www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3, Issue 10 October, 2014 Page No. 8993-8996

Mobile cloud security a Survey

Lorence Oliver, Dr. Rajashree Shettar
Senior Technical Manager
Mindtree Ltd. Global village, RVCE Post
Bangalore, India
oliver.lorence@gmail.com

Professor and Dean (PG Studies), Dept. of CSE
RV College of Engineering
Bangalore, India
rajashreeshettar@rvce.edu.in

***Abstract*— Cloud computing has become part day today life. There are large numbers of vendors providing different cloud offerings. With the evolution of mobile devices, mobile cloud computing has drawn attention. Even though cloud security is a well thought aspect, there is need to look at cloud security from a mobile device perspective. In this paper we have analyzed different research happenings in this area and presented future research needs.**

Keywords—cloud; security; mobile; mcc;

I. Introduction

Cloud computing is a way of increasing capacity as and when needed without investing in infrastructure or training. It is termed as next generation computing infrastructure. “Cloud computing” helps to offload computation and data storage to remote cloud servers. It is classified based on the services provided like PaaS (Platform as a Service), SaaS (Software as a service), IaaS (Infrastructure as a Service) or based on cloud architecture as Public cloud, Private cloud or hybrid cloud. Cloud computing is widely adapted. Because of recent trends in smartphones, hand held devices like mobiles tablets have started replacing the desktop machines, so there is need to look at cloud computing from mobile device perspective.

Mobile devices have certain characteristics which distinguish them from the traditional computing devices. The distinguishing factors are limited computing capacity, limited battery power, limited storage, limited bandwidth or varying network conditions, limited input(keyboard) output(screen size) capabilities. Even though mobile devices are resource constrained they have started replacing the traditional computing devices because of mobility and proximity for common users. Enterprises and common service providers have started adopting cloud technologies and migrating solutions to clouds. Overall usage of cloud solutions has increased and is rapidly expanding. Mobile cloud computing is expected to grow from 42.8 million in 2008 to 998 million in 2014, prediction by API research [14].

Rapid adoption of mobile devices also has attracted the attention of hackers and intruders. There is 400% increase in security attacks on Android devices from 2010 to 2012, reported by department of homeland security [15]. The reasons are: there is valuable data available on mobile devices. Nowadays because of BYOD (Bring Your Own Device) concept, lots of enterprises are allowing their employees to connect to enterprise network through their own device. Enterprise secure data is being accessed through mobile devices or is stored on that. Also the mobile devices being more personal devices, users are storing critical information like passwords on the device. If intruders get access to such critical information that means whole security is broken. For example if user has online banking password on his device and an intruder gets access to this, the intruder may get access to the account itself.

There is security threat for the data generated, stored or consumed, by the mobile devices. The security threat can be for the data at rest or for the data in transit. There is need to look at the security vulnerabilities of this data in conjunction with the limitations of the mobile devices and evaluate the solutions of data security for their adequacy or enhancement needs.

Cloud data security can be achieved in two levels, one at the low level (protocol level) and the other at the application level.

A. low level data security

1) Data security while the data is at rest

Normally cloud systems are multi-tenant systems. That means, data belonging to multiple solution providers or heterogeneous operating systems may reside on the same physical hardware. Data is vulnerable to access by malicious users. Cloud solution provider need to provide assurance about the data to be accessible only to the legitimate users. Different techniques can be used to preserve security of the data. The techniques include sandboxing, encryption, access control etc.

2) Data security while the data is in transit

Cloud systems are heavily dependent on internet or networks. Data will be flowing between end users and the cloud systems. Data flow may use different paths at different times. Cloud systems will also be distributed, so data will flow in-between cloud systems as well. While the data is in transit it is susceptible for access by malicious users. Data encryption techniques are in place to assure data security in transit. Key management is a major issue in this regard.

B. application level data security

In certain cases low level data security if provided may be sufficient, but in highly secure systems, application level security will be required where application will enforce second level of security on the data.

Application level data security may vary from application to application and the solutions employed may be application specific. Application level data security can ensure even the data is secure from cloud service provider.

II. research in this area

There are multiple research happenings in mobile cloud data security. Researches have happened on Enterprise security [1] [2], Security of service requests [3] [4] [5] [6], Secure cloud storage [7] [8], Frameworks for mobile cloud apps [9] [10], Secure architectures [11] [12], Abnormal behavior in Cloud Infrastructure [13].

These researches have provided considerable insight into happenings on mobile cloud security. Still there are areas wide open for research.

A. Enterprise security

In today's world, enterprises cater to different consumer needs and contain large amount of data. The data belongs to different categories. Some data may be very private to the enterprise; some data may be belonging to employees, some data of customers. Enterprises are slowly adapting the cloud because of the benefits provided by cloud (cost effectiveness, scalability, pay per use etc.). Enterprises are on the adaption path but are keeping a close watch on the security aspects of the data. When it comes to data which needs high security, enterprises are adapting private clouds but otherwise public or hybrid clouds are adapted [2]. As enterprises are embracing BYOD concept, they are exposing themselves to higher risk. They are going out of the bounds of controlled devices and private networks.

Even though there is security concern when migrating enterprise data to cloud, cloud service providers are claiming that they are providing high level of security. The reasons being, they deploy latest anti-virus software's, they provide multi-level authentication, physical isolation, restricted physical access. Apart from this they maintain records, auditable by trusted authorities.

B. Security of service requests

Mobile cloud computing needs services provided by service vendors for its success. One of the limitations currently faced by cloud customers is portability [3]. Next generation cloud enabled systems will be dominated by mobile thin clients whereas major computation will be happening in the cloud infrastructure [6]. Different architectures are proposed, that address portability, discovery of services, security of services taking into account mobility and resource constraints of mobile devices.

The architectures provided for service requests are there in their infancy. These architectures need to be evaluated and then may need to undergo standardization process. Once standardized, they can be adapted by the cloud service providers. This will be beneficial for both cloud service providers and consumers. Cloud service providers will be enabled with pre-built service standards. Consumers will be benefitted readily available services from multiple vendors, and they having the power to choose from the best vendor.

C. Secure cloud storage

One of the important aspects of cloud computing is secure storage. Because of multi-tenant architecture it is difficult to ascertain the security of data stored on clouds. Simple usage of cloud storage could be for data backup of mobile devices (No data loss if device is lost, easy to switch to new device) [7]. Mobile devices have become data collection devices, for example for monitoring patients. They do not have large space to store continuous data, so cloud is a best solution [8]. Clouds also maintain replica of same data to provide faster access. Maintaining consistency within these replicas is a challenge. Cloud storages have to provide consistent interfaces to access/modify the data (Example NFS).

There are large numbers of players providing cloud storage, example Amazon S3, Google cloud storage etc. These services can be used without being worried about how much the data can grow, how quickly more space can be added etc. Also service providers provide value added services like backup, archival, disaster recovery. As the data storage uses standard interfaces, it becomes much easier in case of movements or migrations.

D. Frameworks for mobile cloud apps

There is no well-defined model for mobile applications with cloud services [9]. Vendors are providing their own solutions for security aspects. This is a risk for cloud users because they will be tied to the service provider. There will be considerable migration costs if they want to move to another vendor. Various frameworks are proposed to address this. Some frameworks address continuous inflow of highly secure data.

One of the major usages of mobile cloud could be in case of mobiles being used as collection devices. For example a mobile device can be used to monitor the pulse rate of a patient. As the mobile devices are equipped with different kinds of sensors (cameras, voice recorders, temperature, motion, etc.), they can easily collect on ground data and transmit the same to the backend servers. These servers can later process the data and take further actions. The data that flows may be highly secure data (like users geo location) or general data like temperature at certain location. Cloud can provide powerful backend processing and storage. Frameworks are very much necessary to segregate the data that is arriving and provide right amount of security for the same.

E. Secure cloud architectures

One of the challenges of mobile cloud computing is building a secure computing architecture [11]. As on date there is no such architecture exists which is widely adopted. There are few proposals at high level consisting of multi hierarchy, multi-level, cross platform. These architectures need to be evaluated considering different aspects of mobile cloud computing. Each component has to be developed further to meet the requirements. More over the architectures have to go through standardization process so that they can be built and adopted.

The challenges are cloud platform is evolving from the traditional systems and internet. For practical purposes it is essential that the mobile cloud architectures uses as much legacy systems and apply sophistications only for areas where serious challenges are faced in terms of performance, security or ease of use. Second challenge is there is very less standardization attempt. Other challenges are the number of heterogeneous systems.

F. *Abnormal behavior in cloud infrastructure*

Rapid expansion of mobile cloud computing also increased the malware on the mobile cloud infrastructure. Mobile cloud infrastructures have limited processing power at the mobile device. This largely limits deployment and execution of anti-virus software on the mobile device. To prevent or minimize malware in mobile cloud infrastructure it is necessary to detect them. One of the promising methods for malware detection is detecting abnormal behavior. Taehyun Kim et al have proposed a methodology and architecture [13] for monitoring and detecting abnormal behavior. They have used various machine learning algorithms in designing the methodology.

III. Future research

Rapid expansion of mobile cloud computing has necessitated the need for research on multiple areas related to mobile cloud computing. Major areas that need attention are 1) Adaption of existing technologies for mobile cloud 2) Mobile cloud architectures 3) Mobile cloud security 4) Standardization. Prototypes need to be built and they need to undergo evaluation.

A. *Adaption of existing technologies for mobile cloud*

There are multiple standards and architectures that are dominating the internet. Cloud technology is built on top of these standards. While building these standards or architectures, primary focus was on traditional computation infrastructure. As the computation infrastructure has moved from resource rich environment to resource constrained environment. Also the infrastructure had reliable network connectivity and speed. Because of the constraints as mentioned, there are challenges faced for the existing standards or architectures. Careful evaluation is required to understand the challenges and provide solutions.

B. *Mobile cloud architectures*

As discussed above either adapting the existing standards may be required otherwise new architectures have to be built to cater to mobile cloud computing. Even though there are attempts by researchers to provide architectures, those have not evolved to the level of commercialization. There is need for mobile cloud service providers to come together and build standardized architectures so that both service providers and consumers are benefitted.

C. *Mobile cloud security*

Few organizations still have not adapted cloud because of concerns on security. It is obvious that if somebody is giving his valuables under the supervision of some other person, he will be concerned. Until the trust is built on the third party chances are very less that the valuables will be handed over for custody.

Mobile cloud security plays key role in building the trust between the cloud service provider and the cloud users. If trusted architecture, mechanism and processes are built and evaluated then users will move to the cloud environments and reap the benefits.

D. *Standardization*

One of the key lagging aspects in cloud computing is standardization. Even though there are multiple vendors already available for cloud, each one is following their own standards. For example Amazon uses its own services and service structures and Google has its own. The disadvantage of this is customer lock-in. Users will not be able to migrate from one vendor to another. Application or service developments cannot be re-used as the underlying interfaces will be different for different cloud service providers. There are attempts being made by several standards organizations to bring standards for cloud computing. Majorly IEEE-SA (IEEE Standards Association), ITU and NIST have proposed some standards. These standards have to be reviewed, adapted and built.

IV. CONCLUSION

In this paper we have presented different researches happening in mobile cloud security. Research challenges and standardization are wide open. As the existing systems or architectures are built or adopted for traditional computing systems there is need to understand the applicability of systems for mobile cloud computing. The systems have to be adapted. It may not be practical to build mobile cloud computing architecture from scratch instead; the existing systems have to be adapted. Mobile cloud infrastructure need to work seamlessly with the existing infrastructure of internet and cloud computing. Research focus need to be on understanding the limitations of existing infrastructure and provide solutions/enhancements over the existing systems so that mobile cloud solutions work efficiently and seamlessly with the existing systems.

References

[1] Bassam S Farroha, Deborah L Farroha, Architecting Security into the Clouds: An Enterprise Security Model. A US Government work.

[2] Gustavo de los Reyes, Sanjay Macwan, Deepak Chawla, Cristina Serban, Securing the Mobile Enterprise with Network-Based Security and Cloud Computing. Crown 2012.

[3] Saeid Abolfazli, Zohreh Sanaei, Muhammad Shiraz, Abdullah Gani, "MOMCC : Market-Oriented Architecture for Mobile Cloud Computing Based on Service Oriented Architecture". Workshop on Mobile Cloud Computing (MobiCC'12) IEEE 2012.

[4] ZHOU Lian-chi, XIU Chun-di, "Cloud Security Service Providing Schemes Based on Mobile Internet Framework". International Conference on Computer Science and Electronics Engineering, IEEE 2012.

[5] I Kounelis, J. Loschener, D. Shaw, S. Scheer, "Security of Service Requests for Cloud Based m-Commerce". MIPRO 2012.

[6] Slawomir Grzonkowski, Peter M. Corcoran, "Security Analysis of Authentication Protocols for Next-Generation Mobile and CE Cloud Services". IEEE International Conference on Consumer Electronics 2011.

[7] Sue-Chen Hsueh, Jing-Yan Lin, Ming-Yen Lin, "Secure Cloud Storage for Convenient Data Archive of Smart Phones". IEEE 15th International Symposium on Consumer Electronics 2011.

[8] Zhibin Zhou, Dijiang Huang, "Efficient and Secure Data Storage Operations for Mobile Cloud Computing". 8th International Conference on Network and Service Management 2012.

[9] Daniela POPA, Marcel CREMENE, Monica BORDA, Karima BOUDAOUD, "A Security Framework for Mobile Cloud Applications," European Social Fund through the Sectorial Operational Proram Human Resources 2007-2013.

[10] Yu-Jia Chen, Li-Chun Wang, "A Security Framework of Group Location-Based Mobile Applications in Cloud Computing". International Conference on Parallel Processing Workshops 2011.

[11] Susmita Horrow, Sanchika Gupta, Anjali Sardana, Ajith Abraham, “Secure Private Cloud Architecture for Mobile Infrastructure as a Service”. IEEE Eigth World Congress on Services, 2012.

[12] Qiu Xiu-feng, Liu Jian-wei, Zhao Peng-chuan, “Secure Cloud Computing Architecture on Mobile Internet”. IEEE 2011.

[13] Taehyun Kim, Yeongrak Choi, Seunghee Han, Jae Yoon Chung, Jonghwan Hyun, Jian Li, James Won-Ki Hong, “Monitoring and Detecting Abnormal Behavior in Mobile Cloud Infrastructure”. 3rd Workshop on Cloud Management 2012.

[14] Abdul Nasir Khana, M.L.Mat kiaha, Samee U. Khanb, Sajjad A. madanic, “Towards secure mobile cloud computing : A survey”, volume 29, Issue 5, July 2013.

[15] Webroot, “Cloud-Based Mobile Device Security Streamlines Data Protection” 2013.