Security Aspects of Mobile Cloud Computing

Deepak. G, Dr. Pradeep. B. S, Shreyas. S

Abstract— Cloud computing is a distributed computing system that offers managed, scalable and secured and high available computation resources and software as a service. Mobile computing is the combination of the heterogeneous domains like Mobile computing, Cloud computing & wireless networks.This paper mainly discusses the literature review on Cloud and the Mobile cloud computing. Here in this paper we analyse existing security challenges and issues involved in the cloud computing and Mobile cloud environment. This paper identifies key issues, which are believed to have long-term significance in cloud computing & mobile cloud security and privacy, based on documented problems and exhibited weaknesses.

Index Terms— Cloud, Mobile Cloud, SaaS, PaaS, IaaS, Virtualization, Latency, Reliability.

1 INTRODUCTION

As the need of information storage, retrieval and computing are increasing day by day, the approach of organization are moving towards the distributed architecture from the traditional monolithic processing and storage model to a Cloud based approach. Cloud computing incorporates virtualization, on-demand deployment.

Cloud computing is the latest addition to the myriad of distributed computing paradigm, it shifts the location of computing infrastructure to the network in order to reduce the costs associated with the management of hardware and software resources. Cloud computing is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. Cloud consists of the collection of services, applications, information, and infrastructure which comprises pools of computer, network, information, and storage resources.

Cloud environments - by virtue of their flexibility, openness, and often public availability, it challenges many fundamental assumptions on application security. Some of these assumptions are well understood, however many of them are still not understood. Cloud Computing is a particular challenge for applications across the layers of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud- based software applications needs a design of rigorous applications that resides in a classic DMZ. This includes the analysis of the traditional aspects of managing the confidentiality of the information, integrity, and availability. Since the data is public available security is the main concern for securing the theft of data or vulnerabilities [14] for these various security measures like encryption & access schemes has to be taken.

Mobile cloud computing is the usage of cloud computing in combination with mobile devices and mobile internet. Cloud computing exists when tasks and data are kept on the internet rather than on individual devices, providing on-demand access. Here in mobile cloud computing applications are run on a remote server and then sent to the user and also there is no need of powerful configuration for the mobile devices, since the complicated modules are processed on the cloud. Mobile cloud computing can also be defined as an extension of cloud computing with a new adhoc infrastructure based on mobile device. The main role of the mobile cloud computing is that the information is available at our finger tips anywhere at any time, so that users can access information in mobile cloud computing environment through mobile devices. Mobile cloud computing exploits users' information like location context, accessed services and network intelligence. The figure 1 shows the architecture of mobile cloud computing

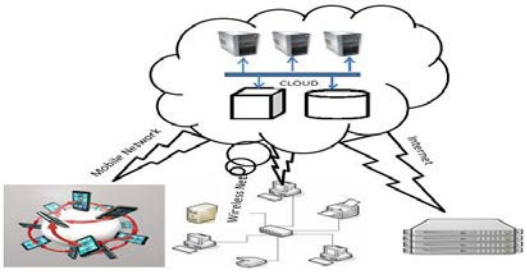

Figure 1: Architecture of Mobile Cloud Computing

Current internet security protocols have been struggling to keep up with the fast evolution from traditional data centers to today's mobile cloud computing technologies and the changing requirements following these advances. Traditional IT architecture uses a static security configuration, but today's

- **Deepak. G,** working as Assistant Professor at Dayananda Sagar College of Engineering, India, And pursuing **Ph.d** at VTU, Belgaum, India. His area of interests includes Security issues of Cloud & Mobile Cloud Computing. **Email-ID:-** deepak.dsce@gmail.com
- **Dr. *Pradeep B.S,*** working as a Director at International R&D division, Infotop Network pvt. Ltd., Linyi, China-276000. His area of interest includes Mobile computing, Security issues in Cloud and Mobile Cloud Computing. **Email-ID:-** pradeepbs78@yahoo.com
- ***Shreyas S,*** pursuing B.E degree in Department of ISE under VTU at Dayananda Sagar College of engineering, Bangalore, India. His areas of interest include wireless Communication, artificial intelligence and Cloud computing. . **Email-ID:-** shreyassrinath94@gmail.com

advanced mobile cloud computing architecture needs dynamic security configuration for handling mobile users.
Mobile cloud computing was defined on 5th March 2010 entry in the open gardens blog as "The availability of cloud computing services in mobile echo system". This incorporates elements, including consumer, enterprise, end-to-end security and mobile broadband-enabled services. Mobile cloud computing provides availability of the services in a mobile ecosystem. This incorporates elements including consumer, enterprise, femto-cells, transcoding, end to end security, home gateways and mobile broadband enabled services. The information housed on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of personal information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. This makes it critical for us to understand the security measures that our cloud provider has in place, and it is equally important to take personal precautions to secure our data [17]. The first thing we must look into is the security measures that your cloud provider already has in place. These vary from provider to provider and among the various types of clouds. What encryption methods do the providers have in place? What methods of protection do they have in place for the actual hardware that your data will be stored on? Will they have backups of our data? Do they have firewalls set up?.

2 Techniques involved in Cloud and Mobile Cloud Computing

Mobile cloud computing is unique from other computing models like global computing, grid computing, and internet computing in various aspects of on demand service provision, user centric interfaces, guaranteed Quality of Service and autonomous system's. The techniques used in cloud computing are as follows

1. Virtualization: It's a technology where we can allow the servers and the storage devices to be shared and utilised in an efficient manner. Virtualization has been the underlying concept toward cloud computing. The term visualize refers to providing an environment that is able to provide the services, supported by a hardware which could be observed on a personal computer, to the end users. The three existing forms of virtualization categorized as: storage virtualization, Server virtualization and Network virtualization.

2. Web Service and Service Oriented Architecture: Web services provide services over the web using technologies like XML, Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI). The service organisation in the core of cloud is managed in the form of Service Oriented Architecture (SOA) and can be defined as something that makes use of multiple services to perform a specific task.

3. Application Programming Interface (API): API's plays the vital role cloud computing. The cloud services depend on the APIs which allow's deployment and configuration through them. Based on the API category used viz. control, data and application, different functions of APIs are invoked and services are rendered to the users accordingly.
4. Web 2.0 /Mash-up: Web 2.0 has been defined as a technology that enables us to create web pages and allows the users to interact and collaborate as creators of user generated content in a virtual community. It enables the usage of World Wide Web technology towards a more creative and a collaborative platform. Mash-up is a web application that combines data from more than one source into a single integrated storage tool.
5. Logs & Audit Trails: Logs & audit trails majorly concentrates on the cloud security. The logs & audit trails helps the cloud providers to track the activities by the cloud users or customers. This also helps to track security breaches.

All According to a Gartner survey on cloud computing revenues, the cloud market was worth USD 58.6B in 2009, is expected to be USD 68B in 2010 and will reach USD 148B by 2014. These revenues imply that cloud computing is a promising platform. On the other hand, it increases the attackers' interest in finding existing vulnerabilities in the model [6].

3 Characteristics of Mobile Cloud and Cloud Computing

Some of the Essential characteristics of the cloud computing are as stated below [15]:-

1. On Demand Self-Service: Provides the computing resources automatically as it's needed.

2. Broad Network Access: Provides access to cloud resources over the network using standard mechanisms provided through thin or thick clients in a heterogeneous manner.

3. Resource Pooling: The resources are capable of being pooled to serve multiple clients using a multi-tenant model, with different physical and virtual resources in a dynamic way. The pooling and assigning of resources is done based on the changing needs of clients or consumers. Example: resources include computation capabilities, storage and memory.

4. Rapid Elasticity: Provides rapid capability provision, for quick scaling out and scaling in of capabilities. The capability available for provisioning to the client can be purchased as demanded.
5. Measured Service: allows in monitoring, controlling and reporting of usage.

6. Agility: improves the ability to re-provision the technological infrastructural resources.

7. Virtualization: plays a vital role in cloud computing where we could share the servers and storage devices and utilize them in an efficient manner. It also helps to migrate the application from one physical server to another physical

server.

4 CLOUD COMPUTING MODELS

Cloud provides offers services that can be grouped into 3 categories:-

Deployment Model	Managed By	Infrastructure Owned By	Infrastructure Located At	Accessible and Consumed By
Public	Third party provider	Third party provider	Off-premise	Untrusted
Private	Organization	Organization	On-premise Off-premise	Trusted
	Third party provider	Third party provider	On-premise Off-premise	
Managed	Third party provider	Third party provider	On-premise	Trusted or Untrusted
Hybrid	Both organization and third party provider	Both organization and third party provider	Both on-premise and off-premise	Trusted or Untrusted

Table1: Summary of cloud deployment models

1. Software as a Service (SaaS): Its can be referred as on demand software, it's a software delivery model in which software and associated data are centrally hosted on the cloud. SaaS is accessed by users using a thin client via a web browser. In SaaS, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customer's side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained, where cloud providers deliver applications hosted on the cloud infrastructure as internet based service for end users without installing the application on customer's computer [1], [2].

2. Platform as a Service (Paas): Platform as a service (PaaS) provides a computing platform and a solution stack as a service. The consumer creates the software using tools and/or libraries from the provider. The consumer also controls software deployment and configuration settings. The provider provides the networks, servers, storage and other services PaaS attempts to support use of the application by many concurrent users, providing concurrency management, scalability, and security. The customer has the freedom to build his own applications, which runs on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a prede-fined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP) etc. Services provided by this model include all phases of the system development life cycle (SDLC) and can use application program interface (API), website portals, or gateway software. Buyers do need to look closely at specific solutions, because some providers do not allow software created by their customers to be moved off the provider's platform.

3. Infrastructure as a Service (Iaas): IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. As the name implies, you are buying infrastructure. You own the software and are purchasing virtual power to execute as needed. This service model is based on the virtualization technology. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk.

5 CLOUD COMPUTING ARCHITECTURE

Deploying cloud computing can differ depending on requirements, each with specific characteristics that support the needs of the services and users of the clouds in particular ways. The cloud computing model has three service delivery models and main four deployment models [8]. The deployment models are:-

a. **Private Cloud** – the cloud infrastructure has been deployed, and is maintained and operated only for a specific organization. The cloud may be hosted within the organization or externally and is managed internally or by a third-party. This model does not benefit from the less hands on management, or from the economic advantages that make cloud computing such an intriguing concept.

b. **Public Cloud** – a public cloud can be accessed by any subscriber with an internet connection and access to the cloud space . The cloud infrastructure is made available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial implications compared to the capital expenditure requirements normally associated with other deployment options.

c. **Community cloud** – the cloud infrastructure is shared among a number of organizations with similar interests and requirements. It can be managed internally or by a third party and hosted within the organization or externally. The costs are shared among fewer users than a public cloud. Hence a community cloud benefits from medium costs as a result of a sharing policy. By means of comparison, with the private cloud the costs increase alongside the level of expertise needed.

d. **Hybrid cloud** – is a combination of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without being entirely dependent on third party services. Hybrid Cloud architecture requires both on-premises resources and off-site (remote) server based cloud infrastructure. Hybrid

clouds lack the flexibility, security and certainty of in-house applications. However, they provide the flexibility of in-house applications with the fault tolerance and scalability of cloud based services.

6 SECURITY ISSUES IN CLOUD COMPUTING

The fundamental factor defining the success of any new computing technology is the level of security it provides [12]. At-least we can access our hard drives and systems whenever we wish to, but cloud servers could potentially reside anywhere in the world and any sort of internet breakdown can deny us access to the data stored in the cloud. The cloud service providers insist that their servers and the data stored in them is sufficiently protected from any sort of invasion and theft. Such companies argue that the data on their servers is inherently more secure than data residing on a myriad of personal computers and laptops. However, it is also a part of cloud architecture, that the client data will be distributed over these individual computers regardless of where the base repository of data is ultimately located. There have been instances when their security has been invaded and the whole system has been down for hours.

Although cloud computing service providers touted the security and reliability of their services, actual deployment of cloud computing services is not as safe and reliable as they claim. In 2009, the major cloud computing vendors successively appeared several accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. This accident resulted in some network sites relying on a single type of storage service were forced to a standstill. In March 2009, security vulnerabilities in Google Docs even led to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours. It was exposed that there was serious security vulnerability in VMware virtualization software for Mac version in May 2009. People with ulterior motives can take advantage of the vulnerability in the Windows virtual machine on the host Mac to execute malicious code. Microsoft's Azure cloud computing platform also took place a serious outage accident for about 22 hours. Serious security incidents even lead to collapse of cloud computing vendors. As administrators' misuse leading to loss of 45% user data, cloud storage vendor Link Up had been forced to close. When it comes to Security, cloud really suffers a lot [7], [11]. The vendor for Cloud must make sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud. Some of the problem which is faced by the Cloud computing [9].

Data Integrity — when a data is on a cloud anyone from any location can access those data's from the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data's. Thus there is a lack of data integrity in cloud computing.

Data Theft—most of the cloud Vendors instead of acquiring a server tries to lease a server from other service providers because they are cost affective and flexible for operation. The customer doesn't know about those things, there is a high possibility that the data can be stolen from the external server by a malicious user.

Privacy Issues—the Vendor must make sure that the customer Personal information is well secured from other operators. As most of the servers are external, the vendor should make sure who is accessing the data and who is maintaining the server thus enabling the vendor to protect the customer's personal information [13].

Infected Application—Vendor should have the complete access to the server for monitoring and maintenance, thus preventing any malicious user from uploading any infected application onto the Cloud which will severely affect the customer.

Data Location—When it comes to location of the data nothing is transparent even the customer don't know where his own data's are located. The Vendor does not reveal where all the data's are stored. The Data's won't even be in the same country of the Customer, it might be located anywhere in the world.

Security on Vendor level — Vendor should make sure that the server is well secured from all the external threats it may come across. A Cloud is good only when there is a good security provided by the vendor to the customers.

Security on User level — Even though the vendor has provided a good security layer for the customer, the customer should make sure that because of its own action, and there shouldn't be any loss of data or tampering of data for other users who are using the same Cloud.

Data security and confidentiality issues — One of the biggest security concerns people have when moving to the cloud is related to the problem of keeping data secure and confidential. In this respect, some particular problems arise: who can create data, where the data is stored, who can access and modify data, what happens when data is deleted, how the Back-up is done, how the data transfer occurs, etc.

Lack of Standards — the immaturity of this technology makes it difficult to develop a comprehensive and commonly accepted set of standards. As a result, many standard development organizations were established in order to research and develop the specifications. Organizations like Cloud Security Alliance, European Network and Information Security Agency, Cloud Standards Customer Council, etc. have developed best practices regulations and recommendations. Other establishments like Distributed Management Task Force. The European Telecommunications standards Institute,

Open Grid Forum, Open Cloud Consortium, National Institute of Standards and Technology, Storage Networking Industry Association etc., centered their activity on the development of working standards for different aspects of the cloud technology. The excitement around cloud has created a flurry of standards and open source activity leading to market confusion. That is why certain working groups like Cloud Standards Coordination, TM Forum, and etc. act to improve collaboration, coordination, information and resource sharing between the organizations acting in this research field [10].

Interoperability issues – the cloud computing technology offers a degree of resource scalability which has never been reached before. Companies can benefit from additional computational needs, storage space, bandwidth allocation, etc. whenever they need and without great investments to support peak load demands. If the demand falls back the additional capacity can be shut down just as quickly as it was scaled up without any hardware equipment sitting idle. This great advantage has also a major drawback. It comes alongside with the risk of managing data within a shared environment (computation, storage, and network) with other cloud clients. Additionally, at one time one company may have multiple cloud providers for different services which have to be interoperable. In time, for different reasons, companies may decide to move their services to another cloud and in such a case the lack of interoperability can block or raise heavy obstacles to such a process. Cloud providers may find the customer lock-in system attractive, but for the customers interoperability issues mean that they are vulnerable to price increases, quality of services not meeting their needs, closure of one or more cloud services, provider going out of business, disputes between with the cloud provider.

Reliability breakdowns – another important aspect of the cloud computing is the reliability or availability of services. The breakdown of an essential service operating in a cloud has an impact on many clients. For example, in April 2012 there was a Gmail disruption that made Gmail services unavailable for almost 1 hour. The company first said that it affected less than 2 % of their customers, then they updated to 10 %, which sums around 35 million clients of a total of 350 million users. These incidents are not rare and evidence the customer lack of control over their data [4].

The irony is that, in terms of reliability, cloud providers have set high standards which are rarely achieved in an internal environment. However, because these outages affect large numbers of consumers it cast doubts in the minds of IT decision makers over the viability of replacing desktop functionality with the functionality offered by the cloud. Also, in this industry, the leading companies have set some high level quality services. Those levels are not easy to be reached by the other cloud service providers which do not have such a well-developed infrastructure. Unfortunately for the clients these quality services may come at higher costs and sometimes the decision makers, lured by the cheaper services, will be reluctant to collaborate with such a provider.

Malicious insider—a malicious insider is a person motivated to create a bad impact on the organization's mission by taking action that compromises information confidentiality, integrity, and/or availability. When sensitive data is processed outside the enterprise the organizational managers are less immediately aware of the nature and level of risk and they do not possess quick and direct capability to control and counter these risks. Experienced security specialists are highly aware of the inverse relationship between loyalty and risk. Even if trusted company employees can make mistakes or commit fraud and the outsiders are not automatically less ethical than them, it is prudent to invest company's long-term employees with higher trust. The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data and services with impact on the internal activities, organization's reputation and customer trust. This is especially important in the case of cloud computing due to the fact that cloud architectures require certain roles, like cloud administrators, cloud auditors, cloud security personnel, which are extremely high-risk.

Misunderstanding responsibilities – if in a traditional scenario the security of data is entirely the burden of the company owning data. In the cloud computing scenario the responsibilities are divided between the two actors: the cloud provider and the client. There is a tremendous potential for misguided risk management decisions if cloud providers do not disclose the extent to which the security controls are implemented and the consumer knows which controls are further needed to be adopted. If an IaaS service model is adopted, then the provider is responsible for physical security, environment security and the virtualization software security, whereas the consumer is responsible for securing everything else above this layer including operating system, applications and data. However, in an SaaS cloud service model the provider is responsible not only for the physical and environmental security but also for all the software services he uses in order to provide that particular software service to the client. In this case, the responsibilities of the consumer in the field of security are much lowered [3].

In case of a public-cloud computing scenario, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario. A public cloud acts as a host of a number of virtual machines, virtual machine monitors, and supporting middleware etc. The security of the cloud depends on the behaviour of these objects as well as on the interactions between them. Moreover, in a public cloud enabling a shared multi-tenant environment, as the number of users increase, security risks get more intensified and diverse. It is necessary to identify the attack surfaces which are prone to security attacks and mechanisms ensuring successful client-side and server-side protection. Because of the multifarious security issues in a public cloud, adopting a private cloud solution is more secure with an option to move to a public cloud in future, if needed.

Latency – this has always been an issue in cloud computing with data expected to flow around different clouds. The other factors that add to the latency are: encryption and decryption of the data when it moves around unreliable and public networks, congestion, packet loss and windowing. Congestion adds to the latency when the traffic flow through the network is high and there are many requests (could be of same priority) that need to be executed at the same time. Windowing is another message passing technique whereby the receiver has to send a message to the sender that it has received the earlier sent packet and hence this additional traffic adds to the network latency. Moreover, the performance of the system is also a factor that should be taken into account. Sometimes the cloud service providers run short of capacity either by allowing access to too many virtual machines or reaching upper throughput thresholds on their Internet links because of high demand arising from the customer community. This affects the system performance and adds to the latency of the system.

(i) IaaS Issues

VM security – securing the VM operating systems and workloads from common security threats that affect traditional physical servers, such as malware and viruses, using traditional or cloud-oriented security solutions. The VM's security is the responsibility of cloud consumers. Each cloud consumer can use their own security controls based on their needs, expected risk level, and their own security management process.

Securing VM images repository - unlike physical servers VMs are still under risk even when they are offline. VM images can be compromised by injecting malicious codes in the VM file or even stole the VM file itself. Secured VM images repository is the responsibilities of the cloud providers. Another issue related to VM templates is that such templates may retain the original owner information which may be used by a new consumer.

Virtual network security - sharing of network infrastructure among different tenants within the same server (using switch) or in the physical networks will increase the possibility to exploit vulnerabilities in DNS servers, DHCP, IP protocol vulnerabilities, or even the switch software which result in network-based VM attacks.

Securing VM boundaries - VMs have virtual boundaries Compared with to physical server ones. VMs that co-exist on the same physical server share the same CPU, Memory, I/O, NIC, and others (i.e. there is no physical isolation among VM resources). Securing VM boundaries is the responsibility of the cloud provider. Hypervisor security - a hypervisor is the "virtualizer" that maps from physical resources to virtualized resources and vice versa. It is the main controller of any access to the physical server resources by VMs. Any compromise of the hypervisor violates the security of the VMs because all VMs operations become traced unencrypted. Hypervisor security is the responsibility of cloud providers and the service provider. In this case, the SP is the company that delivers the hypervisor software such as VMware or Xen.

***(ii)* PaaS Security Issues**

SOA related security issues – the PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks. Mutual Authentication, authorization and WS-Security standards are important to secure the cloud provided services. This security issue is a shared responsibility among cloud providers, service providers and consumers.

API Security - PaaS may offer APIs that deliver management functions such as business functions, security functions, application management, etc. Such APIs should be provided with security controls and standards implemented, such as Oath, to enforce consistent authentication and authorization on calls to such APIs. Moreover, there is a need for the isolation of APIs in memory. This issue is under the responsibility of the cloud service provider.

(iii) SaaS Security Issues - In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers (software vendors). The SaaS model inherits the security issues discussed in the previous two models as it is built on top of both of them including data security management (data locality, integrity, segregation, access, confidentiality, backups) and network security. Web application vulnerability scanning - web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities using web application scanners. Such scanners should be up to date with the recently discovered vulnerabilities and attack paths maintained in the National Vulnerability Database (NVD) and the Common Weaknesses Enumeration (CWE). Web application firewalls should be in place to mitigate existing/discovered vulnerabilities (examining HTTP requests and responses for applications specific vulnerabilities). The ten most critical web applications vulnerabilities in 2010 listed by OWASP are injection, cross site scripting (Input validation) weaknesses [5].

Web application security miss-configuration and breaking - web application security miss-configuration or weaknesses in application-specific security controls is an important issue in SaaS. Security miss-configuration is also very critical with multi-tenancy where each tenant has their own security configurations that may conflict with each other leading to security holes. It is mostly recommended to depend on cloud provider security controls to enforce and manage security in a consistent, dynamic and robust way.

(iv) Cloud Management Security Issues the Cloud Management Layer (CML) is the "microkernel" that can be extended to incorporate and coordinate different components.

The CML components include SLA management, service monitoring, billing, elasticity, IaaS, PaaS, SaaS services registry, and security management of the cloud. Such a layer is very critical since any vulnerability or any breach of this layer will result in an adversary having control, like an administrator, over the whole cloud platform. This layer offers a set of APIs and services to be used by client applications to integrate with the cloud platform. This means that the same security issues of the PaaS model apply to the CML layer as well.

(v) Cloud Access Methods Security Issues

Cloud computing is based on exposing resources over the internet. These resources can be accessed through: Web browsers (HTTP/HTTPS), in case of web applications - SaaS; SOAP, REST and RPC Protocols, in case of web services and APIs – PaaS and CML APIs.; Remote connections, VPN and FTP in case of VMs and storage services – IaaS. Security controls should target vulnerabilities related to these protocols to protect data transferred between the cloud platform and the consumers [2].

7 ISSUES OF MOBILE CLOUD COMPUTING

Some of the Security issues relating to the Mobile cloud are as follows [15], [16]:-

1. Bandwidth: It's the one of major issue that is highlighted in a Mobile cloud computing environment since the radio resources for wireless network is in scarce compared to traditional wired networks.

2. Availability: the resources must be available for the users on the cloud. Mobile users must adopt a discovery mechanism so they can get connected to the cloud and share or access the resources as on the demand.

3. Heterogeneity: this challenge arises when the Mobile users access the cloud through different radio access technologies like GPRS, WIMAX, etc.

4. Security: Since the information is accessed from cloud using wireless technology it's important to secure the users information and communication. For securing the information on cloud we would have to use cryptographic technique to secure the information.

5. Authentication: To secure the data on the cloud we have to provide various authentication methods, so that user has to authenticate before he accessed the cloud.

8 CONCLUSION

Cloud computing, in the recent years, has taken the ability to prove its necessity in terms of data outsourcing. But it also poses a threat to the data owner in terms of privacy and security of data. As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud, such as e-mails, personal health records, company finance data, and government documents, etc. The fact that data owners and cloud server are no longer in the same trusted domain may put the outsourced unencrypted data at risk. The cloud server may leak data information to unauthorized entities or even be hacked. Although Cloud computing can be seen as a new phenomenon which is set to revolutionise the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. This paper helps to identify what mobile cloud computing is and what are the challenges and the issues relating to the Mobile cloud computing.

ACKNOWLEDGMENT

The authors are thankful to management of Rajarajeshwari College of engineering and Dayananda Sagar Institutions Bangalore, India for providing necessary facilities to carry out the research work.

REFERENCES

[1] Cloud Computing Security Issues by Florin OGIGAU-NEAMTIU.

[2] An Analysis of the Cloud Computing Security Problem by Mohamed Al Morsy, John Grundy and Ingo Müller.

[3] Security Issues for Cloud Computing by Kevin Hamlen, The University of Texas at Dallas, USA Murat Kantarcioglu, The University of Texas at Dallas, USA Latifur Khan, The University of Texas at Dallas, USA Bhavani Thuraisingham, The University of Texas at Dallas, USA.

[4] Cloud Computing Security Issues and Challenges by Kuyoro S. O., Ibikunle F. & Awodele O.

[5] Data Security and Privacy Protection Issues in Cloud Computing by Deyan Chen and Hong Zhao.

[6] Cloud Hooks: Security and Privacy Issues in Cloud Computing by Wayne A. Jansen, NIST.

[7] Cloud Computing Security Issues in Infrastructure as a Service by Pankaj Arora, Rubal Chaudhry Wadhawan and Er. Satinder Pal Ahuja.

[8] Security and Privacy Issues in Cloud Computing by Jaydip Sen.

[9] A review on cloud computing security issues & challenges by F. A. Alvi1, B.S Choudary N. Jaferry , E.Pathan

[10] Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques by Rohit Bhadauria and Sugata Sanyal.

[11]Hassan Takabi and James B.D. Joshi, "Security and Privacy Challenges in Cloud Computing Environments", IEEE computer and reliability societies, Nov/Dec 2010.

[12] Tharam Dillon, Chen Wu and Elizabeth Chang," Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[13] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and Security Issues", IEEE, 2010.

[14] Bernd Grobauer, Tobias Walloschek, and Elmar Stocker, "Understanding Cloud Computing Vulnerabilities, IEEE computer and reliability societies, Mar/Apr 2011.

[15] Weiguang SONG, Xiaolong SU, "Review of Mobile cloud computing", IEEE, 2011.

[16] Le Guan, Xu Ke, Meina Song and Junde Song, "A Survey of Research on Mobile Cloud Computing", 10th IEEE/ACIS International Conference on Computer and Information Science, 2011.
[17]Shahryar Shafique Qureshi, Toufeeq Ahmad, Khalid Rafique, Shuja-ul-islam, "mobile cloud computing as future for mobile applications – implementation methods and challenging issues", *Proceedings of IEEE CCIS, 2011.*