AUTOMATED TELLER MACHINE WITH TWO STAGE SECURITY IN BANKING OPERATIONS

S. K. Peer, KLM College of Engineering for Women (skp.klmcew@gmail.com)
Rakesh K. Sharma, University of Maryland Eastern Shore (rsharma@umes.edu)
Daniel I. Okunbor, Fayetteville State University (diokunbor@uncfsu.edu)

ABSTRACT

Cloud computing involves the delivery of hosted services, such as IaaS, PaaS and SaaS over the internet. In this paper, we explore the characteristics of SaaS in ATM cloud data applications. The proposed ATM cloud system is equipped with security measure that will eliminate the use of ATM card and PIN for withdraws and other banking applications once the user is classified as a registered account holder.

Keywords: Bank ATM, PIN, Cloud computing, Iaas model, Paas model, Saas model, Two stage security, Security alert, Account holder.

1. INTRODUCTION

Cloud computing involves data for individuals and business enterprises stored in a remote location called “cloud” with the hope of eliminating costs (capital expenditure, hardware, software, personal maintenance, etc.) associated with local storage and its management; providing universal data access independent of geographical locations (Karthikeyan et al., 2012). Cloud computing is synonymous with database outsourcing that provides database as a service utilizing external service providers (Hecigumus et al., 2002). Clients have the ability to access data via the service providers without necessarily knowing the actual location(s) of the data. Cloud computing promotes demand self- service, ubiquitous network access, location-independent resource pooling, rapid resource elasticity, usage based pricing, and transference of risk (Karthikeyan et al., 2012).

The service providers, also called Cloud Service Providers (CSP), generally have high performance infrastructural facilities with sufficient integrated security defense mechanisms that support data integrity. Seemingly, this is to ensure significant cost savings, higher viability and effective data security protection for clients. Mobile and ATM banking systems are aggressively being migrated to cloud primarily because of the nature of the applications. This seems like a natural to do to allow bank industry to focus to other primary operations. Banks not store their data remotely in the cloud, delegating efforts typically required for local data storage and maintenance to the IT sector. The complexity of this cloud model poses security uncertainty not just for the bankers but for other entities such as the ATM users and the CSPs. With this cloud model, this question is when the user sends a query via the ATM, should the query be directed to CSP without the client (banker) involvement? What is the guaranteed that the user will be delivered the services required and as mandated by the client? In this paper, we would address the data integrity on ATM cloud-based model. This proposed model will ensure that integrity is guaranteed, as required by the client, for data is transmitted from the CSP to the ATM precipitated by the user’s query. The model, based on private cloud, provides authentication, sufficient access controls, and secure communication.

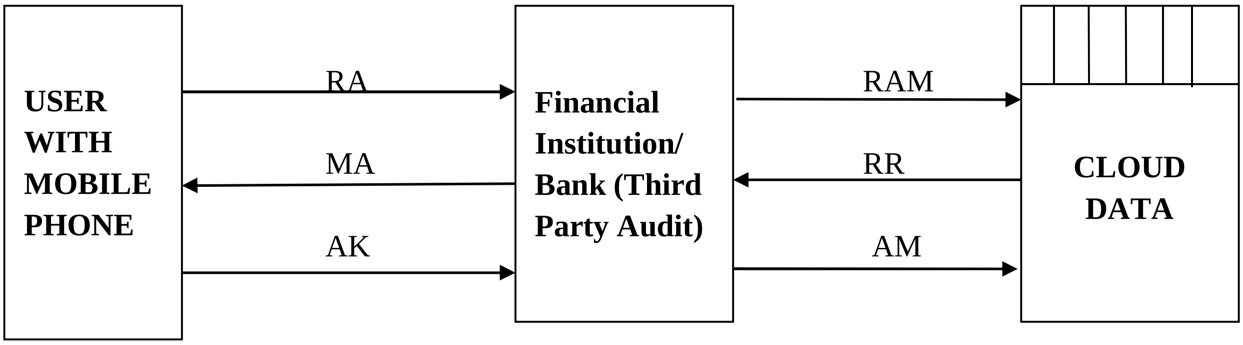
Private cloud is a proprietary computing architecture designed to have more control over the data than that of by using a third-party hosted service or public cloud. It has the advantages of being scalable and self-service. It provides hosted services to limited number of people behind a firewall. It is used to acquire service modes such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service) or SaaS (Software as a service).

This paper presents architecture of a two level security bank ATM operation which includes a private cloud using SaaS model. Section 2 of the paper presents the service models for evaluating suitable service models for banking services. The proposed architecture has two-level security as described section 3.

2. CLOUD COMPUTING SERVICE MODEL FOR BANKING OPERATIONS

As discussed in the preceding section, cloud computing systems deliver hosted services, such as IaaS, PaaS and SaaS over the Internet. IaaS allows the client (or enterprise) to pay for the services (or capacity) needed. PaaS provides software and product development tools hosted as the infrastructure of the service provider to the developers through internet for their applications. SaaS model provides web based services ranging from email to database processing for the user to internet with the service provider through a front end portal. The characteristics of SaaS model are explored in ATM cloud-based applications.

The basic procedure involved in the operation of bank ATM with cloud data is demonstrated as shown in Fig 1. First, request to access (RA) is sent to client with a request message to access private cloud data as soon as the card is inserted into the ATM. Banking operation includes the activities such as withdraws, mini statement, balance enquiry, etc. Typical ATM displays message alert (MA) on the console of user machine in response to user's request. The user is then required to send an access key (AK) to the client (banker), who in turn, sends access message (AM) to the cloud database for requested transaction. Subsequent to this, the user is instructed to enter a numerical number between 10 and 99 that the client will utilize to implement activate ATM for further transactions desired by the user. In case of loss of ATM card and PIN, the user is expected to provide information regarding the amount of cash debited and balance account available in the account. The proposed model provides security measure in the banking system that will allow user performance transactions without ATM card and PIN as described in the following section.



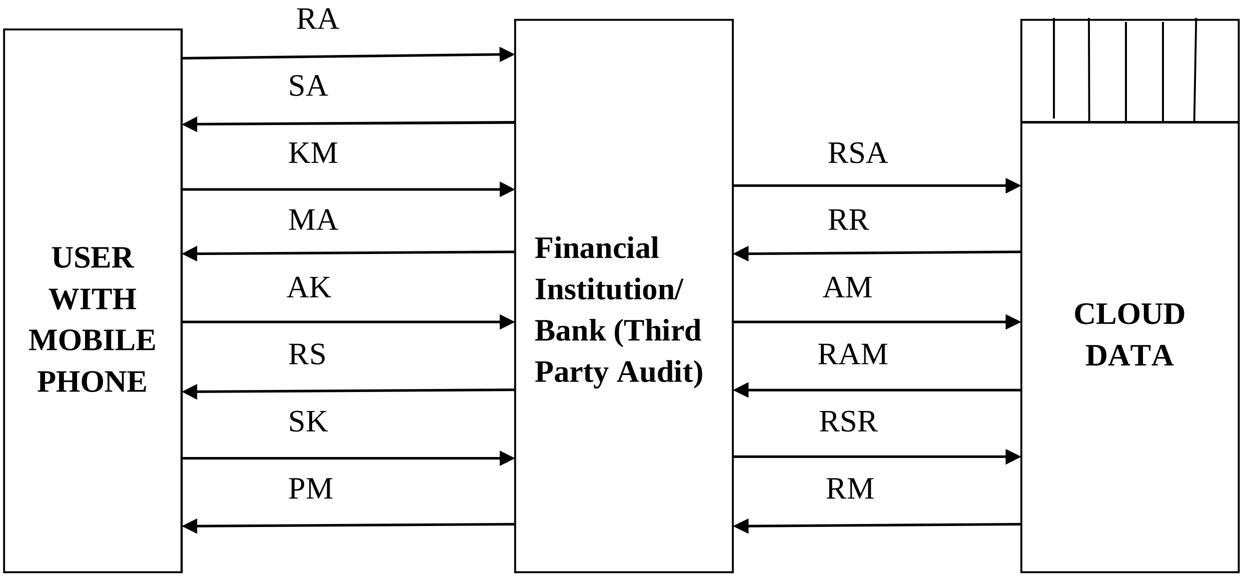
RR: Response to Request
AM: Access Message
RAM: Response to Access Message

AK: Access Key
RA: Request to Access
MA: Message Alert

Fig 1: Bank ATM Operation with Cloud Data

3. PROPOSED BANK ATM OPERATING SYSTEM WITH TWO STAGE SECURITY

The proposed ATM cloud-based system has security measures split in two stages as shown in Fig.2. First, request to access (RA) is sent soon after inserting ATM card into the machine to access private cloud data. In response to request to access, a security alert (SA) is sent to inform the account holder at his mobile number to press button of number '1' on the mobile phone as a key message (KM) to the client, in order to accept to ATM card inserted in the ATM machine for operating through request to access message (RAM) to the cloud data. The account holder may press the button other than the number '1' as a key message on his mobile phone to reject the operation of ATM card inserted into the machine through reply to security alert (RSA) to the cloud data. Once the card is accepted, message to access (MA) is sent to the user in response to request (RR), is order to enter PIN as access key (AK) to the client, which is directed as access message (AM) to the cloud data. Later, response to security (RS) is reached at mobile number of the account holder through response to access message (RAM) from the cloud data, in order to inform the account holder to press the button of number '1' on the mobile to accept the right PIN for further processing or to press a button other than the number '1' to avoid further actions with as security key (SK) to the cloud data being sent as reply to security response (RSR). Following that, a response massage (RM) is sent from cloud to the ATM machine as a process message (PM) displayed on the ATM console while performing the requested transactions.



RSA: Reply to Security Alert
RS: Response to Security
SK: Security Key
RSR: Reply to Security Response
PM: Process Message
SA: Security Alert
AM: Access Message

RAM: Response to Access Message
KM: Key Message
AK: Access Key
MA: Message Alert
RA: Request to Access
RR: Response to Request
RM : Response Message

Fig. 2: Bank ATM Operation Model with Cloud Data in Two Stage Security

REFERENCES

Heligimus H, Iyer, B.R. and Mahrotra, S. (2002). Providing database as a service " in proceedings of International Conference on Data Engineering (I.C.D.E).

Karthikeyan, P.N., Selvalakshni, C.B., and Mallikarjuna Nandi (2012). Direct user Data Authentication in cloud. International Journal of Electronics and computer Science Engineering ISSN 2277-1956 VIN 4. pp. 1954-1959.

Mykletun, E., Narasimha, M., and Tsudik, G(2006). Authentication and integrity in outsourced Databases. Trans. Storage, vol.2, no.2. pp.107-138.

Pang, H. Jain, A, Ramamritham, K ., and Tan, K (2005). Verifying completeness of rational query results in data publishing" SIGMOD, Baltimore, MD, USA, June 2005.

(A complete list of references is available upon request from S.K. Peer at skp.klmcew@gmail.com)