AN ASSESSMENT OF MOBILE CLOUD-COMPUTING SECURITY CHALLENGES

Muhammad Musa

Department of Computer Science, School of Applied Science,
Nuhu Bamalli Polytechnic, Zaria.

ABSTRACT

The recent emergence of cloud computing has drastically altered everyone's perception of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns as a critical issue for the success of information systems, communication and information security. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result, the aim of this paper is twofold; firstly, to analyze cloud computing security issues by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats.

Keywords: Cloud-Computing, Security, Networking, Client, Server

INTRODUCTION

Cloud Computing holds the potential to eliminate the requirements for setting up of high-cost computing infrastructure for the IT-based solutions and services that the industry uses. It promises to provide a flexible IT architecture, accessible through internet for lightweight portable devices. This would allow multi-fold increase in the capacity or capabilities of the existing and new software. In a cloud computing environment, the entire data reside over a set of networked resources, enabling the data to be accessed through virtual machines (Bhadauria, 2011).

In mobile cloud technology, data and software are being resided in data centers somewhere that are not possibly known by the users. Transactions are carried out between users' devices and cloud platforms virtually. Research have shown that there are millions of customers making different transactions on cloud came from various angles of the world which include Europe, United states, UK, Asia and Africa.

Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Cloud computing is seen as a trend in the present-day scenario with almost all the organizations trying to make an entry into it. The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter. Moreover, cloud computing minimizes the capital expenditure. This approach is device and user-location independent (Bhadauria, 2011).

CLOUD COMPUTING LAYERS

According to the different types of services offered, cloud computing can be considered to consist of three layers as follows: -

1. IaaS or Infrastructure as a Service: (IaaS) is the lowest layer that provides basic infrastructure support service. Infrastructure as

a service (IaaS) refers to the sharing of hardware resources for executing services, typically using Virtualization technology. With IaaS approach, potentially multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged for on a pay-per-use basis. The resources are all virtual machines, which has to be managed. Thus, a governance framework is required to control the creation and usage of virtual machines. This also helps to avoid uncontrolled access to user's sensitive information.

2. PaaS – **Platform as a Service**: (PaaS) layer is the middle layer, which offers platform-oriented services, besides providing the environment for hosting user's applications. In

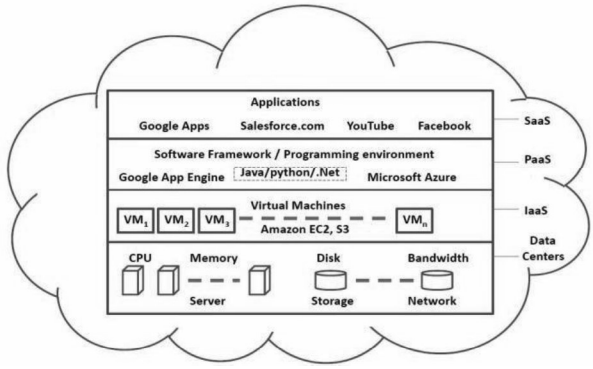

Figure 1: cloud computing layers

the **Platform as a service approach (PaaS)**, the offering also includes a software execution environment. As for example, there could be a PaaS application server that enables the lone developers to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus, the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons.

3. SaaS - **Software as a Service:** (SaaS) is the topmost layer which features a complete application offered as service on demand. **SaaS** ensures that the complete applications are hosted on the internet and users use them. The payment is being made on a pay-per-use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock" (Bhadauria, 2011).

4. CLOUD SERVICES

Cisco identified four categories of cloud services currently in the marketplace or emerging in the near future: public clouds, private clouds, virtual private clouds, and eventually inter-clouds.

Public Clouds

Public clouds are "stand-alone," or proprietary, clouds mostly off-premise, run by third party companies such as Google, Amazon, Microsoft, and others. Public clouds are hosted off customer premises and usually mix applications (transparently) from different consumers on shared infrastructure.

Private Clouds

Private clouds are typically designed and managed by an IT department within an organization. A private cloud is usually built specifically to provide services internally to an organization. Private clouds may be in a collocated facility or in an existing data center. This model gives a high level of control over the cloud services and the cloud infrastructure. Cisco has a strong portfolio of solutions, products, and services, which enable private cloud infrastructures.

Virtual Private Clouds

Virtual private clouds allow service providers to offer unique services to private cloud users.

These services allow customers to consume infrastructure services as part of their private clouds. The ability to augment a private cloud, with on-demand and atscale characteristics, is typical of a virtual private cloud infrastructure. Private cloud customers can seamlessly extend the trust boundaries (security, control, service-level management, and compliance) to include virtual private clouds. The virtual private cloud concept introduces the complexities of migrating workloads and related data from a private cloud. Cisco is already developing a unique set of capabilities in the form of protocols and solutions, which enable long-distance, workload mobility scenarios from private clouds to virtual private clouds.

Inter-cloud

Cisco envisions, that in long term, the inter-cloud will emerge as a public, open, and decoupled cloudcomputing internetwork, much like the Internet. In a sense, the inter-cloud would be an enhancement and extension of the Internet itself. Just as the Internet decouples clients from content (i.e., you don't have to have a preexisting agreement with a content provider to find and access its website in real time), the inter-cloud will decouple resource consumers (enterprises) from cloud resource providers, allowing the enterprises to find resources on demand with providers. Workload migration will be the dominant use case for the inter-cloud, as an open market, establishes trust standards and public subsystems for naming, discovering, and addressing portability and data/workload exchange.

UNDERSTANDING THE CLOUD ARCHITECTURE

The main objective of cloud computing is to facilitate small businesses in a cost-effective fashion to provide access to technologies that are beyond their reach. By using cloud computing, small businesses can expand their IT resources based on service demands and avail equal opportunities of growth to compete with other businesses within the market.

In the current mobile cloud architecture, mobile devices can access cloud services in two ways, i.e.

i. Through mobile network (telecom network) or
ii. Through access points, as shown in Figure 2.

In the mobile network (telecom network provider) case, the mobile devices such as cellular/satellite smartphones are connected to a mobile network through a Base Station (BS) or via a satellite link.

However, if the smartphones are not equipped with a satellite communication module, then external satellite communication devices are used. The telecom networks are further connected to the Internet and provide Internet connectivity to the users. Therefore, if the users have mobile network connectivity, the users can access cloud based services through the Internet. In the access point case, the mobile users connect to the access points through Wi-Fi that is further connected to the Internet service provider to provide Internet connectivity to the users. Therefore, the mobile cloud users can access cloud based services without utilizing telecom services, which may charge them for data traffic. Moreover, Wi-Fi based connections provide low latency and consume less energy compared to 3G connections. Consequently, mobile cloud users prefer to use Wi-Fi Internet connections whenever accessible (Sajjad, 2014).

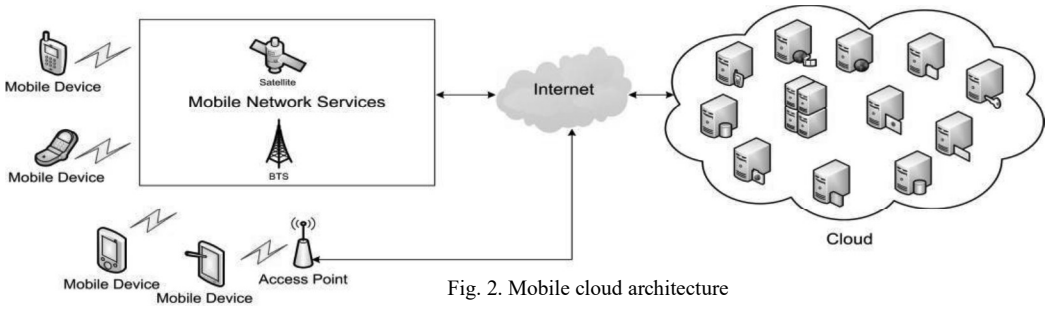

Fig. 2. Mobile cloud architecture

REVIEW OF RELATED LITERATURE

1) Rajnish Choubey (2011) Identified approaches that if adopted will help to make cloud computing more secure and convenient while keeping the cost of implementing cloud low, as follows: -

i. When a user registers for any cloud computing services, strict validation check should be applied about the user's background.
ii. The Cloud Service Provider and the user must sign a Service Level Agreement (SLA), clearly defining the role and responsibilities of both parties and terms and conditions of contract breakup.
iii. Accountability for data loss (if any), because of the cloud service provider need to defined and measures of data backup should be there.
iv. The Cloud Service Provider must ensure strict authentication and validation policy for employees.
v. There should be an audit process for the cloud service providers.
vi. Frame a minimal set of standards for cloud computing.
vii. The cloud service providers should be accredited.

2) Rohit BHADAURIA (2014) From the scenario of mobile cloud computing, they identified security challenges that need to be addressed to enable Mobile Cloud Computing reach its maximum potential as follows:

✓ ***Network accessibility***: Internet has been the major factor towards the cloud computing evolution and without having the network access it won't be possible to access the internet and hence the inability to access the mobile cloud limiting the available applications that can be used.

✓ ***Data Latency***: Data transfer in a wireless network is not as continuous and consistent as it is in case of a dedicated wired LAN. And this inconsistency is largely responsible for longer time intervals for data transfer at times. Also, the distance from the source adds up to the longer time intervals observed in case of data transfer and other network related activities because of an increase in the number of intermediate network components.

✓ ***Dynamic Network monitoring and Scalability***: Applications running on mobiles in a mobile cloud computing platform should be intelligent enough to adapt to the varying network capacities and also, they should be accessible through different platforms without having suffered any loss in the data. Sometimes, a user while working on a smart phone may need to move on to a feature phone and when (s)he accesses the application which (s)he was working on through her/his smart phone, (s)he should not face any data loss.

✓ ***Confidentiality of mobile cloud-based data sharing***: The confidential data on mobile phones using cloud-based mobile device support might become public due to a hacked cloud provider. The root-level access to cloud services and information can be easily accessed from a stolen mobile device. If the stolen device belongs to a system administrator, they may even provide direct and automated access to highly confidential information.

✓ ***Better access control and identity management***: As cloud computing involves virtualization, the need of user authentication and control across the clouds is high. The existing solutions are not able to handle the case of multiple clouds. As multiple users' data are stored by a single hypervisor, specific segmentation measures are needed to overcome the potential weakness and flaws in hypervisor platform.

They also identify the threat to mobile cloud computing as follows:

✓ ***Basic security issues in Saas:***

a) SQL Injection attack
b) Cross site scripting (XSS) attack
c) Man in the middle attack

Network Level Security attack:

Networks are classified into many types like: shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of:

a) DNS attacks, Sniffer attacks,
b) Issue of reused IP address,
c) Denial of Service (DoS) and
d) Distributed Denial of Service attacks (DDoS)
e) BGP prefix hijacking

To ensure network security following points such as: confidentiality and integrity in the network, proper access control and maintaining security against the external third-party threats should be considered while providing network level security.

✓ **Application Level Security**

Application level security refers to the usage of software and hardware resources to provide security to applications such that the attackers are not able to get control over these applications and make desirable changes to their format. The threats to application level security include: -

a) XSS attacks,
b) Cookie Poisoning,
c) Hidden field manipulation,
d) SQL injection attacks,
e) DoS attacks,
f) Backdoor and Debug Options,
g) CAPTCHA
h) Breaking etc

All resulting from the unauthorized usage of the applications.

ENSURING SECURITY AGAINST THE VARIOUS TYPES OF ATTACKS

The main criterion to be filled up by the generic security framework are to interface with any type of cloud environment, and to be able to handle and detect predefined as well as customized security policies. A similar approach is being used by Symantec Message Labs Web Security cloud that blocks the security threats originating from internet and filters the data before they reach the network.

Web security cloud's security architecture rests on two components:

a. *Multi layer security*: In order to ensure that data security and block possible malwares, it consists of multi-layer security and hence a strong security platform.

b. *URL filtering:* It is being observed that the attacks are launched through various web pages and internet sites and hence filtering of the web-pages, ensures that no such harmful or threat carrying web page gets accessible. Also, content from undesirable sites can be blocked.

3. A Survey of Mobile Cloud Computing Application Models: the paper digest more on application models for mobile cloud computing which is designed to achieve a particular objective, such as executing applications that have insufficient resources for local execution, enhancing applications performance (in terms of computation time), or achieving energy efficiency on mobile devices.

Therefore, researchers envision extending cloud computing services to mobile devices to overcome the smartphones constraints (Sajjad, 2014)**.**

4. Cloud Computing: Security Issues and Research Challenges: Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a

cloud provider like Google, Amazon, Salesforce.com and Microsoft etc. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate. The paper also highlight on the following:-

I. Cloud computing security architecture

II. Key security issues in cloud computing: *Data Transmission: Virtual Machine*
Security, Data security: Data Privacy. Data Integrity, Data Location, Data Availability,
Data Segregation (Padhy, 2011).

5. Cloud Computing Security Issues and Challenges

This paper discusses security issues, requirements and challenges that cloud service providers (CSP) face during cloud engineering. Recommended security standards and management models to address these are suggested for technical and business community.

This professional paper discusses security and privacy issues as challenges, and recommends control objectives to technical and business community. It also highly recommends OVF standard as vendor and platform independent, open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines (software stack that incorporates the target applications, libraries, services, configuration, relevant data, and operating system)

The paper also discusses on the following:

Security in the cloud: which include: -

i. Security issues and challenges (Security concern, Audit and monitoring, Privacy breaches),
ii. Security management standards,
iii. Security management models (Software-asa-Service (SaaS) security, Security management (People), Security governance, Risk management, Risk assessment, Security awareness, Education and training, Policies and standards, Third party risk management, Vulnerability assessment, Security image testing, Data governance, Data security, Application security, Virtual machine security, Identity Access Management (IAM), Change management, Physical security, Disaster recovery and Data privacy)

6. Assessing the Security Risks of Cloud Computing.

This paper discusses that, organizations that need cloud-based services must understand the associated risks, defining acceptable use cases and necessary compensating controls before allowing them to be used for regulated or sensitive information. The paper also identifies the following:

Key Findings

✓ The most practical way to evaluate the risks associated with using a service in the cloud is to get a third party to do it.
✓ Cloud-computing IT risks in areas such as data segregation, data privacy, privileged user access, service provider viability, availability and recovery should be assessed like any other externally provided service.
✓ Location independence and the possibility of service provider "subcontracting" result in IT risks, legal issues and compliance issues that are unique to cloud computing.
✓ If your business managers are making unauthorized use of external computing services, then they are

circumventing corporate security policies and creating unrecognized and unmanaged

CONCLUSION AND RECOMMENDATIONS

Conclusion

We understand that, basically the term cloud computing is achieved by coming together of different systems and tools to work as a system. Also, it discovered that, cloud computing is an emerging technology with shared resources, lower cost and rely on pay per use according to the user demand. Based on the survey I conducted by reviewing papers on cloud security issues, the papers generally find the following security challenges in cloud:-

i. ***Privacy Issues*** (Lack of user control, Unauthorized Secondary Usage, Transborder Data Flow and Data Proliferation, Dynamic provision).

ii. ***Security*** (Access, Control over data lifecycle, Availability and backup, Multitenancy, Audit)

Mitigations and necessary counter measures were identified and discussed in the literature review and other parts of this research paper.

Recommendations

1. Organizations that have IT risk assessment capabilities and controls for externally sourced services should apply them to the appropriate aspects of cloud computing.
2.
3. Legal, regulatory and audit issues associated with location independence and service subcontracting should be assessed before cloud-based services are used.
4. Demand transparency. Don't contract for IT services with a vendor that refuses to provide detailed information on its security and continuity management programs.
5. Develop a strategy for the controlled and secure use of alternative delivery mechanisms, so that business managers know when they are appropriate to use and have a recognized approval process to follow (Jay, 2008).
6. Introduction to Cloud Computing architecture White Paper 1st Edition, June 2009: This paper discusses security issues, requirements and challenges with respect to cloud services. The paper also discusses *security and data physics* and *Network security practices* as follows:- Security and data physics

Data is often the most valuable of a company's assets, and it must be protected with as much vigilance as any other asset. It is easy to argue that more vigilance is needed to protect data because of how an intruder can potentially reach a Company's data from anywhere on the Internet. Some steps to take include:

a. *Encrypt data at rest* so that if any intruder is able to penetrate a cloud provider's security or if a configuration error makes that data accessible to unauthorized parties, that the data cannot be interpreted.

b. Encrypt data in transit. Assume that the data will pass over public infrastructure and could be observed by any party in between.

c. Require strong authentication between application components so that data is transmitted only to known parties.

d. *Pay attention to cryptography and how algorithms are cracked and are replaced by new ones over time.* For example, now that MD5 has been proven vulnerable to attack, use a stronger technique such as SHA-256.

e. *Manage who has access to the application and how using the following steps*:

i. Consider using strong, token-based authentication for administrator roles.

ii. For customer login/password access, consider who manages the authentication

iii. For anonymous access to storage, for example anonymous FTP, consider whether a customer would have to register with the cloud provider for access or whether the cloud provider could federate with network security practices.

In cloud computing, applications are deployed in a shared network environment, and very straightforward security techniques such as VLANs and port filtering are used to segment and protect various layers of an application the company's authentication server deployment architecture as well as isolating customers from each other. Some approaches to network security include:

✓ Use security domains to group virtual machines together, and then control access to the domain through the cloud provider's port filtering capabilities. For example, create a security domain for front-end Web servers, open only the HTTP or HTTPS ports to the outside world, and filter traffic from the Web server security domain to the one containing back-end databases (Figure 11).

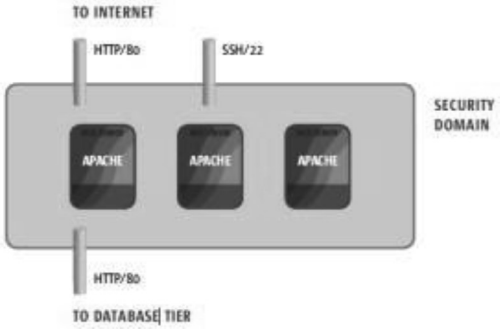

Figure 11. Cloud providers should offer mechanisms, such as security domains, to secure a group of virtual machines and control traffic flow in and out of the group.

✓ Control traffic using the cloud provider's port-based filtering, or utilize more packet filtering by interposing content switches or firewall appliances where appropriate.

server and whether it is under the company or the cloud provider's control.

8. A review on cloud computing security issues and challenges:

The main concern is security privacy and trust. These issues are arising during the deployment of mostly public cloud because in public cloud infrastructure customer is not aware where the data store & how over the internet.

In this paper security privacy and trust issues of cloud computing are reviewed. The paper includes some surveys conducted by IDC that show the motivation for the adoption of cloud computing.

The paper identifies the issues and the solution to overcome these problems. The paper also contains the security model named security access control services SACS is analyzed through the Hadoop map reduce framework and the experimental results are obtained that compare the system performance with SACS model and without SACS model (Alvi, 2009).

REFERENCES

Rajnish C., Rajshree D., Bhattacharjee J. (2011). A Survey on Cloud Computing Security, Challenges and Threats, 3.

Bhadauria R. (2014). A Survey on Security Issues in Cloud Computing, Bulletin of Engineering Tome VII.

Sajjad A.M. (2014). A Survey of Mobile Cloud Computing Application Models, *IEEE Communications Surveys & Tutorials*, 16(1).

Padhy R.P (2011). Cloud Computing: Security Issues and Research Challenges. IRACST - International *Journal of Computer Science and Information*

Technology & Security. (IJCSITS), 1(2).

Heiser J. and Mark N. (2008). Assessing the Security Risks of Cloud Computing" Gartner Research, Publication Introduction to Cloud Computing Architecture White Paper 1st Edition, June 2009.

Alvi F. A. (2009). A review on cloud computing security issues & challenges.

Farrukh S. (2014). State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions. and Computer Sciences University of California at Berkeley.