International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Review Article

Security Risks in Cloud Computing: A Review

Somayyeh Jafarpour and Ammar Yousefi*

Department of Computer, Payame Noor University (PNU), Iran

Accepted 10 July 2016, Available online 15 July 2016, **Vol.6, No.4 (Aug 2016)**

Abstract

Cloud computing is a computer technology that provides computation and storage resources on the internet. However, it is plagued by security issues despite its numerous advantages. In this paper, we reviewed the current major security issues in cloud computing such as lack of control of data, lack of trust and multi-tenancy. We have also discussed cloud computing and its service and deployment models and have presented ways by which the present security issues in cloud computing can be resolved.

Keywords*: Cloud computing, storage, security risks, deployment models*

1. Introduction

Cloud computing, one of the most prominent buzzwords in the information technology (IT) world, is a large-scale parallel and distributed computing system (Dogra & Kaur, 2013). It is a collection of interconnected and virtualized computing resources that allow users to have full access to applications, software development and deployment environments, and computing infrastructure assets such as data storage and processing (Hussein & Mousa, 2012). The cloud computing model transfers the enterprise operating systems, applications, data centers, and storage servers on the cloud, thus, providing users with more flexible services that are transparent, cheaper, scalable, and highly available (Buyya *et al*, 2009).

Cloud computing provides a pool of computing resources that the users can access through the internet without having a detailed understanding of the infrastructure (Buyya *et al*, 2011; Sosinksy, 2011). Its two distinctive features include: (i) the use of computation resources is under demand, and (ii) the computational resources are assigned dynamically and accurately only when strictly required. Here, the users are not required to purchase and maintain the necessary resources including network, server, storage, application, service, etc. In cloud computing, these resources can be rapidly provisioned and released with minimal effort or interaction with the service provider (Dogra and Kaur, 2013).

However, there are many unaddressed security issues of cloud computing (Sangeetha and Saranya, 2014; Gokulan *et al*, 2014). The major security challenge with the clouds is that the owner of the data may not have control over where the data is placed. Some of the other security issues include authentication, network security, and legal requirements. In cloud computing, the impact of such issues is intensified due to multi-tenancy and resource sharing since actions from a single customer can affect all other users. With the increase in the use of mobile devices with internet accessibility including smartphones and tablets, the number of web-based malicious threats will also continue to increase (Donald *et al*, 2013). Moreover, it is important to secure data in the mobile cloud environment. Thus, the security issues in cloud environments should be addressed so as to allow a better and secure deployment of clouds throughout different industries (Ali and Rabiya, 2014). Recently, many research papers have focused on the security issues in cloud computing (Hashizume *et al*, 2013; Gonzalez *et al*, 2012; Balasubramanian and Mala, 2015). However, it remains unclear as to which are the most relevant issues in cloud computing with respect to vulnerabilities, threats, requirements and security solutions for cloud computing. Furthermore, the security aspects related to virtualization in cloud computing is a fundamental yet still underserved field of research (Fig 1).

Therefore, in this paper, we aim to discuss the various security issues in cloud computing and present their solutions. We have also described different service models and deployment models of cloud computing. We believe this review will contribute to the future research works in the area of cloud data security.

* Corresponding author: **Ammar Yousefi**, Ph: 00989133079104; Fax: 00983132630643

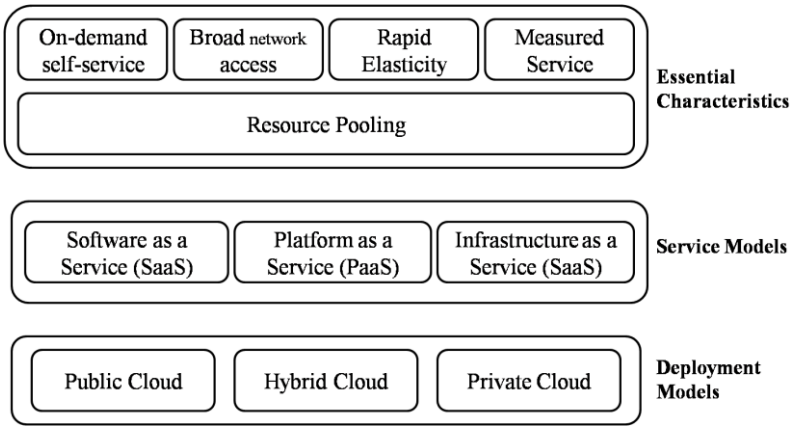

Fig. 1 Visual working definition of cloud computing (Mell and Grance, 2011; Badger *et al*, 2012; Dillon, Wu, & Chang, 2010)

2. Service models for cloud computing

Cloud computing involves the following three service models (Mell and Grance, 2011; Badger *et al*, 2012; Dillon, Wu, & Chang, 2010):

2.1 Cloud Software as a Service (SaaS)

Here, resources such as software or an application are provided to the user and can be accessed from any online device. The user is not required to manage or control the cloud infrastructure such as the network, servers, operating systems, storage, or even individual applications.

2.2 Cloud Platform as a Service (PaaS)

Here, the cloud provider provides a computing platform, tools, and development environment so that the users can build, test, and deploy web-based applications. The user cannot manage or control the cloud infrastructure but can control the deployed applications and application hosting environment configurations.

2.3 Cloud Infrastructure as a Service (IaaS)

Here, the cloud provider provides the user with processing facilities, storage facilities, networks, and other fundamental computing resources that the user can deploy and run the random software, which can include operating systems and applications. The consumer may not be required to manage or control this cloud infrastructure but can control the storage, operating systems, deployed applications, and selective networking components.

3. Deployment models for cloud computing

In cloud computing, there are three deployment models (Mell and Grance, 2011; Badger *et al*, 2012; Dillon, Wu, & Chang, 2010):

3.1 Private cloud

Here, the cloud infrastructure is exclusively used by a single organization that comprises multiple consumers (e.g., business units). The infrastructure may be owned, and managed and operated by the organization or a third party, and it may or may not exist on the organization's premises.

3.2 Public cloud

The cloud infrastructure is owned by the cloud provider and is available for open use by the general public. A public cloud can be accessed by multiple users from multiple locations since the cloud houses different services from different customers.

3.3 Hybrid cloud

Here, the cloud infrastructure is a composition of distinct cloud infrastructures (private or public) that are bound together by proprietary or standardized technology. It enables data and application portability.

4. Cloud computing architecture

The cloud computing architecture can be divided into four layers: the hardware/data center layer, the infrastructure layer, the platform layer and the application layer, as shown in Fig 2 (Zhang, Cheng, & Boutaba, 2010).

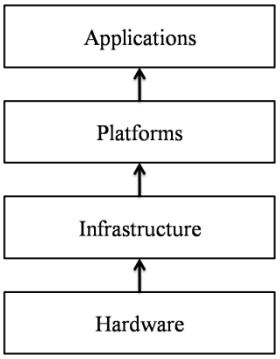

Fig. 2 Cloud Computing Architecture (Dogra and Kaur, 2013)

Compared to the traditional service hosting environments, the cloud computing has a modular architecture. Each layer is loosely coupled with the other layers, thus, allowing each layer to evolve separately.

4.1 Hardware Layer

This layer is used for managing physical resources, including physical servers, routers, switches, and power and cooling systems. It is implemented in the data centers, which contain many servers that are interconnected through switches, routers or other fabrics. This layer is associated with issues like fault tolerance, configuring hardware, traffic management, and power and cooling resource management.

4.2 Infrastructure Layer

This layer, also known as virtualization layer, creates a pool of storage and computing resources by partitioning the physical resources in the cloud by using virtualization technologies such as Xen, KVM, and VMware.

4.3 Platform Layer

This layer consists of operating systems and application frameworks so as to reduce the burden of deploying applications directly into virtual machine containers.

4.4 Application Layer

This layer is placed at the highest level of the cloud computing architecture hierarchy. It deals with applications that can be used by the users.

5. Security issues in cloud computing

Security is a key requirement in cloud computing. The data processed in different clouds such as private and public clouds are subject to different security exposures. Hence, it is important to understand the various challenges associated with cloud computing. These issues can be studied in terms of the following aspects:

5.1 Information Security

This refers to the protection of confidentiality and integrity of data and ensuring data availability (Badger *et al*, 2012). Generally, measures such as Organizational/Administrative controls, Physical Controls, and Technical Controls, are considered for data security. The Organizational/Administrative controls specify who can perform different operations, including creation, access, disclosure, transport, and destruction, on data. The Physical Controls protect the storage media and the facilities housing storage devices. The Technical Controls are used for identity and access management, encryption of data, and other data audit-handling requirements for complying with regulatory requirements.

5.2 Data Privacy

This privacy addresses the confidentiality of data for specific entities (Badger *et al*, 2012). Privacy carries legal and liability concerns, and should be viewed also as an ethical concern. Protecting privacy in any computing system is a technical challenge. In a cloud, it is difficult to provide data privacy due to the distributed nature of clouds and the consumers' lack of awareness regarding the storage of data and its accessibility.

5.3 System Integrity

Clouds require protection against intentional attacks on its functionality. A cloud has stakeholders, including consumers, providers, and a variety of administrators. It is important to partition the access rights for each of these groups while keeping malicious attacks at bay. Any lack of visibility into the mechanisms of a cloud makes it difficult for consumers to check the integrity of applications hosted by the cloud (Badger *et al*, 2012).

Cloud computing is often associated with privacy and security issues, e.g., malware injection attack, wrapping attack, and DDoS attack, because of multi-tenancy, outsourcing of application and data, and virtualization due to relocation to the clouds (Ristov *et al,* 2012; Chadha and Bajpai, 2012). With regard to the service models, the IaaS model only provides basic security such as perimeter firewall, load balancing, etc., but applications in the cloud require higher levels of security (Ali and Rabiya, 2014; Kuyoro, 2011). In the PaaS service model, the integrity of applications and proper enforcement of accurate authentication checks during data transfer should be maintained across the entire networking channels (Kuyoro, 2011). In the SaaS model, the applications are accessed using web browsers over the internet; therefore, there is a need to provide web browser security (Kuyoro, 2011). With regard to deployment models, a hybrid cloud is more secure than public and private clouds. The private cloud is more secure than the public clouds, which is considered as the least secure model (Kuyoro, 2011; Ali and Rabiya, 2014).

Most of the security problems in cloud computing can be broadly categorized into three aspects: (i) loss of control of data, (ii) lack of trust (mechanisms), and (iii) multi-tenancy**.**

5.4 Loss of control of data

The users can lose the control over data in cloud computing because of the third-party models of the cloud. The data, applications, and resources are located with the provider; the user identity management is handled by the cloud; and the user-access control rules,

security policies, and enforcement are managed by the cloud provider. The consumer has to rely on the cloud provider for data security and privacy, and availability, and monitoring and repairing of services or resources.

5.5 Lack of trust (mechanisms)

The cloud computing process is associated with certain risks due to loss of control in passing sensitive data to other organizations. However, trust relationships, including weak relationships, must exist between the user, cloud provider, and other third parties so that a service can be provided quickly (Pearson and Benameur, 2010). When a cloud service is adopted, a significant risk is introduced because of non-transparency and the globalized nature of the cloud infrastructure. Organizations that outsource key business processes in the cloud may not even know that the contractors also sub-contract and may be unaware of the identity of the sub-contracting cloud providers in this chain. Moreover, the data protection measures may not be propagated down the contracting chain, and the customers may not trust some of the subcontractors. Therefore, 'on-demand' and 'pay-as-you-go' models may be based on weak trust relationships, which involve third parties with lax data security practices. In order to provide extra capacity in real time, new providers can be added to the chain but they may not be adequately verified regarding their identity, practices, reputation, and trustworthiness.

5.6 Multi-tenancy

In cloud computing, multi-tenancy refers to sharing of resources and services to run software instances that serve multiple consumers (tenants) (OWASP-10). The main reason for cloud providers to have multi-tenancy is to reduce the costs by sharing and reusing resources among tenants. Here, the physical resources and services, as well as administrative functionality and support, can also be shared. In a multi-tenant environment, security depends more on the logical segregation (at multiple layers) rather than on the physical separation of resources. Some of the security issues due to multi-tenancy are as follows.

(i)Inadequate logical security control: Here, the security is more dependent on the logical segregation (at multiple layers) than on the physical separation of resources. Therefore, this indicates that a tenant deliberately or accidentally cannot interfere with the security control of the other tenants.
(ii)Malicious or ignorant tenants: A malicious or an ignorant tenant can become a security risk if the provider has weaker logical controls among the tenants.
(iii)Shared services can become a single point of failure: Due to the inappropriate architecture of the common services, they can easily become a single point of failure on misuse or abuse by a tenant.
(iv)Uncoordinated change controls and misconfigurations: When multiple tenants share the underlying infrastructure, all changes are required to be well-coordinated and tested.
(v)Co-mingled Tenant Data: The providers tend to store the data from multiple tenants in the same database, table-spaces, and backup tapes so as to reduce the costs. This may make the data vulnerable and can lead to data destruction, especially if the data is stored in shared media (databases, backups, and archives).
(vi)Performance Risks: Due to the involvement of multiple tenants, one tenant's heavy use of the service may impact the quality of service provided to other tenants.

Other security concerns from users can be briefly summarized as follows (Gupta *et al*, 2011):

• System failure and data availability: When storing data at remote systems owned by other parties, there may be a risk of system failures of the service provider.
• Data error: Client data should be error free on the cloud. In the case of incorrect storage strategy, the data stored in the cloud, which is remote to the client, might not be stored correctly on the storage server of the Cloud.
• Long-term availability: The users must be able to access their data whenever they need it even if the cloud computing provider is acquired and swallowed up by another company.
• Data location: The clients are unaware of the whereabouts of data or the exact location where their data is stored.
• Data segregation: The client needs to be sure that encryption must be available at all stages, which must be designed and tested by experienced professionals.
• Data recovery: Clouds provide data recovery to some extent in the case of a disaster. If a provider does not replicate the data and application infrastructure across multiple sites, then there can be a complete loss of the data.

6. Resolving Security Issues in the Cloud

The different security issues in the cloud can be resolved using different ways. The lack of control of data can be minimized but since the data applications may still need to be in the cloud, the consumers may not be able to manage taking back control. The trust mechanisms followed in cloud computing need to be improved by leveraging technology, policy, regulation, and contracts (for example, incorporating incentives). A high level of trust should be provided with respect to the degree of isolation. Multi-tenancy may be minimized by adopting a private cloud, but this may compromise with the basic reasons for using a cloud. Alternatively, virtual private cloud (VPC) can be used, but it is still not a separate system and requires strong separation. Although these provide superior isolation, the consumers' data is still stored on actual servers along with other consumers' data but are logically

separated. If the actual server fails, all the consumers' data and applications stored on it are also lost.

The present isolation facility within the clouds (i.e., virtualization) can be easily attacked (Grobauer *et al*, 2011; Afoulki *et al*, 2011, 2012), especially when the same physical hardware hosts many tenants in the cloud. Therefore, the cloud service providers should use (i) encryption scheme for data security; (ii) stringent access controls to prevent unauthorized access to the data; and (iii) scheduled data backup and safe storage of the backup media. This requires the establishment of information security system and trustworthiness between both the cloud providers and the clients (Shaikh and Haider, 2011).

6.1 Minimization of loss of control

There are many layers of access control in cloud computing (Masud *et al*, 2013). Depending on the deployment model used, some of these accesses are controlled by the provider and the rest are controlled by the consumer. However, the provider is required to manage access control procedures (to the cloud) and user authentication in all deployment models. In some cases, the consumer-side can manage its users as well as the access control. For this, there should be a high level of trust between the user and the provider with respect to security, management, and maintenance of access control policies. However, this can be difficult when numerous users from various organizations with different access control policies are involved. In consumer managed access control, the consumer retains the access control decision-making process and is required to put less trust on the provider. This model requires a pre-existing trust relationship and a pre-negotiated standard way to describe the users, resources, and access decisions between the client and provider. Furthermore, such an approach should be at least as secure as the traditional access control model.

The effect of the failures of underlying components needs to be known so that correct recovery measures can be performed. This can be resolved with an application-specific run-time monitoring and management tool (Jansen and Grance, 2011). The application logic should allow the consumer to monitor all aspects of the application as well as the data flow. The run-time monitoring and management tools should 1) aid the application user in determining the status of the cloud resources; 2) help in determining the real-time security posture of the application; 3) enable the user to move the application (or part of it) to another site; 4) enable the application user to change the application logic on the fly; and 5) provide communication facilities with cloud providers. These monitoring tools may be further enhanced or used along with other tools to provide the required degree of monitoring.

The lack of control of data can also be minimized by using services from different clouds through an intra-cloud or multi-cloud architecture (Grozev and Buyya, 2014), However, the use of different clouds may lead to certain issues such as policy incompatibility and data dependency between clouds. Moreover, it is unsafe to spread sensitive data across multiple clouds as redundancy could increase the risk of exposure of data.

6.2 Minimization of lack of trust

In cloud computing, consumers cannot dictate their requirements to the provider, i.e., the service level agreements with the provider are one-sided. In particular, the communities of interest clouds have specific security policy requirements that should be communicated to the providers so that they can ensure that the requirements can be met. Thus, a policy language can be created to convey the policies and expectations of both the parties and used in an intra-cloud environment (Someswar and Hemalatha, 2012). The consumers are also required to verify that the provided infrastructure and its purported security mechanisms meet the requirements stated in the consumer's policy. This can be achieved by using some form of reputable, independent, comparable assessment, description of security features, and assurance and risk assessment by certified third parties.

6.3 Minimization of multi-tenancy

Multi-tenancy issues present another set of risk and trust requirements (Saraswathi and Bhuvaneswari, 2013). Ideally, these issues can be reduced if multi-tenancy is minimized; however, the providers cannot be forced to allow cloud access to only a few tenants. Therefore, this can be resolved by increasing isolation between tenants and increasing trust in the tenants.

The lack of provision of proper security in local devices can allow malicious services on the cloud to attack local networks. Presently, the local host machines include desktop computers, portable laptops or mobile devices, which may not be secured given the cloud consumers' concerns about the security of the cloud provider's site. Thus, this lapse in security can compromise the cloud and its resources for other users also (Kumar *et al*, 2013). Therefore, devices used to access the cloud should have strong authentication mechanisms, should be tamper-resistant, and should have cryptographic functionality in case of traffic confidentiality.

Another concern in cloud computing is the robustness and durability of these devices. Thus, memory curtaining techniques can be used for sensitive areas of memories that contain the master keys generated by users (i.e. provides isolation of sensitive memory areas). In addition, remote attestation or Trusted Platform Module type requirements can also be used.

Conclusions

Cloud computing is a service model that provides computation and storage resources on the internet. However, despite its advantages, cloud computing involves many security issues. The cloud users have

less control over the data and applications being used. In addition, the cloud environment is more subjected to data theft, unsecured internet access, and malicious access. Therefore, efforts have been made to enforce confidentiality, privacy and integrity of data. The solutions to cloud computing security issues should be based on the identification of the problems and approaches in terms of loss of control, lack of trust, and multi-tenancy problems.

References

N. Dogra, H. Kaur,(2013), Cloud Computing Security: Issues and Concerns, *International Journal of Emerging Technology and Advanced Engineering*,3, 331-335.

M.K. Hussein, M.H. Mousa,(2012), A Light-weight Data Replication for Cloud Data Centers Environmen, *International Journal of Engineering and Innovative Technology*,1, 169-175.

R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic,(2009), Cloud computing and Emerging IT platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, *Future Generation Computer Systems*,25, 599-616.

P. Mell, T. Grance, (2011). The NIST Definition of Cloud Computing, *National Institute of Standards and Technology 7.* Retrieved 14 March 2016 from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

L. Badger, T. Grance, R. Patt-Corner, J. Voas,(2012). Cloud Computing Synopsis and Recommendations, *National Institute of Standards and Technology*. Retrieved on 14 March 2016 from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

T. Dillon, C. Wu, E. Chang,(2010), Cloud Computing: Issues and Challenges. In Proceedings of the 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA '10). *IEEE Computer Society,* Washington, USA, 27-33.

Q. Zhang, L. Cheng, R. Boutaba,(2010), Cloud computing, State of the-Art and Research Challenges, *Journal of Internet Services and Applications*,1, 7-18.

A. Gupta, P. Pande, A. Qureshi, V. Sharma,(2011), A proposed Solution: Data Availability and Error Correction in Cloud Computing, *International Journal of Computer Science and Security*,5, 405-413.

S. Ristov, M. Gusev, M. Kostoska,(2012), A new methodology for security evaluation in cloud computing, *Proceedings of the 35th International Convention*, pp. 1484-1489.

K. Chadha, A. Bajpai,(2012), Security Aspects of Cloud Computing, *International Journal of Computer Applications*,40, 43-47.

J. Ali, N.S. Rabiya,(2014), Secure Cloud – A Survey, *International Journal of Computer Science and Information Technologies*,5, 5447-5449.

S.O. Kuyoro, F. Ibikunle, O. Awodele,(2011), Cloud Computing Security Issues and Challenges, *International Journal of Computer Networks*,3, 247-255.

S. Pearson, A. Benameur,(2010), Privacy, Security and Trust Issues Arising from Cloud Computing. *2nd IEEE International Conference on Cloud Computing Technology and Science, IEEE Computer Society*, pp. 693-702.

T. Ristenpart, E. Tromer, H. Shacham, S. Savage,(2009), Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, *CCS'09*, Chicago, Illinois, USA.

N. Gonzalez, C. Miers, F. Redígolo, M. Simplício, T. Carvalho, M. Näslund, M. Pourzandi,(2012), A quantitative analysis of current security concerns and solutions for cloud computing, *Journal of Cloud Computing: Advances, Systems and Applications*,1, 11.

B. Grobauer, T. Walloschek, E. Stocker,(2011), Understanding Cloud Computing vulnerabilities, *IEEE Security Privacy*,9, 50-57.

Z. Afoulki, A. Bousquet, J. Rouzaud-Cornabas(2011), A security-aware scheduler for virtual machines on IaaS clouds, *University of Orléans*, pp. 1-12.

Afoulki Z, Bousquet A, Briffaut J, Rouzaud-Cornabas J & Toinard C, MAC protection of the OpenNebula Cloud environment, in High Performance Computing and Simulation (HPCS), 2012 International Conference on. Madrid, Spain. Pp. 85 -90. 2012.

F.B. Shaikh, S. Haider,(2011), Security Threats in Cloud Computing, *6th International Conference on Internet Technology and Secured Transactions*, Abu Dhabi, United Arab Emirates, pp. 214-219.

G.M. Someswar, Hemalatha,(2012), Identification and Implementation of Suitable Solutions to Critical Security Issues in Cloud Computing, *International Journal of Engineering Research and Development*,4, 1-10.

W. Jansen, T. Grance,(2011), Guidelines on Security and Privacy in Public Cloud Computing, *National Institute of Standards and Technology (NIST).*

N. Grozev, R. Buyya,(2014), Inter-Cloud architectures and application brokering: taxonomy and survey, *Software: Practice and Experience*,44, 369-390.

M.A.H. Masud, M.R. Islam, J. Abawajy,(2013), Security Concerns and Remedy in a Cloud based e-learning system, *Security and Privacy in Communication Networks*,127, 356-366.

M. Saraswathi, T. Bhuvaneswari,(2013), Multitenancy in Cloud Software as a Service Application, *International Journal of Advanced Research in Computer Science and Software Engineering*,3, 159-162.

S. Kumar, S.P. Singh, A.K. Singh, J. Ali,(2013), Virtualization, The Great Thing and Issues in Cloud Computing, *International Journal of Current Engineering and Technology*,3, 338-341.

R. Buyya, J. Broberg, A. Goscinsky,(2011), Cloud Computing: Principles and Paradigms, *John Wiley and Sons,* pp. 674.

B. Sosinksy,(2011), Cloud Computing Bible, *John Wiley and Sons Inc*., Hoboken.

T. Sangeetha, M. Saranya, Survey of Security Auditing Issues in Cloud Computing, *International Journal of Electrical Electronics & Computer Science Engineering*,1, 33-36.

V. Gokulan, T. Kalaikumaran, S. Karthik,(2014), Procuring Data Storage Security In Cloud Environment By Using Two Step Secure Protocol, *International Journal of Software and hardware Research in Engineering*,2, 102-107.

D.A. Cecil, O.S. Arul, L. Arockiam,(2013), Mobile Cloud Security Issues and Challenges: A Perspective, *International Journal of Engineering and Innovative Technology*,3, 401-406.

K. Hashizume, D.G. Rosado, E. Fernández-Medina, E.B. Fernandez,(2013), An analysis of security issues for cloud computing, *Journal of Internet Services and Applications*,4, 2-13.

V. Balasubramanian, T. Mala,(2015), A review on various data security issue in cloud computing environment and its solutions, *ARPN Journal of Engineering and Applied Sciences*,10, 883-889.