July 2013. Vol. 3, No.3 ISSN 2305-1493
International Journal of Scientific Knowledge
Computing and Information Technology

www.ijsk.org

SECURITY ARCHITECTURE FOR MOBILE CLOUD COMPUTING

Ali Newaz Bahar[1*], Md. Ahsan Habib[2], Md. Manowarul Islam[3]

[1, 2, 3] Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Bangladesh
* E-mail of the corresponding author:bahar_mitdu@yahoo.com

ABSTRACT

Cloud computing has become another buzzword to its tremendous business prospects. On the other hand cloud computing application on mobile internet are developed frequently, its leads security problems, in particular, is one of the most argued-about issues in the mobile cloud computing field. So, one of the key challenges is to design the cloud computing security architecture for mobile device on the internet. In this paper we proposed security architecture for mobile cloud.

Keywords: Cloud computing, SaaS, PaaS, IaaS, MCC.

1. INTRODUCTION

Cloud computing is a remote, internet-based computing, which provides shared resources, software, and information to computers and other devices such as mobile, PDA on demand. Now a day's, cloud computing is more and more cult to its agility, low cost, device independence, reliability (multiple redundant sites), scalability, security and reduced maintenance cost.

Mobile cloud computing is a computing idea, where a mobile user got all the cloud computing services in his or her mobile devices through internet. Mobile cloud merged the elements of mobile networks and cloud computing, thereby providing the optimal services for mobile users. In mobile cloud computing, mobile devices do not need a powerful configuration (e.g., CPU speed and memory capacity) since all the data and complicated computing modules can be processed in the clouds [1] [2].

In cloud computing, top three IT cloud services challenges are security, availability and performance. The cloud computing security issue is always the key factor and it is ranked one [3].

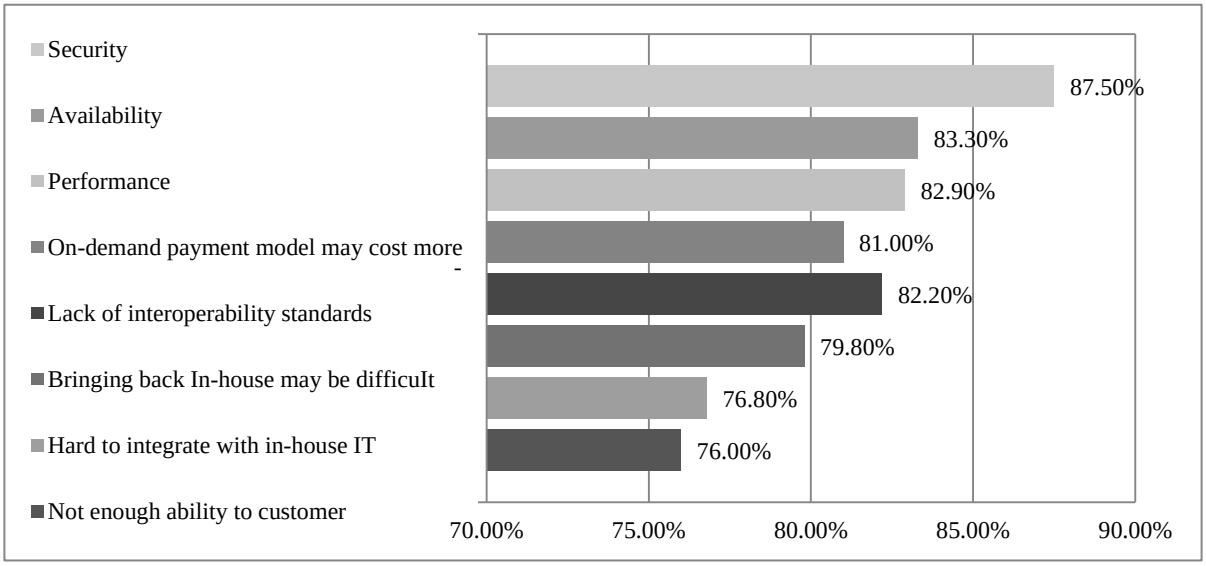

Figure 1: Results of IDC survey ranking security challenges, 2010 [3]

2. THE CLOUD COMPUTING

2.1 Cloud Services

Cloud computing service are broadly classified into three delivery models: the Infrastructure as a Service (IaaS); the Platform as a Service (PaaS); and the Software as a Service (SaaS) [8, 9, 10, 11].

2.1.1 Software as a service (SaaS)

It is a model of software deployment whereby the provider licenses an application to the customers for use as a service on demand. The capability provided to the End users is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web enabled e-mail). The end users does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

2.1.2 Platform as a service (PaaS)

It is the delivery of computing platform and solution stack as a service. The capability provided to the end users is to deploy onto the cloud infrastructure user created or acquired applications created using programming languages and tools supported by the provider. The end user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage. PaaS providers offer a predefined combination of OS and application servers, such as WAMP platform [12] (Windows, Apache, MySql and PHP), LAMP platform (Linux, Apache, MySql and PHP), and XAMP(X-cross platform) limited to J2EE, and Ruby etc. Google App Engine, Salesforce.com, etc are some of the popular PaaS examples.

2.1.3 Infrastructure as a service (IaaS)

It is the delivery of computer infrastructure (typically a platform virtualization environment) as a service.

The capability provided to the end users is to provision processing, storage, networks, and other fundamental computing resources where the end user is able to deploy and run arbitrary software, which can include operating systems

and applications. The user does not manage or control the underlying cloud infrastructure but it has control over operating systems, storage, deployed applications, and possibly limited control of select networking components. Some of the common examples are Amazon, GoGrid, 3tera, etc.

Figure 2: Cloud Service

2.2 Cloud Application Deployment Models

There are three deployment models for Cloud computing: public, private, and hybrid [4]-[7].

2.2.1 Public Cloud

In this model, computing resources are dynamically provisioned over the Internet via Web applications or Web services from an off-site third party provider. Public clouds are run by third parties, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks.

2.2.2 Private Cloud

The physical infrastructure may be owned by and managed by the organization or the designated service provider [9] with an extension of management and security control planes controlled by the organization.

2.2.3 Hybrid Cloud

This model of Cloud computing is a composition of two or more Clouds (public or private) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

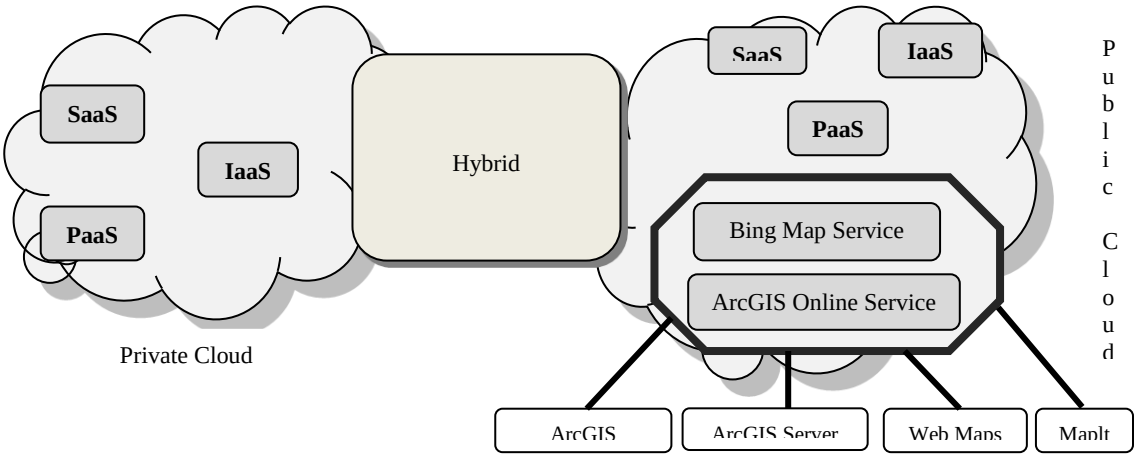

Figure 3: Cloud Application Deployment Models

3. MOBILE CLOUD COMPUTING

Mobile computing [13] means using portable devices to run stand-alone applications and/or accessing remote applications via wireless networks. In mobile cloud computing mobile network and cloud computing are combined, thereby providing an optimal services for mobile users. Cloud computing exists when tasks and data are kept on the internet rather than on individual devices, providing on-demand access. Applications are run on a remote server and then sent to the user [1, 2]. Figure 4 shows an overview of the mobile cloud computing architecture.

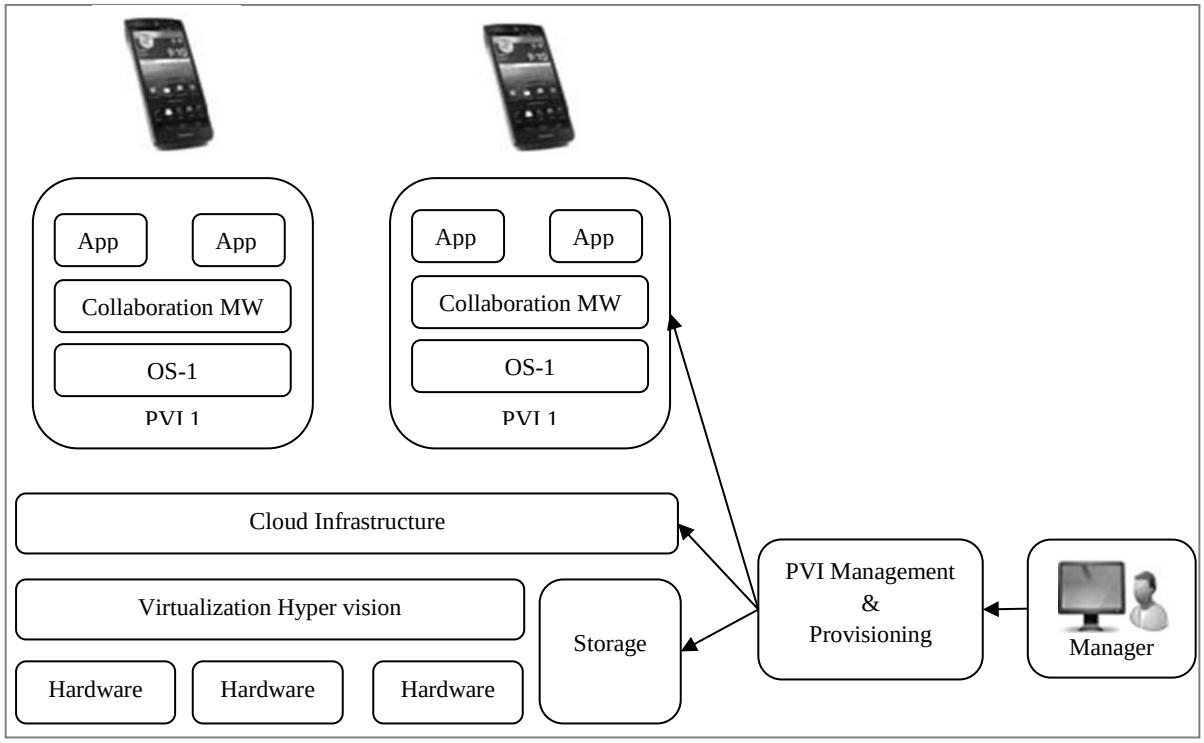

Figure 4: Mobile Cloud Computing Architecture

4. DATA SECURITY ISSUES IN THE MOBILE CLOUD

4.1 Privacy and Confidentiality

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

4.2 Data Integrity

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

4.3 Data Location and Relocation

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information.

Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each other's' resources.

4.4 Data Availability

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

5. PRIVACY DESIGN BY MOBILE CLOUD

The Fig. 3 shows a likely minimalist of mobile cloud computing architecture that maintains privacy and usability when data is encrypted and outsourced into the Cloud. This proposed architecture is mainly designed to overcome one of the challenging problems, this model ensuring that organizations that make legitimate requests are granted access to encrypted data

This architecture needs to collaborate between two agents the consumer's agent and the requestor's agent and two service providers the Cloud access control service provider (ACSP) [14] and the Cloud data service provider (DSP). The consumer's agent encrypts data prior to sending it to the Cloud DSP, and issues access delegation to the Cloud ACSP that will handle data utilization requests from the requestor.

When one party wants to access the data through his or her mobile device, he or she contact the cloud access control service provider for access authorization, for the sake of privacy protection requester would not go directly to the Cloud DSP [15]. Upon authentication of the requestor, and satisfaction of any criteria set out in the access delegation, the Cloud ACSP would issue an access authorization to the requestor.

This proposed authorization message would consist of three components, each with a different effect. First, it would indicate to the Cloud DSP that the requestor had been authenticated, and was permitted to access the consumer's data. Second, the Cloud ACSP would include in the message any available information regarding the subset of data to be released to the requestor, with the goal of restricting requestor access to be only the minimum required for its stated purposes.

Finally, the authorization message would also contain a decryption key for the released data, engineered so as to only allow the requestor decrypt capabilities. Should the requestor be able to circumvent this system, contacting the Cloud DSP directly and managing to succeed in retrieving data, the absence of the appropriate decryption key implies that all that is retrieved is meaningless cipher text. Similarly, if the Cloud DSP were compromised or actively colluded with the requestor, again, only cipher text could be obtained.

July 2013. Vol. 3, No.3 ISSN 2305-1493
International Journal of Scientific Knowledge
Computing and Information Technology

www.ijsk.org

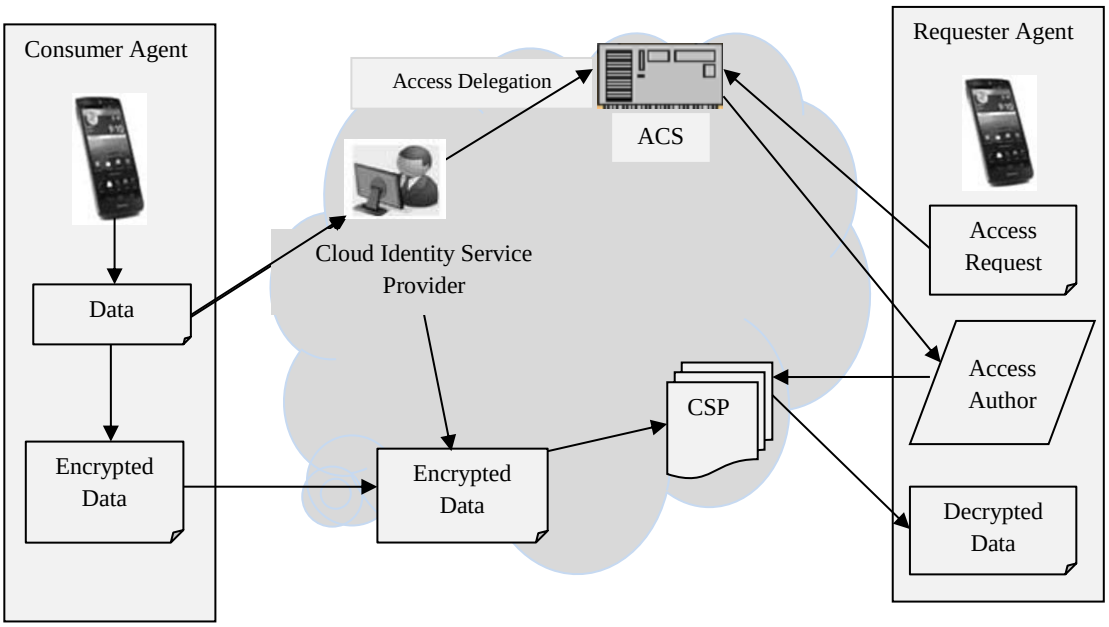

Figure 5: Privacy design model for mobile cloud

6. PRIVACY SCHEMA DETAILS

Our proposed security model involves three steps:

- Key Generation
- Encryption
- Decryption

6. 1. Key Generation

Before the data is encrypted, Key generation should be done by the Cloud Identity Service Provider. Let F be a pseudo-random function, let Ƞ be a pseudo-random permutation and let H be a cryptographic hash function.

Generate pk = (N, g) and sk = (e, d, v), such that ed ≡ 1(modp′ q′), e is a large secret prime such that e > λ and d > λ , g is a generator of QRN and v R ← {0, 1}k.

Output (pk, sk).

Tag Block (pk, sk, m, i):

1. Let (N, g) = pk and (d, v) = sk.

Generate Wi = v||i.

Compute Ti,m = (h(Wi) · gm) d mod N.

2. Output (Ti,m, Wi).

6.2 Encryption

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:

1. Cloud service provider should give or transmit the Public Key (N, g) to the user who wants to store the data with him or her.

2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.

3. Data is encrypted and the resultant cipher text (data) C is C = mg (mod N).

4. This cipher text or encrypted data is now stored with the Cloud service provider.

6.3 Decryption:

Decryption is the process of converting the cipher text (data) to the original plain text (data).

Steps:

1. The cloud user requests the Cloud service provider for the data.

2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, C.

3. The Cloud user then decrypts the data by computing, m = Cd (mod N).

4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

7. CONCLUSION

In the field of computing, Mobile Cloud Computing (MCC) has brought a new dimension to Networking Service. The main vision of this service is interconnected "Mobile Cloud" where application providers and enterprises will be able to access valuable network and billing capabilities across multiple networks, making it easy for them to enrich their services whether these applications run on a mobile device, in the web, in a SaaS Cloud, on the desktop or an enterprise server.

Mobile Cloud Computing (MCC) is a combination of mobile networks and cloud computing, so the MCC security related issues are then divided into two categories: mobile network security and data security on the cloud.

In this paper, we have discussed the data security issues considering on mobile cloud computing and securing mobile cloud computing user's privacy.

REFERENCES

[1] http://www.smartdevelopments.org/?p=84

[2] http://www.readwriteweb.com/archives/why_cloud_computing_is_the_future_of_mobile.php

[3] F. Gens. (2010, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDCeXchange,Available:<http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

[4] R.J. Bayardo, and R. Srikant (2003) Technological Solutions for Protecting Privacy. IEEE Computer, 36(9), p. 115-118.

[5] E. Bertino (2009) Privacy-preserving Digital Identity Management for Cloud Computing. IEEE Data Engineering Bulletin, 32, p. 21-27.

[6] J.Brodkin (2008) Seven Cloud-Computing Security Risks. InfoWorld. seven-cloud-computing-security-risks, p.853.

[7] R. Buyya, C.S. Yeol, and S. Venugopal (2008) Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. In Proc. of 10th IEEE International Conference on High Performance Computing and Communications (HPCC'08), p.5-13.

[8] NEC Company, Ltd. and Information and Privacy Commissioner, Ontario, Canada. "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach, (2010), http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf.

[9] https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework.

[10] http://andromida.hubpages.com/hub/cloud-computing-architecture.

[11] Sun Microsystems, Inc., "Introduction to Cloud Computing Architecture", White Paper, 1st Edition, (2009) June.

[12] http://www.wampserver.com/en/ [accessed on 15 July 2012]

[13] Mahadev Satyanarayanan, "Mobile computing: The next decade," Proc. 11th Intl. Conf. on Mobile Data Management (MDM'10), Kansas, MO, 2010.

[14] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, Saint Malo, France, Sep. 2009.

[15] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing,"2009