Secure Framework in Data Processing for Mobile Cloud Computing

[1]MR.ANAND SURENDRA SHIMPI & [2]MR.R.P.CHANDER

[1,2]AHCET, Chevela HYDERABAD, India &
anand02cs004@gmail.com

Abstract—Generally Mobile Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users 'physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a new secure framework. In addition to providing traditional computation services, mobile cloud also enhances the operation of traditional ad hoc network by treating mobile devices as service nodes, e.g., sensing services. The mobile services or sensed information, such as location coordinates, health related information, should be processed and stored in a secure fashion to protect user's privacy in the cloud. In this paper, we present a new mobile cloud data processing framework through *trust management* and *private data isolation*. Finally, an implementation pilot for improving teenagers' driving safety, which is called FocusDrive, is presented to demonstrate the solution.

Keywords- *Trust Management and Private Data Isolation, Security, Privacy, Mobile Cloud, Data Security*

I. INTRODUCTION

User mobility, which means "Anytime, Anywhere" is becoming a reality. Using mobile devices, computing power from cloud computing technology and Internet accessibility together is creating a new flow, which is mobile cloud computing for enterprises. The use of mobile devices to establish ad-hoc communication systems is a viable solution that provides global connectivity to support a broad range of applications. Mobile cloud is a machine-to-machine service model, where a mobile device can use the cloud for searching, data mining and multimedia processing. In this paper, we propose a new mobile cloud framework called MobiCloud. In addition to providing traditional computation services, MobiCloud also enhances the operation of the ad hoc network itself by treating mobile devices as service nodes.

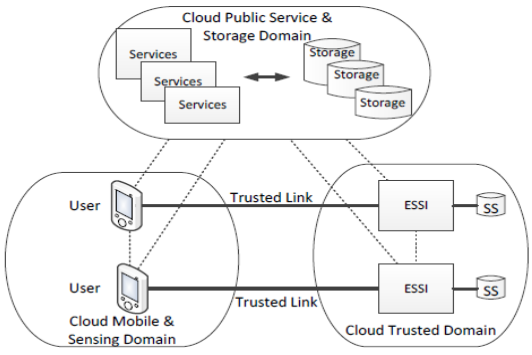


Figure 1. Reference Service Model of mobile cloud

A. "MobiCloud" Framework

In this paper we explores a secure mobile cloud computing framework, called MobiCloud, which transforms traditional MANETs into new service-oriented communication architecture, in which each mobile device is treated as a Service Node (SN), and it is mirrored to one or more Extended Semi-Shadow Images (ESSIs) in the cloud in order to address the communication and computation deficiencies of a mobile device. In MobiCloud, a mobile device can outsource its computing and storage services to its corresponding ESSI and Secure Storage (SS). With this framework, the device will send its sensed information such as moving trajectory to the cloud. As a return, the cloud can provide better location-based services according to the mobility information provided by the mobile device. In MobiCloud mobile users must trust the cloud service provider to protect the data received from mobile devices. However, it is a big concern for mobile users for storing their privacy sensitive information in a public cloud. This paper targets to address this privacy issue.

B. MobiCloud Service Model

The proposed new secure data processing mobile cloud
infrastructure is highlighted in Figure 1, The mobile cloud
is composed by three main domains: (i) the cloud mobile and sensing domain, (ii) the cloud trusted domain, and (iii) the cloud public service and storage domain. In this framework, each mobile device is virtualized as an ESSI in the cloud trusted domain and each ESSI can be represented as an SN in a particular application (a.k.a., a service domain). The

introduced ESSIs can be used to address communication and computation deficiencies of a mobile device, and provide enhanced security and privacy protections. A mobile device and its corresponding ESSI can also act like a service provider or a service broker according to its capability, e.g., available computation and communication capabilities to support a particular communication or sensing service. This approach takes maximum advantage of each mobile node in the system by utilizing cloud computing technologies. In this way, the cloud's boundary is extended to the customer device domain. Note that an ESSI can be an exact clone, a partial clone, or an image containing extended functions of the physical device. The networking between a user and its ESSI is through a secure connection, e.g., SSL, IPSec, etc.

II. MOBILE CLOUD SECURE DATA PROCESSING MODEL

ESSI plays important role in Mobicloud. An ESSI is a virtual machine that is designed for an end user having full control of the information stored in its virtual hard drive. However, the networking functions and running processes are customized through the mobile cloud service provider.

Note that the cloud trusted domain and cloud public service and storage domain are physically isolated to provide strong security protection to user's data. They can belong to two different cloud service providers. Within the cloud trusted domain, strict security policies are enforced through a distributed Firewall system (i.e., each ESSI runs its own Firewall). Data flows in/out the trusted domain must be scanned through the distributed Firewall system to make sure no malicious traffic is sent/received. The mobile cloud data processing model includes three main components: trust management, multi-tenant secure data management, and ESSI data processing model, which are described in details in the following subsections.

A. Mobile Cloud Trust Management

The trust management model of mobile cloud includes identity management, key management, and security policy enforcement. An ESSI owner has the full control over the data possessed in the ESSI, and thus a user-centric identity management framework is a natural choice. The user-centric identity management (also frequently referred to as identity 2.0) allows an individual has full control of his/her identities, in which third party authenticates them. It also implies that a user has control over the data his/her sharing over the Internet, and can transfer and delete the data when required. In this paper, we introduce an integrated solution involving identity-based cryptography and attribute-based data access control as the building blocks to construct the trust management system for mobile cloud. Particularly, the presented mobile cloud communication framework usually involves the establishment of a virtual private communication group.

We propose a fully functional identity-based encryption (IBE) scheme. The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie--Hellman problem. Our system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. We give precise definitions for secure IBE schemes and give several applications for such systems.

1) Mobile Cloud Identity and Trust Management:

Trusted Authority (TA) is assumed to manage security keys and certificates for mobile users. In the following presentation, without special notice, we always assume that there is a TA available, which is responsible for key and certificate distribution. Based on this assumption, the TA is responsible to deploy an Attribute-Based Identity Management (ABIDM) for mobile cloud's identity and trust management. The basic identity representation of ABIDM is shown in Figure 2. Using ABIDM, we first need to define the "point of network presence (PoNP)". A mobile node's relationship can be thought of as lines radiating from the PoNP to the various counterparties. Each line is distinct and tagged with the attribute used by a particular counterparty. In particular, we define a default PoNP (i.e., native PoNP) for everyone. The default PoNP has to be linked by a unique native ID. The uniqueness of the native ID is not difficult to achieve. Indeed, any user can have a unique native ID by simply hashing any one of his/her unique identifiers, such as a driver license ID, email address, social security number, etc. Each PoNP has two properties: type and value. The type value provides the information such as (i) the identity issuer, (ii) the private key issuer, and (iii) the validation period. The identity and private key issuer can be either selfgenerated or derived from a Trusted Authority (TA). The value of the PoNP can be used as a part of the user's identity with its type for a particular scenario. Identity-based cryptography can be used, and a private key is assigned to the PoNP identity. A message receiver can use the sender's identity to verify the received signature for authentication purpose.

Each PoNP is associates with one or multiple attributes (i.e., A1...An), and each attribute has type and value properties. Attributes can be assigned as predefined attributes that do not change frequently, which are called as static attributes.

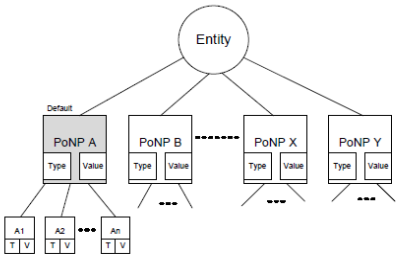
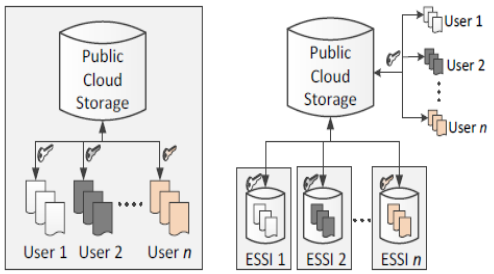


Figure 2. Identity representation scheme.

To differentiate PoNPs, the number of attributes can be reduced for each PoNP for later secure communication. The major benefit of using this identity representation is the "standardization" of identity management. In practice, the numbers of PoNPs for every mobile node can be restricted to a certain number of known scenarios. This can be done by consulting the TA, which provides the public key certificate services and provides the ontology of identities and attributes for mobile users. Self-managed identity and private keys can be used to form a self-managed and trusted ecosystem. This feature will be useful for managing trust based on social network applications.

B. Multi-tenant Secure Data Management

As shown in Figure 1, the dashed lines represent the ad hoc connection between entities, and the solid lines represent dedicated secure connections. The cloud public service and storage domain provides services for all mobile devices and ESSIs. A mobile device can request services directly from the public service and storage domain, or it can request services through its ESSI. An ESSI is the security policy enforcer for its associated mobile device(s). The user can specify what data should be protected and stored in its ESSI. Users' private information is maintained in their corresponding Secure Storage (SS).



(a) Multi-tenancy with shared data management framework

(b) Multi-tenancy with isolated data management framework

Figure 3. Multi-tenant Secure Data Management in MobiCooud

Multi-tenancy is one of the key features of cloud services. To secure each user's data, traditional approaches are shown in Figure 3(a), where users' data is stored in one big database and a unique encryption key is used to secure data for each user. This approach has several drawbacks. First, it is not scalable when the database is huge. Data storage operations can incur heavy data operations that require extensive computing resources. Second, data encrypting keys for users are maintained in a centralized location, which is vulnerable to the singlepoint failure problem. Moreover, users usually have concerns that the cryptographic key is maintained by the cloud provider. To address these drawbacks, the presented solution utilizes a decentralized approach, which is presented in Figure 3(b). The proposed multi-tenant data management system partition the data into two security levels: (i) critical data and (ii) normal data. The critical data must be secured by the data encrypting key generated by the user, and the normal data is secured by the data encrypting key generated by the cloud storage service provider. The presented multi-tenant secure data management system can address the drawbacks of traditional approaches. First, the data operations such as indexing, data retrieval, data addition, etc., are distributed to ESSIs. In addition, the security functions, such as encryption/decryption/integrity, are also distributed to ESSIs. As a result, the computation overhead is distributed to multiple processors in the cloud system. Second, ESSIs enhance the users' security by adding one additional layer of security, in which the critical data are stored in each ESSI. As a result, compromising one ESSI will not impact other ESSIs.

C. ESSI Data Processing Model

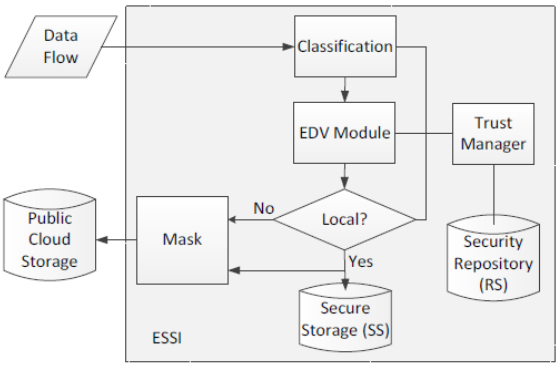


Figure 4. Data processing in ESSIs.

The ESSI's data processing model is built on the security capability model enabled for Linux Kernel 2.2 and above. Based on the security capability model, we can build a Trirooted ESSI that has a cloud root, a user root, and an auditing root. The privilege of the user root includes maintaining users data in its SS and encryption/decryption/verification related processes. The cloud root is to perform the maintenance functions of ESSI, and it does not have the access to SS and related security functions. The auditing root is used to log the activities of both cloud root and user root. The log data can 617 be only accessible for investigation purpose when regulation violations are identified. Usually, the log data is

maintained by a third trusted party. In this way, the cloud provider cannot easily breach the privacy of users. The ESSI's data processing model is presented in Figure 4. SS is installed in ESSI's virtual hard drive. A user's private information and security credentials are stored in the Security Repository (RS) managed by the ESSI mapped to the user's mobile device. The critical data is stored in the SS. Data flow arriving at the ESSI is processed as follows: (i) Data flow is inspected by the classification model that classifies the data as critical data or normal data. (ii) If the data is classified as normal, the normal data will be sent to the public cloud storage through a masking procedure. (iii) The Encryption/Decryption/Verification (EDV) module is then used on the critical data and stores the processed data in SS. The masking procedure is used to remove private information associated with the user and anonymize the data content. The masking procedure can be configured differently according to the level of the criticality of the data. It is up to the user's preference, and it is operated through the trust manager. For example, ESSI can generate a masked index value for the public cloud storage for indexing purpose. This index value includes the ESSI's identifier (can be a pseudonym) and corresponding indexing category. Once the public cloud storage service receives the index value, it then uses it to identify which ESSI is responsible for the requested searching data.

III. DISCUSSION AND FUTURE WORK

We have developed a pilot mobile cloud system to implement the cloud trusted domain as presented in Figure 1. To demonstrate the presented security and privacy protection features, we have developed a pilot application "FocusDrive" project , which is presented in the following subsection.

A. FocusDrive Project

The FocusDrive project is conducted by the *Secure Networking And Computing (SNAC)* research group at ASU. Studies show teenagers are especially prone to text-and-drive, which can be as dangerous as DUI (Drive Under Influence). The goal of FocusDrive is to improve the driving safety of teenage drivers in collaboration with their parents. Particularly, it focuses on restricting improper usage of cell phone texting while teenagers are driving. FocusDrive develops an application running in mobile phones as a background application to dynamically monitor the speed of the phone. Running this application, a cellphone will automatically enable and disable the texting function according to the driving speed and road conditions.

B. Future Work

In this paper, we present a prototype of the secure data processing model for mobile cloud computing. In the future, we will focus on the follow research: (i) investigate more application scenarios that require data sharing between cloud private domain and public domain; (ii) investigate the robustness of the Tri-rooted ESSI solution; and (iii) investigate the security monitoring, auditing, and misuse detection in the mobile cloud system.

REFERENCES

[1] D. Huang, X. Zhang, M. Kang, and J. Luo, "Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication," in *Proceedings of 5th IEEE International Symposium on Service- Oriented System Engineering*, 2010.

[2] "Identity 2.0," http://en.wikipedia.org/wiki/Identity 2.0.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. of Computing*, no. 3, pp. 586–615, 2003.K. Elissa, "Title of paper if known," unpublished.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute- Based Encryption," *Proceedings of the 28th IEEE Symposium on Security and Privacy (Oakland)*, 2007.

[5] J. Su, J. Scott, P. Hui, E. Upton, M. Lim, C. Diot, J. Crowcroft, A. Goel, and E. de Lara, "Haggle: Clean-slate networking for mobile devices," *Technical Report, UCAM-CL-TR-680, University of Cambridge*, 2006.

[6] D. Huang and D. Medhi, "A Key-chain Based Keying Scheme For Many-to-Many Secure Group Communication," *ACM Transactions on Information and System Security*, vol. 7, no. 4, pp. 523 – 552, 2004.