR X_R

Swap X_L and X_R

Next i

Swap X_L and X_R (Undo the last swap)

$X_R = X_R$ XOR P_{33}

$X_L = X_L$ XOR P_{34}

$X_L=X_L$ XOR P_i

$X_R=F(X_{L)}$ XOR X_R

Fig 4: Cloud Security

Recombine X_L and X_R

VI.CLOUD COMPUTING TRENDS 2015-2016

They are Five Cloud Computing Trends that will drive cloud strategies through 2015 and 2016.

1.Hybrid Cloud Computing

Hybrid Cloud means using a combination of public or private cloud services. As it is proved from some recent developments, hybrid cloud computing is set to become an imperative, in the form of a unified integrated cloud model, consisting both internal and external cloud platforms that can be leveraged based on specific business requirements.

Data Scientists and Cloud Experts recommend that organizations should make immediate efforts on integrating the application and dynamic data infrastructures to form a hybrid solution. [7].

II. Cloud Services Brokerage

Cloud Service Brokerage(CSB) has graduated from being an option to a key strategic factor for users and IT alike. CSB involves a service provider playing a key role in assisting the consumption of cloud computing. CSB as a trend is predicted to gather speed over the next couple of years as users choose to use cloud services, independent of IT bureaucracy. [7].

III. Cloud Friendly Decision Frameworks

Many data Scientists now agrees that Cloud Computing offers a platform of completely indispensible features and benefits, like cost-effective use-based models of IT consumption and service delivery, greater agility and lesser complexity. It also allows the IT to focus its resources on delivering new services that fuel innovation and accelerate the business. [7].

IV. Application Design Must Be Cloud-Optimized

Now the way IT Sector go about cloud computing is to basically just transfer their whole organization work-loads to the cloud. This is a good technique where the workloads need a variable supply of resources. But to fully extract the potential of cloud model to deliver standard world class applications, we need to start developing applications that are cloud-optimized [7].

V. Datacenters Need To Adopt Implementation Models of Cloud Service Providers

In a cloud computing environment, the data center and other details are handled by the service provider while the organization only concerns itself with consumption of services. But as enterprises carry on building/expanding their own data centers, they will be far better served applying the cloud computing implementation models of Cloud Service Providers to increase performance, efficiency, and agility. [7].

VII.CONCLUSION

Cloud computing security involves different areas and issues. Many security mechanisms have been developed to prevent various attacks and protect cloud computing systems. Researchers continue to develop new technologies to improve the security of cloud computing. In this paper several real world cases where companies' clouds were infiltrated by attacks are presented. Social engineering attack, XML signature wrapping attack, malware injection, account hijacking and wireless local area network attack are discussed.

The above which are discussed in this paper are major security problems which stops the growth of cloud computing so far.

REFERENCES

[1] Cloud Security Alliance, "Top threats to cloud computing", CloudSecurity Alliance, March 2010.

[2] K. Decker, "What Joni Mitchell might say about cloud computing", 2010. Available: http://decker.com/blog/2010/05/what-joni mitchell-might-sayabout-cloud-computing/

[3] D. Fisher, "Attackers using Amazon cloud to host malware", Available:http://threatpost.com/en_us/blogs/attackers-using-amazon-cloud-hostmalware-060611

[4] S. Gajek, M. Jensen, L. Lioa and J. Schneck, "Analysis of signature wrapping attacks and countermeasures", IEEE International Conference on Web Services, 2009.

[5] A. Hickey, "Researchers uncover 'massive security flaws' in Amazon cloud", http://www.crn.com/news/cloud/231901911/researchers-uncovermassive-security-flaws-in-amazon-cloud.htm

[6] Chimere Barron, Huiming Yu and Justin Zhan, "Cloud Computing Security Case Studies and Research" Available:http://thescholarship.ecu.edu/bitstream/handle/10342/3630/AsgharyKarahroudy_ecu_0600M_10476.pdf?sequence=1

[7] "The Five Strategic Cloud Computing Trends That Will Drive Your Cloud Engagement Through 2015-16" Available:http://www.regalix.com/by_regalix/insights/articles/five-strategic-cloud-computing-trends-will-drive-cloud-engagement-2015-16/