ISSN:0975-9646

Security in Mobile Cloud Computing: A Review

Prashant Pranav#1, Naela Rizvi#1

1,1 Master's Scholars, Department of Computer Science & Engineering,
Birla Institute of Technology, Mesra
Ranchi, Jharkhand, India

Abstract.- With the implementation of cloud platforms in mobile system, the storage of bulk data by client has become easier. IT Industries are also exploiting the benefits of cloud computing by producing more and more smart phones that takes full benefit of the features of clouds. As the use of smart phones by users is increasing rapidly, the issue of security related to use of cloud computing technique in mobile computing environment has emerged as one of the biggest challenges in this regard. Security with respect to mobile cloud computing can be addressed at three levels viz. mobile terminal, mobile network security, and cloud storage. Although many attempts have been made in developing a model which ensures privacy and security of data in mobile cloud system, no model is free from malicious attacks. In this review paper, we have focused on few models which are aimed at giving security and privacy of data in mobile cloud.

Keywords- Mobile cloud, cloud computing, security, privacy, architecture

I. Introduction

Cloud computing and mobiles are two significant technological trends observed in last few years. When cloud computing, mobile computing and wireless networks are combined together such that rich computational resources can be given to mobile users, it gives rise to Mobile Cloud Computing. Network operators as well as cloud service providers also enjoy the availability of rich computational resources as such. Because of mobile cloud computing, all the computational power and storage capacity which were previously with held with mobile devices are transferred to more powerful and centralized platforms located in cloud. It provides various IT resources and information services over the mobile network by the means of on-demand self service. Mobile users are presented with new type of services and facilities by taking the full advantage of cloud computing. Resources in mobile cloud computing are located in various virtualized distributed computers and not on a single local computer. Different companies offer different mobile cloud products such as android operating system offered by Google for the benefits of consumers and enterprises. Geographic search and Google maps are new services launched by Google with the use of mobile terminals in cloud computing. Microsoft introduced a program called LiveMess which is a platform including software and services and through which users can access and share their data and applications. Apple introduced iCloud for storage and backup of data for apple users. Mobile cloud computing can break through the hardware limits of limited calculation ability and limited storage capacity and allows convenient access to data.

In section 2 we discuss the architecture of mobile cloud computing with services required at client's and servers' level. Security issues in mobile cloud computing at all the three levels is discussed in section 3 while section 4 gives a brief review of some of the literature related to security in mobile cloud. Section 5 gives the advantages, disadvantages and future work of the discussed models.

II. Architecture Of Mobile Cloud Computing

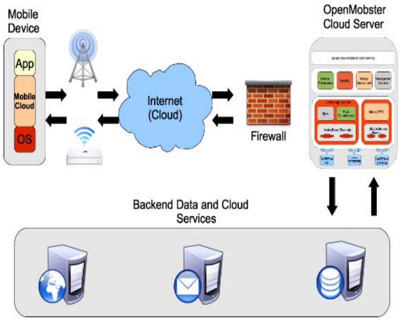

Fig. 1 Architecture of Mobile Cloud Computing Environment

A. *Services Required by Mobile Client*

Some of the services required by mobile cloud clients are discussed below:

- **Sync:** It keeps track of and synchronizes the state changes if any to the mobile or its application.
- **Push:** Any state update from the cloud server is managed by push.
- **OfflineApp:** It manages and creates the coordination between services such as Sync and Push.
- **Network:** It establishes proper communication easily and handles the communication channel which is used for receiving Push notification from the server.
- **Database:** Local data storage for the mobile application is managed by databases.

B. *Services Required by Mobile Server*

Some of the services needed by mobile cloud servers are discussed

- **Sync:** It synchronizes device side app state changes with the original location of data. It also needs to mobilize the backend data.
- **Push:** It monitors data channels from backend for updates and once updates are detected devices gets notification regarding this.

- **Secure Socket-Based Data Services:** On the basis of security requirements, this service must provide plain socket server or a SSL-based socket server or both.
- **Security:** Authentication and authorization services are provided by this service in order to allow mobile devices connected to cloud server to access the system.

III. Security Issues In Mobile Cloud Computing

Below we address the security in mobile cloud computing at three levels:

A. *Mobile Terminal*

It is an open operating system which allows wireless access of internet anytime anywhere. It also supports third-party software and personalization. So security issues in mobile terminals are very important and as such below we discuss them with respect to malware, software vulnerabilities and other point of view.

1) *Malware:* Malware gets access to personal information of users as they automatically downloaded and carried which remains unknown to the users. So many anti malware software have been developed but due to limited resources and capacity of mobile terminals significant computational resources are difficult to achieve. So, solutions for malware detection and prevention in mobile terminals are needed.

2) *Software Vulnerabilities***:** In case of application software, user name and password are transferred to network by using FTP and these are stored in clear text format. This allows illegal access of mobile phones from computers on the same network and so personal information not remains secured.

Where as in operating system, there exist coding bugs and in some conditions these leads to the destruction of mobile phones by attackers.

B. *Mobile Network Security*

The mobile devices can access the network in many ways such as by using phone services, sending Short Messaging Service (SMS) and other internet services. Also through Wi-Fi and Bluetooth network can be accessed by smart phones. So, these accesses modes lead to security threats and malicious attacks.

C. *Mobile Cloud*

The security in mobile cloud is addressed with respect to two issues viz. platform reliability and data and privacy protection. These two are discussed below:

Platform Reliability: Because cloud provides high storage of valuable information resources, so there is always the threat of being attacked. These attacks may be from outside malware, cloud users or insiders. The target of the attackers is to destroy the cloud services. For example DOS (Denial of Service) close the services of the cloud by destroying the platform available.

Data and Privacy Protection: The ownership and management of users' data resides at separate locations and also the users do not know the exact location of the infrastructure where their data are stored. So, data protection and privacy is of great concern in mobile cloud computing environment.

IV. LITERATURE REVIEW RELATED TO SECURITY ISSUES IN MOBILE CLOUD COMPUTING ENVIRONMENT

Few papers have been reviewed on the basis of security related issues in mobile cloud computing environment. All of them have their respective merits and demerits. While [1, 4, 5 and 6] increase privacy as well as performance of the system, secure storage of data is guaranteed by [1 and 6]. [2] Ensures maximum system reward and reduce expenses too. [8] is more efficient in terms of energy consumption. The papers are tabulated below with detailed description, methodology used and result achieved.

TABLE 1
COMPARISON OF VARIOUS SECURITY MODELS

An Efficient Model for Privacy and Security in Mobile Cloud Computing	This paper addresses the issue of privacy and the security of client in context of Mobile Cloud Computing. Two models viz. Mobility Node Model (MNM) and Centralized Owner Model (COM) are presented which tackles the issue of security by the user of proxy server and trusted leader respectively.	IBE (Identity Based Proxy Encryption) scheme is used to develop two models namely MNM and COM. IBE protocol works in 6 steps : 1) Setup, 2) Key Generation, 3) Encryption, 4)Re-Encryption Key Generation, 5)Re-Encryption, 6)Decryption The encrypted message on cloud server is forwarded by data owners. Cloud in turn maintains the storage capacity and computational power of data. Data owner authorize the mobile client to access the data from cloud	Overhead, accessibility of data, addition of new user and encryption time were compared for both models. MNM is more complex in terms of overhead and accessibility of data than COM because MNM requires a new key every time to serve request while COM works with the same key. Adding new users in MNM is more difficult than COM. COM is faster than MNM in terms of encryption time.

Security Aware Resource Allocation for Mobile Cloud Computing System	The request for using cloud resources by a mobile is classified according to the level of security requirement of a novel resource allocation algorithm proposed. SMDP based resource allocation model is also described in this paper	The problem of resource allocation in a secure way for mobile cloud computing system is formulated with a finite state SMDP under the average cost criteria. SMDP (Semi Markov Decision Process) is a form of Markov-Decision process in which the time of transition between decisions is a continuous time random variable having same probability distribution. At each step decision is taken regarding accepting the request or not and if accepted then efficient resource allocation for the request.	The SMDP-RAS strategy was evaluated in terms of request blocking probability and system reward. As the arrival rate increases, the system blocking probability becomes higher. For same arrival rates but increasing number of VMs the block probability decrease. The system reward increases as the traffic becomes heavier.
Resource Allocation for Security Services in Mobile Cloud Computing	Mobile devices uses cloud for searching, processing and mining. In order to achieve security cloud security services is classified into two categories namely Critical Security Services (CS) and Normal Security Services (NS). CS gives strong security protection but at the cost of consumption of more resources. CS users need to pay more than NS users.	In order to maximize the system reward due to increasing number of CS and NS users, a Security Service Admission Model (SSAM) is proposed. Semi-Markov Decision process is used to model the system reward. In the system model resources are constraint in some portion where each portion represents a VI. Mobile users choose some specific defined security services based on their location in the VI. The cloud decides whether to accept or reject the request	The blocking probability which is an important QoS parameter for mobile cloud is compared for various defined security services. Blocking probability gets lower as the number of network resources such as VIs increases. Also blocking probability increases with increase in arrival rate.
A Security Framework of Group Location-Based Mobile Applications in Cloud Computing	Many application providers outsource their database (ODB) because of powerful storage capacity and scalability of cloud. So, a secure framework focusing on location information of mobile terminals is used. For security issues of location based (LBS) services a security model using ODB is presented for LBS. A mechanism on top of the proposed framework is suggested which ensure enhanced privacy and authentication.	LBS security model using ODB based system is framed comprising of users, service providers and cloud databases. The authentication processor is activated after the verification of user identity and device identity. The LBS processor in turn asks for customer's precise location After that the service processor accesses the service related information from the cloud database. The above process is implemented through IMSI-Based JOIN Secure (IJS) algorithm. Through this algorithm user's true identity can be hidden.	The comparison of different key generation functions indicates the superiority of network coding for small data set as compared to popular hash functions.
A Study of Incremental Cryptography for Security Schemes in Mobile Cloud Computing Environment	As the resource constraints of mobile devices are limited, the confidentiality of the data to be uploaded on the cloud must be checked. Most of the available security schemes execute complex	To decrease TAT and energy consumption of a file modification operation, the original file is divided into equal sized blocks of n bits. Mobile users provide a password which is then transformed decryption and integrity keys.	Performance is evaluated in terms of TAT and energy consumptions for different operations. For uploading and downloading operations, the system takes more time to complete. For block modification operation,

	security operation remotely on cloud or trusted third party. An incremental cryptographic version of the EnS, CoS and SnS are compared with original version on the basis of TAT (Turn Around Time) and energy consumption.	Each block of file is encoded and final encrypted file is generated by performing some concatenation operation using cryptographic hash functions. Each block gets a message authentication code. After that user uploads and downloads files.	the proposed methods only encrypt and upload the modified block which in turn improves TAT and energy consumption of the device.
Efficient and Secure Data Storage Operations for Mobile Cloud Computing	A security framework is used for secure data storage in public cloud. A Novel Privacy-Preserving Cipher Policy Attribute-Based Encryption focusing on security of users is used. PP-CP-ABE ensures security of light-weighted devices by heavy encryption and decryption operation. Attribute-Based Data Storage (ABDS) system is used to achieve minimized overhead of computation storage and communication.	Encryption of data is done before forwarding it to SSP. The work of ESP is to provide encryption service to the data owner without knowing the actual Data Encryption Key (DEK). The decryption service provider (DSP), on the other hand provides decryption service required by users. The DSP does not know the data content. The data content cannot be revealed even if ESP, DSP and SSP collide. The ESP, DSP and SSP form the core of the proposed system.	The framework was analyzed for computation, communication and storage performance. Computation overhead is linear for ESP and DSP and constant for the user. SP perform more than 90% of the encryption and 99% of decryption. Storage performance was analyzed in terms of cipher text storage and key storage overhead. More storage space are available.
Secure Web Referral Services for Mobile Cloud Computing	Due to the browsing of malicious websites, the security of mobile users is at a great threat. In order to achieve security against phishing websites and SSLStrip-based MITM (Man In The Middle) attack anew secure web referral service called Secure Search Engine (SSE) for mobile devices is proposed.	SSE comprises of different components like SSE Service, SSL Verifier, Phishing filter, SSE crawler, URL Service, DNS Service and Storage Service, The crawler picks up an unprocessed URL from the set of URLs in the URL Service and then sends HTTP request. Crawler derives the IP address in the URL with the help of DNS Service and passes them to storage service. Crawling services operated within a certain time interval and so within the interval a new phishing website can be issued.	The performance of phishing filter was evaluated for false positive and false negative parameters. The percentage of false negative of the browser reduces as the time frame increases. The false positive of all the techniques are low and the result from SSE phishing filters are the lowest.
Policy Based Security Channels for Protecting Network Communication in Mobile Cloud Computing	A set of policy-driven security protocol is used for ensuring integrity and confidentiality of data in Mobile Cloud Computing. Trusted authority entities and the “elastic” virtualized nature of cloud is used to provide energy efficient key management mechanism. Implementation is done in a real cloud computing environment and saving are studied with respect to energy consumption and execution time.	A system model consist of mobile cloud client, cloud service provider (CSP), trusted key authority (KTA) which is trusted by both client and CSP. Two security channels are used: - Public Key Based Channel which links the cloud customer with KTA and KTA with KVM. - Symmetric Key Policy Based Security Channel that secures the actual client network communication with virtualized services. Four security protocols are proposed, three of which are supportive protocol and fourth one is main protocol.	Asymmetric key management policy based delegation reduces the energy consumption of the mobile client and enhances the service interaction time. The energy saving increases from 1.015 J (47.8%) with two cloud services to 9.869 J (89.9%) with 10 consumed services.

V. CONCLUSION AND FUTURE WORK

We have analyzed few security models of mobile cloud computing. While some possess specific advantages, they are also disadvantageous in some aspects. Like [2and 3] sometimes leads to rejection of request and hence affect system reward. Also system cost of mobile users increases. [4] Does not consider power consumption problem of mobile devices. [5] leads to extra file management overhead and [8] does not take into consideration the time and energy limit of users.

So, in the future, models can be developed which consider the security issues but not at the cost of system reward and mobile users' energy and time limit. Models can also be designed which ensures minimum overhead.

TABLE 2
MODELS: ADVANTAGES, DISADVANTAGES AND FUTURE WORK

Paper Name	Advantages	Disadvantages	Future Work
An Efficient Model for Privacy and Security in Mobile Cloud Computing	More secure storage of data in cloud. Secure connection between data owner and cloud and hence increased privacy.	MNM Model is not suitable for large environment and also adding new user is difficult. In COM Model same key is used for different mobile clients.	The implementation of relation between different trusted leaders internally can be focused.
Security Aware Resource Allocation for Mobile Cloud Computing System	SMDP-RAS strategy effectively meets the blocking probability requirement even though the request traffic is high.	Sometimes VMs are inefficient for incoming request due to limited system capacity. These leads to rejection of requests and system reward are affected.	Need for an optimal VM allocation strategy to handle incoming requests.
Resource Allocation for Security Services in Mobile Cloud Computing	It results in maximum system reward and reduces system service expenses	The system cost of mobile user increases due to large service holding time. So, system reward degrades	Optimal system resources will be considered in future to obtain maximum reward with considering more system metric for the construction of reward function.
A Security Framework of Group Location-Based Mobile Applications in Cloud Computing	IJS algorithm improves privacy, authentication and continuity.	Does not consider reasonably the computational weakness of the client and power consumption problem of the device.	Optimization of encryption mechanism based on IMSI characteristics can be done in future
A Study of Incremental Cryptography for Security Schemes in Mobile Cloud Computing Environment	Incremental version shows significant improvement in performance by performing the block(s) modification operation.	Initially for encryption and uploading, this version consumes more resources on mobile device. Extra file management overhead.	Model can be designed which prevents from excessive file management overhead and which allows for consumption of lesser resources initially while uploading and encryption.
Efficient and Secure Data Storage Operations for Mobile Cloud Computing	Using PP-CP-ABE, light weight device can securely perform encryption and decryption operation without revealing the data and perform outsourcing with service provider. ABDS effectively achieve optimal information in terms of minimizing overheads of computational storage and communication.	PP-CP-ABE suffers from linear growing cipher text size	A new CP-ABE scheme with constant cipher text size and with more privacy preserving outsourcing scheme. Implementation of a user space secure file system based on public cloud storage
Secure Web Referral Services for Mobile Cloud Computing	SSE phishing filter produces low false positive and false negative	Initially the SSE service takes more time to respond and build a cache.	Other web attacks such a s Cross-site Scripting (XSS) can also be secured using SSE.
Policy Based Security Channels for Protecting Network Communication in MCC	Reduces energy consumption considerably. Service interaction time also increases.	Time and energy analysis of the security operation in the cloud is not mentioned	The work can be done using symmetric key generation in future.

REFERENCES

[1] Ragini., Mehrotra, P., Venkatesan, S.: An Efficient Model for Privacy and Security in Mobile Cloud Computing. International Conference on Recent Trends in Information Technology, 1-6 (2014).

[2] Liu, Y., Lee, M.J.: Security-Aware Resource Allocation for Mobile Cloud Computing Systems. Computer Communication and Networks (ICCCN), 24th International Conference on, 1-8 (2015).

[3] Liang, H., Huang, D., Cai, L.X., Shen, X., Peng, D.: Resource Allocation for Security Services in Mobile Cloud Computing. IEEE INFOCOM 2011 Workshop on M2MCN, 191-195 (2011).

[4] Chen, Y.J., Wang, L.C.: A Security Framework of Group Location-Based Mobile Applications in Cloud Computing. International Conference on Parallel Processing Workshops, 184-190 (2011).

[5] Khan, A.N., Mat Kiah, M.L., Khan, S.U., Maddani, S.A, Khan, A.R.: A Study of Incremental Cryptography for Security Schemes in Mobile Cloud Computing Environments. EEE Symposium on Wireless Technology and Applications (ISWTA), September 22-25, 2013, Kuching, Malaysia, 62-67 (2013).

[6] Zhou, Z., Huang, D.: Efficient and Secure Data Storage Operations for Mobile Cloud Computing. Network and service management (cnsm), 2012 8th international conference and 2012 workshop on systems virtualiztion management (svm), 37-45 (2012).

[7] Xu, L., Li, L., Nagaranjan, V., Huang, D., Tsai, W.T.: Secure Web Referral Services for Mobile Cloud Computing. IEEE Seventh International Symposium on Service-Oriented System Engineering, 584-593 (2013).

[8] Itani, W., Kayssi, A., Chehab, A.: Policy Based Security Channels for Protecting Network Communication in Mobile Cloud Computing. Security and Cryptography (SECRYPT), Proceedings of the International Conference, 450-456 (2011).

[9] Suo, H., Liu, Z., Wan, J., Zhou, K.: Security and Privacy in Mobile Cloud Computing. Wireless Communications and Mobile Computing Conference (IWCMC), 9th International, 655-659 (2013).

[10] Dev, D., Baishnab, K.L.: A Review and Research towards Mobile Cloud Computing. 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 252-256 (2014).

[11] Shamir, A.: Identity–based cryptosystems and signature schemes, Advances in Cryptography,Procedings of Crypto’84 Lecture notes in Computer Science, 47{53}, (1984).

[12] Raj, H.., Nathuji, R ., Singh, A., England, P.:Resource Management for Isolation Enhanced Cloud Services, in Proceedings of ACM workshop on Cloud computing security, pp. 77–84 (2009).

[13] Lee, Y.T., Wang, L.C., Gau, R.C.: Implementation Issues of Location-Based Group Scheduling for Cloud Applications, in IEEE VTS Asia Pacific Wireless Communications Symposium Conference (APWCS 2010), (2010).

[14] Kumar, K., Lu, Y.H: Cloud Computing for Mobile Users: Can Offloading Computation Save Energy. Computer, vol. 43, no. 4, 51–56, (2010).

[15] Khan, A.N., Kiah, M.L., Khan, S.U., Madani, S.A.: Towards Secure Mobile Cloud Computing: A Survey, Future Generation Computer Systems, vol. 29, 1278-1299, (2013).