Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Contemplate for Online Plebiscite Capturing Using ATM Terminals

Kausal Malladi
P.G. Student - M Tech,
Department of Computer Science,
International Institute of Information Technology - Bangalore., India.

Srivatsan Sridharan
P.G. Student - M Tech,
Department of Computer Science
International Institute of Information Technology - Bangalore., India.

Abstract — Voting is one of the fundamental rights provided to the citizens of any democracy. Online voting has been gaining a lot of momentum but has always been restricted to discussions rather than its implementation. Keeping in mind the number of ATM terminals installed across the world, a solution for online voting is proposed using Automated Teller Machines. The process of online voting could be deployed with three phases - the voter registration, ATM card registration and online vote capturing. A Secret Voting Password (SVP) provided to voter during registration acts as an authentication mechanism which enables the voters to securely cast their vote. The concept of Reverse SVP is provided to address the predominant issue of booth capturing. The objective of such system also rests in providing a cost effective solution to the government along with ensuring non-traceability and integrity of the votes cast while providing great convenience to voters.

Key Words - Authentication, Databases, Distributed Database, Encryption, Security.

I. Introduction

Automated Teller Machine is the system which has been designed to give money instantly to the customers at a lightning speed. ATM systems have been installed at various places across the globe by various financial institutions. These systems have been given the secure way of authentication by providing a Personal Identification Number (PIN). This PIN will be asked to the customers when their card has been recognized by the terminal. So the process of authentication starts after the card is sensed by the terminal. As the scope of this system could be extended to any application involving secure transactions, this paper proposes an online voting using the same. The usage of the ATM Terminals could be extended to numerous other government related services which could reach the end users at a very fast phase and thus utilize these systems installed efficiently rather than using it only for instant cash withdrawal.

Though there is much criticism regarding the usage of ATM terminals for non - financial services, they could indeed be used effectively to meet various needs of the end users. To answer this criticism, it is necessary to look on to the initial purpose of laying this ATM terminal worldwide. The main purpose of the ATM installation was proposed earlier that these terminals would function as a mini financial institution and would encompass all the services of the financial institutions like loan processing, all financial withdrawals and deposit etc. But because of few limitations (like unavailability of man power to get all the deposits from the ATM on a daily basis to facilitate the deposits in ATM) it has been forced to become a currency vendor machine. This state of ATM terminals now could be improved by facilitating socio-public services through the ATM terminals, thus increasing their utilization rate. Some of the (non – financial) services that are being proposed in this paper are online voting, voter identity registration. The paper deals with the design and implementation issues of Voting System using the ATM terminals, along with the voting right registration, ATM card registration for voting right Implementation and the mechanism in place to check for authenticity during voting and performance issues related to the traffic during the implementation of these systems in ATM Terminals.

II. Existing System

There is increasingly widespread adoption of *ATM* systems across the globe. ATM system across the globe is known for its famous instant cash delivery to the customers. Customers need to swipe their ATM card provided by their financial institutions. Also they are supposed to provide their Personal Identification Number to complete their process of authentication. When their authentication is complete, the customer is allowed to select the type of transaction to be made by them - either balance enquiry or instant cash withdrawal. No other services that are non - financial especially the online voting has been implemented in the ATM Terminals until today. So to overcome the disadvantage of the Electronic Voting Machine (EVM) the paper proposes the online voting solutions.

III. Proposed System

The ATM card and the PIN that is being currently being used by the system is necessary along with the user Mobile number registered officially with the financial institutions which provide the user with the ATM card. From the globally known fact that estimates that almost all the populations who have their ATM card are also the user of at least a mobile, this technique is being proposed. The proposed system consists of three main functionalities being implemented, namely, the franchise right registration, ATM Card registration for voting right Implementation and the real process of online voting through ATM Terminal.

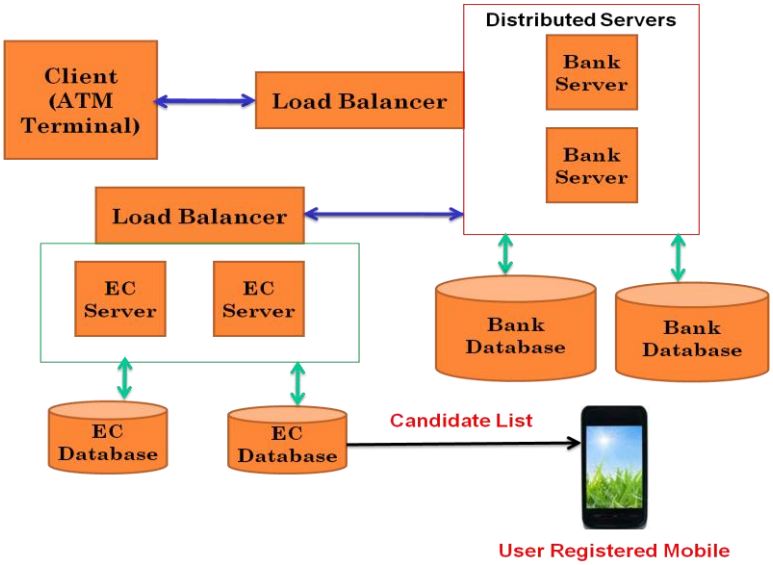

Figure 1. Architecture of Proposed System.

Franchise Exercise Right Registration. If the user comes to ATM Terminal and swipes the ATM Card and enters the PIN Number, user is provided with two options, one the financial services and other, non-financial services. Now if the user selects Non-Financial services, there is an option of the Election - Related services, which in turn composes of this registration process. Once the user selects this process, the Bank Server sends all the Details of this ATM Card (Account Number, Address, Mobile Number, and PAN Number) to the distributed Election Commission Servers Located in various parts of the country. It is assumed that all the ATM cards are compulsorily associated with the Users Unique Personal PAN Card Number and this PAN number is unique key for recognition in Election Commission Server. Also the existence of mobile with the entire ATM Card holder is assumed to be true, but solution could exist even without the presence of it. Then PAN card number sent by the bank is checked on the Election Commission Server for the avoidance of duplicate entry and if the match is found the entry is rejected, else the application is accepted where-in the user is allowed to enter a six - digit non palindrome Secret Voter Password (SVP) that should be used during the online voting process. Then the back-end verification is made by the election commission to ensure additional fold of security mechanisms. After the back-end verification, SVP is updated on to the Election Commission Server. The swiped ATM card itself, after the success of back-end verification, is then made the valid card to be used during voting in the ATM terminal and any more attempts to register different ATM card by the same individual is prohibited by adding the this entry of the valid ATM card for voting in the Election Commission Server and sending the user a message to the registered mobile that the registration is accepted. Similarly the Constituency details are obtained from the address field of the ATM card, and that address is made as the current residential address of the end-users. Any address change of the end-user is entertained only after proper back-end verification by Election Commission. *ATM Card Registration*. If the user visits ATM Terminal, swipes the ATM Card and enters the PIN Number, they are provided with two options, one the Financial Services and other, non financial services. Now if the selection made by the user is non-financial services, there is an option of the Election - Related Services, which in turn composes of this ATM Card registration process. Once the user selects this process, the Bank Server sends all the Details of this ATM Card (Account Number, Address Mobile Number, and PAN Number) to the distributed Election Commission Servers located in various parts of the country along with the demanded SVP from the end-user. In this case, there are two possibilities. If the PAN number associated with the ATM Card is not found in the election commission server database itself, then user is prompted to first register himself for establishment of his/her voting rights. In deeper context, if an entry for the PAN number is found it is checked whether the individual is already has registered with a valid ATM card to exercise the franchise. If yes, then the ATM Card Registration request is rejected else the card swiped is accepted and corresponding update is made. If all these verifications succeed but the SVP validation fails, then the user is rejected from making this ATM Card to be used for franchise exercise right. Successive Thrice failures of the SVP leads to the blocking of the user voting rights by blocking the entry and SVP Password in the election commission server. User has to undergo a manual back-end verification to get back the voting rights. *Online Voting Process.* This model has two different scenarios in place for Elections and for

by-elections. For any election like general, state or local-body elections, a visible advertisement on the day of election is scrolled in the display screen of the ATM terminals. This has a link to the voting process of the election services inside non financial services. On the normal day this service icon is present but kept disabled. All the ATM Terminals are updated with the timer to have the check on the duration of voting on the day of election (for the e-voting services to be enabled on that particular day within stipulated time period). Also the user is sent a message about the candidates in fray in his registered location along with their ID's with which the user should cast the vote to their officially registered mobile. Once user swipes the card, enters the PIN number and validation is successful, this advertisement scrolls on the ATM screen. The user now clicks the link and then the SVP of the end user is requested to be entered. In case of adverse conditions in the ATM terminal for the polarization of the user's franchise, the additional fold of authentication is provided to the voter. It is by allowing the voter to enter the SVP in the reverse order i.e., if the SVP is 259369 allowing to enter as 963952. Then the emergency information is sent to the near-by patrol and the user is allowed to cast vote, but it is made invalid. So the voter is given an additional advantage of recasting the vote after 4 hours from the cast of first invalid vote in a different ATM Terminal.

Once the verification is made on the election commission server, routed via National Financial Switch, the details of the user i.e., if this ATM card is officially registered for e-Voting process, whether the user had already voted and if the SVP entered matches, then the user is given a chance to vote by providing the option of entering the candidate ID obtained through user gadgets, else appropriate Error Message is Popped up on the ATM Terminal display to the end-user. Thrice wrong entry or reverse entry of the SVP makes the card blocked from further voting process. Once user exercises his choice, it is confirmed and then the vote is recorded and possible necessary update is made on to the Election Commission server to capture that the information that the user has voted. Once results are out, the Already Voted field is freed for all the voters form the Election Commission servers.

In case of the by-elections to any levels of democracy, the SMS is sent to officially registered Mobiles of the customers, about the election process on the day of election. It is here assumed that all the users have also registered and associated compulsorily a mobile number with the ATM card. Then there is no advertisement scrolling on the ATM Terminals on the day of election, thus the user, based on the SMS has to navigate through to non-financial services, then onto e-voting process which is enabled as there is election happening. This is done after ATM card swipe and PIN Validation, and the user is thus prompted for SVP and from this point the scenario discussed above is sequentially followed.

IV. Architectural Components

The functional units of the proposed system contain the different stand-alone modules which are needed to be interfaced in proper fashion to obtain the desired functioning of the authenticated online voting service. Architecture depicts the various stand alone modules which has their specific functionalities which could be efficiently utilized by providing the requisite coordination among each others. The necessary components are just needed to be added to the existing system, such as the Load balancer one before the National Financial Switch (NFS) and each across different distributed bank and Election Commission servers, so that the Existing ATM terminals need not be entirely modified to incorporate the proposed system features and balance the network traffic load. To have a balanced load onto these distributed servers and reduce the response time for a request message generated, the load balancers are in place. Distributed server is necessary to handle the work load of all the transactions and querying happening on the databases.

V. Failures In Existing System

Exploiting the lack of cryptography, casting multiple votes, accessing administrator and poll worker functionality, tampering the system configuration, tampering the ballot definitions, impersonating legitimate voting terminals, tampering the election results and linking voters with their votes, attacking the start of an election are possible failures in the existing systems. An important failure in the existing system is the lack of the authentication mechanism in the voting terminal. Any individual is not authenticated before they are allowed to cast their votes in the terminal. Also the main problem of accessing the functionality of the poll worker is an issue that is of a serious concern in many developing countries which needs to be addressed. The true verification of their identity with any other available means is not the concern of the EVMs which is a serious threat to current System's Integrity as it could not been able to even control polarization for a particular candidate in the polling booth.

VI. Remedies To Failures

There is a complete authentication of the end user in the ATM terminal. Complete authentication of the customer is provided with the help of the SVP being used in the ATM Terminal. This could deal with all the failures that are pertaining with that of authentication mechanisms. All the transactions between the ATM Terminal and the financial institution are encrypted with 2048 bit (SALSA) encryption standard which exists already. Also for the voting transactions a different 2048 bit encryption standard is being used along with an additional tier of encryption using the fact that all the ATMs are inside a privately connected network. The Ethernet Hardware Address (EHA) of each ATM Terminal updated on to the back end distributed servers is used as the secret key for encrypting the message between ATM Terminal and the corresponding financial institution's distributed servers along with the timestamp. So when the voting transaction begins after validation of PIN and simultaneous validation about the voting right for the card is made, the additional level of encryption starts so that any packet that the National Financial Switch (NFS) receives with the encryption done using the EHA as secret key, it decrypts and then simply forward it to the Election commission server.

Thus the exploiting the lack of cryptography problem is completely handled in case of this mechanism. Due to the back-end updates about the cast vote, the issue of casting multiple votes is also addressed. If there is an access of ATM Terminal by any unauthorized individual and polarization of the voting mechanisms is said to have happened, the voter could enter the SVP in the reverse order which allows the transaction to happen but the vote casted becomes invalid. Also providing voter, the opportunity to vote in a different ATM Terminal after certain duration wipes off the issue of accessing poll worker functionalities during voting (avoiding the failure similar to that of booth capturing). Tampering the election results and linking of the votes cast by the voters to a specific candidate in fray becomes highly impossible due to the fact that there is a presence of two level of encryption, one the original 2048-bit (SALSA) encryption performed using the value entered by the voter and two, the vote cast and the SVP validate request are encrypted additionally using the EHA of the privately connected terminal. As the NFS just acts here as a forwarding router, even if it happens to sense a packet encrypted using the EHA as the key, the Election commission alone could receive this encrypted vote. For SVP validation, the hashed value of the SVP using Account number and time stamp itself is decrypted using the Encrypted SVP value in Election Commission database and if the output of this process matches with that of the encrypted secret key, it is said to have been validated. During the declaration of results using the key as the SVP of that particular voter (which itself is kept encrypted and SVP validation is performed similar to that of Salt table in Unix Operating system) the vote cast is rehashed and then the result is declared.

VII. Phases In The Proposed System

Customer must be given an ATM Card by the financial institutions which can be used in the ATM terminal where the session is first established between the ATM terminal and the bank application server with the help of PIN entered by the user. The three options proposed in the solution are then displayed when the user selects non-financial services.

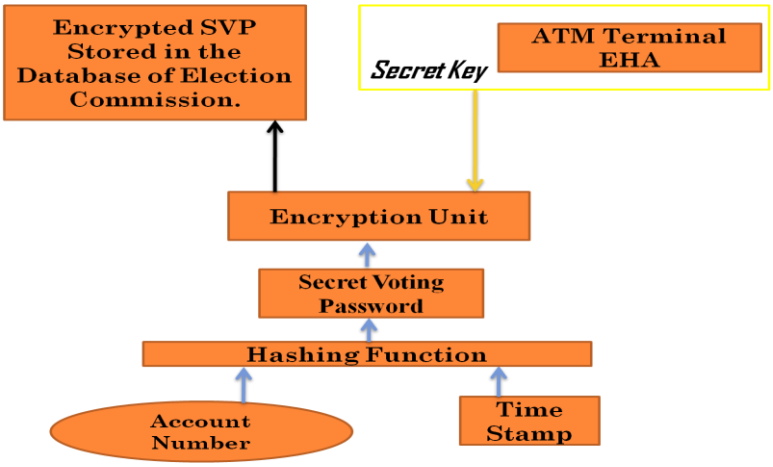

Figure 2. SVP from the user and SVP Storage.

SVP Validation storage and Validation. The SVP is asked to be entered by the user during the process of registration of the user from the ATM terminal, the hash function is calculated for the SVP over the ATM account number and timestamp (which is the Salt). When an encrypted message comes with the SVP Validation Request message, it is decrypted (as it is encrypted with the 2048 bit standard) and then the SVP entered is compared with the salt by rehashing the encrypted SVP with the current time stamp. If both the values match SVP is said to have been validated. The SVP Entered on to the ATM Terminal is temporarily stored locally until next phase of transactions happen.

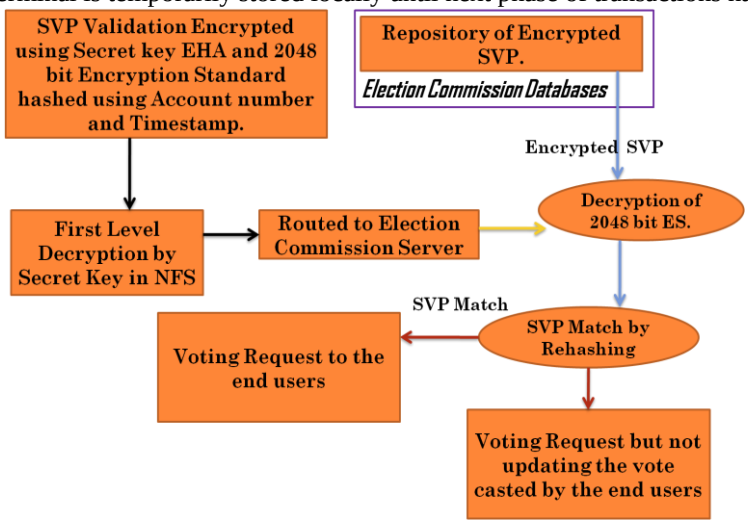

Figure 3. SVP Validation Process

Online Plebiscite Capturing. This process happens after the SVP match or reverse match occurs. In this case, for both the match and mismatch the flow is identical except the last transaction that captures the vote for a match while rejects and provides a timer after which the voter can use different ATM Terminal to recast their vote, for a mismatch. The vote cast is now hashed with the SVP and time stamp (as SVP is temporarily stored until the next transaction happens) and forwarded to the election commission server. The encrypted vote is stored in the database. During result declaration, the result is then obtained by performing the rehash on the result itself to obtain the voter's choice.

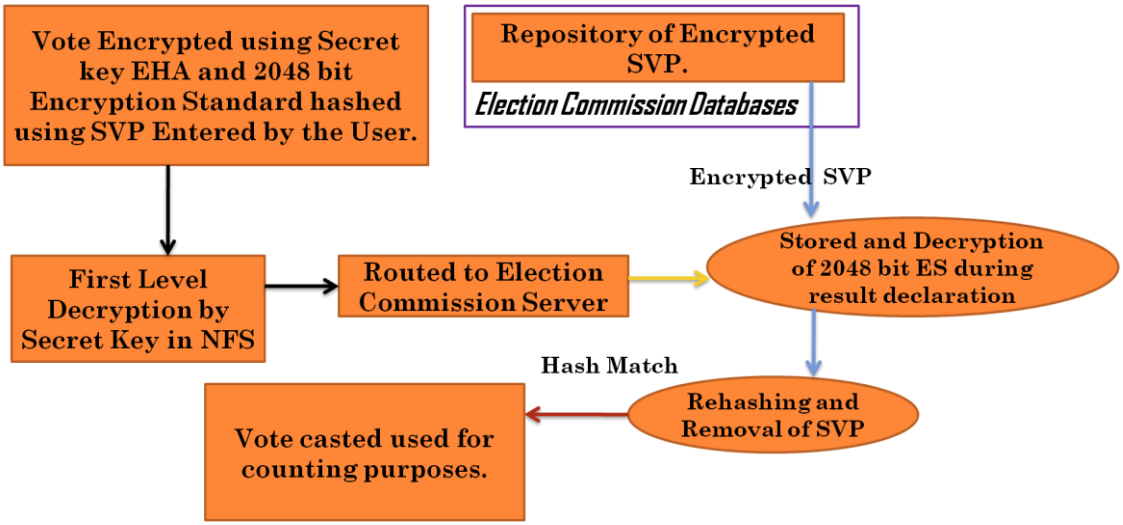

Figure 4. Online Validation Process

VIII. Conclusion And Future Work

Security models such as the voter-verified audit trail allowed for voting systems that produce a paper trail that can be seen and verified by a voter could also be developed in the near future. In such a system, the correctness burden on the voting terminal's code is significantly less as voters can see and verify a physical object that describes their vote and are allowed to vote in terminal only after their identity is proved. Also instead of invoking a complex hash and rehashing functions the use of double encryption standard with use of two pins - one for voting and one for emergency could reduce the complex transactions involved in the process. Any aspect of scalability issues related to the server utilization could also be improved in the near future.

References

[1]. B. Harris. *Black Box Voting: Vote Tampering in the 21st Century*. Elon House/Plan Nine, July 2003.

[2]. A. D. Rubin. Security considerations for remote electronic voting. *Communications of the ACM*, 45(12):39–44, Dec. 2002.

[3]. Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, and Tadayoshi kohno *Analysis of an Electronic Voting System*, in IEEE, May 2004.

[4]. *Voting: What Is; What Could Be*, July 2001. http://www.vote.caltech.edu/Reports/ .

[5]. *D.E Jones. The case study of the Diebold Accu-TS FTP voting system Site, July 2003. http://www.cs.uiowa.edu/jones/voting/dieboldftp.html*.

[6]. Valeria C., Michele C. janni, Philip S. Yu. Dynamic Load Balancing on Web-server Systems , IBM T.J. Watson Research Center, IEEE Internet Computing, vol. 3, no. 3, pp. 28-39, May-June 1999.

