International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 8 (September 2014) www.ijirae.com

# A Case Study on Secure Online Transactions Using Root Trust Protocol

Nagaraja Metta[1] Mohan Kumar S[2]
*Dept of ISE, MSRIT* *Dept of ISE, MSRIT*

***Abstract — As the world becomes more interconnected, integrated and intelligent, mobile devices are playing ever-increasing roles in changing the ways that people live, work and communicate. The mobile devices become an ideal platform for carrying identity credentials and using them for logical access and online transactions. It is a trend to use mobile devices for mobile-centric applications and expand the mobile capabilities. By using these mobile centric applications we make on-line transactions. But how to trust these applications while requesting transactions and also how to ensure that right user is making transactions. In this project, we present a dual root trust model in the mobile application for online transaction that provides a dual trust root model, we consider both the user's mobile device and cloud services as trust model. We design trust execution environment embedded in a mobile device to provide security using AES algorithm for device specific transaction conformations for online transactions. None of the parties can make transactions independent of each other.***

***Keywords—IaaS, DRTM, TEE, OTP, UTP.***

## I. INTRODUCTION

World is becoming more interconnected due to mobile devices. Because of these devices life has become easy for every one's life. These devices act as lifestyle devices, because it includes camera, GPS, and also they help us to do day to day tasks. Since these devices are small in size, they can be carried from one place to another place, due to its small in size, the user may lose it or it can be theft by someone else. So all the data present in the mobile can be hacked by the stolen persons. They may launch the applications by the credentials stored on the devices.

In present days world, cloud has become natural choice for storing the credentials [2][3]. But it is one of the critical challenges to address security issues of mobile applications that depend on both mobile device and cloud. The cloud should not launch the applications without user's acknowledgements and to ensure that the right person is using the mobile device.

By considering all above issues, in this paper we presented the Dual Root Trust Model (DRTM) for all mobile online transactions. Here both the cloud and mobile device should work together. Independent of any of these the transactions will not take place. During transactions, the user is verified with proper acknowledgements.

## II. RELATED WORK

Filyanov[1] A. had designed and developed a secure transaction confirmation architecture called UTP. It provides assurance only to remote server, the user of a client system has indeed confirmed a proposed action. The "just one device" transaction confirmation is similar to proposed work. But UTP provides more assurance to service providers than to client users since the feedback available to client users remains Susceptible to manipulate by malwares. Krautheim[4] proposed the Private Virtual Infrastructures that represents a new cloud management model, and shares the responsibility of security in cloud computing between the service provider and the client. This dual root infrastructure assumed changes to the IaaS. In this paper we focus on building trust between parties involved in an online transaction in the application level.

## III. PROPOSED SYSTEM MODEL

The proposed DRTM works only by considering both mobile device and cloud. To use this DRTM, one must have smart phone with trusted execution environment (TEE) [6][7][8], which allows execution of trusted applications and there should be a cloud, which provides dedicated virtual machine. The Fig-1 shows the architecture of DRTM.

 

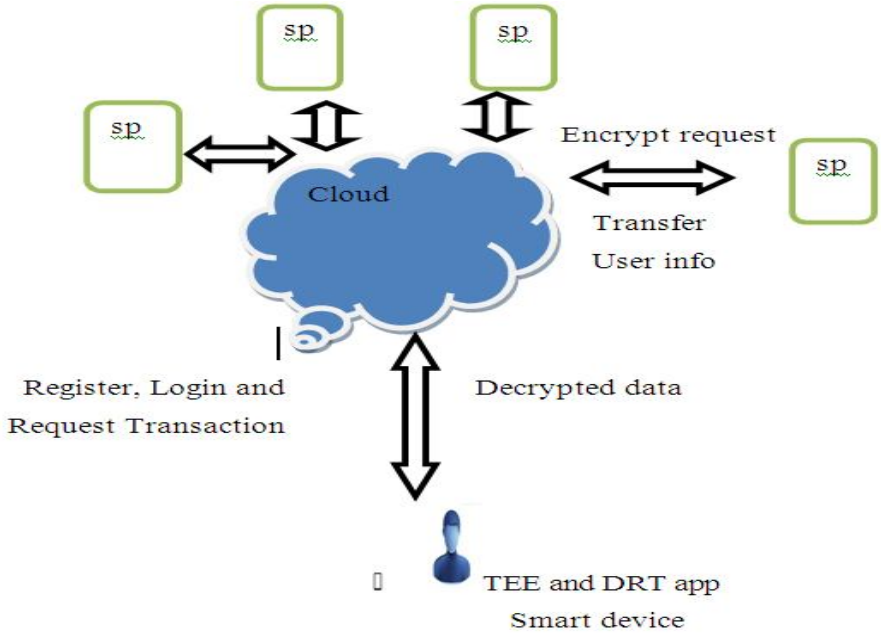


*Fig-1, DRTM Architecture*

### A. DRTM Components

There are four main components in the presented DRTM. Each one plays a important role.

*Mobile Device:* To use DRTM, Smart Mobile Device is used. It should have TEE. Each device is identified with international mobile equipment Identity (IMEI) number.

*User:* User should have smart mobile device. With this he launches the applications.

*Cloud:* All user credentials and data is stored and managed in the cloud. The user can access the cloud by setting base URL in the mobile device.

*Service Provider:* The service provider provides services to user.

### B. Description of DRTM transaction Procedure

Step 1) First user needs to install the DRTM secure app into his mobile device.
Step 2) He need to set the Base URL to connect to Cloud.
Step 3) If he his first to use DRTM, then he need to Register with username, mail-id and phone number.
Step 4) The Cloud will send user-id and Password to user email ID.
Step 5) The user need to log in with the credentials which are sent to his mail id
Step 6) After Log in, he will make online transaction request to service provider.
Step 7) Transaction request are encrypted. The cloud will forward the request to service provider.
Step 8) Then service provider verifies the user credentials details such as credit card number IMEI number of user mobile, and card validity. If IMEI number matches, then Service provider will generate One Time Password (OTP) and send it to valid user mail id.
Step 9) Once the user enters the OTP, the service provider verifies it credentials', if it matches, displayed with transaction successful message.

 

In order to make secure transaction, we implemented with AES algorithm. The steps in AES algorithm is as follows. The AES algorithm has four main operations. Add Round Key, Byte Sub, Shift Row, and Mix Column. All four operations together is considered as one round. The encryption uses a set of derived keys from the cipher key. First, the credit card details entered on mobile which is plain text, is organized into 4*4 byte matrix. This is called state matrix. Here we are using 16 byte (128 bit) key, so for encryption following steps needs to be considered.

1) Need to derive the set of round keys from the cipher key.
2) We need to initialize the state matrix with block data.
3) Need to add the initial round key to the starting state array.
4) Then perform the nine rounds of state manipulation.
5) Then perform last round manipulation. In this round we get cipher text.

Fig-2 shows the credentials data flow of information about AES encryptions process, which gives flow of encryption.

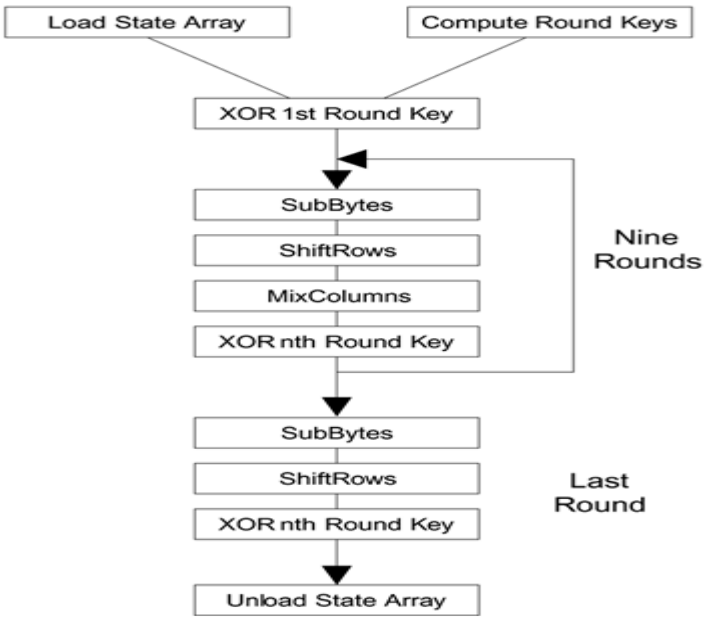


*Fig-2, AES algorithm process.*

The service provider can decrypt the data by reversing all the steps taken in encryption using inverse functions.

## IV. SECURITY ASSESSMENT

In DRT, all entities in the system are considered semi trusted. If someone other than DRT user knows the DRT user id and password and tried to make a transaction using his mobile device, In such cases, the cloud can easily detect the misbehaviors since each user has registered and been bounded with a mobile device in the cloud and also we are providing OTP to conform the right user making transaction. We have the trusted execution environment which allows the application to execute in secure manner.

## V. CONCLUSION AND FUTURE ENHANCEMENT

We proposed a dual root trust model, which allows the users to make online transactions in secure manner. The transaction can be done only by considering both mobile device and cloud service. This gives the dual root trust model approach. As it is device specific conformation based transaction, this approaches right user using the right device and request for transactions.

 

In future we can provide authentication along with confidentiality with the use of public key cryptography and also can be enhanced by providing computational performance evaluations on trust zone embedded devices. It would be interesting to consider attribute based encryption systems with different types of expressibility.

## VI. REFERENCES

[1] A. Filyanov, J. M. McCuney, A. Sadeghiz, and M. Winandy, "Unidirectional trusted path: Transaction confirmation on just one device," in Proceedings of the 2011 IEEE/IFIP 41st International Conference onDependable Systems&Networks, ser. DSN '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 1–12.
[2] D. Huang, "Mobile cloud computing," in Proccedings of the sixth conference on computer systems. ACM, 2011, pp. 301–314.
[3] P. M. M. N. B. G. Chun, S. Ihm and A. Patti, "Clonecloud: Elastic COMSOC Multimedia Communicatoins Technical Committee (MMTC) E-letter, vol. 6(10), Octorber 2011, pp. 27–31.
[4] F. J. Krautheim, "Building trust intoutility cloud computing," Ph.D.dissertation, University of Maryland, 2010.
[5] Li Li, Dijiang Huang, Zhidong Shen, Samia Bouzefrane, "A Cloud based Dual-Root Trust
Model for Secure Mobile Online Transactions" in 2013 IEEE wireless network communications and networking conference.
[6] J. Azema and G. Fayad, "M-shield mobile security technology: making wireless secure," 2008.
[7] ARM, "Trustzone technology overview," 2009.
[8] D.Davenport, "Nexus S Enables the NFC Secure Element," is available at http:// thinkd2c.wordpress.com/2011/07/07/ nexus-s- enables-the-nfc-secure-element/ , 2011.

 