A Paper on Securing the Mobile Cloud Computing

R. Sathiyaraj, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
E-mail id - sathiya.peace@gmail.com

ABSTRACT: ***The cloud computing app on the mobile internet has tremendous business prospects. Nonetheless, it contributes to several security problems by integrating cloud technology with mobile Internet. One challenge is to develop a stable, mobile-based cloud infrastructure. After review of the safety risks and stable architectures of cloud computing available and taking mobile internet's features into account, this paper designs a general safe cloud architecture on mobile Internet which offers advantages such as multi-jerarchy, multi-level, elasticity, and cross platform and unified user interface. The use of cloud computing in mobile networks gives mobile users more advantages and possibilities, such as storing, downloading and computing data on demand, and offers these users more storage and computing power. Mobile cloud computing enables people to use mobile devices in full, everywhere and every time, to store, download, share and retrieve their personal data. The security risks have been an obstacle to mobile cloud computing's rapid adaptability. Major efforts have been put into developing stable cloud computing environments and facilities in academic institutions and academia. Despite these efforts, the safety strategies of mobile cloud computing still have a range of limitations and challenges.***

KEYWORDS: ***Cloud Computing, Applications, Network access, Authentication, Encryption, Mobile, Security.***

INTRODUCTION

Over recent years, there has been an enormous growth in the use of mobile technologies. According to Ericsson's annual mobile traffic survey, more than four billion smartphones will be available on the market by 2020 and 85% of the population worldwide will be using smartphones by 2020, rising by 85% between 2017 and 2019. The use of cloud computing has contributed directly to the increased use of mobile services, since they allow users to freely access and use various platforms and applications and enable them, at any point or anywhere, to store their data on remote servers. In addition to the risk of worms and other bad codes in mobile applications, despite multiple cloud services being used, a number of concerns remain regarding the security of restricting mobile device resources, the possibility of connection via a network, even if it is unsafe, and the lack of authenticity and encrypted platforms [1]. This paper work aims to develop a security platform for authenticating users and encrypting data. In order to produce a secure electronic signature, researcher use the features of "homomorphic encryption". Then researcher will use the multiple cloud computing features to enhance the authentication mechanism by splitting up verification tasks on different virtual machines so that the attacker can never retrieve or intercept the mobile users ' passwords or other personal details.

To order to avoid the threat of an intruder accessing the user account, researcher will also use a channel that classifies information according to their degree of sensitivities and creates a new password per new connection. As a major safety element of mobile cloud computing networks with high accessibility, researcher have developed a mechanism for recovery by adding a new backup server that communicates with the storing server and can be taken over by infection and attacks or the storage server [2]. The OS handles computer hardware resources and offers a user- and application device interface for hardware. The hypervisor is a software framework, which allows users to build virtual machines remotely on cloud servers. The virtual machine has hardware and a software stack specified by the user. Also in case of hardware failure the virtualisation phase would improve the availability of the users hosting services. The virtual machine can be transferred to another server with the full software stack, where host resources are not available without great care.

Virtualization is also beneficial to providers of cloud services. Following the study of the current cloud-based computing safety risks and safe architectures, this paper establishes a stable general cloud-based internet computing architecture that benefits from multi-hair engineering, multistage, elasticity, cross platforms and a single user interface. This paper analyzing the risks of cloud computing technology [3] and its secure architectures is designed according to the "SaaS (Security as a Service)" principle and its inner characteristics, multi-hierarchy, "multi-level Elasticity", "cross-platform" and "single-user Interface" General Secure Cloud Architecture on Mobile Internet. In order to examine the security hazards and the stable architectures of the cloud technologies, this paper establishes multiple Hierarchy, multi-level, elasticity, inter platform and a single user interface. SeaaS (Security as a Service) and the internal features of a mobile internet, i.e. multiple access modes, variety of applications. Security is a major concern when using the Cloud Mobile, as many attackers regularly seek to exploit mobile network vulnerabilities to access data stored on remote cloud servers. Increased security and data protection options can be offered via multi-cloud computing in place of a single cloud. It reduces the risk of data loss, doubles resources and allows protection activities to be split between many servers. Despite the use of multi-cloud infrastructure, there is also the potential for network access even though the security issues relate to limiting mobile device resources.

MOBILE COMPUTING SECURITY CONCERN

Here, introduce multi-cloud computing, homomorphic cryptography and MCC security, and present key threats and attacks within an MCC environment for cloud computing.

- *Computing Web Multi Cloud***:** Mobile cloud computing is a model for downloading applications and mobile data using cloud computing. This technology has changed lives because all necessary data, applications and services are now everywhere and at any time. The main use of mobile cloud computing is for deporting the personal data to remote cloud servers from the mobile device. Type in anything that people want. Then click Quill It on the right to paraphrase the input. The mobile cloud often benefits from these advantages in terms of protection because the information stored in the cloud often are very private and sensitive [4]. This means that attackers are targeted who seek to harness various vulnerabilities in computer networks so that data can be robbed or deleted. Therefore, it is better to use multi-cloud servers to reduce the risk of data loss and stop users from corrupting or stealing data, instead of using a single cloud database [5]. It is easier to remove data. The use of multi-cloud has opened up many security and mobile network management options.
- *Authentication homomorphic:* The standardized encryption makes the calculation without decryption of encrypted data. The homomorphic cryptosystem is used for data calculations saved on remote cloud servers without decryption. This computational principle has provided a wide range of security and information confidentiality opportunities and allows customers of cloud computing services to have greater privacy. Various cryptosystems, such as RSA and Pillar, are homomorphic. But it is a very limited crypto system as it takes so much time and calculative resources and only works to supplement or multiply. Some studies attempt, but sadly there is still no true application, to consider algorithms totally homogenous. Homomorphic encryption seems to be the ideal solution for cloud users, but it does pose problems as it takes so much time to calculate and uses mushy calculation resources. Some research tries to optimize time, but other studies use homomorphic encryption for very sensitive, small-size data or to compute digital signatures to achieve practical results. After evaluating the available cloud computing safety threats, safety architectures and taking the characteristics of mobile web consideration, the overall secure, and multi-hierarchy, elasticity, cross-platform and a single user interface cloud computing architecture has been built on mobile web.

First, the architecture involves a cloud secure application service resource category, e.g. data protection, cipher-text data query, confirmation of data integrity, early alert for security incidents and content security. Secondly, a cloud protected network infrastructure tool is designed for cloud computing, consisting of virtual machine isolation, protected virtual machine control, secure virtual machine replication and safe virtual machine mirror and the deployment of virtual technology on various device platforms, such as operating systems. Thirdly, the secure architecture provides various safety levels of cloud infrastructure, which refers to the available experience in the construction of mobile communication and internet network infrastructure due to various security requirements by different users. In the fourth position, the cloud security management framework is designed to control the user, to control key issues (cloud protection application, cloud-secure framework, cloud safe infrastructure), to provide comprehensive integrated protection and security management of the governed domain (web-based protected network, web-secure platform and cloud-based infrastructure).

- *Evaluation criteria for security frameworks*: Several of the security mechanisms provided in the survey concern file / data protection, generated and exploited on a mobile device or cloud server. The remaining frameworks cover the safety aspects of mobile apps or a mobile app that uses cloud services to improve mobile device capabilities. The survey therefore divides current MCC security frameworks into three categories: (a) data security frameworks and (b) security frameworks for applications. Computational specifications, scalability and assumptions play a major role in a stable implementation in an MCC environment.

SERVICE MODELS

Programming as a Service (SaaS), once in a while presented as a Service or Application Clouds, a specific cloud is answerable for a specific business capacity and business exercises, that is, they give applications/benefits through a cloud framework or stage as opposed to giving cloud highlights to them. Additionally, a cloud is considered to be a sort of standard application programming reasonableness, for models, Google Docs, Salesforce CRM, and SAP Business by Design. All in all, Cloud Computing isn't constrained to Infrastructure/Platform/Software as Service frameworks, despite the fact that it improves the abilities of these frameworks. I/P/SaaS can be viewed as explicit "utilization designs" for cloud frameworks which allude to models previously drew closer by Grid, Web Services, and so forth [6]. Cloud frameworks offer incredible potential to actualize these models and create them further. Stage as a Service (PaaS), a stage can plan computational assets dependent on the creating and facilitating attributes of utilizations and administrations. Typically, devoted APIs are utilized in PaaS to deal with the conduct of a server facilitating motor which performs and duplicates the exhibition dependent on customer requests. Every supplier uncovers his/her own API as per the separate center capacities, hence, applications can be improved for one explicit cloud supplier however can't be moved to another cloud have in spite of the fact that there have been endeavors to widen normal programming models with cloud capacities, for models; Force.com, Google App Engine, and Windows.

Framework as a Service (IaaS), otherwise called Resource Cloud, (controlled and adaptable), offers types of assistance to the client. Fundamentally, they give improved virtualization capacities. Various assets might be offered through an assistance interface: Data and Storage Clouds oversee access to information of conceivably powerful size, contrast asset activity and access requirements and/or quality definition, for models; Amazon S3, SQL Azure. Figure Clouds get ready access to computational assets, that is, the CPUs. Such low-level assets can't be utilized all alone and are commonly revealed as a feature of a "virtualized domain" (not to be joined with PaaS). Therefore, Compute Cloud Providers give the entrance to ordinarily virtualized figuring assets (for example crude access to assets, not at all like PaaS, which bears full programming stacks to improve and make applications), to perform cloudified administrations and applications. IaaS gives additional capacities over a basic process administration, for models, Amazon EC2, Zimory, and Elastichosts. There are some types of security threats associated with the compliance of programs in VMs to user requirements. For instance, if the protection level is met by the running environment and if the running flow is abnormal. Early alert functions and security audit functions include management of security policies, system log management and tactical audit management, etc. The mobile internet with a cloud computing model is a type of runtime system in which multi-sThis paperce and heterogeneous services coexist, while at the same time integrating safe customisation of services and protection with multi-level security.

MOBILE NETWORK USER'S SECURITY

There are numerous sorts of security vulnerabilities and dangers to various cell phones, for example, PDAs, PDAs, mobile phones, PCs, and so on. A few applications can likewise cause security and 7 protection issues for portable clients. The four paper principle issues concerning client or supporter security are talked about underneath:

1. *Security for versatile applications:*

Probably the most straightforward approaches to recognize any security dangers is to introduce and run security programming or an antivirus program on the cell phone. In any case, since cell phones have restricted handling capacities and force, it could be hard to ensure these gadgets against dangers. A few methodologies have been created to move the security and risk location systems, for example, validation, token administration, approval, and information encryption to the mists. Applications should experience a few degrees of danger assessment before it tends to be utilized by certain versatile endorsers. Confirmations will be completed to guarantee that all substance sent to the cell phones are not noxious in nature. Rather than running these enemy of infection and risk identification programming locally, cell phones just need to perform lightweight capacities, for example, executing follow transmitted to the cloud security servers [7].

2. *Privacy:*

Private data, for example, the client's present area and other significant information could bargain a user's, protection. For instance, the utilization of the worldwide situating framework (GPS) for area based administrations (LBS). These dangers to security can be limited by choosing and investigating the idea of the applications, and what are the particular administrations that ought to be moved to the cloud [8]. In any case, this offers ascend to worries that cloud suppliers or organizations will utilize and the data or give this data to government offices, and so on without the consent or information on the clients.

3. *Data:*

Proprietorship Another issue pertinent to Mobile Cloud Computing concerns responsibility for bought computerized media. With distributed computing, it is currently conceivable to store media records, for example, sound, video, and digital books remotely. This brings up the issue of who really possesses these media. On the off chance that a client purchased the media through a specific help and the media is put away in a remote stockpiling, there is the danger of losing access to the bought media.

4. *Data Access and Security:*

Issues identifying with access and security are critical to applications and software engineers that depend on remote information stockpiling and web access to work. For instance, the online schedule and contact applications are utilized by supporters of store significant dates and other client data, yet should a force blackout happen, at that point it would influence their day by day work. Portable Cloud Computing is powerless in light of the fact that it requires different focuses where access can be intruded. Fast and solid sign gathering can likewise antagonistically influence administrations to cell phones clients.

SECURITY OF APPLICATION

The security of utilizations manages the assurance of versatile applications or portable application models, which utilize the cloud assets to offer better types of assistance for portable clients in the MCC condition. A top, down spatial shrouding system, with or without advancement, was proposed by Wang and Wang (S. Wang and Wang, 2010). It uses the cloud assets to give a progressively adaptable, effective and better protection conservation system for area based administrations. The in-gadget spatial shrouding without improvement requires correspondence with the cloud server to get the client include in various framework cells. This procedure of correspondence causes delay and acquires overhead. Another method was proposed to conquer this correspondence postponement and overhead called the in-gadget spatial shrouding with streamlining. The viability of this strategy relies upon the recorded lower bound of the quantity of clients in every matrix cell. This verifiable information is utilized to foresee the quantity of client in every cell. On the off chance that this isn't right, at that point client protection can be undermined. The cloud is additionally liable for keeping up and sharing every phone's chronicled data during fire up. This support and preparing of verifiable data forces extra weight on the cloud, when contrasted with different methods.

MCC SECURITY PROBLEMS

Mobile cloud computing has become very popular and is used by various users more and more. However, there are several restrictions preventing it from being used. In spite of massive technological developments in the production of mobile devices, battery lives, storage capacity and computational power are still subject to constraints. Various security issues are also preventing Mobile Cloud Computing from reaching a more mature stage, especially in connection with its use in banking transactions, data sharing and data storage [9]. Many hackers are attempting to recover mobile users ' personal data via these security vulnerabilities. Several attacks, mainly targeting mobile cloud computing services, have been developed:

- Attack falsification- The attack permits attackers to forge digital signatures and tags for authentication or download requests during the interchange of data between the different entities within the network.
- Server Attack- As the data flow between users and cloud servers runs via the Internet, most hackers become authentic cloud servers to access the entire data stream. The attack of this kind occurs in a variety of different ways, including IP and MAC spoofing.
- Force and Reply attack- Data encryption requires significant computing capacity. The computing resource restrictions in mobile devices mean that users are vulnerable to brutes by using small encryption keys and Some attacks are designed to listen to the network to capture fragments that constitute users ' personal data to create a false identity and later to recover the data stored on the cloud server.

SECURE CLOUD COMPUTING MOBILE INTERNET ARCHITECTURE

Target of project- The development goal for the Sea AS definition is: (1) guarantee security of information and privacy protection for different Internet mobile users; (2) ensure the security of cloud computing system virtualization operating environment; (3) provide custom security services according to the different requirements.

Safe design of architecture- Since examining the security and safe architectures of the available cloud computing and taking into consideration the characteristics of the mobile Internet, and overall stable cloud architecture with the advantages of a multi hair, a variety of levels, elasticity, cross-platform, and unified user interface has been developed [10].

SCHEME FOR AUTHENTICATION AND PRIVACY

Mobile devices also represent the most vulnerable to mobile networking because they are relatively easy to hack, consumer awareness of computer security typically is not available and mobile data can be retrieved quickly if they lose or steal. Mobile devices can easily be infected because of several vulnerabilities in mobile systems through malware or any other malicious program (11). Authentication in mobile cloud computing is considered a key element of security enforcement. The authentication process is important to verify the identity of the mobile user by preventing unauthorized access to mobile cloud accounts and to protect users from existing security threats. Therefore encryption solutions with the least possible computation, memory and space overhead are required in view of the limitations of mobile cloud computing.

DATA ENCRYPTION

Encryption encrypt client information prior to storing them on the cloud server to ensure security and confidentiality. But as researcher know, a large amount of data cannot be encrypted by mobile devices using a strong crypto systems, as it is overloaded. The encryption takes place according to the level of sensibility of data in order to circumvent this problem. This paper details in two main categories, i.e. sensitive data that is coded with robust cryptography systems such as RSA, and public data, which is coded by somewhat weak cryptography systems that do not need very much processing capacity and small key sizes such as triple DES to maintain a minimum level of security. This process allows information to be encrypted without the mobile device becoming overwhelmed in calculations. A new electronic signature is generated by the user from a single password, then he sends the signature and encrypted data to a remote cloud server in one package.

CONCLUSION

Mobile Multi Cloud Computing is being rapidly used because it provides vast network management facilities and mobility and versatility. Multi Cloud Computing is of major use in mobile networking, but there have been a number of security issues and they interfere with its use and deployment, both for mobile operators and cloud services. This process allows information to be encrypted without the mobile device becoming overwhelmed in calculations. A new electronic signature is generated by the user from a single password, then he sends the signature and encrypted data to a remote cloud server in one package. The architectural development and implementation is flexible to different scale systems with different actual requirements, can integrate various operating systems and heterogeneous networks seamlessly.

REFERENCES

[1] N. Fernando, S. W. Loke, and W. Rahayu, “Mobile cloud computing: A survey,” *Futur. Gener. Comput. Syst.*, 2013, doi: 10.1016/j.future.2012.05.023.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” *Wirel. Commun. Mob. Comput.*, 2013, doi: 10.1002/wcm.1203.

[3] J. Samad, S. W. Loke, and K. Reed, “Mobile Cloud Computing,” in *Cloud Services, Networking, and Management*, 2015.

[4] A. U. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, “A survey of mobile cloud computing application models,” *IEEE Commun. Surv. Tutorials*, 2014, doi: 10.1109/SURV.2013.062613.00160.

[5] A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. A. Madani, “Towards secure mobile cloud computing: A survey,” *Futur. Gener. Comput. Syst.*, 2013, doi: 10.1016/j.future.2012.08.003.

[6] I. Mobile, “IEEE COMSOC MMTC E-Letter Mobile Cloud Computing Dijiang Huang Arizona State University , Arizona , USA Vol ., No ., 2011 IEEE COMSOC MMTC E-Letter Vol ., No ., 2011,” *Computing*, 2011.

[7] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, “Security and privacy challenges in mobile cloud computing: Survey and way ahead,” *JThis papernal of Network and Computer Applications*. 2017, doi: 10.1016/j.jnca.2017.02.001.

[8] M. Satyanarayanan, “The emergence of edge computing,” *Computer (Long. Beach. Calif).*, 2017, doi: 10.1109/MC.2017.9.

[9] D. G. Feng, M. Zhang, Y. Zhang, and Z. Xu, “Study on Cloud Computing security,” *Ruan Jian Xue Bao/JThis papernal Softw.*, 2011, doi: 10.3724/SP.J.1001.2011.03958.

[10] L. E. Li and T. Woo, “VSITE: A scalable and secure architecture for seamless L2 enterprise extension in the cloud,” in *2010 6th IEEE Workshop on Secure Network Protocols, NPSec 2010*, 2010, doi: 10.1109/NPSEC.2010.5634451.

[11] C. Brindley, “Authentication and trust: Turning the cloud inside out,” in *ISSE 2010 - Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*, 2011, doi: 10.1007/978-3-8348-9788-6-7.