Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No.3, June 2017 – www.caeaccess.org

Security and Privacy Issues in Cloud Computing

Awodele O.
Comp. Sc. Dept.
Babcock University
Ogun State, Nigeria

Ominike Akpovi A.
ICT. Department
Petroleum Training Institute
Delta State, Nigeria

Adebayo A. O.
Comp. Sc. Dept.
Babcock University
Ogun State, Nigeria

Tayo O. O.
Comp. Sc. Dept.
Babcock University
Ogun State, Nigeria

ABSTRACT

Cloud computing technology has gained extensive popularity around the world and this is justified by the fact that many enterprise applications, data and services are migrating into cloud platforms. As more businesses are moving data and applications to the cloud, there are growing concerns about cloud security and privacy issues. In this research work, the key security & privacy issues (i.e. network and data security, governance, compliance and legal issues, and communication interface & virtualisation security) were identified and discussed and solutions were provided. With these in mind, cloud customers will be able to assess and compare cloud computing services, with respect to security and privacy, so that they can make informed choices. In addition, cloud service providers (CSPs) can also address the discussed issues to offer better security and privacy.

Keywords

Cloud Computing, Security, Privacy, Cloud Service Providers (CSPs)

1. INTRODUCTION

Cloud Computing is becoming a well-known catchword nowadays and the cloud has essentially altered the computing landscape, communication infrastructures and networked services. Investment in cloud services is increasing as more organizations are becoming interested in cloud services. There is increased patronage in cloud services from both organizations and individuals [1].

The US National Institute of Standards and Technology defines cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models” [2].

Cloud services are various applications and services running somewhere in the cloud infrastructures and these can be accessed through a private network or the Internet. Those who use the cloud other wise called cloud users, care less about the storage location of their data or how the cloud service will be provisioned. In cloud computing, service providers develop, deploy and deploy scalable, reliable, high performance applications on high end infrastructures. A Cloud Service Provider (CSP) is responsible for providing cloud services to consumers. CSP’s should handle customers’ sensitive personal information (SPI) such as email addresses, telephone numbers, credit card numbers etc with utmost professionalism. CSP’s are also responsible for cloud service management, cloud deployment, privacy and security of cloud services [9]. These benefits of the cloud system also come at a price. For example, private data could be stored somewhere on the Internet and the cloud user trying to access such data may be exposed to security and privacy issues [3]

The cloud is an open platform and thus it is susceptible to attacks of various degrees. Data access and utilization management, data security and trust issues are primary security concerns in cloud computing. These immanent security and privacy issues may discourage users from deploying cloud computing solutions [4]. It should be noted however that the security concerns are not peculiar to the cloud computing systems alone. This is so because data is almost always vulnerable to attack wherever it is stored. Thus, there is the need to plan for network security in both cloud based infrastructure and non cloud based infrastructure. [5].

Some of the major advantages of cloud computing include provision of on demand services, consumers being charged for only the services they consume, ease of maintenance, elasticity and distributed storage of services. Thus, consumers are provided with cloud services whenever they request for them and they are charged accordingly, using a pay-as you-go model.

Figure 1 shows some of the benefits of cloud computing. The cloud can cater for as many services as are required. There are no limits to the number of services that can be deployed and so cloud users can enjoy the functionalities of many services. Another huge advantage is that services are stored in a distributed fashion. i.e. The storage of cloud data is not restricted to any particular location [6]. Examples of some well known cloud computing providers are Amazon, Microsoft Azure and Google. The motivation for this work stems from the fact that despite the traction gained by cloud computing, some people are still sceptical and rightly so, about deploying cloud computing systems because of security and privacy concerns. This work identifies, discusses and provides solutions to these concerns.

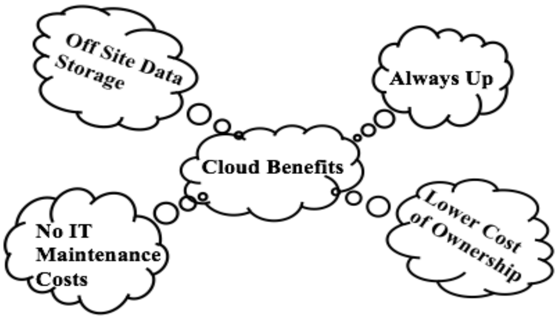

Figure 1: Benefits of Cloud Computing

2. REVIEW OF RELATED WORKS

In [7], “Security and Privacy issues in cloud computing” the authors reviewed cloud computing technology, its deployment and service models. They also focused on key security and privacy issues that affect cloud computing.

In [8], “Challenges and Security issues in cloud computing from two perspectives: Data Security and Privacy protection” the authors investigated the challenges and security issues in cloud computing from the data security and privacy protection perspective.

In “Security and Privacy in Cloud Computing: Vision, Trends, and Challenges” by [3] the authors explored some of the challenges and limitations of cloud security, focusing on data utilization management aspects and access control. [1] in his paper titled Security and Privacy in Cloud Computing, discussed related challenges, opportunities, and solutions relating to cloud security and privacy

[9] in the paper “On Current Trends in Security and Privacy of Cloud Computing” analysed privacy and security requirements in cloud computing and suggested open open research areas in cloud computing systems. [10] in their paper titled “Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective”, identified and categorized cloud security and privacy attributes. These categorised features were then used to define the expectations from cloud computing service providers so that consumers could make well educated choices.

[2] in their paper titled Security and Privacy Challenges in Cloud Computing Environments, explored the roadblocks and solutions to providing a trustworthy cloud computing environment. [4] in their paper titled “Security and Privacy in Cloud Computing: A Survey” discussed with several Cloud Computing service providers about their security and privacy concerns. They observed that the security and privacy concerns presented by most cloud computing system providers were not adequate. They proposed the deployment of more security strategies in the cloud environment to achieve the desired control, availability, confidentiality and data integrity. They also proposed a modification in that privacy acts to enhance the relationship between cloud providers and users.

3. KEY CHARACTERISTICS OF CLOUD COMPUTING

The five key features of cloud computing according to the US National Institute of Standards and Technology include “on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service”. These characteristics ensure seamless and transparent use of the cloud services. Rapid elasticity defines the speed with which resources can be scaled up (or down). The term measured services means that cloud computing resources are controlled and optimized by the service providers through load balancing, metering and automated resource allocation. [2]

3.1 Key Cloud Delivery Models

The three key cloud delivery models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Despite the differences in these models, they also share common security- and privacy-related issues. Figure 2 shows the key cloud delivery models.

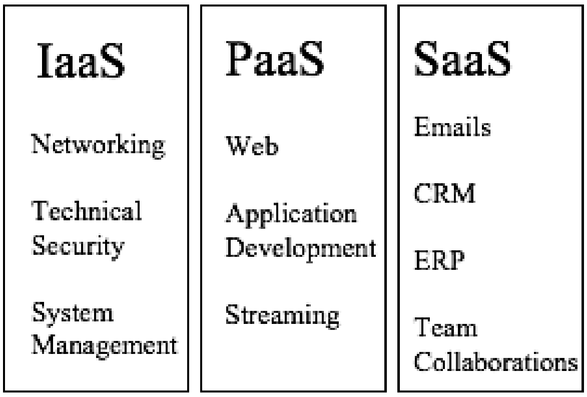

Figure 2: Cloud Delivery Models

Infrastructure as a service (IaaS): This is involved with providing the infrastructure such as servers, hardware, storage, routers and the other networking modules to the users. The end user can use some or all of these infrastructure components and pay for only what he has used. In this model, the cloud user is able to run and deploy any software, which includes applications and operating systems. The end user does not have the rights and privileges to monitor or supervise the cloud infrastructure.[7]

Platform as a service (PaaS): PaaS enables programming environments to access and utilize additional application building blocks. i.e. This model can be described as application development environments offered by cloud providers. These environments affect the application architecture, such as constraints on which services the application can request from an operating system.

Software as a service (SaaS): In SaaS, application software is enabled and provided as on-demand services by the cloud providers. i.e. It gives the user the ability to use the software and its functions on demand, remotely, through the internet. It is common for cloud clients to acquire and use software components from different providers, thus it is important that the information handled by these composed services is well protected. [9] [2]

3.2 Cloud Deployment Models

Cloud computing is mostly based on accessing resources over the Internet and the prominent cloud deployment models include public, private, community, and hybrid clouds.

Public Cloud: In this model, the cloud infrastructure is hosted in the vendor’s premises. So the user does not have a control and visibility over where the cloud infrastructure is hosted. Thus, all the members of a public cloud share the same infrastructure.

Private Cloud: The private cloud is much secure and expensive than public cloud. It is dedicated to an individual organization to do its tasks, it is built within the organization and is being managed at the same organization. These Organizations use a specific software that will enable cloud functionality, such as OpenStack, vCloud Director or VMWare. [7]

Community Cloud: A community cloud is similar to a private cloud, but the major distinction here is that the cloud resource is shared among members of a closed community that have similar interests. For example, Siemens IT Solutions and Services set up a media cloud for the media industry. A community cloud may be managed by a third party or may be or managed internally by the community, in a collaborative fashion as in the grid computing model [5]. The cloud infrastructure is to be shared by organizations with common security and compliance objectives in a given community. It is less expensive than a public cloud but more expensive than a private cloud. [11]

Hybrid Cloud: A Hybrid cloud combines two or more different cloud infrastructure types; these can be private, public, or community clouds. The goal is to provide extra resources in cases of high demand and this is achieved by transferring computation tasks from a private cloud to a public cloud as computing needs and cost vary. In a hybrid cloud environment, multiple internal or external suppliers of cloud services are used.

3.3 Cost Benefit Implications of Deploying Cloud Services

Before making a decision on whether to obtain services from CSP's, customers need to do a critical needs assessment. The customers need to know how much would it cost to have their own IT infrastructure, how much are the CSP is charging for the service they want, what added value the CSP is providing and ultimately, if the provided service would achieve their business goals. With answers to these questions, cloud consumers can effectively plan their business operations with low IT overhead and low operational cost. The consumer needs to be aware of the Capital Expenditure (CAPEX) costs such as floor space, power and cooling, hardware and software costs and Operational Expenditure (OPEX) costs such as hardware maintenance and software upgrade costs when doing the needs assessment. [12]

4. CLOUD PRIVACY AND SECURITY ISSUES

Here, the key cloud computing security and privacy issues are discussed. These are:

1. Network and Data Security

Network and data security in cloud computing has several facets such as data confidentiality, integrity, availability and backup and disaster recovery. These are briefly discussed below:

Data Confidentiality: Data confidentiality is a key issue to be considered when outsourcing highly sensitive data to the cloud. Confidential data should be inaccessible to unauthorised users and one way of ensuring confidentiality is by the use of strict access control policies. Policies should be in place to prevent unauthorised users from inferring anything from the information being stored in the cloud database. Data confidentiality is achieved through encryption of data. With data encryption however, there is the issue of key distribution / management of keys. Different encryption algorithms have been proposed such as Rivest Shamir Adelman (RSA), Triple Data Encryption Standard (3DES) and Homomorphic encryption. In Homomorphic encryption, computations are carried out on encrypted data (cipher text), thus generating an encrypted result, which, when decrypted, matches the result of the same operations performed on the original data (plaintext). This can be a huge advantage for applications that outsource encrypted data to the cloud. The major drawback of this method is its computational complexity and cost [3].

Data Integrity: The term integrity explains the wholeness and completeness of data which is a key issue in IT systems. It is the process of verifying data. It guarantees the quality and correctness of data. In cloud computing the integrity of data storage is a necessary and important requirement. The integrity of data proves its regularity, consistency and validity. As the cloud service requirements increase, the CSP may need to scale up their storage systems and this may lead to high chance of data loss, data corruption, disk failure, node failure or hardware failure. Thus, monitoring data integrity in cloud is so important to prevent the possibilities of data crash and corruption. It is easier to achieve data integrity in centralized systems than in distributed cloud computing environment. Data integrity can be ensured by auditing processes. A cloud auditor independently evaluates cloud services and cloud infrastructure. Periodic third party auditing mechanisms could be initiated to verify data integrity data integrity [7].

Data Availability: The service created for users must be available to them when needed. However, some situations exist in which data availability cannot be guaranteed. For example, in unavoidable situations like natural disasters, it is important to know if the data can be utilized, verified or recovered by the data owners. The cloud customers must be aware of the security measures being taken by the cloud service provider. They should also read the fine print of the Service Level Agreement (SLA) entered into with the service providers. [6] High availability in cloud infrastructures can be achieved by designing fault-tolerant cloud systems. Cloud systems should be designed for server failure, zone failure and cloud failure.

Backup & Disaster Recovery: It is essential for CSP's to provide a backup and disaster recovery plan for data protection, recovery, resiliency of data centre, data availability and to allow business continuity after network or system failures. The cloud users must be informed about the backup type and requirements and what disaster recovery plan is available.

2. Governance, Compliance and Legal Issues.

The physical location of the server farm and cloud infrastructures should be confidential as physical security of infrastructure is also very important. The CSP must have a procedure or set of procedures to secure customers' data if there is a suspected threat or breach and this must be shared with the customers upon request. In addition, the sanitization of data stored in the cloud is a critical issue to be discussed. Cloud users should be assured their data will always be secure even if the cloud service providers collapse or are acquired by another company. Cloud users should also know how they can obtain their data back and in what format [13]. Compliance refers to an organizations' responsibility to operate. Compliance is a tricky and somewhat complicated subject in cloud computing because security and privacy laws and regulations vary from region to region [9]. What might be legal in certain regions might be considered illegal in other areas. Cloud customers should understand the terms and references of any service level agreement (SLA) entered into with the CSP or CSP's in the case of nested services (when a consumer gets different services from different vendors) in its entirety, including penalties for defaulting and mode of compensation.

3. Communication Interface & Virtualization Security

The cloud user has a part to play in ensuring security of cloud services. This is so because the nature of connections and devices used by the cloud user to connect to the cloud has its own security implications. For example, wired / wireless connections, using secure browsers etc. In addition, authentication of users only provides a proof of identity. It does not limit the actions or operations that a legitimate user of a computer system can perform. So an authenticated user may carry out some unauthorised operations if auditing and access control measures and policies are not introduced. Furthermore, in multi-tenancy, hypervisors ensure that multiple operating systems, can run concurrently on a single physical machine. The different operating systems may be owned by different customers called tenants. This method of sharing physical resources could also introduce some vulnerabilities and the cloud users should know if the CSP's can identify and defend side-channel attacks? [10]

5. CONCLUSION AND FUTURE WORKS

Cloud computing involves accessing a shared pool of networked computing infrastructure and resources. The cloud offers benefits such as reduced costs, reduced management responsibilities, increases organisational efficiency etc. Despite the many advantages associated with cloud computing, there are many vulnerabilities for cloud privacy and security. In this paper cloud service and deployment models was discussed. This paper also identified the key security and privacy issues in cloud computing and discussed solutions. Due to the intricacies of the cloud, it may be difficult to achieve end-to-end privacy and security and this may prove to be a hurdle for adoption of cloud computing systems. A challenging research area open for researchers is insider trust issues in CSP's. Trust issues involve a cloud provider administrator using the administrator account to invade the consumer's cloud security and/or privacy. Further efforts can be channelled towards ensuring adherence regulatory compliance frameworks and better non-disclosure norms by the cloud providers to guarantee extensive commercial success of cloud services.

6. REFERENCES

[1] Z. Tari, "Security and Privacy in Cloud Computing," IEEE Cloud Comput., vol. 1, no. 1, pp. 54–57, 2014.

[2] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Secur. Priv. Mag., vol. 8, no. 6, pp. 24–31, 2010.

[3] Z. Tari, X. Yi, U. S. Premarathne, P. Bertok, and I. Khalil, "Security and privacy in cloud computing: Vision, trends, and challenges," IEEE Cloud Comput., vol. 2, no. 2, pp. 30–38, 2015.

[4] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing?: A Survey Security and Privacy in Cloud Computing:," Sixth Int. Conf. Semant. Knowl. Grids, vol. 2, pp. 126–149, 2010.

[5] W. Kong, Y. Lei, and J. Ma, "Data Security and Privacy in Cloud Computing," Int. J. Distrib. Sens. Networks, vol. 2014, pp. 512–514, 2014.

[6] Arjun and Vinay, "A Short Review on Data Security and Privacy Issues in Cloud Computing," IEEE, 2016.

[7] M. M. U. B. YahyaKord, Tamandani Qahtan, "Security and Privacy Issues in Cloud Computing," IEEE, pp. 896–900, 2016.

[8] S. Mahdi Shariati, M. Abouzarjomehri, and H. Ahmadzadegan, "Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection," 2nd Int. Conf. Knowledge-based Eng. Innov., pp. 1078–1082, 2015.

[9] S. Sahin, "On Current Trends in Security and Privacy of Cloud Computing," Proc. AICT'13, pp. 1–5, 2013.

[10] A. Abuhussein, H. Bedi, and S. Shiva, "Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective," Internet Technol. Secur. Trans., pp. 388–395, 2012.

[11] G. Kulkarni, N. Chavan, R. Chandorkar, R. Waghmare, and R. Palwe, "Cloud security challenges," Telecommun. Syst. Serv. Appl. (TSSA), 2012 7th Int. Conf., pp. 88–91, 2012.

[12] J. Kozhipurath, "Cloud Service Costing Challenges," IEEE, 2012.

[13] P. K. G. Gandhi, "Cloud Computing Security issues: An Analysis," IEEE, pp. 3858–3861, 2016.