International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

Research Analysis of Cyber Attacks in Cloud Computing Domains with Suitable Solutions

Prof. Dr. G. Manoj Someswar[1]& Podugu Ravi Kumar[2]

1. Research Supervisor & Visiting Professor, Department of CSE, Bharath University, Chennai, Tamilnadu, India.
2. Research Scholar, Department of CSE, Bharath University, Chennai, Tamilnadu, India.

Abstract:

The last few years will surely enter in the history of IT Security. The period highlighted the introduction of STUXNET, the first malware able to take the control of low-level industrial devices. STUXNET was conceived to take the control of a particular device which is a centrifuge of nuclear power plants. This fact made everybody reflect on the fact that cyber-security was not anymore a matter of securing servers and software, company data and continuity, but a matter of citizen safety. In a few days, the world understood that all our critical infrastructures (electric grids, water grids, gas and oil pipelines, air traffic control systems, hospital networks etc.) are indeed vulnerable to cyber attacks. It is the need of the hour to combat all forms of cyber attacks with a professional bent of mind and by utilizing effective control measures to retaliate cyber attacks in cloud computing environments in particular.

Keywords: STUXNET; Distributed Denial of Service; Managed Service Providers (MSPs); Video Game Attacks; Host Security; Network Availibility; Health Insurance Portability and Accountability Act (HIPAA); Cyber Threat Intelligence

INTRODUCTION

The first half of 2011 has been instead characterized by a long list of massive cyber attacks against international companies. Several of those attacks were mere Distributed Denial of Service Attacks, i.e. nothing extremely complex from a technical point of view. What surprised in these attacks was the efficacy of the hacker groups in raising consensus and support in the cyber-underground by using traditional IT communication applications such as IRC and Forums. However the most significant event of 2011 was what we would call the "Video Game Attacks". [1] While there is no proof of the existence of a unique entity at the origin of these attacks, it is a matter of fact that in less than one month, three of the most important Video Game companies of the world, Sony, Sega and Epic Games, were successfully attacked. Impressing in this case was the cumulative number of the "victims" of the attacks. More than 100 million of users were subject to data theft. The data stolen included also credit card numbers, private data, user logins and password. 100 millions, more than the double of the Italy population, 1/3 of the Europe population, something less than half of the US population. In the case of the Sony PSN attack, what raised more attention was the fact that the attack was launched taking advantage of the S3 Cloud of Amazon.[2] A fact never happened before, the potential begin of a sort of WAR of Clouds, were the enormous resources of clouds are indeed used by malicious actors to attack other infrastructures and clouds. For that reason, and knowing, by looking at the most recent trends, that cloud will be the IT

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

paradigm of the next future, it would be a good idea to look at what will be the impact of cloud on the traditional ICT Security. The concept at the basis of Cloud Computing is the idea of moving from an "IT as Architecture" approach to an "IT as Service" approach. More generally, under this name can be grouped anything that involves delivering hosted services over the Internet.

A common classification identifies three categories of services made possible by the Cloud:

• Infrastructure as a Service (IaaS)
• Platform as a Service (PaaS)
• Software as a Service (SaaS)

The concept of cloud could seem no more than "traditional hosting". There are indeed at least three characteristics differentiating Cloud Computing from Service Hosting:

•A cloud service is sold on demand, typically by the minute or the hour.
•A cloud service is dynamic and elastic in the sense that the user can get as much or as little resources he needs at any given time.
• The service is fully managed by the provider.

A significant impulse to the evolution of this paradigm was given by the evolution of virtualization technologies and by the increasing access to broadband Internet connections, but it is not a mystery that the biggest driver for the success of cloud has been the economic crisis of the last years. One of the advantages of Cloud is, in fact, the possibility of enhancing the IT level of a company, while at the same time taking under control the costs of the investment (no internal infrastructure to be maintained, reduced need of IT personnel, reduced need for security personnel etc.) One of the effects of the cloud paradigm is that it forces the decoupling of IT needs from the underlying infrastructure. In other words, it inserts a sort of air gap between the company needing an IT service and the cloud provider. Under a certain perspective this fact should be an advantage, forcing people to concentrate the attention on the business processes and the objectives that an IT service should facilitate. On the other hand cloud is still too embryonic as paradigm, to have already encapsulated processes, standards, governance procedures, accommodating this approach shift. In the following, we provide a brief overview of what are the main ICT security challenges of the cloud in the coming time. We divided those challenges in two classes, the technical challenges and the high level challenges.

SECURITY CHALLENGES

From a technical point of view, the main security challenges are due to the fully distributed nature of the cloud. A non-exhaustive list of technical challenges could be the following:

• **Perimeter' Security:** with the complete decentralization of services, processes and data imposed by the cloud paradigm, it is not anymore possible to clearly separate internal and external world. How can be assured the same security level guaranteed by the traditional perimeter security (i.e., firewalls, bastion hosts etc.)?

• **Host' Security:** hosts, in cloud, are rarely under the control of the company using the cloud services, so how could be guaranteed the host security? • Security' of' virtual' environments: cloud makes large use of virtualized systems. How can be guaranteed the security of those virtualized systems is a matter of research, especially considering the possible interactions between multiple virtualized systems hosted by the same physical server.

• **Computation' security:** when using the cloud to perform processes, we are basically relying on the correctness of computations executed "somewhere" in the world, without any guarantee about the integrity of those

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

computations. There is then a strong need for mechanisms providing process integrity assurance.

• **Network availability:** this is the most critical issue the technical community will have to face in the coming time. The cloud paradigm relies on the principle of network availability. Without an Internet connection the cloud cannot deliver its services. Unfortunately it is not easy to guarantee 100% network availability, the DDOS of the last months magnified the vulnerability of the cloud under this perspective.[3] Despite their number, the presented technical challenges should not worry the IT management. In fact the technologies used to implement the modern clouds are indeed well known, largely tested, and it is reasonable to think that these security issues will quickly be solved. Since cloud is more an IT model concept than a technical revolution, the most relevant challenges deal with what we normally identify as Governance of the IT Security. In particular in this area there is a: **•Demand for greater Transparency**. Demand for Robust assurance approach of cloud suppliers. The challenges here are due to the fact that a cloud user have to deal with the way in which the third party (cloud provider) runs it's organization, its infrastructure and its "security culture". Some relevant key points, from a governance point of view, could be: • **How to select the cloud provider:** There is the need for parameters allowing to clearly identify the cloud provider that better fits with the needs of the cloud user. Possible source of benchmarking information could be Reputation, History and Sustainability. Soon will be needed to introduce parameters evaluating security standards adopted, quality of service provided, support guaranteed, for example in case of data and service transfer to other provider). • **Information Handling:** here not only the classical aspect of confidentiality, availability and integrity need to be taken into consideration from a governance point of view. Relevant issues are related also to the way in which these properties are guaranteed in case of particular situations (e.g. let consider the case in which a company is subject of authority investigations; how the cloud provider will guarantee that only the data of this company will be disclosed to the authority and not the data of other companies hosted by the same infrastructure?) • **Law Compliance:** Cloud is, as per definition, a distributed system. This mean that data and processes can be hosted potentially everywhere in the world. Different places mean different laws. How the cloud provider will address the heterogeneity of the laws to which are subjected the services it provides to third parties? • **Business continuity**: the business continuity of a company is a relevant matter in the security governance. There is the need for a rigorous definition of the processes to be run after a disaster (being that due to errors, natural catastrophes, or cyber attacks). In this context, of extreme relevance is the concept of user awareness. The case of Sony, posed a strong accent on this point: in that case, only after 5 days from the attack, the company started to inform the end users about a possible disclosure of their personal data. Again security governance needs to clearly define the ways through which awareness should be maintained. • **Transparency:** Service providers must demonstrate the existence of effective and robust security controls, assuring customers that their information is properly secured against unauthorized access, change and destruction.

• **Certification:** Cloud computing service providers will need to provide their customers

assurance that they are doing the "right" things. Independent assurance from third-party audits and/or service auditor reports should be a vital part of any assurance program.

DATA INTERPRETATION & ANALYSIS

Cyber attacks on cloud environments have almost reached the same level as attacks on traditional IT with increased adoption of cloud-based services by the enterprise, our research study shows.

Our research survey is based on an analysis of data from cloud and on-premise infrastructures of 2,200 customers. In the past year, brute force attacks on cloud environments climbed from 30% to 44% of customers and vulnerability scans increased from 27% to 44% approximately.

Brute force attacks typically involve a large number of attempts testing multiple common credential failings to find a way in, while vulnerability scans are automated attempts to find a security weakness in applications, services or protocol implementations that can be exploited.

These types of incidents have been far more likely to target on-premises environments in the past, but are now occurring at near-equivalent rates in both environments.

The key finding of the report is that attacks seem to be increasing across all environments, and, in parallel, the types of attacks in the cloud are increasingly consistent with those experienced on premise.

All these points will need, in the coming months to be clarifies, standardized and included in the companies' governance procedures. Cloud is an opportunity, but an opportunity that has to be handled in the correct way, with clear in mind the business objectives to be achieved and the security level to be guaranteed. In this sense cloud, most probably more deeply than other IT models, would require a strict collaboration between the core business management and the IT security management, to optimize the trade of between governance, assurance requirements and technical security.

Companies are increasingly using clouds to reach for business agility, lowering costs and putting pressure on internal IT teams to improve.

The question of whether a company should use public or private cloud service cannot be answered without some definitions first.

Fortunately, the Cloud Security Alliance has done a tremendous amount of good work by publishing a comprehensive guidance on cloud computing. In the guidance, a public cloud is defined as such where multiple customers, who are not related to each other, share the service. Consequently, a private cloud is the opposite of public, but with a twist. There are two types of private clouds defined: on-premise and off-premise. [4]

As the names suggest, the former is in the customers data centre, most likely operated by the IT team, while the latter are services provided to customers with infrastructure, platform or software, while ensuring that the service is not shared with other customers. There is however an important aspect associated with the "not shared" property, of which businesses need to be aware.

In most private cloud deployments a lower level of the technology stack is often shared with other customers. For example, if I subscribe to a private email system, the network or storage it uses might be shared with other private email instances.

From our experience, the main decision points that drive selection between public and

private clouds are legal concerns (mainly data privacy requirements), system architecture requirements, and cost.[5]

Many companies choose private clouds to comply with data privacy legislation. The seventh data protection principle requires companies to protect data from unauthorized and unlawful processing, as well as against accidental loss, destruction or damage. This openly worded principle can be interpreted and implemented in numerous ways. Consequently, companies may opt for a more expensive private cloud offering to reduce the risk of breaching this important principle.

We have also seen companies choosing private cloud offering – for example, Amazon's VPC and Dedicate Instances, to allow integration of the cloud architecture into their enterprise IT systems architecture. Such a decision should be driven by capabilities of the cloud provider and level of integration required.

Finally, our recommendation is for companies to research cloud providers' offers carefully and make risk assessments based on their business requirements. There is ultimately a trade-off in choosing one or another, and any choice needs to be justified.

Cyber-criminals and hackers are increasingly attacking cloud infrastructure, which they see as a "fruit-bearing jackpot" as more organizations are making use of public cloud to store their data than ever before, a security company claims.

While organizations are embracing the cloud, it is suggested that IT decision-makers shouldn't assume that data they store off-premise is harder for hackers to acquire. Our research survey shows that there has been a 45 per cent increase in application attacks against cloud deployments.

Our research survey is based on an analysis of one billion events in the IT environments of more than 3,000 of its customers between January 1st and December 31st , 2015, which revealed more than 800,000 security incidents.

One of the key findings was an increase in attack frequency on organizations that store their infrastructure in the cloud.

"This is not surprising," says the *Alert Logic Cloud Security* report. "Production workloads, applications, and valuable data are shifting to cloud environments, and so are attacks." [6]

Hackers, like everyone else, have a limited amount of time to complete their job. They want to invest their time and resources into attacks that will bear the most fruit: businesses using cloud environments are largely considered that fruit-bearing jackpot.

The pattern of attacks directly follows the increase in the number of organizations using cloud hosting from providers such as Amazon, Google and Microsoft.

Attackers are seeing this trend as well and are making concerted efforts to infiltrate businesses making use of cloud environments, just as they previously did with physical data centres.

Our research also shows that some businesses have a misconception about what security precautions they need to take when using cloud-based storage, services, and other software deployments.

Our research work suggests that many "mistakenly assume cloud providers take care of all their security needs" when in reality "security in the cloud is a shared responsibility".

Cyber-criminals are now more sophisticated, with attackers using "advanced

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

techniques" in order to infiltrate the networks of their target organization.

"Unlike in the past when hackers primarily worked alone using 'smash-n-grab' techniques, today's attackers work in groups, each member bringing his or her own expertise to the team," says the report, which argues that these techniques also allow cyber-criminals to avoid capture.

"With highly skilled players in place, these groups approach infiltration in a much more regimented way, following a defined process that enables them to evade detection and achieve their ultimate goal: turning sensitive, valuable data into profits."

However, while there has been a rise in cyber-attacks that target the cloud, Will Semple, vice president of security services for Alert Logic, warns organizations that on-premise networks are still a significant target for cyber-criminals.[7]

"While cyber-criminals are increasingly targeting cloud deployments, on-premises deployments are still being targeted at the same frequency as they always were," our research says.

"The key to protecting your critical data is being knowledgeable about how and where along the 'cyber kill chain' attackers infiltrate systems and to employ the right security tools, practices and resource investment to combat them " is the main conclusion of our research work.

Earlier this year, a new security vulnerability called Venom allowed hackers to take over whole swathes of cloud-based data centres, possibly including those of Amazon, Rackspace and Oracle.[8]

Healthcare Cyber Attacks

Our Research Survey has shown the following results in the Healthcare Domain as far as Cyber Attacks are concerned.

Even as Health Insurance Portability and Accountability Act (HIPAA) regulations take hold, a potentially rewarding vertical market for cloud adoption can be found in healthcare technology. The demand on managed service providers (MSPs) will continue to increase as the industry's need to secure data storage and cloud-based file sharing grows.

Our research work has shown that cyber thieves are costing the U.S. healthcare system an approximate $6 billion annually. Criminal cyber attacks on the healthcare industry have increased a startling 125 percent within the past 5 years, and nearly 90 percent of survey respondents reported having some sort of data breach in the past 2 years.[9]

One of the motivators for cyber thieves to hack healthcare systems is the lucrative nature of the information acquired. According to Bloomberg, thieves can use the information found in healthcare documents to apply for loans and open up lines of credit in the victim's name.[10] What separates these hackers from typical identity thieves is the medical nature of the information, which allows some to use the victim's insurance ID to seek free medical care.

Furthermore, crimes are detected much later than normal ID thefts. As Carmine Clementelli, a security expert with PFU systems, suggested, "The main reason medical records are so valuable is largely because health and insurance sector breaches take so long to detect while banking and credit fraud is detected quickly."[11]

Despite the severity of the issue, there are some simple solutions that could remedy many

of the problems. A little less than 50 percent of those surveyed said they did not have the proper personnel with relevant expertise to address the issues of data security. [12] Beyond the lack of personnel to address the issue is the portion of employees without appropriate credentials granted access to information. Sixty-five percent of employees believe they have access to sensitive data not needed to do their job. This lack of responsibility in securing sensitive data – coupled with the lack of technical knowledge on how to fix these issues – is causing millions of people to be victimized by attacks, as well as costing the U.S. government millions of dollars.[13]

Yet, the industry is not without a blueprint for attack prevention.

The damage can be greatly reduced by managing data-access permissions, making sure employees only have access to the data they need to do their jobs and by monitoring for unusual activity.

This plays right into the hand of MSPs. The government has relaxed restrictions on potential security solutions, creating a promising opportunity for MSPs to introduce cloud storage and file sharing solutions. With companies looking for solutions to their data storage and safety issues, leading MSPs can leverage their knowledge of cloud security to thrive in this progressing market.[14]

Providing these cloud based solutions will not only benefit the developers, but also provide for the common good by creating safety for people's privacy. In order to take full advantage of this opportunity as an MSP, make sure to keep up with new technologies, regulations and advancements in cyber security.[15]

The shift to Cloud Computing has allowed businesses of all types to lower their IT costs, access scalable resources and reduce on-site burden of their IT Infrastructure. More and more of them are using the cloud to manage their Enterprise Resource Planning (ERP) System. It makes considerable sense to use the advantages of the cloud to reduce the challenges of a system such as an ERP System but at the same time it introduces risks as well. ERP systems are mission critical assets in the true sense and they are highly vulnerable to cyber attacks by hackers and also by viruses and other malacious entities which will have a catastrophic effect in the long run. That is the reason why cloud security is such an urgent and growing priority in the fullest perspective.

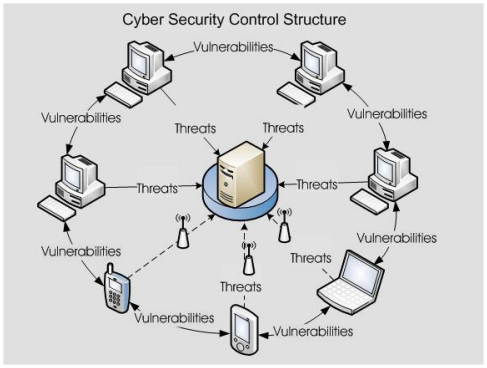
DESIGN OF CYBER SECURITY MODEL

We made an elaborate study at Global Research Academy, Hyderabad, India for the purpose of designing and developing suitable models needed for this research work. Our research work lays emphasis on the design and development of suitable cyber security models which can be implemented in an industrial setting or a company with a small, moderate or large workforce and which will enable the organization to understand the intricacies in the case of cyber attacks and the measures to be employed for combating these attacks by way of educating the workforce. This will enhance the capabilities of the users and workforce to adopt suitable methods and avoid the risks of cyber attacks in their cloud environments either in the area of application development or in data communication.

In order to understand these models, it is essential to understand the Cyber Security Control Structure (Figure 1) which will give an insight into the various vulnerabilities and

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

threats that can be encountered in a cloud environment and will help in developing ways and means to overcome such vulnerabilities in future. This will greatly serve as a risk mitigation measure if properly implemented in the real time scenario.



Copyright@Global Research Academy, Hyderabad, India

Figure 1: Cyber Security Control Structure

Copyright@Global Research Academy, Hyderabad, India

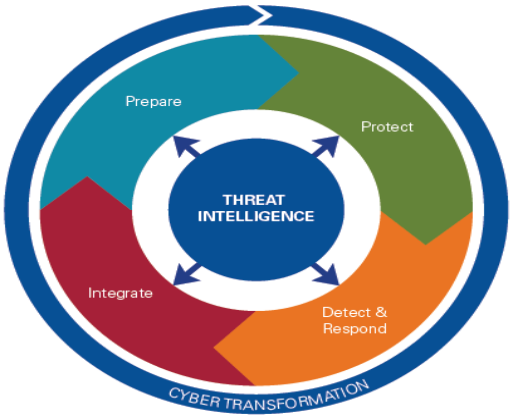
Figure 2: Cyber Security Building Blocks Pyramid

In Figure 2, the Cyber Security Building Blocks Pyramid is designed by us with a view to provide for a comprehensive understanding of the cyber attacks and how these cyber security measures provide for the right inputs to counter attack vulnerabilities at different levels which are called as Tiers. We have shown atleast 5 tiers which are as follows:

Tier 1: Personal Effectiveness Competencies
Tier 2: Academic Competencies
Tier 3: Workplace Competencies
Tier 4: Industry-Wide Technical Competencies
Tier 5: Industry-Sector Functional Areas

The above Cyber security Industry Model defines the latest skill and knowledge requirements needed by individuals whose activities impact the security of their organization's cyberspace. The model incorporates competencies identified by us and complements the Framework by including both the competencies needed by the average worker who uses the Internet or the organization's computer network as well as cyber security professionals. The model will be updated to reflect future changes to the Framework.

Figure 3 shows that companies can adopt suitable strategies intelligently with a view to recognize and understand the impact of cyber attacks in their cloud environments which can hamper their applications development and cause security breaches threatening financial and physical damages across the company's infrastructure.



Copyright@Global Research Academy, Hyderabad, India

Figure 3: Cyber Threat Intelligence

The above Design provides for Intelligent Capability to enable the Organizations to identify potential threats and vulnerabilities in order to minimize the "threat attack window" and limit the amount of time an adversary gains access to the network before they are discovered. Organizations which adopt this proposed approach will understand that "Threat Intelligence" is the mechanism that drives cyber security investment and operational risk management. The number of cyber threat intelligence professionals is on the rise and the concept of threat intelligence is now all pervasive. Our research has shown that increased awareness of cyber security threat is a positive trend and many organizations now need to concentrate on this critical issue and focus on putting in place the fundamentals of intelligence management to gain real value from threat intelligence. This will be a pre-requisite for instilling confidence in Top management and ensure that their Organization is well equipped to meet the ever increasing challenges of cyber security.

Our Research also indicates that much can be learnt from law enforcement agencies and intelligence organizations. They have recognized that intelligence-led decision making is the heart and soul of their organizational culture and operations. The same needs to be clearly implemented by other organizations both in the private sector and public sector.

SOLUTIONS

Our research work provides for 4 suitable solutions for Cyber Security:

1. Use Private Clouds: In general, companies are tempted to go for public clouds because of low costs but these types clouds are often riddled with vulnerabilities and security challenges. Private Clouds cost more but they have fewer entry points and more stringent safety measures in place. Moreover, private cloud providers are in a better position to monitor your account, enabling them to preemptively deflect attacks and minimize their impact.

2. Create Stronger Passwords: Password prediction is one of the most common and most avoidable sources of cyber security attacks. It is always recommended to change passwords frequently and adopt strategic methods when they are generated. Research has shown that the best practices include generating passwords which are atleast 8 characters long, contain no complete words, contain no references to the company or individuals and utilize a wide variety of symbols and characters which will make it difficult to the hackers to hack them.

3. Secure Data Transfer Channels: All the data that is transferred back and forth to the cloud travels through the Internet which is supposed to be most vulnerable to attacks. Therefore, it is mandatory to select secure data transfer channels for sending data and also for money transactions by encrypting the data that is sent. This has been found to be very effective in sending the data in a secure manner and avoid unwanted attacks by hackers and other vulnerabilities as such.

4. Knowledge of Software Interfaces: The use of Application Programming Interfaces (APIs) is very common by programmers, developers and other users in order to access ERP software applications on the cloud. In such cases, it is necessary to evaluate existing API for vulnerabilities and investigate ways to strengthen it or to switch to a more secure API as a better alternative.

From the above it is clear that using the cloud comes with a certain amount of risk but it also helps to avoid other common types of attacks by adopting suitable measures in order to

tackle them effectively. If the above measures are used and adopted wisely, it will be the safest and most cost effective place for any ERP system. If there is a need for the service of technical experts in order to evaluate cloud service providers, it is recommended to provide for migrating the ERP system, create ironclad protections and rely upon talent solutions provided by our research work which will fulfill the cyber security goals and objectives of the users effectively in the widest perspective.

RESULTS, CONCLUSION & FUTURE SCOPE

Research has shown that cyber attacks have been on the rise in recent times. The effect of cyber attacks in cloud is severe. The denial of service attacks on cloud data services may not only disrupt the services and keep the genuine customers out of enterprise services, but also increase the costs due to the underlying pay-as-you-go model. There is no way cloud service providers can vouch that a service request is genuine or the result of a cyber attack. Thus, the cloud service providers should not only be able to detect and prevent the cyber attacks on the services deployed on their clouds, but also should establish clear guidelines on how to resolve the disputes arising from such attacks. It is thus clear that some of the challenges related to cloud security, privacy and trust go beyond the technological solutions. We need to look at the social and legal aspects of the cloud data services.

To thwart potential cyber attacks, the cloud system should consider security, privacy, and trust as an essential requirement at the design time. However, there are a number of conflicting application requirements that require balancing acts. For example, balancing between data provenance (reveal enough information to trust the data and its source) and privacy (hide enough information not to identify individuals in the data) itself is a significant challenge in clouds. Other issues related to data security in cloud that need further research include seamless data migration among cloud providers, secured and privacy preserving big data analytics, interoperability among cloud service providers, strong user authentication, users' control of their own data including secure deletion etc.

REFERENCES

[1] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. 2012. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley Professional

[2] Chen, Y., Paxson, V., & Katz, R. H. 2010. What's new about cloud computing security. University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010), 2010-5.

[3] Fielding, R. 2000. Representational state transfer. Architectural Styles and the Design of Network-based Software Architecture, Doctoral dissertation, University of California, Irvine

[4] Fisher, S. 2007. The architecture of the apex platform, salesforce. com's platform for building on-demand applications. In *Software Engineering-Companion, 2007. ICSE 2007 Companion.* pp. 3-3.

[5] Fung, B., Wang, K., Chen, R., & Yu, P. S. 2010. Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys (CSUR)*, 42(4), No.14

[6] Halfond W. G. J., & Orso A. 2005. AMNESIA: analysis and monitoring for NEutralizing SQL-injection attacks.

In *Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering* (ASE '05). ACM, New York, NY, USA, 174-183.

[7] Hernandez, R. T. 1988. ECPA and online computer privacy. *Fed. Comm. LJ*,*41*, 17.

[8] Hunker, J., & Probst, C. W. 2011. Insiders and insider threats—an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), 4-27

[9] Iseminger, D. 1999. *Active Directory Services for Microsoft Windows 2000*. Microsoft Press.

[10] Jansen, W., & Grance, T. 2011. Guidelines on security and privacy in public cloud computing. NIST special publication, 800-144.

[11] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. 2009. On technical security issues in cloud computing. In *IEEE International Conference on Cloud Computing*, pp. 109-116

[12] Liu, D. 2012. Homomorphic encryption for database querying. Australian Provisional Patent 2012902653, 2012

[13] Liu, D., & Wang, S. 2012. Programmable order-preserving secure index for encrypted database query. In*IEEE 5th International Conference on Cloud Computing*, pp. 502-509

[14] Mahajan, M. 2007. Proof Carrying Code. *INFOCOMP Journal of Computer Science*, 6, 100-109

[15] Shacham, H., & Waters, B. 2008. Compact proofs of retrievability. In *Advances in Cryptology-ASIACRYPT*,pp. 90-107