American Journal of Systems and Software, 2014, Vol. 2, No. 1, 27-32
Available online at http://pubs.sciepub.com/ajss/2/1/5

DOI:10.12691/ajss-2-1-5

Mobicloud and Secure Data Access Framework

J. Pourqasem[1], S. Karimi[1], S.A. Edalatpanah[2,3,*]

[1]Department of Computer Science, Faculty of Engineering, University of Guilan, Rasht, Iran
[2]Department of Applied Mathematics, Lahijan Branch, Islamic Azad University, Lahijan,Iran
[3]Department of Applied Mathematics, Faculty of Mathematical Sciences, University of Guilan, Rasht, Iran
*Corresponding author: saedalatpanah@gmail.com

Received February 09, 2014; Revised February 25, 2014; Accepted March 03, 2014

Abstract Cloud provides the environment for the mobile users called mobicloud to performs computationally intensive operation such as searching, data mining, and multimedia processing. Addressing the trust management, secure routing, and risk management issues in this framework are notable. To this end, we present a secure mobile cloud data access framework through trust management and private data isolation.

Keywords: *cloud computing, mobicloud, architecture, trust management*

Cite This Article: J. Pourqasem, S. Karimi, and S.A. Edalatpanah, "Mobicloud and Secure Data Access Framework." *American Journal of Systems and Software*, vol. 2, no. 1 (2014): 27-32. doi: 10.12691/ajss-2-1-5.

1. Introduction

Cloud computing has grown rapidly in the past few years due to the increasing network bandwidth, mature virtualization techniques, and emerging cloud based business demands. What is more, by 2013, mobile devices will overtake PCs as the most common web access entities worldwide as predicted by Gartner [1]. Thus, a mix of cloud computing with mobile technologies is highly expected. Mobile Cloud Computing (MCC) is a term that refers to an infrastructure where both data storage and data processing are done outside of mobile devices from which an application is launched. Besides that, a mobile entity is not limited to only a mobile device; more importantly, it could also be cloud resources, infrastructure, services, and human beings. Hence, with this understanding, MCC further refers to a cloud system where mobility happens in infrastructure, resources, services, user devices and even human beings. The trend of the MCC system is not just aimed to providing fixed services for users in certain areas, but is especially to look forward to establishing connections among mobile users all over the world. Due to the mobility of MCC users, a geographically distributed cloud system is a natural choice that allows users to connect to cloud resources that are geographically "close" to their mobile devices, which usually means less communication delay compared to the centralized approach.

This research article is presented as a position paper to highlight research directions and possible solutions for enhancing secure mobile computing using cloud computing. MobiCloud transforms traditional MANETs into a new service-oriented communication architecture.

In MobiCloud, a mobile device can outsource its computing and storage services to its corresponding ESSI and Secure Storage (SS). Moreover, 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 [2], 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.

The new secure mobile cloud framework is shown in Figure 1. The mobile cloud is composed by three main domains: the cloud mobile and sensing domain, the cloud trusted domain, and the cloud public service and storage domain.

MobiCloud transforms each mobile node from a traditional strictly layer- structured communication node into a service node (SN). Each SN can be used as a service provider or a service broker according its capability, e.g., available computation and communication capabilities to support a particular service. To reduce the uncertainty caused by mobility, we incorporate every SN into the MobiCloud as a virtualized component. Each SN is mirrored to one or more Extended Semi-Shadow Images (ESSIs) in the cloud in order to address the communication and computation deficiencies of mobile device. We note that ESSI can be differentiated from a virtual image in that an ESSI can be an exact clone, a partial clone, or an image containing extended functions of the physical device. In addition, the ESSIs create a virtualized MANET routing and communication layer that can assist the physical mobile nodes and maximize availability of pervasive computing services for each mobile user. The networking between a user and its ESSI is through a secure connection, e.g., SSL, IPSec, etc.

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.

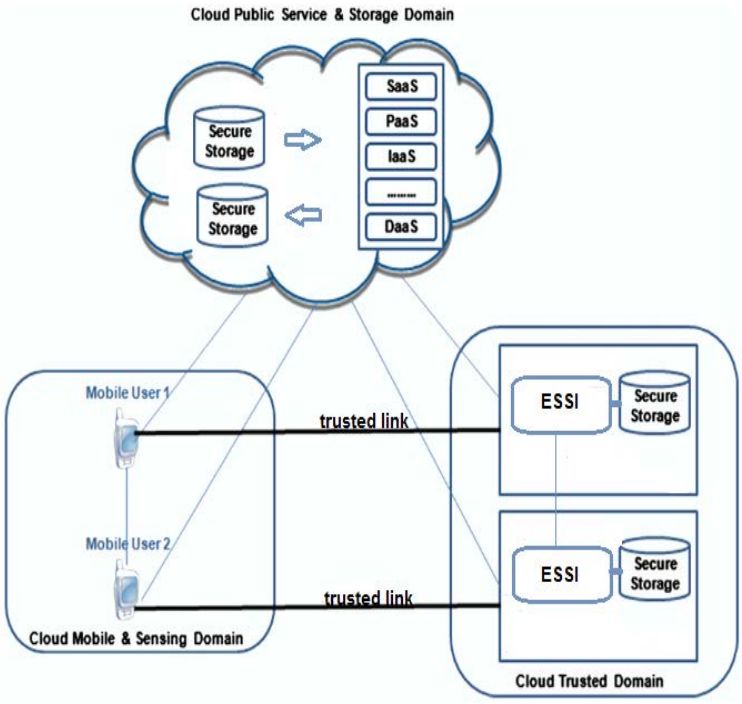

Figure 1. Reference Service Model of mobile cloud

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. User's private information is maintained in their corresponding Secure Storage (SS).

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 user's 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.

In this paper, we first describe the MobiCloud architecture and its support for security service provisioning, resource and security isolation. We then focus on the trust management by describing the several services that can help both cloud and MANET to achieve the proposed system-level functionalities, such a sidentity management and key management.

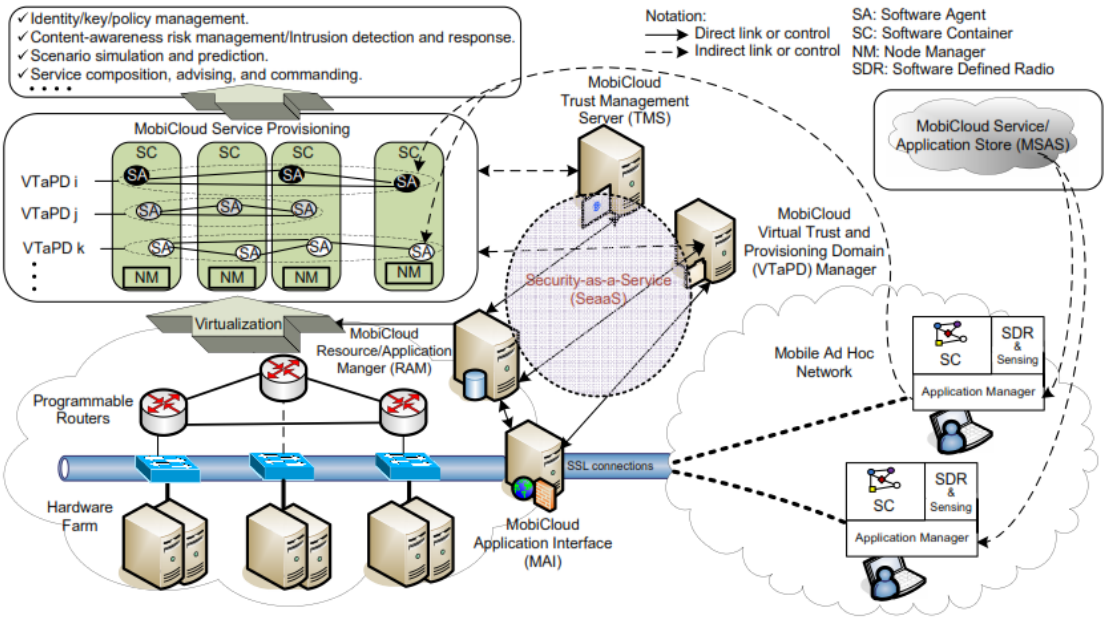

Figure 2. Mobicloud architectur

2. Mobicloud Architecture

The conceptual infrastructure for MobiCloud is shown in Figure 2. Similar to existing cloud-based computation and storage outsourcing [3], a mobile node can leverage hardware farms on cloud to augment its computing capabilities. Now, we describe the functionality and properties of each component of Figure 2. MobiCloud uses Software Agents (SAs) (i.e., application components) to link the cloud services and mobile devices. The same SA can run on both the mobile device and the cloud platforms correspondingly. Each device can have multiple SAs for different cloud services or MANETs, which are managed by application manager of the device. Each device also provides sensing data about the device itself (such as processor type, utilization, battery state, and location with GPS support), and about the neighboring mobile nodes (such as neighbor's identity or addresses, link quality, neighboring durations, etc.), which are managed by the sensor manager.

On the cloud side, the MobiCloud Application Interface (MAI) exports services that can be consumed by to mobile devices. In addition, the MAI also provide interfaces to VTaPD manager and Resource and Application Manager (RAM). Middle-ware based solutions are required when the cloud components do not use web-based interfaces. Several unique cloud components and constructions are proposed for MobiCloud. We introduce programmable routers [4] that can be used to create multiple VTaPDs. VTaPDs are created mainly for isolating information flows and access control by creating multiple virtual domains. There are two main reasons for multiple virtual domains: (i) Security ,a user's device may run multiple applications at different security domains, e.g., its simultaneous communication with two individuals from different administrative domains; and (ii) context-awareness, it may be necessary to separate services for different local and network settings.

In each VTaPD, one or more SAs are used for every ESSI. A Node Manager (NM) is responsible for managing the loading and unloading of SAs in the ESSI. The ESSI also provides additional capabilities beyond the functions of a mobile device. For example, the cloud will be able to run services that are not available in MANETs, such as search, data mining, media processing, trust pre-establishment (e.g., credential exchange and establishing security keys in advance), etc. The MobiCloud Resource and Application Manager (RAM) constructs VTaPDs when it is directed by MobiCloud VTaPD manager and MobiCloud Trust Manager Server (TMS).They form the core for providing Security-as-a-Service (SeaaS). With SeaaS, MobiCloud can offer security service composition capability according to requests from mobile applications. In our SeaaS service model, the VTaPD manager plays the central role since it collects context-awareness information from the MANET (such as device sensing values, location, and neighboring device status) and used it for intrusion detection and risk management. The MobiCloud TMS is the Trust Authority (TA) for MobiCloud. It handles the attribute-based key distribution and revocation. It provides identity search and federation services for mobile devices belonging to multiple administrative domains. It also performs policy checking and enforcement functions to provide a unified trust management system for MobiCloud.

Finally, the MobiCloud Service and Application Store (MSAS) serves as the repository for SAs and applications. When service composition is needed, the MSAS will install the required SAs or applications through the MAI. For example, when a mobile device needs to talk to another device using different frequency bands, the Software Defined Radio (SDR) needs to install a new driver and the node needs another authentication module. In this scenario, the SAs for the new drivers and authentication module will be installed. This operation needs collaborations between TMS and MSAS.

2.1. Secure and Resource Isolation Through VTaPDs

VTaPDs are established to provide data access control and information protection. We must note that the framework may not need/imply the division of the administrative domain into VTaPDs. The actual administrative work is handled by the MobiCloud VTaPD manager. Every node that belongs to a particular VTaPD will have the complete routing information for VTaPD, but not others. Each node can reside in a different physical system. Each node would have to support our communications framework which includes secure group communication to sending data to all the ESSIs in the same VTaPD. The bandwidth for a communication link can be divided by using different encryption/decryption/authentication keys. An advantage of the MobiCloud framework that provides network virtualization through multiple VTaPDs is that it facilitates prioritization of critical/emergency services in a network. For example, using the proposed virtualization approach, prioritized and normal service classes can be defined using different VTaPDs. They can share the same physical MANET but prioritized based on the VTaPD. MANET operations and communications can be migrated into the cloud when peer-to-peer communication is under stress either from insufficient bandwidth or attacks.

In multi-tenant environments each mobile user's ESSI can be considered as his/her tenancy in the MobiCloud. In the multi-tenant environment, data access control is one of the most critical security concerns that need to be addressed. Data isolation mechanisms prevent users from accessing resources belonging to other tenants. There are generally two kinds of access control and isolation patterns: (i) implicit filter and (ii) explicit permission. Inpattern (i), when one tenant requests to access shared resources, a common platform level account (i.e., the ESSI identity with corresponding SA and cloud resource requests) is delegated to handle this request. The delegated account is shared by all tenants and has the privileges to access resources of all tenants. However, the key of this mechanism is to implicitly compose a tenant-oriented filter that will be used to prevent one user from tapping into resources of other tenants. This can be achieved by using a cryptography-based solution, i.e., group key management based solutions to secure information flows through different VTaPDs that share the same physical system. In pattern (ii), access privileges for the resources have been explicitly pre-assigned to the corresponding tenant accounts by using the Access Control List (ACL)

mechanism. Therefore, there is no need to leverage an additional common delegated account across tenants.

3. Mobile Cloud Trust Management

The trust management model of mobile cloud include sidentity management, key management, and security policy enforcement. An ESSI owner has the full control over the data processed in the ESSI, and thus a user-centric identity management framework is a natural choice. The user-centric identity management that allows an individual to have multiple identifiers, (For example, the identifiers carried on a national ID card) 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 sharing data over the Internet, and can transfer and delete the data when required. In this paper, we introduce an integrated solution involving identity-based cryptography [5] and attribute-based data access control [6].

3.1. Mobile Cloud Identity Management

Trusted Authority (TA) is assumed to manage security keys and certificates for mobile users, 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 3.

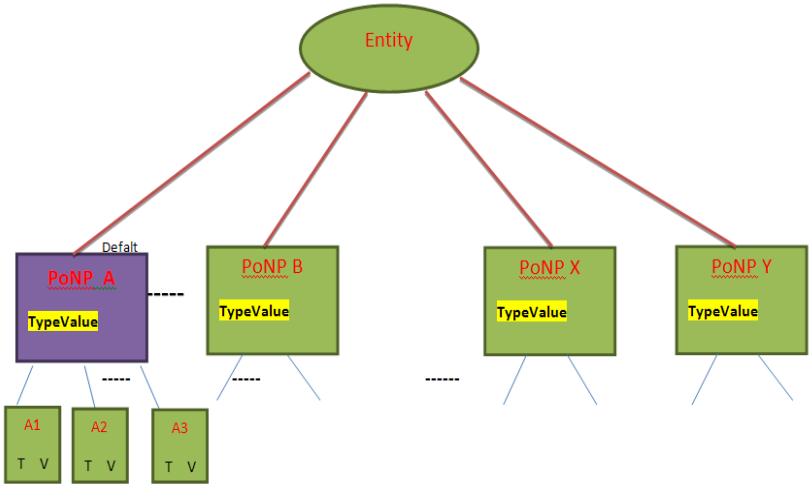

Figure 3. Identity representation scheme

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 each individual. 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 military ID, SSN, etc. It is not necessary to use identifiers from the same administrative domain. Each PoNP has two properties: Type and Value.

The type provides the information such as the identity, the private key and the validation period. The identity and private key issue can be either self generated 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 (A1 ... An), and each attribute has type and value properties.

The major benefit of using this identity representation is the standardization of identity management. In practice, the numbers of PoNPs for every mobile node should not be many. They can be assigned to mobile users as predefined attributes that do not changed frequently. We call these attributes as static attributes. To differentiate PoNPs, we will be able to narrow down the numbers of attributes that can be potentially used for later secure communications.

3.2. An Example of Mobile Cloud Trust Management

An ABIDM example is presented as follows:

Identity Representation:

PoNP: {Native}, Type: {ID, TA, Exp Date}, Value: {011};

A0: {attribute}, Type: {name}, Value: {identity ->David Kurt};

A1: {attribute}, Type: {B }, Value:{0};

A2: {attribute}, Type: {B1}, Value:{1 };

A3: {attribute}, Type: {B2}, Value:{1};

PoNP: {identity}, Type: {name, Self-Gen, Exp Date}, Value: {David Kurt};

Aj: {attribute}, Type: {organization}, Value: {ASU-Fulton-CIDSE-CSE};

Aj+1: {attribute}, Type {device}, Value: {communication -> Mac address - >01:23:45:67:89:ab};

Aj+2: {attribute}, Type: {email}, Value: {David.Kurt@asu.edu};

PoNP: {communication}, Type: {Mac address, TA, Exp Date}, Value: {01:23:45:67:89:ab};

A: {attribute}, Type: {organization}, Value: {ASU-Fulton-CIDSE-CSE};

Ak+1: {attribute}, Type: {owner}, Value: {David Kurt};

Ak+2: {attribute}, Type: {device model}, Value: {iPhone 3G};

The first PoNP is "Native", in which its value is unique for each entity. Attribute A0 usually points to other PoNPs. The number of bits for the ID value should be long enough to guarantee that every entity will have a unique value, where represents the bit at position x from the leftmost side. For demonstration purposes, three bits are used for the native ID value. The second PoNP describes the identity "David Kurt" and his associated attributes; the attribute "organization" describes where David works; the device attribute points to another PoNP "communication"; email is another attribute for David. The third PoNP is "communication", the entity is represented by a MAC address and the attribute "owner" describes who owns this device. In this example, attributes for different PoNP can be overlapped; on the other hand, an attribute in one PoNP may not exist in another PoNP.

ABIDM introduces a user graph approach, where directional links link PoNP to its attributes. An attribute can also point to another PoNP (e.g., {communication - > Mac address >01: 23: 45: 67: 89: ab}).

3.3. Efficient Key Management for Secure and Private Data Access Control

In the mobile cloud communication environment, a secure communication session can be either one-to-one or one-to-many [7] (e.g., an ESSI wants to share a picture with several ESSIs, which form an ad hoc group). In the terminology of secure group communication, these communication patterns can be represented as group (or subgroup) communication. Thus, a shared key needs to be established among group members. In literature, a secure group communication includes 3 phases [8]: (i) secrets pre-distribution, (ii) group key update, and (iii) secure group communication. Phase (i) can be done offline before sending the encrypted data. Based on current hardware/software solutions, phase (ii) can be processed very quickly. Thus, the main bottleneck is in phase (iii). To address this bottleneck, the design goal is to reduce the group-based key management overhead and support efficient key distribution in a dynamic communication environment, where the communication peers may keep on changing.

Attribute Based Encryption (ABE) had been proposed for data encryption and decryption. ABE is an extension of IBE scheme in that multiple public attributes are known as the public key. Using threshold secret sharing scheme [9], the encrypt operation can construct an data access policy by forming an encryption policy tree, where leaf nodes are attributes and the internal nodes are logical gates such as "AND" and "OR".

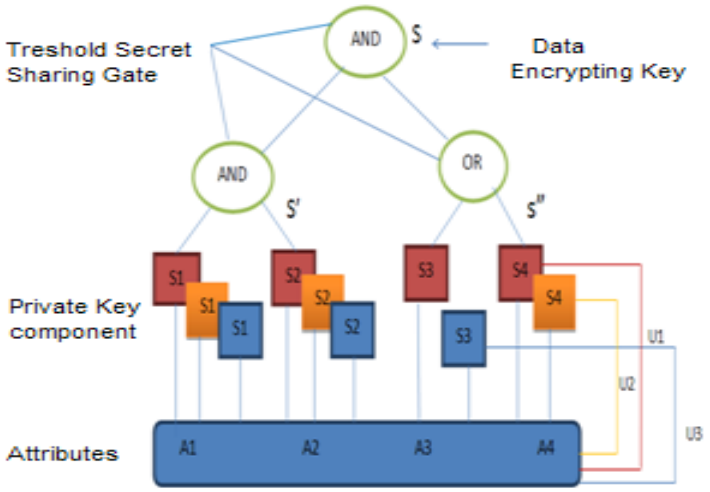

Figure 4. Attribute – based encryption

In Figure 4, we present an example to illustrate using ABE [10] for data encryption and decryption. In this example, attributes A1 - A4 are arranged as leaf nodes of the attribute tree. Each attribute can have multiple secret components for different users. We must note that users can share an attribute; however the corresponding private key components for that attribute are different. This is represented by different colors of the keys. Thus, u1 has private key components {red: S1; S2; S3; S4}, u2 has private key components {green: S1; S2; S4}, and u3 has private key components {blue: S1; S2; S3}. The internal nodes of the attribute tree are logical gates, such as "AND" and "OR". They are implemented using threshold secret sharing scheme [9]. The secret S can be derived from S′ and S″ using the secret sharing scheme. At the bottom level the encryption is performed using a construction similar to identity-based encryption (IBE) [11]. During decryption, in order to satisfy the AND gate, must have all the secrets under it to reconstruct the higher level secret; to satisfy the OR gate, is only required to have one of the secrets. The encryption algorithm of ABE is performed in a top-down manner by constructing the ciphertext at the bottom level of the attribute tree. The decryption algorithm of ABE is performed in a bottom-up manner using the user's pre-Distributed secrets to reconstruct higher level secrets until they reach the root. In this presented example, based on the pre-distributed secrets, u1- u3 can decrypt the secret sand thus they can access the data encrypted by using the DEK S.

3.4. Bootstrap of Secure Communication Group

ABIDM uses identity-based signature schemes for authentication and attribute-based encryption scheme for

data access control. A mobile user uses ABIDM to establish a virtual private communication service among ESSIs. The goal of ABIDM is to establish a common sharing group key among a selected group of users (or ESSIs). Based on the presented example, the bootstrap of the secure group communication using ABIDM is presented as follows:

Sender 011 would like to establish a virtual private communication group {001,011,100,101,110,111}.

Sender 011 uses BFM to derive the group-based attribute composition as B0+B2, where "+" is a logical OR gate.

(M ={001;011;100;101;110;111} =B1¯B2 B3 +B1 B2 B3 +B1¯B2¯B3 +B1¯B2 B3 +B 1 B2¯B3 +B1 B2 B3 =B0 +B2

Where Bi and¯Bi represent the bit values "1 and 0", respectively, at position i. The final group access tree only involves two attributes assigned to B0 or B2 to secure the encrypted data, in which both group members 000 and 010 are not able to access.)

Sender 011 uses attribute-based encryption scheme [12] to encrypt a group key ks.

Sender 011 generates the signature for the encrypted message based on identity-based signature scheme (e.g., [13]) using the private key of identity "011".

Sender 011 sends the encrypted group key and its signature to receivers.

Each receiver verifies the signature and decrypts the group key ks.

Note that the verification is based on the sender's ID (i.e., 011) and see if it satisfies the logic B0+ B2.

Then, the group-based secure communication session begins.

4. Conclusions

To transforming from traditional MANET to service – oriented communications and achieving secure computing for mobile users, we presented a mobile cloud framework called MobiCloud. We then described components of mobicloud architecture and interaction across its trust cloud framework. This comprehensive framework has been presented to focus on important and security issues such as virtual trust and provisioning domain construction, resource and information flow isolations and access control of users. Finally we introduce the trust management solution which is integrated with attribute – based identity management and attribute-based encryption.

References

[1] M. Walshy, "Gartner: Mobile to outpace desktop web by 2013," Online Media Daily, January 2010.

[2] 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 ServiceOriented System Engineering, 2010.

[3] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," in Proceedings of the ACM workshop on Cloud computing security, 2009.

[4] J. Lockwood, N. McKeown, G. Watson, G. Gibb, P. Hartke, J. Naous,R. Raghuraman, and J. Luo, "Net FPGA-an open platform for gigabit-rate network switching and routing," in IEEE international Conference on Microelectronic Systems Education, 2007.

[5] D. Boneh and M. Franklin, "Identity-based encryption from the weilpairing," SIAM J. of Computing, 2003.

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

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

[8] 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, 2004.

[9] A. Shamir, "How to Share a Secret," Communications of the ACM, 1979.

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

[11] D. Boneh and M. Franklin, "Identity-based encryption from the weilpairing," SIAM Journal of Computing, 2003.

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

[13] P. Barreto, B. Libert, N. McCullagh, and J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," Advances in Cryptology-ASIACRYPT 2005.