International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

A Technical Review on Mobile Cloud Computing: Security Issues and Research Challenges

Vinodray Thumar[1]
Research Scholar, Faculty of Engineering & Technology
C. U. Shah University, Gujarat, India
Dr. Vipul Vekariya[2]
Associate Professor, C.E. Department
Noble College of Engineering & Technology,Gujarat, India

ABSTRACT

Cloud computing is a platform based on Internet which provides the resources in an effective manner. Cloud computing is an emerging technology with in internet world which provides an opportunities to utilize software, applications and hardware resources without any upfront investment to every individual. With the rapid change in mobile applications and advancements in cloud computing, a new era is being expected in the form of mobile cloud computing. The growing use of Mobile cloud computing platform minimizes the performance, compatibility and lack of resources issues in mobile computing environment. With the advancement of mobile cloud computing, Lack of data security and confidentiality of user is the only an obstacle that must be overcome in wide adoption of mobile cloud computing. Important research is in progress in this emerging area in order to reduce the security concerns but still a lot work has to be done to produce a security. This paper presents a concept of cloud computing, literature review of Mobile cloud computing, its security issues and challenges.

Key words - Mobile Cloud Computing, Security Issues, Data Security, Privacy

I. INTRODUCTION

Cloud computing refers to the use of networked infrastructure software and capacity to provide resources to users on-demand. With cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, Laptops, mobiles and other devices computing devices. With Design perspective, Cloud computing is flexible, scalable and elastic offering IT services a way to easily increase capacity or add additional capabilities on demand without investing in new and expensive infrastructure and license software.

II. OVERVIEW OF CLOUD COMPUTING

2.1 Cloud Service Models

The cloud computing model is based on three service delivery models and three cloud deployment models [1, 2, 3, 4, 5].

There are three service delivery models are:

Infrastructure as a service (IaaS): this model offers the cloud services like hardware resources, storage and network infrastructure services. The virtualization is the base of this model.

This layer provides fundamental storage and computing capabilities as consistent services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The client's can deploy their own software on the infrastructure.

The Amazon web services Elastic Compute Cloud (EC2) and S3 are an examples of IaaS [a, b].

Platform as a service (PaaS): this model offers the cloud application development platform for the developers. They also deliver a set of APIs for the developers to develop and launch their own customized applications. They do not need to install development tools on their local devices and machines.

The development environment is encapsulated and offered as a service for which other higher levels of service can be built. Every client has the freedom to build his own applications which runs on the provider's infrastructure. To meet scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform which includes Linux, Apache, MySql and PHP servers.

The Amazon Simple Storage Service, Google App Engine5 and Microsoft Azure6 are an examples of PaaS [c] [d][e].

Software as a service (SaaS): This model facilitates the customers to access the applications hosted on the cloud. Instead of installing the applications on their own machines, the users access these applications installed on the cloud using their own browsers. This model can be hosted directly on the cloud or may be PaaS and IaaS.

This model offers a complete application to the customer as a service on demand. A single instance of the service runs on the cloud and multiple end users are serviced. On the client's side, there is no need for upfront investment in servers or software licenses but for provider's, the costs are lowered, since only a single application needs to be hosted and maintained. The SaaS Provider's manages the software on "usage" basis. They are established on negotiated prices. It includes future versions/releases. They provide maintenance and patches services.

The Google Docs and salesforce's customer relationship management software are examples of SaaS [f] [g].

2.2. Cloud Deployment Models

In cloud computing, there are three different deployment models and each model has its own pros and cons. There is also another model called community model but it is used in rare cases. [h][i]

Private cloud: This cloud model is in organization within its own data center. The organizations manage all the cloud resources which are owned by them. The private cloud offers comparatively more security than other two deployment cloud models.

Public cloud: In Public cloud, all the external users through internet who can register with cloud and can use cloud resources on a pay-per-use model. This cloud is not secure like private cloud because it is accessible to the internet users.

Hybrid cloud: It is one type of private cloud which uses the resources of one or more public clouds. It is a mix of both private and public cloud.

Community Cloud: The cloud infrastructure exclusively used by specific community users within an organization for a shared cause. It may be owned, operated and managed by themselves or a third party.

2.3 Cloud Computing Benefits

Cloud computing is enabling the enterprise to:

Expand scalability – With utilization of cloud computing, IT staff can quickly meet changing user loads without having to engineer for peak loads.

Lower infrastructure costs – With external clouds, customers do not own the infrastructure. Due to such facilities organizations can eliminate capital expenditures and consume resources as a service, paying only for what they use. Clouds enable IT departments to save on application implementation, maintenance and security costs, while benefiting from the economies of scale a cloud can offer compared to even a large company network.

Increase utilization – With sharing computing resources between multiple clients, cloud computing can increase utilization, further reducing IT infrastructure costs.

Improve productivity – In cloud computing environment, users can access systems, regardless of their location or what device they are using.

Improve reliability – Cloud computing can provide multiple redundant sites cost effectively, facilitating business continuity and disaster recovery scenarios.

Increase security – Because of centralization of data and increased security, specific resources from cloud computing providers, cloud computing can enhance data security. Cloud computing can also relieve an IT organization from routine tasks, including backup and recovery. Cloud service providers have more infrastructures to handle data security than the average small to midsize business.

Access to more sophisticated applications – External clouds can offer CRM and other advanced tools that were previously out of reach for many businesses with smaller IT budgets.

Downsize the IT department – By moving applications out to a cloud, IT departments can reduce the number of application administrators needed for deployment, maintenance and updates. It departments can then reassign key IT personnel to more strategic tasks.

III. CHALLENGES OF EXISTING CLOUD COMPUTING SOLUTIONS

3.1 Challenges of Existing Cloud Computing Platform

Like any new trend or technology, we must address some challenges that cloud computing poses before we can recognize its full value.

A lack of interoperability – The absence of consistency across cloud computing platforms creates unnecessary complexity and results in high switching costs. Each cloud service provider has a different application model, many of which are proprietary, vertically integrated stacks that limit platform choice. Consumers don't want to be locked with a single provider and are often reluctant to relinquish control of their mission critical applications to hosting service providers.

Application Compatibility – Most of the traditional public clouds are not interoperable with existing applications and they limit the addressable market to those willing to write new applications from scratch.

Difficulty in meeting compliance regulations –Frequent requirements may limit the use of the shared infrastructure and utility model of external cloud computing for some environments. Achieving compliance often requires complete transparency of the underlying IT infrastructure that supports business critical applications, while cloud computing by design places IT infrastructure into a 'black box' accessible only through well-defined interfaces. Hence internal compute clouds may be a better solution for some applications that must meet stringent compliance requirements.

Inadequate security – By design, cloud vendors typically support multi-tenancy cloud environments. IT managers must look for a balance between the securities of an internal, dedicated infrastructure versus the improved economics of a shared cloud environment.

RQ1: What mobile cloud security requirements have been addressed in recent publications?

RQ2: What solutions are offered to them?

RQ3: Which mobile cloud security requirements have been under-researched?

RQ4: What changes can be identified in addressing mobile cloud security requirements and solutions?

Cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry for last few years. But as more and more information on individuals and companies are placed on the cloud, concerns are beginning to grow about just how secure environment it is.

These are the following important issues for the cloud computing.

a. Security

b. Privacy

c. Reliability

d. Legal Issues

e. Open standard

f. Compliance

g. Freedom

h. Long-term Viability

3.2 Solution for existing issues

The important counter measures which may be taken by the community to ensure security are :

a. Data encryption.

b. Identity management.

c. Access control.

d. Reporting of security incidents, personnel and physical layer management should be evaluated.

e. Minimization of personal information sent to and stored in the cloud.

f. CSP should maximize the user control and provide feedback.

g. Organizations need to run applications and data transfer in their own private cloud and then transmute it into public cloud.

h. There are many legal issues exist in the cloud computing, Cloud Security Alliance should design relevant standards as quickly as possible.

IV. LITERATURE REVIEW : SECURITY ISSUES

In one research paper, the security issues are discussed as Manages Service Model in order to ensure data and application security in cloud environment. According to the survey of International Data Corporation, for IT executive security is biggest concern in cloud services. There are some serious issues and challenges which cloud computing are facing in the domain of cyber security. [6]

Overview of Mobile cloud computing is presented with some security architecture. Privacy and integrity of the data is important aspect of Mobile cloud computing security. There are mainly two types of security concerns like mobile network security and cloud security. In first type the security for mobile applications and privacy are explained. The second type is about securing the information on the cloud with proper data integrity, authentication and digital rights.[7]

Mobile cloud computing architecture is presented in [8]. There are various mobile cloud computing applications like mobile commerce, mobile learning, mobile health care and mobile gaming. Security issues and existing solutions are also presented in detail in this research article. It is also discussed open issues linked with cloud security, authentication, quality of service, low bandwidth, network access management, and standard interface.

The paper presents Mobile cloud computing architecture along with the overview of the different security services at different layers of the cloud computing delivery service model. The secure cloud physical services are available in backbone layer in this architecture. At the infrastructure and supervisor layers, secure cloud process hosting services are available. Secure cloud application services are available at the application, platform and infrastructure layer of the cloud delivery service model. [9]

In research article [10], It has been presented six computing paradigms shift that how computing evolved from internet computing to grid computing and then from grid computing to cloud computing. The novel paradigm shift that mobile cloud computing brought into this world are also highlighted. They discussed about various issues and challenges in the area of mobile cloud computing like Performance issues because of intensive applications, Security issues, Privacy Issues, Bandwidth Costs, Reliability Issues

The framework of data service mechanism is proposed in [11]. It provides best data access control and confidentiality of data stored in the cloud. Security model explains that the algorithm used in it ensures that only authorized data sharers can access the data. The first phase contract with setup, second phase is with data encryption, third phase is with data sharing, Fourth phase is with access data and fifth phase is with policy updating.

The security issues related to private and confidential data and mobile cloud applications are explained in detail in this research article. It is proposed a mobile computing applications security framework to make sure that the security of the data is achieved when it is transmitted between the components of the same mobile application. The framework also verifies that the integrity of the applications either at the time of installation or updating on the mobile device is intact. [12]

There are two different security services in [13]. Critical Security service and Normal Security service are discussed in this research paper. The Critical Security service consumes more cloud resources but provides better security and protection. Critical Security service also produces more reward to the cloud service providers. The authors proposed a Security Service Admission Model in order to allocate cloud resources properly to the large number of increasing service users

Service level agreement, audit, certifications and risk treatment methods being an important structural chunk of cloud security and controls are defined into a single framework [14]. In this framework virtual ISMS is compared with the conventional ISMS. The virtual ISMS is a structured way to manage risk and organizational assets over the cloud. As cloud client and provider are jointly responsible for data security and control in the cloud, so they can adopt virtual ISMS as a standard complaint management process for the protection of shared assets. It is more important from the client's perspective that they should be cognizant of what they are purchasing with cloud.

The significant key drivers and constraints for secure cloud computing from are discussed in [15]. The trust, privacy and user approach towards cloud computing are the social issues while on the other side encryption, scalability, reliability, data rights and transparency are the stern technological issues in cloud computing. Most of the cloud users are unaware of the risk of storing and transmitting private information in a shared environment. So that key technological constraints like compliance, transparency, encryption, integrity and multi-tenancy should be addressed carefully. The transparency is the biggest challenge for the enterprises at present, and due to this, they are reluctant to switch to cloud computing environment. Once the cloud becomes transparent and the users have full control to access, manage and report pertaining to the state of data and services, only then it will help increase the trust and minimize the social and technological constraints.

The Identity and Access Management protocols and standards are the important data security. It is an adequate level of protection for organizational assets through implementing appropriate policies. The emerging challenges can be minimized through discussing authentication, authorization and auditing issues. The life cycle consist on five stages: *Provisioning and Deprovisioning, Authentication and Authorization, Self-Service, Password Management, and Compliance and Audit.* [16]

The cryptographic algorithm Diffie-Hellman for secure communication, in contrast to key distribution management is explained in [17]. There are three modules in this framework like administration, authentication and encryption modules. Each module has different, but interconnected functions. The administration module is used by the cloud provider for user registration and administration. The authentication module is used for authentication of users, and encryption module is used for data encryption. The authentication realization is a two-way process. The system requires the user to enter normal login and password, then it generates one-time password and sends it on the user mobile for authentication. Once the one-time password is supplied, the system authenticates the user and grants access to the system.

Various security, privacy and trust issues in existing environment of cloud computing are discussed in [18]. Users can recognize tangible and intangible threats associated with its use. Security plays a important role in current era of long dreamed vision of computing as utility. It can be divided into four parts as safety mechanisms, cloud server monitoring or tracing, data confidentiality and avoiding malicious insiders' illegal operations and service hijacking. It is also discussed the importance of data privacy in cloud computing. It is a key point from user perspective so that it is vital to understand its allied issues like user control over the data and legal jurisdiction requirements.

The security control measurements in cloud computing are equivalent to the ones in the conventional IT set up [19]. The client should know answers to the seven safety questions prior to making the selection of cloud providers. These questions are relevant to data segregation, data location, privileged user access, recovery,

forensic support, viability and regularity compliance, on a long-term basis. Moreover, the client has to exclusively analyze the data privacy, protection and security problems throughout the data life cycle over the cloud. The data life cycle passes through seven phases: data generation, transfer, use, share, storage, archival and destruction. The data identification, data isolation and privacy protection are the primary concerns and must be kept into consideration during the design and development of cloud-based applications. The integrated and complete security solutions are expected to meet the data security and protection objective in depth.

The importance of the legal agreements between the service provider and client called Service level Agreement is discussed in [20]. The cloud service provider can secure trust of a client through SLAs and service quality. A typical SLA normally consists of eight main contents, including Security, Definition of Service, Problem Management, Responsibilities, Performance Management, Customer Duties and Disaster Recovery and Business Continuity & Termination. The basic security concerns that SLA should contend with include privileged user access, regulatory compliance, forensic analysis support, data location/relocation and data segregation, data recovery and viability. The present-day SLAs encompass only the subject of services provided, and waivers are offered in case the desired services do not meet the agreement. The SLA should also describe how the security in the cloud is maintained and what are the methods and procedures used in maintaining security to make it client compliant.

It is discussed about the cloud computing security challenges by proposing a solution called the Trusted Computing Platform in [21]. It is used to provide authentication, confidentiality and integrity in cloud computing environment. Trusted cloud computing system is built as the hardware for cloud computing and it ensures privacy and trust. Various phases to implement this framework are as Authentication, Role Based Access Control, Data Security, Tracing of User's behavior.

The security issues related to policies, software and hardware are described in [22]. Security is classified into Software Security such as virtualization software, encryption, host operating system and Physical security such as back-up, firewall, server location and these two types has to be addressed to provide secure cloud. Policies between Cloud Service Provider and Clients which ensures security must include factors that need to be considered during breach of security such as Insider threats, Access control, System Portability.

The existing security threats of Virtual infrastructure are mentioned by describing a threat model in which a hacker can be either cloud user or non-cloud user. Security attacks of Virtual infrastructure involve attacks such as hypervisor attacks, vSwitch attacks, Virtual machine attacks. A virtualization-aware security solution is proposed in which the security software is installed in a dedicated and privileged Virtual machine with privileged access to hypervisors to secure other Virtual machines. It is advised to use micro-hypervisor with microkernel to provide high level security. [23]

The basic cloud computing concepts such as cloud computing model, service models, deployment models and its characteristics are described in [4]. A data security model is proposed and it uses an encryption algorithm in Amazon EC2 Micro platform to provide security. An encryption algorithm which recovers fast from failures is selected by comparing with few other encryption algorithms based on P-value and rejection rate. It is advised to use AES (Advanced Encryption Standard) for higher security requirements.

The data protection and authentication by deploying Host Identity Protocol is discussed in [24]. It is tested on various architectures to address the multi-tendency challenges of hybrid cloud. It was used to secure internal connectivity in the clouds and a load balancer terminated tunnels towards end-users.

Live Migration Defense Framework can be used to improve security in Virtual Machines. It ensures the data integrity and encryption for security enhancement. It can identify the old and new location to perform internal adaptations and corresponding actions based on the location fingerprint training.[25]

V. CONCLUSION AND FUTURE WORK

Cloud computing is emerging and demanding shared computing resources available from the Internet. When we use these services wisely it will help to reduce cost and capitalize investment for management. But there are several challenges to be faced by cloud computing such as data security and privacy issues. In this paper,

we have discussed the issues related to data location, storage, data security, network security, privacy, confidentiability availability and integrity. Establishing trust is the way to overcome these security issues as it establishes entities' relationship quickly and safely. In this paper, we have conducted a review of literature on the trust management systems. Majority of the proposed systems put special emphasis on the CIA (Confidentiality, Integrity and Applicability) model. Based on the critical analysis and the gap analysis, we intend to conduct research on security and integrity issue as a continuum to this research.

REFERENCES

[1] Akhil Bhel, "Emerging Security Challenges in Cloud Computing", Information and Communication Technologies, 2011 World Congress on, Mumbai, 11th - 14th Dec 2011, pp 217 - 222, Print ISBN: 978-1-4673-0127-5, DOI: 10.1109/WICT.2011.6141247.

[2] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE 3rd International Conference on Communication software and Networks(ICCSN), 27-29 May 2011, pp 245-249, Print ISBN: 978-1-61284-485-5, DOI: 10.1109/ICCSN.2011.6014715.

[3] K.Mukherjee, G.Sahoo, "A Secure Cloud Computing", International Conference on Recent Trends in Information, Telecommunication and Computing, Mar 12th 2010, Washington DC, pp 369-371, ISBN: 978-0-7695-3975-1, DOI: 10.1109/ITC.2010.95.

[4] Eman M.Mohamed, Hatem S Abdelkader, Sherif EI-Etriby, "Enhanced Data Security Model for Cloud Computing", 8th International Conference on Informatics and Systems(INFOS), Cairo, 14-16 May 2012, pp 12-17, Print ISBN: 978-1-4673-0828-1.

[5] Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 21-23 April 2012, pp 1216-1219, Print ISBN: 978-1-4577-1414-6, DOI: 10.1109/CECNet.2012. 6202020.

[6] K. opovi and Z. Hocenski, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, (**2010)** May 24-28.

[7] Soeung-Kon, J. -H. Lee and S. W. Kim, "Mobile Cloud Computing Security Considerations", Journal of Security Engineering, no. 9, (**2012)** April.

[8] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", Wireless Communications and Mobile Computing - Wiley, (**2011)** October.

[9] A. N. Khana, M. L. M. Kiaha, S. U. Khanb and S. A. Madanic, "Towards secure mobile cloud computing: A survey", Future Generation Computer Systems, vol. 29, Issue 5, (**2013)** July.

[10] M. R. Prasad, J. Gyani and P. R. K. Murti, "Mobile Cloud Computing: Implications and Challenges", Journal of Information Engineering and Applications, vol. 2, no. 7, (**2012)**.

[11] W. Jia, H. Zhu, Z. Cao, L. Wei and X. Lin, "SDSM: A secure data service mechanism in mobile cloud computing", IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), (**2011)** April 10-15.

[12] D. Popa, M. Cremene, M. Borda and K. Boudaoud, "A security framework for mobile cloud applications", 11th Roedunet International Conference (RoEduNet), (**2013)** January 17-19.

[13] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource Allocation for Security Services in Mobile Cloud Computing", IEEE Infocom 2011 Workshop on M2MCN, (**2011)**.

[14] K. Julisch and M. Hall, "Security and Control in the Cloud", Information Security Journal: A Global Perspective, vol. 19, **(2010)**, pp. 2099-309.

[15] D. Mohammed, "Security and Cloud Computing: An Analysis of Key Drivers and constraints", Informatio Security Journal: A Global Perspective, vol. 20, **(2011)**, pp. 123-127.

[16] S. A. Almulla and C. Y. Yeun, "Cloud Computing Security Management".

[18] D. Sun, G. Chang, L. Sun and X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environment", Procedia Engineering, vol. 15, **(2011)**, pp. 2852-2856.

[19] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering, IEEE.

[20] B. R. Kandukuri, R. Paturi V and Dr. A. Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing, IEEE.

[21] Zhidong Shen, Qiang Tong " The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems, Dalian, (ICSPS), 5-7 July 2010, Vol 2, pp 11-15, Print ISBN: 978-1-4244-6892-8, DOI: 10.1109/ICSPS.2010.5555234.

[22] Eystein Mathisen, "Security Challenges and Solutions in Cloud Computing", International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 31 May -3 June 2011, Daejeon, Korea, pp 208-212, ISBN: 978-1-4577-0872-5.
[23] Amani S. Ibrahim, James Hamlyn-Harris and John Grundy, "Emerging Security Challenges of Cloud Virtual Infrastructure", 17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop, 30 November-03 December 2010.
[24] Miika Komu, Mohit Sethi, Ramasivakarthik Mallavarapu, Heikki Oirola and Rasib Khan, Sasu Tarkoma "Secure Networking for Virtual Machines in the Cloud", Cluster Computing Workshops (CLUSTER WORKSHOPS), IEEE International Conference, Beijing, 24-28 Sept. 2012, pp 88 – 96, Print ISBN: 978-1-4673-2893-7, DOI: 10.1109/ClusterW.2012.29.
[25] Sebastian Biedermann, Martin Zittel and Stefan Katzenbeisser, "Improving Security of Virtual Machines during Live Migrations", Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference, Tarragona, 10-12 July 2013, pp 352 - 357, DOI: 10.1109/PST.2013.6596088.

Web Sources

[a] http://aws.amazon.com/
[b] Amazon, "Amazon Elastic Compute Cloud (Amazon EC2)", http://aws.amazon.com/ec2/.
[c] http://code.google.com/appengine
[d] http://www.microsoft.com/windowsazure/
[e] Amazon, "Amazon Simple Storage Service (Amazon S3)", http://aws.amazon.com/s3/.
[f] Google Apps, "Get online email, calendar documents and more working for your organization", http://www.google.com/apps/index1.html.
[g] Salesforce, "Software as a service – SaaS", http://www.salesforce.com/saas/.
[h] D. Linthicum, "Cloud Computing? Thank SOA", [Online] Available at: http://www.thecloudtutorial.com/cloud-computingsoa.html.
[i] J. M. Willis, "Cloud Computing and the Enterprise", IT Management and Cloud, [Online] Available at: www.johnmwillis.com/ibm/cloud-computing-and-the-enterprise