**Mobile Cloud Computing : Issues from Data Storage Security**

**1Fadhillah Moulita Andiani , I Nyoman Aditya Yudiswara**

**1Information and Technology Major, Faculty of Computer Science, Bina Nusantara University**

***Abstract-*** Cloud computing is a promising technology, which transforms the traditional Internet computing paradigm and IT Industry. Nowadays, the market of mobile devices is growing at very high speed and becoming an important thing for human needs. It makes cloud computing is expected to expand in mobile environments, where mobile devices and sensors are used as the information collection nodes for the cloud. Cloud computing in mobile environments called as Mobile Cloud Computing. However, users also concerns about data security. These concerns are originated from the fact that sensitive data resides in public clouds, which are operated by commercial service providers that are not trusted by data owner. Because of risk associated with data storage many IT professionals are not interested towards to Mobile Cloud Computing. This paper will explain : (i) Overview of Mobile Cloud Computing (ii) Issues of Data Storage in Mobile Cloud Computing (iii) Existing Solution for Data Storage (iv) Proposed Possible Solution To Provide Data Confidentiality.

**Keywords** : *cloud, cloud computing, mobile cloud computing, data storage, security*

1. **Introduction**

T

he cloud computing is used of computing resources (hardware and software) that are delivered as a service over a network like internet. Through internet and vital remote services cloud computing can do centralize data, applications without physical hardware, paying money and use services of computing by maintaining storage, memory and processing bandwidth. Today, cloud computing was expanded to mobile environments that everyone can be used anywhere and anytime. With the emergence of cloud computing in mobile web, mobile users can use infrastructure, platform, software provided by cloud providers on-demand basis. Mobile cloud computing brings new types of services and facilities for mobile users to take full advantages of cloud computing.

This paper will presents an data storage issues on mobile cloud computing. Section I provides a brief overview of mobile cloud computing, including definition and advantages.

Section II discusses the issue of data storage in mobile cloud computing. Section III presents several security mechanism of data stored. Then, section IV proposed a possible solution to provide data confidentiality. The last in section V will summarize and conclude the topic of this article.

I.1 Mobile Cloud Computing

Mobile cloud computing was introduced not long after the concept of cloud computing launched in 2007. It defined combining the cloud computing services in ecosystem of mobile that brings the cloud computing and wireless network, which provides wonderful services to the clients[1]. Mobile cloud computing itself is a new paradigm for mobile applications whereby the data processing and storage are moved from the mobile device to powerful and centralized computing platforms that located in clouds[2]. Mobile cloud computing provides business opportunities for mobile devices with user experiences.

Using mobile cloud computing, mobile devices do not need a powerful a configuration because all the computing modules can be processed in the clouds. But there are many limitations in mobile devices like limited processing power, low storage, less security, and unpredictable internet connectivity.

I.2 Advantages of Mobile Cloud Computing

Cloud computing is a promising solution for mobile computing due to many reasons. This section describe how the cloud can be used to overcome obstacles in mobile computing, thereby pointing out advantages of mobile cloud computing.

1. Improving data storage capacity

Storage capacity is important thing for mobile devices. Mobile cloud computing is developed to enable mobile users to access or store the large data on the cloud through the internet. The example is Image Exchange which utilizes the large storage space in clouds for mobile users[3]. This mobile photo sharing services enables mobile users to upload images to the clouds immediately after capturing. With mobile photo sharing services, users can access all images from any devices. Instagram and Facebook also the successful mobile photo sharing application, and it is also a typical example of using cloud in sharing images.

1. Extending battery lifetime

Besides storage capacity, battery is also one of the main concern for mobile devices. Computation offloading technique is proposed with the objective to migrate the large computations and complex processing from resource-limited devices to resourceful machines. This avoids taking a long application execution time on mobile devices which result in large amount of power consumption, evaluate the effectiveness of offloading techniques through several experiments. The results demonstrate the remote applications execution can save energy significantly[4].

1. Improving Reliability

Storing data or running an application on clouds is an effective way to improve the reliability since the data and application are stored and backed up on clouds. This reduces the chance of data and application may lost on the mobile devices. Mobile cloud computing also can be designed as a comprehensive data security model for both service provides and user, the cloud can be used to protect copyrighted digital contents from being abused and unauthorized distribution[5]. For example, back sounds copyright in youtube. Once users uploaded a video used back sound that do not have copyright, then youtube will automatically block the video.

1. **Issues of Data Storage in Mobile Cloud Computing**

Section I in this paper describe about advantages of mobile cloud computing and as explain in the advantages that data storage is an important thing for mobile devices. Even though mobile cloud computing provides less cost and less resource management, it also has some security threats especially in data storage. These point below presented the categorize of data storage issues in mobile cloud computing.

II.1 Data Privacy

Mobile cloud computing does not provide control over the stored data in cloud data center. The cloud service providers have full of control over the data, cloud also may perform any malicious tasks such as copy, destroying, modifying, etc. Although the cloud have full of control over the data, users still used it because of its simplicity. These situations lead to greater security threats to cloud clients. Once the data entity successfully attacked, it will leads to data breach and takes an unauthorized access to data of all cloud users and causes data lost on cloud. Especially for SaaS (Software as a Service) providers may also lost the technical data and have great risk over the data storage. Besides of that risk, data processing also has great risk while data being transformed among multiple tenants. Because of virtualization multiple physical resources are shared among users, this leads to launch attacks by malicious insiders of the organization. These situations may allow the malicious user to perform attacks on stored data of other customer while processing data[6].

II.2 Data Integrity

Data integrity is crucial in mobile cloud computing security as if data is not expected after transmission or storage on the cloud it could have huge security implications for a company which deals with a lot of sensitive data. Data storage and processing data take place on the cloud service provider’s end, outside of the mobile computing ecosystem and make data integrity is crucial[7]. Data integrity is of up most importance, more specifically the accuracy and consistency of the users ‘s data. The violation of the integrity of data can have a tremendous effect on mobile users and could mean business and economic loss as well other devastating losses to the user.

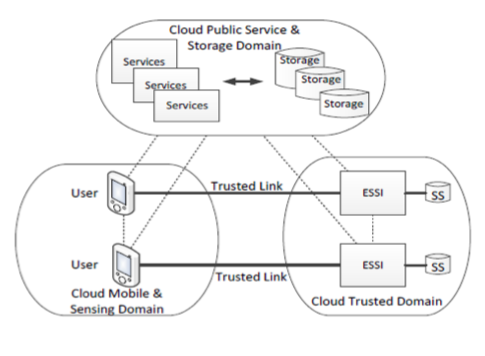
II.3 Data Recoverability and Vulnerability

The cloud ensures dynamic and on-demand resource provisioning to the users, due to resource polling and elasticity characteristic. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to obtain the data of previous users. The study has been conduct to data recovery, it were able to recover Amazon machine images files 98% of the times. The data recovery vulnerability can be major threats to the sensitive user data[8].

**III. Various Existing Solution for Data Storage**

For the last few years Mobile Cloud Computing has been an active research field. In this paper the main focus in securing data storage in mobile cloud computing. Significant efforts have been devoted in research organization to build secure mobile cloud computing. This section explain the various methodologies for data security in mobile cloud computing.

Anand Surendra Shimpi[9] proposed a secure framework for processing data in mobile cloud computing. This framework stores data in a secured fashion which helps in protecting the user’s privacy, called MobiCloud. In MobiCloud, a mobile device can outsource its computing and storage services to its corresponding EESI and Secure Storage(SS).



**Figure 1. Reference Service Model of Mobile Cloud**

The proposed new secure data processing mobile cloud infrastructure is highlighted in Figure 1, which mobile cloud is composed by three main domains: cloud public service and storage domain, cloud mobile and sensing domain, and cloud trusted domain. In this framework, each mobile devices is virtualized as an EESI in the cloud trusted domain and each EESI can be represented as an service domain in a particular application. The networking between a user and its EESI is through a secure connection, e.g., SSL, IPSec, etc. Anand Surendra have developed a pilot mobile cloud system to implement the cloud trusted domain as presented in Figure 1, named “Focus Drive”. It used to improve the driving safety of teenage drivers in collaboration with their parents.

Jibets Mishara[10] proposed a secure architecture for MCC to integrate mobile applications with the various cloud services. This secure architecture improves the storage and processing data on mobile devices in a secured manner. It helps in maintaining the integrity and security of data. Itani et al[11] proposed an Energy efficient framework for integrity verification of storage services using incremental cryptography and trusted computing. This framework results in saving 90% of processing energy of mobile devices when compared to other conventional techniques with more security.

Eugene E. Marinelli [11] developed Hyrax, a platform from Hadoop which supports cloud computing on Smartphones. It allows user’s applications to utilize data and computing process on networks on Smartphones. It offers a sane performance in data sharing and tolerates node departure. Eugene also implemented a distributed media search and data sharing approach.   
  
The other existing solution is from the mobile platform providers (e.g Android, IOS). It is implemented several security solutions to secure user data and applications. These solution were included into the operating system of the devices. Five types of security features have been implemented by the difference platforms: traditional access control, application provenance, encryption, isolation and permission-based access control. Each mobile platform implements a different strategy to secure data. The application of these strategies will allow securing data on the mobile device, however, when the data will be sent and stored in the Cloud, it will become out of the user control.

The solution before is from mobile based from platform providers. From cloud side there are other framework to give solution for purposed to secure data access, it is called “Mobile cloud framework elastic applications”. But this solution is provided for specific application model , i.e elastic application with code migration. However, the solution presented in cannot be applied to these new models, i.e component-based applications.  
  
SSL protocol is commonly used solution based from The mobile cloud application providers have to secure the data exchanged between the mobiles and Cloud. But as it has already been proved that SSL increases the energy consumption of mobile devices.  
  
Jia et al. provide a secure data service mechanism through Identity based proxy re encryption. This mechanism provides confidentiality and fine grained access control for data stored in cloud by outsorcing data security management to mobile cloud in trusted way.The goal of this protocol is that only authorized persons/sharer can access the data while unauthorized persons will learn nothing. In this mechanism 3 entities are involved: Data Owner (DO), Data Sharer (DS) and Cloud Servers. Both DO and DS utilize data storage service to store and retrieve file. CS provide services to mobile clients.   
  
Yang et al. provides provable data possession scheme of resource constrained mobile devices by using Diffie-Hellman key exchange, Bilinear mapping and Merkle Hash Tree (MHT ) . Diffie-Helman key exchange is used to securely distribute symmetric key, MHT is constructed as a binary tree where leaves in MHT are the hash value of authentic data. There are 3 participants involved in this scheme. First is Mobile end user. It has trusted Platform Model (TPM) chip in mobile device to produce and store secret key. It uses the services provided by cloud. The second is Trusted Party Auditor (TPA). It is performs all encryption/decryption on behalf of mobile user. The third is Cloud Storage Service Provider (CSP). It provides storage service to client and also provide proof of data possession by any number of times whenever needed and then get data.   
  
Zhou et Al. proposed a scheme for efficient and secure data storage operations by introducing the concepts of Privacy Preserving Chipper text Policy Attribute Based Encryption (PP-CP-ABE) and Attribute Based Encryption (ABDS) system. Through PP-CP-ABE lightweight devices can securely outsource encryption/ decryption operations to Cloud Service Provider (CSP).There are 5 entities involved this scheme. First is Data Owner (DO): It can be wireless mobile device or a sensor which uses the storage service of cloud. The second is Trust Authorithy (TA), It is responsible for distributing cryptography keys and is very trusted. The third is Encryption Service Provider (ESP): It encrypts the file of data owner without knowing the actual encryption key. In this scheme encryption operations are offloaded to ESP. The fourth is Descryption Service Provider (DSP): DSP provide decryption service to data owner. DSP does not have any information about actual content.   
And the last is Storage Service Provider(SSP). It provides storage services to clients. Before uploading file on the cloud, file is encrypted by ESP.

**IV. Possible Solution to Provide Data Confidentiality**

From all discussed issues, data security is the most prevalent issue during data transfer. Here are some possible solution to provide data confidentiality. The first is to create a new model of security where Detection System (IDS) and Cloud Intrusion Detection System Services (CIDSS) take place in the cloud which obviously saves the device CPU process and memory. This detection services solution gave several benefits : better detection malicious code, reduced consumption of resources on mobile devices, and reduced software complexity of mobile devices.

The second solution is achieve the security by implementing the homomorphic encryption mechanism with the combination of level-6 encryption that can be adopted when the data passes between cloud, mobile and cloudlet without any requirement of external applications. Level-6 encryption is mainly used for secure text encode and decode which requires the use of JavaScript and browsers. To save the mobile resources, level-6 encryption should rely and be executed remotely on the cloud.

This solution provides the best security and scalability feature during data sharing:

* If the data with malicious codes are downloaded by a user, the cloud account and data will be extracted and the unfair accounting will occur.
* Only verified data should be downloaded and the applications with abnormal activities should be blocked.
* Through broadcasted SSID, the information can be leaked and unauthorized user can gain access.
* Disable the SSID broadcast and utilize an enhanced key authentication algorithm.

Besides the two solutions above, there are also another solutions to protect data in the organization :

1. Protect the data with proactive security plan.

Security planning is not an easy task for an organization. This includes understanding the threat landscape (i.e. hacking cybercrime attacks, media & social scams, etc.) and working to protect the organization against these threats, require both policy and technology.

1. Prepare the response to the inevitable sophisticated attacks.

With the evolution of advanced continual threats, hackers aim on finding vulnerability. It is certain that eventually the organization will move towards data breach. Since the malware attacks are on the increase in today’s technology, the unified and tested response plan is under critical state for the right resources and skills.

1. Promote the culture of security awareness.

It is important to note that the careless mistakes of one employee will affect the master plan of chief security officer. That’s why every employee must work in a group with security professionals to ensure the safety of enterprise data. Security must be built on the culture of the organization.

**V. Conclusion**

The concept of cloud computing provides a great opportunity to users to utilize their services by on-demand basis. The requirement of mobility in cloud computing gave birth to mobile cloud computing. MCC provides more possibilities for access services in convenient manner. It is expected that after some years a number of mobile users will going to use cloud computing on their mobile devices.

There are many issues in mobile cloud computing due to limitations of mobile devices. Security is the main concern in mobile cloud computing. In mobile cloud computing data of owner is stored on the cloud, which is not secured.

This paper has provided the description about the basics of mobile cloud computing and advantages of mobile cloud computing. Mainly it discussed about issues of data storage in mobile cloud computing. This paper has explored a number of mechanisms for providing data security so that mobile cloud computing can be widely accepted by a number of users in future. It also proposed a mechanism to provide confidentiality.

**REFERENCES**

[1] Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud ,”Mobile Cloud Security Issues and Challenges: A Perspective”, International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 1, July (2013),pp.25-28.

[2]White Paper, Mobile Cloud Computing Solution Brief. AEPONA, 2010.

[3]Vartiainen, and K. V. -V. Mattila, “User experience of mobile photo sharing in the cloud,” in Proceedings of the 9th International Conference on Mobile and Ubiquitous Multimedia (MUM), December 2010.

[4]J. Yang, H. Wang, J. Wang, C. Tan, D. Yu1, “Provable data possession of resource constrained mobile devices in cloud computing,” Journal of Networks 6 (7) 1033–1040, 2011.

[5]P. Zou, C. Wang, Z. Liu, and D. Bao, “Phosphor: A Cloud Based DRM Scheme with Sim Card,” in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), pp. 459, June 2010.

[6]C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Services Comput. 5 (2) 220–232, 2012.

[7]S. L. Albuquerque and P. R. Gondim, “Security in cloud-computing-based mobile health,” It Professional, vol. 18, no. 3, pp. 37–44, 2016.

[8]O.D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, O.S. Ogundele, Elliptic curve cryptography for securing cloud computing applications, Int. J.Comput. Appl. 66 (2013).

[8]Anand Surendra Shimpi and R. Chander,“Secure Framework in Data Processing for Mobile Cloud Computing”, International Journal of Computer & Communication Technology, ISSN (Print) 0975- 7449, vol. 3, Iss. 3, 2012

[9] Jibitesh Mishra, Sanjit Kumar Dash and Sweta Dash, “Mobile Cloud Computing: A Secure Framework of Cloud Computing for Mobile Application”, Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012, pp. 347- 356.

[10] Itani et al, “Towards secure mobile cloud: A survey”, Proceedings of Analyses paper, 2012

[11] Eugene E. Marinelli, “Hyrax: Cloud Computing on Mobile Devices”, Dissertation of Thesis, Carnegie Mellon University, Pittsburgh, 2009