Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

State-of-the-art Security Mechanisms for Mobile Cloud Environments

Girish Neelakanta Iyer*
School of Computer Science and Technology
Karunya University, Coimbatore,
Tamil Nadu, India

Durga S
School of Computer Science and Technology
Karunya University, Coimbatore,
Tamil Nadu, India

Abstract— Mobile Cloud Computing (MCC) environments are characterized by several features such as flexible usage of Cloud resources, increased battery efficiency by offloading data processing into Cloud etc. One of the main issues in using Cloud services by mobile users, is the security concerns. Security issues in Mobile Clouds can be categorized into two types: security issues for mobile users such as privacy concerns and data storage and access in Cloud such as authentication and access control. In this paper, we provide a comprehensive survey of various security issues and solution approaches present in the literature. We compare and summarizes important contributions and features of such schemes.

Keywords— Cloud Computing, Mobile Cloud, Security, Access Control, Privacy

I. INTRODUCTION

Cloud Computing can be defined as a model which delivers applications as services (known as Software as a service or SaaS) over internet and providing hardware and system software for users to implement, deploy and maintain their custom-made applications and/or services [1]. The increased popularity and usage of mobile devices such as smart phones, laptops and tablets, mobile Clouds (MCC) are increasingly popular. The mobile Cloud Computing forum defines MCC [2] as follows:

Mobile Cloud Computing at its simplest, refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smartphone users but a much broader range of mobile subscribers.

Mobile devices are generally small in size, less in processing power and memory. They also suffer from constraints such as power limitations. Through Mobile Cloud Computing (MCC), such mobile devices should be able to access and use Cloud resources seamlessly. It helps to overcome many of the above issues by offloading some of the applications and/or data into Cloud. Security is one of the primary concerns in such environment. Frequent handovers, unreliable network access through wireless backbone and secure authentication are some of the security concerns. Several security vulnerabilities and threats such as malicious codes are known to mobile equipment. Further, several data management issues pertaining to MCC such as protection of end-to-end user data, need to be addressed. In this paper, we present a survey of the state-of-the-art security concerns and secure mechanisms in MCC environments.

Reminder of this paper is organized as follows: In Section II, we describe the key security challenges in Cloud Computing. In Sections III, IV and V, we describe a comprehensive classification and survey of various security mechanisms for MCC in literature. Finally Section VI concludes this paper.

II. KEY SECURITY ISSUES IN MOBILE CLOUD COMPUTING ENVIRONMENTS

There are several security issues for users in using mobile Clouds. In [3], the authors classify the security issues in MCC into two categories. The security for mobile users and the security for the data.

A. *Security for mobile users*

We now list some of the security issues from the user's perspective:

- Security for mobile applications: Installing and running security applications such as McAfee and Norton are the easiest and simplest way to detect issues such as virus and worms in mobile applications. But, mobile devices have limited processing and battery power which makes it difficult for the mobile users to install and use such heavy anti-virus applications.
- Privacy*:* Mobile users increasingly use location-based services due to the advantages of GPS positioning devices. Mobile users need to provide their private information such as location information to such services and it becomes potential threat to their privacy.

B. Securing data on Clouds

Users can store and access their data and applications in Cloud. When storing data in Cloud, several issues need to be addressed such as data authentication and integrity. Here, we list some of such issues [3]:

- INTEGRITY: Data integrity is an important concern by the mobile users. A typical solution to this should consider mobile specific issues such as energy consumption.
- AUTHENTICATION: Authentication is always an important issue when data resides in Cloud. Mobile clients need to be authenticated in an appropriate manner to access their data residing in the Cloud.
- DIGITAL RIGHTS MANAGEMENT: The unstructured digital information such as videos have often being distributed illegally and are pirated. These contents need to be protected from illegal access in MCC context.

III. SECURITY MECHANISMS FOR MOBILE USERS

In this section, we brief the security mechanisms proposed in the literature for mobile users. As mentioned before, privacy and security for mobile applications fall under this category.

In [4], the authors describe an appropriate access control model which has the ability to provide the security services based on the user permission. Further, the services can be altered according to the changes made in the permission. It results in increased flexibility, independence and expansibility of Cloud service access control. It also helps to realize the controllability, customizability and adaptability of Cloud security services for the mobile internet framework.

In [5], the authors propose a security model for Location based services (LBS) using outsourced databases (ODB) such as Amazon Simple DB [6] and demonstrate the use of distributed storage and International Mobile Subscriber Identity (IMSI) as user identification to secure the location data. It has enhanced privacy and authentication mechanisms. They also show that network coding schemes are better than hash function schemes.

In [22], the authors propose a dynamic method for secure access of Cloud in mobile environments which can permit the operation privilege of the mobile user who stores data or computes on cloud, to change automatically when the location and time change.

IV. SECURITY MECHANISMS FOR DATA SECURITY IN MCC

There are several proposals in literature addressing the security of data residing in the Clouds which needs to be accessed and modified by mobile devices. The main issues to be addressed include integrity, authentication and digital rights management.

In [7], the authors propose a model for protecting the traffic between endpoints and the Cloud. The approach is a Virtual Private Gateway (VPG) with layered security model, which provides multi-level protection of all the information, data, and physical assets including the data centres. It also addresses, DoS and DDoS protection and protection from both physical and logical security threats. In [8], the authors proposes an adaptable security model called as Security as a Service (SeaaS) which is a multi-layer, multi-level, elastic, across-platform and unified-user-interface Cloud computing secure architecture according to the characteristics of mobile internet.

In [9], the authors propose an intelligent and heterogeneous mobile access management scheme using the information available at Mobile Access Controller. The proposed Context Management Architecture (CMA) is responsible for acquiring, processing, managing and delivering context information. The key advantages include context awareness and content management. In [10], the authors propose a secure mobile Cloud data processing framework through trust management and private data isolation. Strict security policies are enforced through a distributed firewall system. The scheme also results in Standardization of identity management.

In [11], the authors propose a provable secure storage service with public provable data possession (PDP) for resource-constrained mobile devices in mobile Cloud computing. It also has a trusted computing technology for mutual authentication between end-users and third-party auditor. They have remote authentication of mobile end user. Other advantages include public PDP with the support of dynamic data update and this is the first scheme to explore the application of PDP scheme.

In [12], a security service admission model is proposed based on semi-markov decision process to model the rewards obtained by the critical security services. They classify security models in Cloud into critical security (CS) services and normal security (NS) services. It models admission control and resource allocation for Cloud security services. In [13], an elastic application framework is proposed for mobile Clouds. It identifies security threats and objectives for such elastic applications. This mechanism also supports secure migration of weblets between device and Cloud.

In [14], the authors propose a scheme to provide confidentiality and fine-grained access control for data stored in the Cloud. This mechanism enables the mobile users to enjoy a secure outsourced data services at a minimized security management overhead. It also proposes an identity based proxy re-encryption scheme to make mobile users easily implement fine-grained access control of data and also guarantee the data privacy in the Cloud. In this scheme, specifically, the mobile user can securely shift the data computing and distribution overhead to the cloud while the cloud has no idea about data content in the whole process. Additionally only authorized users can decrypt the cipher text while unauthorized users would learn nothing about the data.

In [15], a secure private Cloud architecture for mobile IaaS is proposed which emphasizes on authentication mechanisms and user access control. The scheme is flexible and provides on-demand access to Cloud services. In [16], the authors propose a practical and privacy-preserving solutions for mobile devices to the server based scheduling problem in Cloud environments. Algorithms take advantage of the homomorphic properties of well-known cryptosystems in order to privately and efficiently compute common user availabilities. We also formally outline the

privacy requirements in such scheduling applications. This scheme satisfies privacy properties and results in higher computation and communication efficiency.

In [17], a security solution approach for data security risk in mobile Cloud storage is discussed. Based on the threat model and design principle, a security function model is discussed and several deployment strategies are discussed. In [18], the authors propose a scheme to enhance communication by addressing trust management, secure routing, and risk management issues in the network. It discusses important and inter-related system components including virtual trust and provisioning domain construction, resource and information flow isolations, trust management (i.e., identity management and attribute-based data access control), context-aware routing, intrusion detection, and context-aware risk management.

In [23], the authors analyze the impact of data protection to transaction performance in MCC. The authors transmitted different size data encrypted using different encryption algorithms and measured the time consumption and the battery voltage change to reflect the effect brought by data protection and concluded that data protection has significance impact on transaction processing. They also proposed a framework for dynamically protecting data considering the environment condition and transaction type synthetically, expecting to balance the security request and terminal's resource consumption.

V. SCHEMES THAT HANDLE BOTH MOBILE USER SECURITY AND DATA SECURITY

There are a few proposals which handle both the issues. In [19], the authors propose a security model which consists of a two phase protocol: smart phone verification and cloud verification. Security vulnerabilities are discussed and various response options are provided. But only a protocol and message flow is proposed. The scheme is neither implemented nor compared with other schemes present in the literature.

In [20], the authors identify and analyse a number of security challenges and potential privacy threats in VCs. This include challenges of authentication of high-mobility vehicles, scalability and single interface, tangled identities and locations, and the complexity of establishing trust relationships among multiple players caused by intermittent short-range communications. This directional security scheme solves several security challenges. In [21], a streamlined security architecture is proposed for enterprises to simplify and enhance their security while achieving cost savings. Supports reliability and disaster recovery as well. It also provides any time, any device and anywhere access.

VI. CONCLUSIONS

Security is an important issue for mobile users to use various features of Cloud Computing on the go. In this paper, we have discussed various security mechanisms existing in literature for mobile Clouds pertaining to user applications as well as for data storage on Cloud. We have provided a comparative study of various schemes and classified them into schemes that handle security issues of mobile users, schemes that handle data storage on Cloud and scheme that handle both of them.

TABLE I
COMPARISON OF VARIOUS SECURITY MECHANISMS FOR MCC

Scheme	**Basic Mechanism**	**Network Security**	**Cloud Security**	**Virtualiz-ation Support**	**Cloud Infrastr-ucture Security**	**DoS attacks prevention**	**Access Control Model**	**Multilevel protection**	**Layer based Security**
CBS [7]	Protecting the traffic between endpoints and the Cloud	YES	YES	YES	NIL	Possible	NIL	Possible	NIL
SeaaS [8]	Security as a Service	NO	YES	YES	YES	NIL	NIL	Possible	YES
CSSCA [4]	Access Control Model	NO	YES	NO	NIL	NIL	Exists	Possible	NO
CORAS [9]	Content Management Architecture	NO	YES	NO	NO	NO	NO	Possible	NO
SDP [10]	Secure mobile cloud data processing framework through trust management	NO	YES	YES	YES, Storage Infrastructure support	YES	YES	Possible	NO
PDPCloud [11]	secure storage service with public provable data possession	NO	YES	YES	YES, Storage Infrastructure	NO	YES	YES	YES

					support				
IJS [5]	Security model for Location based services	YES	YES	NO	YES, Database security	NO	YES	NO	NO
SSPMCloud [19]	Secure verification model	NO	YES	NO	NO	NO	YES	NO	NO
SSAM [12]	Security service admission Model	NO	YES	NO	NO	NO	YES	NO	NO
VC [20]	Directional security scheme to solve several security challenges	YES	YES	YES	YES	YES	YES	YES	YES
NBSCC [21]	Streamlined security architecture	YES	YES	NO	YES	YES	YES	YES	YES
EAF [13]	Elastic Application Framework	NO	YES	NO	YES	NO	YES	NO	NO
SDSM [14]	A scheme to to provide confidentiality and fine-grained access control for Cloud data	NO	YES	NO	YES	NO	YES	NO	NO
SPC [15]	Secure private Cloud architecture	NO	YES	YES	YES	YES	YES	NO	NO
SchedGM [16]	Practical and privacypreserving solutions for mobile devices	YES	YES	NO	YES	NO	YES	NO	NO
SSMCS [17]	Security solution approach for data security risk	NO	YES	NO	YES, Storage Infrastructure Support	NO	YES	NO	NO
MobiCloud [18]	A scheme to enhance communication	YES	YES	YES	YES	NO	YES	NO	NO
DSAS [22]	Dynamic method for secure access of Cloud in mobile environments	YES	YES	NO	NO	NO	Exists	NO	Two Layers
DPD [23]	Dynamically protecting data considering the environment condition and transaction type synthetically	NO	YES	NO	NO	NO	Exits	YES	NO

ACKNOWLEDGMENT

Authors would like to acknowledge Dr Ganesh Neelakanta Iyer for his valuable comments on completing this research work.

Reference

[1] Armbrust Michael, Fox Armando, Griffith Rean, Joseph Anthony D., Katz Randy H., Konwinski Andrew, Lee Gunho, Patterson David A.,Rabkin Ariel, Stoica Ion, and Zaharia Matei. Above the clouds: A berkeley view of

cloud computing. Technical Report UCB/EECS- 2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[2] Mobile cloud computing forum. http://www.mobilecloudcomputingforum.com/, 2011.

[3] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing*, pages n/a–n/a, 2011.

[4] Zhou Lian-chi and Xiu Chun-di. Cloud security service providing schemes based on mobile internet framework. *In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, volume 3, pages 307 –311, march 2012.

[5] Yu-Jia Chen and Li-Chun Wang. A security framework of group location-based mobile applications in cloud computing. *In Parallel Processing Workshops (ICPPW), 2011 40th International Conference on*, pages 184 –190, sept. 2011.

[6] Murty J. *Programming Amazon Web Services: S3, EC2, SQS, FPS, and SimpleDB*. O'Reilly Series. O'Reilly, 2008.

[7] G. de los Reyes, S. Macwan, D. Chawla, and C. Serban. Securing the mobile enterprise with network-based security and cloud computing. In *Sarnoff Symposium (SARNOFF), 2012 35th IEEE*, pages 1 –5, may 2012.

[8] Qiu Xiu-feng, Liu Jian-wei, and Zhao Peng-chuan. Secure cloud computing architecture on mobile internet. In *Artificial Intelligence, Management Science and Electronic Commerce* (AIMSEC), 2011 2nd *International Conference on*, pages 619 –622, aug. 2011.

[9] Andreas Klein, Christian Mannweiler, Joerg Schneider, and Hans D. Schotten. Access schemes for mobile cloud computing. *In Proceedings of the 2010 Eleventh International Conference on Mobile Data Management, MDM* '10, pages 387–392, Washington, DC, USA, 2010. IEEE Computer Society.

[10] Dijiang Huang, Zhibin Zhou, Le Xu, Tianyi Xing, and Yunji Zhong. Secure data processing framework for mobile cloud computing. In *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, pages 614 –618, april 2011.

[11] Jian Yang, Haihang Wang, Jian Wang, Chengxiang Tan, and Dingguo Yu. Provable data possession of resource-constrained mobile devices in cloud computing. *Journal of Networks*, 6(7), 2011.

[12] Hongbin Liang, Dijiang Huang, L.X. Cai, Xuemin Shen, and Daiyuan Peng. Resource allocation for security services in mobile cloud computing. In *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, pages 191 –195, april 2011.

[13] Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham, and Sangoh Jeong. Securing elastic applications on mobile devices for cloud computing. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, CCSW '09, pages 127–134, New York, NY, USA, 2009. ACM.

[14] Weiwei Jia, Haojin Zhu, Zhenfu Cao, Lifei Wei, and Xiaodong Lin. Sdsm: A secure data service mechanism in mobile cloud computing. In *Computer Communications Workshops* (INFOCOM WKSHPS), 2011 *IEEE Conference on*, pages 1060 –1065, april 2011.

[15] S. Horrow, S. Gupta, A. Sardana, and A. Abraham. Secure private cloud architecture for mobile infrastructure as a service. In Services (SERVICES), 2012 *IEEE Eighth World Congress on*, pages 149 – 154, june 2012.

[16] Igor Bilogrevic, Murtuza Jadliwala, Praveen Kumar, Sudeep Singh Walia, Jean-Pierre Hubaux, Imad Aad, and Valtteri Niemi. Meetings through the cloud: Privacy-preserving scheduling on mobile devices. *Journal of Systems and Software*, 84(11):1910 – 1927, 011.

[17] Xiaojun Yu and Qiaoyan Wen. Design of security solution to mobile cloud storage. In Honghua Tan, editor, *Knowledge Discovery and Data Mining, volume 135 of Advances in Intelligent and Soft Computing*, pages 255–263. Springer Berlin / Heidelberg, 2012.

[18] Dijiang Huang, Xinwen Zhang, Myong Kang, and Jim Luo. Mobicloud: Building secure cloud framework for mobile computing and communication. In Service *Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium on*, pages 27 –34, june 2010.

[19] Ji Soo Park, Ki Jung Yi, and Jong Hyuk Park. Ssp-mcloud: A study on security service protocol for smartphone centric mobile cloud computing. In James J. Park, Hamid Arabnia, Hang-Bae Chang, and Taeshik Shon, editors, *IT Convergence and Services, volume 107 of Lecture Notes in Electrical Engineering*, pages 165–172. Springer Netherlands, 2011.

[20] G. Yan, D. Wen, S. Olariu, and M. C. Weigle. Security challenges in vehicular cloud computing. *Intelligent Transportation Systems, IEEE Transactions on*, PP(99):1 –11, 2012.

[21] G. de los Reyes, S. Macwan, D. Chawla, and C. Serban. Securing the mobile enterprise with network-based security and cloud computing. In *Sarnoff Symposium* (SARNOFF), 2012 35th IEEE, pages 1 –5,May 2012

[22] Rong Ouyang, Yunfa Li, Zujie Ren and Jian Wan, "Dynamic Method of Secure Access Cloud in Mobile Environment", Proceedings of the 2nd International Conference on Green Communications and Networks 2012 (GCN 2012): Volume 1, 2013

[23] Hongliang Lu, Xiao Xia, and Xiaodong Wang, "How to Dynamically Protect Data in Mobile Cloud Computing?", ICPCA-SWS 2012, LNCS 7719, pp. 364–371, 2013.

