To secure data in mobile cloud computing environments more efficiently and controllably

Megan Smith *(Graduate Student)*

Computer Science Department, Georgia State University  
Atlanta, Georgia 30302 USA

msmith145@student.gsu.edu

Abstract— Mobile cloud computing has emerged as a fast growing and popular application by providing convenience to mobile users and by maximizing the effectiveness of shared resources. Due to the clouds ability to compute large amounts of data, security services, such as encryption, decryption and authentications, are performed in the cloud in order to protect that processed data. However, with the restrictions of mobile devices and cloud resources and with the increased use of mobile cloud applications, the need for more condensed security and privacy schemes has become apparent. There has been a growing interest in mobile cloud computing research for this reason, largely focusing on adapting a controllable mobile cloud computing environment that effectively reallocates resources to improve computation, communication and storage. Our solution focuses on combining these two popular research directions into a singular effort. This approach updates the cloud security platform to take into account varying levels of user security needs, while reducing complex cryptographic algorithms and operating the mobile cloud on a group-based access control model.

Keywords— mobile cloud computing, security services, privacy, cryptographic algorithms, access control

1. Introduction

It is a well-known fact that the majority of Americans own a smart phone or a similar mobile computing device, all in which are equipped with a wireless internet service. Mobile devices however come with many limitations: low storage capacity, poor data sharing calculation capabilities, and short battery life to name a few [6]. Mobile cloud computing improves mobile devices by reducing the burdens of these limitations. Mobile cloud computing allows massive data storage to be implemented in the cloud and enables complex data processing to be executed among several shared resources, all while reducing energy consumption. Figure 1 outlines the general architecture of the mobile cloud computing environment.

The main focus of this paper revolves around securing that reallocated data. Security and privacy is a growing concern of individual users and of cooperate users, especially as popularity of mobile cloud environments increases. To help alleviate these concerns, we focus on developing a cloud security service customizing architecture for differential security demands and constructing an efficient resource allocation model for mobile cloud security services.

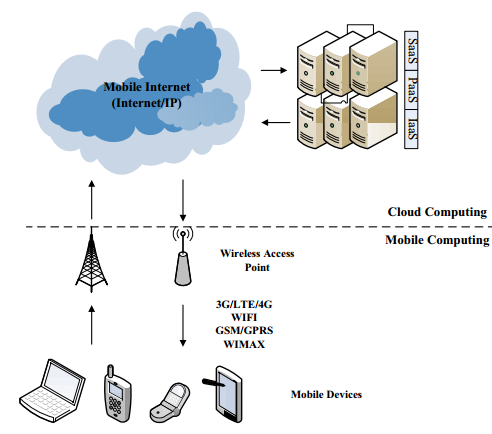


Figure 1. Architecture of mobile cloud computing

1. current issues in mobile cloud computing

Mobile cloud computing has been a large research topic in recent years, all in the rush to keep up with growing demand for a more secure and efficient mobile cloud network. A main focus of this research involves resource limitations of mobile devices; thereby creating a need for light-weight security schemes. This research has produced the following major concerns.

1. *Resource allocation for mobile devices is limited:*  Mobile devices inherently come with a limited amount of processing resources. Therefore, one of the main objectives of mobile cloud computing is to increase the processing/storage capabilities of mobile devices and reduce the energy consumption while executing computational intensive jobs. In order to achieve this objective, mobile users offload processing intensive and storage demanding portions of mobile applications from resource constrained mobile devices to the resource enriched cloud [1].
2. *Varying levels of security needs among end-users*: Currently, mobile cloud applications do not offer security services beyond the very low standard of either a pin key or a text-based password key. Mobile users do not even get the option to choose both of these security services, it is either one or the other. Adapting the mobile cloud to offer security services, beyond mere pin and password keys, allows cloud users to create a more secure cloud environment [4].
3. *Lack of Access Control:* Access control mechanisms are considered tools to ensure authorized user access and to prevent unauthorized access to information systems. A lack of access control in the mobile cloud, given that cloud services in the mobile internet framework have a certain degree of openness and heterogeneity, make cloud resources vulnerable to unauthorized user access and acquisition. Different data subjects may have different security requirements, also the same data subjects at different times may have different security requirements. Considering these diversities, cloud security services should be able to adapt to the permission changes dynamically and accordingly, as well as make some appropriate access control decisions. Therefore, a cloud service access control model is needed [4].
4. *Lack of Supervisory Control:* More important than finding problems and vulnerabilities which exist in the mobile cloud, is the ability to achieve flexibility, scalability, and efficient usage of available resources in the cloud. Current research shows that mobile cloud providers are challenged in the area of adaptability, workload analysis, and prototypes. The major areas lacking supervisory control include: partitioning, migration and resource allocation. Partitioning is important to divide the data of the mobile cloud into partitions in order to maximize transaction and query performance. Migration provides flexibility in the mobile cloud that dedicates resources where they are most needed. Resource allocation is necessary to analyse and classify resource requirements and to decide how those resources are to be allocated to the virtual machines [6].
5. improved security service schema

Good dynamic, differentiated cloud security services in the mobile cloud environment will include complexity, mobility, openness and instability of the user groups. The following section introduces a security service scheme designed to coordinate the openness of the mobile cloud. Figure 2 displays the proposed security service scheme as a whole [2].

1. On-demand security scheme

In order to adapt the cloud to provide varying levels of security needs based on the users desired level of security, a cloud security service customizing architecture for differential security demands will be developed. This new version of cloud computing gives users’ different levels of security services through a dynamic and scalable virtualization technology. This proposed framework will enable the developers of the cloud environment to design proper hardware and software architecture according to a different hierarchy, so as to realize the deployment, management and dispatch strategy of the security service resources, and provide the users in the mobile cloud environment with a flexible and efficient service system. Essentially, the user will be provided with an interface to interact with the clouds settings and determine which security services they would personally like to utilize.

1. Security self-adaptive scheme

In the mobile cloud environment, due to the frequent changes of user demands, operation behaviours and other service parameters, it is difficult for administrators to conduct real-time supervision and control. Therefore, a security self-adaptive mechanism for cloud services is required. When any of the above changes happen, this proposed self-adaptive scheme can make real-time dynamic adjustments, make automatic mapping and combinations which are chosen from the pre-established security policies, then provide appropriate security protection methods, and finally accomplish the purpose of ensuring the optimal status of mobile cloud services. The self-adaptive security scheme also gives some corresponding protection measures from the aspects of distributed security monitoring, elastic cloud services, and fine-grained access control policies. Hence, a self-adaptive security mechanism is proposed for mobile cloud services and it is modelled so that users can get real-time dynamic responses of parameter changes when mobile cloud services are being offered [2].

1. Cloud service access control scheme

Aiming at satisfying the security demands of mobile cloud services, a proposed cloud service access control model which supports permission changes will be developed. By bringing in the concept of dynamic changes and a hierarchy structure, this model can not only help manage the users’ authorities dynamically, but also assist in protecting the cloud service itself and the cloud information. This access control model realizes the dynamic permission management by introducing the role players and the authorized groups. When a user begins to perform a task, the status, behaviours and lifetime of the activated role is supervised by the role player. Furthermore, this model separates the access control into two levels: the service level guarantees that only authorized users can invoke services, while he service attribution level ensures that the service attribution and information can be accessed only when the authorized users successfully pass the service level. This access control model is a role-based, dynamic, hierarchical model [2].

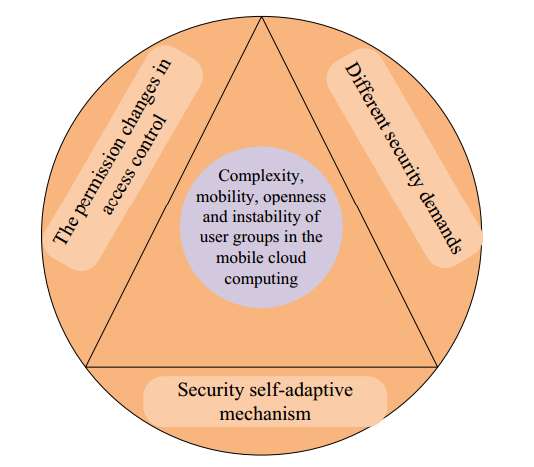


Figure 2. Considerations on an improved design of security service schema for the mobile cloud environment

1. Classifying security needs in the cloud

There are two types of security services, critical security services and normal security services. In order to provide the most efficient cloud security service, it is necessary to provide resource isolation amounts for different cloud users. To enhance security services, we need to separate cloud resources allocated for different security processes owned by different users.

* 1. Normal Security Services

The mobile cloud is a machine-to- machine service model, where a mobile device can use the cloud for searching, data mining, and multimedia processing. To protect the processed data, security services such as encryption, decryption, and authentication are performed in the cloud. These basic security services are grouped into the normal security service classification [1].

* 1. Critical Security Services

The difference between critical security services and normal security services is that critical security services provide strong security protection such as using a longer key size, strict security access policies, isolations for protected data, and so on. The critical security service usually occupies more cloud computing resources, however it generates more rewards to the cloud provider since the critical security service users need to pay more for using the critical security service. In general, critical security services involve more complex security implementations such as stronger authentication and encryption algorithms. As a result, the critical security services usually consume more cloud resources such as CPU time to compute complex cryptography algorithms and occupies more hard drive spaces [5].

* 1. Security Service Admission Model

To construct an efficient resource allocation model for mobile cloud security services, we present an admission control mechanism based on the total cloud system reward, which takes into account both the cloud income and the cost of the resource occupation. Thus, the system reward is computed in the system resource management model based on the following factors: the arriving and departing rates of critical security services and normal security services, the numbers of running critical security services and normal security services in the system, the available total system resources (measured by the number of virtual images - the availability of system resources), and the reward for critical security services or normal security service. To satisfy the security service requirements of end users, either critical or normal security services, the mobile cloud needs to consider how to admit mobile users’ service requests to obtain the maximal system reward with the limited cloud resources. To address the above presented admission issue for security service requests, we proposed a Security Service Admission Model based on Semi-Markov Decision Process to leverage the maximal system rewards with the system resource constraints. We apply the model to analyse the system reward of different security services, and derive the optimal resource allocation policy in the mobile cloud computing environment. The proposed model derives a cloud service blocking probability and achieves the maximum system gain of the mobile cloud by considering both system expenses and incomes. Figure 3 shows the blocking probability of critical security services under various arrival rates [4].

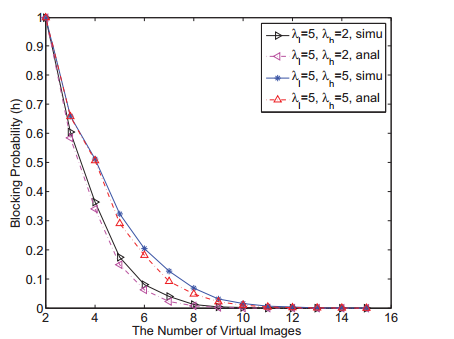


Figure 3. Blocking Probability for critical security services

1. reducing the complexity of cryptographic algorithms

In a mobile cloud computing environment, cloud users may inquire the data from sensing devices. A simple solution to protect the data is to encrypt the sensing data with a group key and broadcast the encrypted data where only legitimate users can reveal the data content with the group key. However, this approach demands high key management overhead.

* 1. Encryption and Decryption Architecture for Mobile Cloud Computing

Ciphtertext Policy Attribute-Based Encryption schemes were proposed to facilitate key management and cryptographic access control in an expressive and efficient way. With this scheme, an attribute is a descriptive string assigned to a user and each user may be tagged with multiple attributes. Multiple users may share common attributes, which allow sensors to specify a data access policy by composing multiple attributes. To decrypt the message, the decryptor’s attributes need to satisfy the access policy. The policy essentially is to encrypt the data and enforce data access policies so that only eligible users can decrypt it [5].

* 1. Data Management Issues and Solutions

The main challenges with the current encryption/ decryption based model include the intensive computational resources required for sensors or mobile devices to run the encryption and decryption algorithms. It is also very important, given the sensitivity of data and multi-tenancy nature of the public cloud, that critical user secrets should not be exposed to the cloud. Another major issue is how to upload/download and update encrypted data stored in the mobile cloud system. Frequent upload/download operations will cause tremendous overhead for resource constrained mobile devices.

To address the cost issue of frequent data updates, it is reasonable to divide a file into independent blocks that are encrypted independently. This blocking method can be seen in Figure 4. To update files, the data owner can simply download the particular blocks to be updated. In this way, we can avoid re-encrypting the entire data set. Data access control can be enforced on individual blocks using “lazy” re-encryption strategy [3].

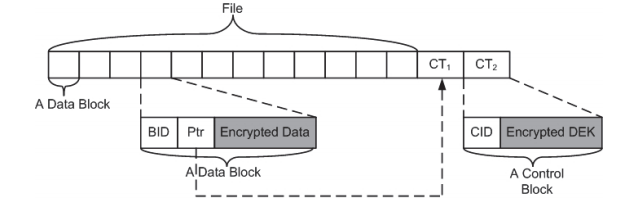


Figure 4. Illustration of a file organized into blocks with multiple control blocks

1. evaluation results

A simulation of the proposed blocking method to decrease the encryption/decryption overhead that comes with multiple data updates has been performed and evaluated. The simulation was developed and ran in a Java IDE. Its purpose was to test the blocking method for accuracy and efficiency. The simulation reads a large folder, containing many files, and then times the amount of time, in nanoseconds, that it takes to upload, encrypt, decrypt and return the data back to the user. The same simulation is performed for a single file, where the file is uploaded, encrypted, decrypted and download back to the user. Each simulation was ran 20 times and then compared graphically to each other. The results determined that for large data files, the processing time to upload, encrypt, decrypt and download back to user was larger than if a single, smaller file was processed. The simulation results can be seen in Figure 5.

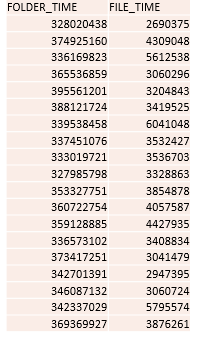


Figure 5. Simulation results of the Blocking Method

The purpose of this simulation was to mock the occurrence where an actual mobile cloud user updates a single file in a large folder that is already uploaded and being stored in the mobile cloud environment. The results show that if an update occurs, it is in fact more efficient to use the blocking method to re-encrypt a single updated file than to re-encrypt the entire dataset that is store in the cloud.

1. conclusion

In conclusion, we proposed a combination of effective strategies in order to improve resource allocation in the mobile cloud environment and supply mobile cloud users with more efficient, and rewarding options while using the mobile cloud. This paper presented an improved security service scheme that helped realize the controllability, customizability, and adaptability of mobile cloud security services. Allowing users to choose whether they wanted critical or normal security services provided a personalized, on-demand, self-adaptive cloud security service module with the ability to dynamically adjust your cloud settings with an improved access control model. We have also proposed a Security Service Admission Model to consider both the maximal system reward and system service expenses. The system reward is derived through the model by taking into considerations of the critical or normal security service rewards and their cloud system expenses.

We extensively compared the original versions of encrypting and uploading on mobile devices involving extra file management overhead on the basis of turnaround time and energy consumption. Our new proposed version shows significant improvement in performance while performing the blocking method operation.

In general, we were able to reduce the computational expenses of mobile cloud computing by allowing users to define their own personal level of security and by incorporating better encryption/decryption operations for updated files that are stored in the mobile cloud environment.

References

1. Zhou Lian-chi; Xiu Chun-di, “Cloud Security Service Providing Schemes Based on Mobile Internet Framework”, *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, vol.3, no., pp.307,311,23-25 March 2012
2. Qinyun Dai; Haijun Yang; Qinfeng Yao; Yaliang Chen, “An improved security service scheme in mobile cloud environment”, *Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on*, vol.01,no., pp.407, 412, Oct.30 2012-Nov. 1 2012
3. Zhibin Zhou; Dijiang Huang, “Efficient and secure data storage operations for mobile cloud computing”, *Network and service management (cnsm), 2012 8th International Conference and 2012 workshop on systems virtualizations management (svm*), vol., no., pp.37, 45, 22-26 Oct.2012
4. Hongbin Liang; Dijiang Huang; Cai, L.X.; Xuemin Shen; Daiyuan Peng, “Resource allocation for security services in mobile cloud computing”, *Computer Communications Workshop (INFOCOM WKSHPS), 2011 IEEE Conference on*, vol., no., pp.191, 195, 10-15 April 2011
5. Khan, A.N.; Kiah, M.L.M.; Khan, S.U.; Madani, S.A.; Khan, A.R., “A study of incremental cryptography for security schemes in mobile cloud computing environments”, *Wireless Technology and Applications (ISWTA), 2013 IEEE Symposium on*, vol., no., pp.62, 67, 22-25 Sept. 2013
6. Hui Suo; Zhuohua Liu; Jiafu Wan; Keliang Zhou, “Security and privacy in mobile cloud computing”, *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International*, vol., no., pp.655, 659, 1-5 July 2013