International Journal of Advanced Scientific Technologies ,Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,March.2017

Cloud Computing Security Issues , Challenges and its Solutions in Financial Sectors

Dr. K. Sailaja,
Associate Professor,
Dept. Of MCA
MTCA,Palamner

Prof. M. Usharani,
Dept. Of MCA,
SPMVV,
Tirupati.

Abstract:- Cloud Computing is a computer model that provides services in the form of on-demand services, it's accessible for everyone, everywhere and every time , including clouds referring to the internet and the web. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. In a cloud computing environment, the entire data resides over a set of networked resources, enabling the data to be accessed through virtual machines. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is a key requirement for cloud computing combine as a robust and feasible versatile solution. Due to the ever growing interest in cloud computing, there is effort to evaluate the current trends in security. More and more finance sectors are shifting to cloud based services like Public, Private cloud computing and hybrid cloud computing. But at the same time they are concerned about security issues. Limited control over the data may suffer various security issues which include data leakage, insecure interface, sharing of resources, data availability and inside attack .In this paper, i presented main security issues, challenges and its solutions in cloud computing for financial Institutions.

Index terms:- cloud computing, on demand services, scalability, throughput, pay-per-use, public cloud, private cloud, Hybrid cloud, data leakage, insecure interface, data availability.

I.INTRODUCTION

According to U.S National Institute of Standards and Technology (NIST), ―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 cloud provider interaction. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. In such an environment users need not own the infrastructure for various computing services. In fact, they can be accessed from any computer in any part of the world. This integrates features supporting high scalability and multi tenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their performance. Moreover, cloud computing minimizes the capital expenditure. This approach is device and user-location independent. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels. Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by small and medium enterprises. Cloud adoption is increasing quickly as organizations are looking to reduce IT cost, increase agility and better support business functions. However, security of data and systems in the cloud remains a key issue and critical barrier to faster adoption of cloud services. Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by small and medium enterprises.

With the increasing preference for need based, pay-per-use technology services, cloud computing is set to become the norm, even as it redefines the way IT delivers value. Based on our interactions with global banking and financial firms, we believe that cloud adoption in the financial services industry is gaining momentum, and offers a huge potential for operational optimization. Financial institutions are developing and adopting cloud strategies within their organizations. Such strategies are being defined for adoption of clouds that combine internal data centres with private clouds. The challenges for most financial institutions are controls and security available within the cloud, as institutions are seeking transparency, auditing controls and data encryption from cloud providers. Institutions see value in the form of flexible infrastructure capacity and reduced time for resource provisioning. The adoption of the cloud is driven by services for customer relationship management, application development and email.

In this paper, i presented that how cloud computing is applicable to the financial services industry and introduced cloud computing and its characteristics and

also presented security issues, challenges that different financial services firms have faced while implementing cloud computing and its solutions.

II. LITERATURE SURVEY

Gartner in [13] recognized seven security risks that are essential to be considered before enterprises make decisions regarding the transformation into a cloud computing model [14].

These problems are as follows:

1) Authorized user access: the potential risk of exposing organizational data over an external processing platform, due to the limited physical, logical and personal controls outside the organizational boundaries.

2) Conformance to regulations: Processing data outside the organizational boundaries is still subject to accountability measures, for instance in case of auditing an external third-party space.

3) Storage space: cloud customer has no clue about the exact location of their data that requires service provider commitment to comply with privacy restrictions.

4) Data separation: clouds hold the customers' data over a shared place where data segments are not stored in sequential manner, for that a reliable and well-tested encryption schemes are needed.

5) Recovery: service providers are supposed to make it clear how they will handle disasters and failures.

6) Investigation: breach or intrusion attempts are hard to be tracked and spotted over the cloud due to the dispersion of the data and resources. While in some cases it could be impossible because of the high complexity level.

7) Long-term viability: if a rare case of service provider bankruptcy or acquisition occurs there should be a guarantee of data availability. An organization needs to be sure that it will not lose a huge amount of important data on the long-run.

In [14,15] the authors examined different security and privacy concerns related to cloud computing. They discussed and outlined the risks, their influences, and the opportunities. Adequate levels of reliability, confidentiality, and sensitive data protection are examples of many security concerns. Clouds as a computing model demonstrate a promising future; at the same time they highly require serious acts to cover their weak points. The weaknesses and problems come from unresolved issues in the existing technologies, which are used to build the cloud. Despite the origins or locations of risks and threats, the cloud security as an issue should be handled in a comprehensive manner [16,17]. Service providers seek fulfilling security requirements over the clouds, but face different challenges to guarantee high level of security. For that, authors in [18] discussed the requirement and challenges, also suggested standardization and management approaches to guide cloud engineers and users. Cloud computing as an approach introduces new risks, influences others, and magnifies some. These risks and their effect on security risks and vulnerabilities were explained in [15]. Standardizing the cloud services security is an important issue that emerged due to the increased demand and importance of clouds [19]. For instance, standardized Security Level Agreement (SLA) guarantees transparent assurance and increases the trust among cloud adopters. These standardized guarantees assist in having mutual trust, reduced risks, and better dissemination of cloud service among organizations as customers, service providers and investors.

III. ARCHITECTURE OF CLOUDCOMPUTIG

In cloud computing data storage, data transfer and many other works can be done. So we can say that those all data has to be secure. It seems that data security is main aspect of cloud computing. Cloud computing syndicate grid computing, virtualization, distributed computing, network computing etc. Fig. 1 shows the architecture of cloud computing.

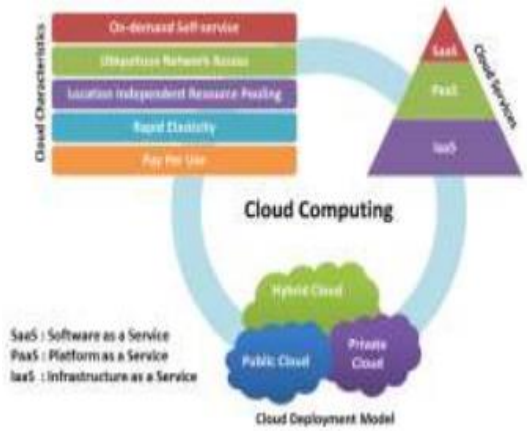

Fig.1 Architecture of cloud computing .

In simple way the cloud computing is one kind of platform which provides cloud usage to their users. Cloud computing permits an access to data and resources from anyplace at any time. But the condition is only that there is an internet access to that particular used of cloud computing. Various cloud providers are there like amazon, yahoo, Google etc. Various cloud services used in recent and past years are online storage, social networking sites, online data backup etc. As shown in figure we can say that cloud computing provides 3 kinds of services like Platform as Services (PaaS), Software as Services (SaaS), and Infrastructure as Services (IaaS). Some examples of PaaS are Google Apps, Facebook, YouTube, etc. Examples of SaaS are Microsoft Azure, Google App Engine, and Amazon Simple DB/S3. Examples of IaaS are Amazon EC2, GoGridetc

The Cloud Computing model consists of five essential characteristics, three delivery models, and four deployment models.

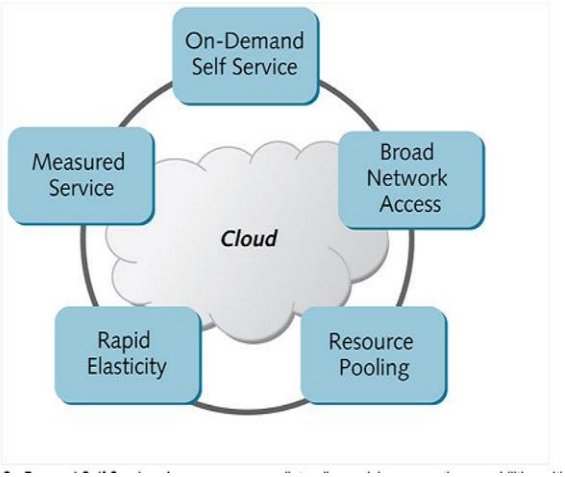

Fig.2 Characteristics of cloud computing

The key characteristics of cloud computing include the following:

a). On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

b). Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms(e.g., mobile phones, tablets, laptops and workstations).

c). Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or data centre). Examples of resources include storage, processing, memory and network bandwidth.

d). Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

e). Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

IV. SECURITY STRENGTHS IN CLOUD COMPUTING

Security is one of the biggest arguments used against the actual cloud computing system. However, cloud computing systems are often safer than mainframe systems managed at the local level, at least for small and medium companies (banks). This may list the strengths of cloud computing systems: private cloud, data centralization, multi-factor authentication, sharing security, economy of scale and others. Private cloud is probably the most important argument in favour of using cloud computing systems by organizations (banks). An interesting comparison is between the current situation of internet banking and cloud computing. Security issues were also an inhibitor to adoption of internet banking (about mid 90's), which can be considered a precursor of cloud computing. Similarly, as cloud computing providers who continue to address market concerns relating to safety, economy and convenience of cloud computing will become a commonplace like online banking and other online financial transactions today.

Figure.3.Cloud Security

Despite the conventional and economical benefits, cloud computing may not be for everyone. For example, a security and risky perspective, public cloud computing may not appeal to organizations with missions like extreme advertisement and / or highly sensitive data. However, for most, cloud computing security advantages described above along with the ability to create private cloud (which allows customers to control who is in the cloud, where data is stored, who has access etc.) should provide the necessary security guarantees to satisfy most organizations.

Centralization of data falls into two categories: preventing leak of data and monitoring. Using back-up systems is inefficient in terms of time and at high risk of data loss through the physical degradation of the backup devices that visibly reduce cloud computing efficiency while saving data and its potential.

Multi-factor Authentication: A sizable part of the cloud computing providers mainframe systems combines elements like passwords, hard token elements, biometric elements, increasing the security level. For many companies it is more profitable to resort to such a system than to implement its own cloud security system with these benefits.

Security patching: Cloud computing offers this concept and also offers the possibility of testing. There are organizations that do not have the resources to implement such a concept or that implementation would result in huge consumption of time, so the existence of the cloud system is a plus.

Economy of scale: IT services centrally managed and maintained to improve services and reduce operating costs. Cloud computing providers have the ability to invest in staff, resources and facilities that allow customers to pay only for what they use rather than invest in the resources to be managed and maintained over time. Thus, without repeating the Cloud features mentioned above, providing IT Cloud offers economies of scale, as the IT system must be scalable, fair and secure.

Security certifications: Many industries require IT systems and facilities to maintain a certain type of information security and/or privacy certification. For example, compliance with the Federal Information Security Management Act, or FISMA, is required for the federal government while Health Insurance Portability and Accountability Action (HIPAA) compliance is required for the Cloud Computing and its Challenges and Benefits in the Bank System healthcare industry. These certifications can be prohibitively expensive for smaller organizations to achieve. however, many cloud vendors provide access to systems and facilities that are already certified. Even if your business does not require a certification, it may be comforting to engage with vendors who offer them as it demonstrates mature business practices as it relates to information security.

Physical security: Reputable cloud computing vendors often host their systems in facilities that have much stronger physical security controls with meaningful certifications that many small-to-midsize companies cannot provide on their own.

Reduce cost of testing security: a SaaS provider only passes on a portion of its security testing costs. By sharing the same application as a service, you don't foot the expensive security code review and/or penetration test. Even with Platform as a Service (PaaS) where developers get to write code, there are potential cost economies of scale (particularly around use of code scanning tools that sweep source code for security weaknesses).

Pre-hardened, change control builds: this is primarily a benefit of virtualization based on Cloud Computing. Now it is the chance to start 'secure' (by your own definition) – create your Gold Image - VM and clone away. There are ways to do this today with bare-metal OS installs but frequently these require additional 3rd party tools, which are time consuming to clone or add another agent to each endpoint.

Reduce exposure through patching offline: Gold images can be kept up to date securely. Offline VMs can be conveniently patched "off" the network.

Easier to test impact of security changes: Spin up a copy of your production environment, implement a security change and test the impact at low cost, with minimal start up time. This is a big deal and removes a major barrier to implement security in production environments.

Convenience and continuous availability: Public clouds offer services that are available wherever the end user might be located. This approach enables easy access to information and accommodates the needs of users in different time zones and geographic locations. As a side benefit, collaboration booms since it is now easier than ever to access, view and modify shared documents and files. Moreover, service uptime is in most cases guaranteed, providing in that way continuous availability of resources. The various cloud vendors typically use multiple servers for maximum redundancy. In case of system failure, alternative instances are automatically spawned on other machines.

Resiliency and Redundancy: A cloud deployment is usually built on a robust architecture thus providing resiliency and redundancy to its users. The cloud offers automatic failover between hardware platforms out of the box, while disaster recovery services are also often included.

Other advantages of Cloud computing security, mention are: reliable access, automatic data backup and encryption features that are unique to each client.

V. SECURITY ISSUES IN CLOUD COMPUTING

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.A cloud is good whenever good security is provided by the servce provider. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. when a malicious user can access the cloud by act as 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 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 accessible 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.

VI. PRIVACY ISSUES

Confidentiality:- Confidentiality is very important in cloud computing. Because everything is handled by a third party. So cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. A client can encrypt data stored on a cloud to ensure privacy, but this is not possible. Most of the cloud computing is virtual machines where a client computation is executing. 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 malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

VII. SOLUTION OF SECURITY ISSUES

a) Find Key Cloud Provider : First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

b) Clear Contract : Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

c) Recovery Facilities : Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

d) Better Enterprise Infrastructure : Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber attacks.

e) Use of Data Encryption for security purpose : Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor. IT leaders must define strategy and key security elements to know where the data encryption is needed.

f) Prepare chart regarding data flow : There should be a chart regarding the flow of data. So the IT managers can have idea where the data is for all the times, where it is being stored and where it is being shared. There should be total analysis of data.

g) Cloud Computing Security : Cloud Computing Security as "Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing." Note that cloud computing security referred to here is not cloud-based security software

products such as cloud-based anti-virus, anti-spam, anti DDoS, and so on.

h) Security Issues Associated with the Cloud : There are many security issues associated with cloud computing and they can be grouped into any number of dimensions .According to Gartner , before making a choice of , users should ask the vendors for seven specific safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability.

In 2009, Forrester Research Inc. evaluated security and privacy practices of some of the leading cloud providers (such as Salesforce.com, Amazon, Google, and Micro soft) in three major aspects. They are security and privacy compliance, and legal and contractual issues. Cloud Security Alliance (CSA) is gathering solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. The CSA has identified thirteen domains of concerns on cloud computing security.

VIII. SECURITY CHALLENGES IN CLOUD COMPUTING

a). Administrative access : In case of cloud environment administrative access is done through network that enables high exposure and risk .

b). Data Transmission : In Cloud computing most of the data is not encrypted while processing that may be used by intruder for modification. Cryptographic attacks like man in middle are carried out when there is intruder between communication path which can interrupt or alter communication.

c). Virtual Machine Security : To execute number of process on limited physical servers virtualization technique is used in cloud computing. Because of dynamic nature of virtualization it is difficult to maintain security. Vulnerability was found in files shared mechanism of virtual machine that grants users of guest system that can read or write any host file , security file.

d). Network Security : Domain Name Server (DNS) attack , Sniffer Attack , Reuse of (Internet Protocol) IP network challenges are associated with network security . DNS is used to convert domain name into IP address but in DNS attack user is routed to other than original cloud. Connection between sender and receiver get rerouted through some intruder connection. Sniffer attacks are launched by applications and capture data packets flowing through network that are not encrypted. Reuse IP challenge also exist as old IP remains for some time lag into DNS cache which can be assign to new user that can alter the data .

e). Data Security : Data stored on cloud server is not encrypted by default, users must have to encrypt data before storing it on cloud therefore there are security challenges exists regarding data that resides in clouds.

f). Data Integrity : Loss of data can happen at any level in clouds. Each transaction of data follows ACID properties (Atomicity, Consistency, Isolation , Durability).

g). Data Privacy : As cloud computing involves exchange of data with users , other cloud servers there are chances of data leakage from cloud or unauthorised access to stored data. Now a day cloud servers might contains user's sensitive data so privacy is needed but not properly preserved.

h). Data Availability: Uptime is not 100 % of some cloud servers so user can't access data stored on cloud.

I). Cookie Poisoning: In application as a service cloud contents of cookie are alter to access webpages to hack user data. This security challenges are observed in in cloud computing.

IX. CONCLUSION

Cloud computing has caused more debate than many other recent technological advancements. Regardless, there has been a tremendous rise in its adoption by financial services firms over the last couple of years. Continued growth of cloud computing within the financial services industry will require vendors and firms to overcome its challenges together. Financial institutions can realize significant benefits by way of lower costs and faster time to market by proactively adopting cloud solutions without waiting for a regulatory mandate. Since major shifts in technology can take years to make an impact, the migration of core financial services applications to the cloud might take some time.

In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Financial services firms can meet the technical challenges of cloud computing and build a comprehensive and effective cloud strategy. Financial institutions are developing and adopting cloud strategies within their organizations. Such strategies are being defined for adoption of hybrid clouds that combine internal data centres with private clouds. The challenges for most financial institutions are controls and security available within the cloud, as institutions are seeking transparency, auditing controls and data encryption from cloud providers.

REFERENCES

[1] AbhinavGarg, "cloud computing for The financial services Industry"
[2] Shyam Nandan Kumar, Amit Vajpayee "A Survey on Secure Cloud: Security and Privacy in Cloud Computing", American Journal of Systems and Software, 2016, Vol. 4, No. 1, 14-26.
[3] Scott Galyk, "Cloud Security Implications for Financial Institutions", Financial managers society white paper,2015.
[4] How cloud is being used in the financial sector: survey report – march 2015.
[5] Asoke Nath et al, " Security Issues and Challenges in Cloud Computing : A Brief Overview", International Journal of Emerging Technology and Advanced Engineering, Volume 6, Issue 1, January 2016.
[6] "Secure Use of Cloud Computing in the Finance Sector", European Union Agency For Network And Information Security, December 2015.
[7] Yerneni Sushmitha et al, "A survey on cloud computing security issues", International Journal of Computer Science and Innovation Vol. 2015, no. 2.
[8] D. G. Vyawahare et al, "A Survey on Security Challenges and Solutions in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 3, March 2016.
[9] Sadhana Malgey et al, "A Review on Security Issues and their Impact on Cloud Computing Environment" , international Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 6, June 2016.
[10] Parul Chachra, " A Survey of the Existing Security Issues in Cloud Computing" , International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014.
[11] Rohit BHADAURIA et al, "a survey on security issues in Cloud computing", ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering Tome VII [2014] Fascicule 4 [October – December].
[12] Monjur Ahmed et al, "cloud computing and security issues in the Cloud", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.
[13] J. Brodkin, "Gartner: Seven Cloud-Computing Security Risks," InfoWorld, 2008.http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
[14] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, Vol. 1, Hangzhou, 23-25 March 2012, pp. 647-651.
[15] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security Privacy, Vol. 9, No. 2, 2011, pp. 50-57.http://dx.doi.org/10.1109/MSP.2010.115
[16] M. Almorsy, J. Grundy and I. Müller, "An Analysis of the Cloud Computing Security Problem," Proceedings of the2010 Asia Pacific Cloud Workshop, Australia, 30 November 2010.
[17] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" Computer, Vol. 42, No. 1, 2009, pp. 15-20. http://dx.doi.org/10.1109/MC.2009.20
[18] [18] K. Popović and Z. Hocenski, "Cloud Computing Security Issues and Challenges," Proceedings of the 33rd International Convention in MIPRO, 2010, pp. 344-349.
[19] [19] S. Ramgovind, M. Elo and E. Smith, "The Management of Security in Cloud Computing," Information Security for South Africa, Sandton, 2-4 August 2010, pp. 1-7.