RESEARCH ARTICLE OPEN ACCESS

A Security Implementation for Thearchitectural Approach on E-Voting System

Bimal Kumar[1] Dr. Siddappa.M[2] Dr.K.F.Bharathi[3]
1. Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool
2. Professor, Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur
3. Assistant Professor, Department of OAS, JNTUACEA
Corresponding Author: Bimal Kumar

ABSTRACT: E-Voting system is one of the emerging way of technology for candidates casting their supportable vote for the candidates for they to be elected. The whole system is divided into two main sector with one on the client side communication and another on server side communication. The whole system which comprises of Mobile Devices as the Voting Devices are connected to their respective servers. For the selfless authentication a unique authentication protocol called Single Token Authentication Protocol (STAP) is being created with the respective tokens through which the user is given a probable chance for the voting once. Once the Vote is being casted for the supported ones the session token expires. Individual architecture which comprises of the client and server operations is presented for the ease in use of the overall performance. The experimental output which comprises of all the respective results of the proposed architecture.
Index Terms: e-Voting System, STAP, Authentication Protocol,

Date Of Submission: 26-04-2019 Date Of Acceptance: 06-05-2019

I. INTRODUCTION

FREE and reasonable decisions and voting are the basic elements for an equitable country. Decisions permit the masses to pick their delegates express their inclinations for how they will be represented. Along these lines, the uprightness furthermore, exactness of race process is crucial to the uprightness of the majority rules system itself. Today, some new mechanical advancements are creating. Along these lines, internet business security and reasonable trade including electronic voting is turning into a well-known pattern. In this manner, researchers from Myanmar begin to supplant electronic voting rather than conventional paper voting in favor of sparing human asset and time. Along these lines, the execution of secure electronic voting frameworks is exceptionally basic in each country.

The principle objective of e-Voting is to give voters a decent condition so voters can cast their votes with least cost and endeavors. There are such huge numbers of properties that have been proposed to make the e-Voting secure process. A portion of these properties are the followings which must be fulfilled.

(1). **Qualification:** Only qualified voters are allowed to cast their votes.
(2). **Security**: There is no relationship between voter's recognizable proof and a stamped ticket.
(3). **Uniqueness:** No voter can cast his vote more than once.
(4). **Receipt-freeness**: A voter does not increase any data (a receipt) which can be utilized to demonstrate to a coercer that she voted absolutely.
(5). **Decency:** No halfway outcome is accessible before the last result turns out.
(6). **Unquestionable status**: Voters can check that their polls are checked effectively. There are two kinds of obviousness: singular question a status and widespread obviousness.
(7). Uncoercibility: No voter can demonstrate what he voted to others to avoid gift.
(8). Effectiveness: The calculations can be performed inside a sensible measure of time.

There are various kinds of voting frameworks. Among them the broadest sorts of them are:

· Paper-Based Voting Systems
· Direct-Recording Electronic Voting Systems
· Public Network DRE Voting Systems
· Precinct Count Voting Systems
· Central Count Voting Systems

Paper-based Voting Systems (PVS): record, tally, and deliver a classification of the vote check from votes that are thrown on paper cards or sheets. Voters might be permitted by a few PVSs to make determinations by methods for electronic information gadgets. Such information gadgets

don't record, store or classify freely voter determinations.

Direct-Recording Electronic Voting Systems (DRE) voting frameworks: record votes by methods for a vote show furnished with mechanical or electronic optical segments. Voter could initiate these segments. Such frameworks record voting information and vote pictures in PC memory segments. Likewise, information preparing is accomplished by the utilization of PC programs.

Public Network DRE Voting Systems (PNDRE): Make utilization of electronic votes and transmit vote information from the surveying stations to different areas over an open system. The votes might be transmitted as individual tickets as they are thrown, or intermittently as clusters of polls, or as one single group, at the end of voting.

Precinct Count Voting Systems (PCVS): put the tickets in a forbidden frame at a specific place, say, a surveying station. They give instruments that store vote check electronically and transmit the outcomes to a focal area over open media transmission systems.

Central Count Voting Systems (CCVS): Tabulate tickets from various areas at a focal area. Voted votes are securely put away briefly at the surveying station. These tickets are at that point transported or transmitted to a focal tallying area. CCVSs may, at times, deliver printed provides details regarding the vote tally. The point of this paper is to build up an electronic voting framework which can be utilized for college grounds decision and gives security and put stock in properties. And afterward the framework properties will be formally breaking down.

Voting is major in our cutting edge social orders. In accordance with this, portable applications are being produced and sent on advanced cells to influence the voting to process considerably more straightforward and compelling. These applications have raised our way of life whereby individuals can administer the entire world at their fingertips‟-voting frameworks have been acquainted with upgrade a few highlights of the appointive procedure [1]. It is for the most part seen as a medium for advancing majority rules system, setting up faith in constituent administration, adding honesty to decision results what's more, enhancing the general effectiveness of the appointive procedure [2].It is a reality that, with appropriate usage, on the web voting framework can dispose of a few cheats, pace up the getting ready of results and make voting more proper for the open.

Be that as it may, if not definitely conceived and plot, internet voting may demolish the trust in the whole constituent process [2,3]. This exploration work examines the outline of a web based voting framework that can be utilized at college level to continue with their yearly decision. This framework will be an inside and out paperless one since it will dispose of all the manual undertakings. Understudies can get to the application on their cell phone, wherever and at whatever point they want and pick their understudy bodies gave they have web association. Understudies will never again need to sit tight for extend periods of time to get the outcome since the framework will give continuous outcomes

It effectively met its points furthermore, destinations and every one of the necessities specified before were met. It will be useful for the clients who wish to vote since the voting procedure will be made simple by utilizing this application. In any case, in the wake of having tried the framework, in future we tend to include extra usefulness of picture approval for the security limitation and uniqueness which will give extremely solid security to the private data about vote. Besides, a commencement clock can be acquainted with set the beginning and closure time of the race. Close by, the clients are educated of the beginning time through a message and can begin voting. In the middle of, measurements are given and once the clock is finished, the voting process is blocked naturally and the clients can just view the last outcomes.

II. RELATED STUDY

Presently a day's decision procedure is assuming a critical part in Indian government. Race is a procedure to choose a great contender for who will lead our country. In majority rule government individuals pick there pioneer by giving their significant vote. As of late utilized Indian voting framework is an electronic voting framework, In that framework voter accessibility is obligatory, is the downside of electronic voting framework. So web based voting framework is the answer for this downside voter can be voting the contender for wherever from indicated Election Day and date.

Internet voting framework security is fundamental concern. In on the web voting process keep up the strict protection and uprightness of the vote threw and confirmation before the voter is thrown their votes. In web based voting vote throwing transference is moreover considered. What's more, votes are computed naturally after decision time is discharged and consequently sort the votes.

In web based voting framework confirmation is the principle is issue, just confirmed client is voting in favor of hopeful. Just approve individual can give their vote. Individual can be approving by a few strategies that can be close to home ID number (PIN), discharge message

or client personality confirmation. Every single validated datum can be gathered by client. All verifications are checked by principle database at that point consider that voter. Validation is checked by biometric ID process.

In this paper we proposed a method for integrating cryptography and steganography. The strength of our system resides in the new concept of key image. We are also able to change the cover coefficients randomly. This strategy does not give any chance to steganalytic tools of searching for a predictable set of modifications. Also, considering the complexity of elections, we have provided sufficient proof of authenticity of an individual in form of both biometric measures and secret key.

III. PROPOSED RESEARCH WORK

The Proposed Architecture which states the total condition of the collaboration of the client and server side components for the efficient implementation of the E-Voting System. The architecture is divided into two parts Server Side Component and Client Side Component. The server side component comprises of the server side interaction with the e-voting server and its components. The client side component interacts with the voter and his interaction with the voting machine. A Strategical security algorithm is used to make the system more secure than that is being attacked or misguided by the various other user.

In this architecture, the system has it maintainable security architecture which cannot compromised by the any type of the security attack which can make the system resilient and take out the data which is being undertaken in the time of the server interaction and client interaction. The Token key is generated for the each and every user for the efficient use of the system.

3.1 Server Side Deployment:

The server side component comprises of the data which represents the data which is being updated from the client end. The data which is being shared from the client end is taken into consideration and is adjoined to the comprising server to take its necessary steps to store it in the variable space. When the client side component is activated and the client starts the authentication strategy from the voting machine. The request is sent to the server side for the overall authentication and data administration.

Authentication Accessing Servers 1:

The server tries to authenticate the client information that is provided by the client by the total information that is available in the aadhar seeding server. The data is fetched from the aadhar seeding server for the proper authentication with the data that is provided by the client. When all the coordinates that is being provided by the client and data sharing server matches, then the authentication is successful.

Authentication Accessing Servers 2:

The Secondary authentication is taken into the consideration with the finger print authentication that is provided by the Finger Print Server with its corresponding database. Once the finger print data authentication request created from the client side for the Casting of the vote. The finger print request is fetched from the voter device and is sent to the finger print authentication database for the accessing and successful authentication of the data. On the post authentication the voter is allowed to cast his vote.

Authentication Accessing Servers 3:

The third authentication server is the location accessing server. Each and every voter should be authenticated with the tagged server called the location server in which the location of the voter is present. The exact location of the voter is shared from the voting device of the particular user. Through this location shared from the voter's data that is shared is matched with the existing data that is present in the location sharing database. On the successful matching the voter is allowed to cast his vote.

Authentication Accessing Servers 4:

The final authentication is done from the server side with respect to the other miscellaneous data that is provided by the user. Those data which is being taken out is given for the cross verification with the data sharing server and through that all the verifying data of the user is taken into consideration and that is cross verified with existing data in the data sharing server. When all the four accessing servers are provides the proper authentication which leads to the casting of e-vote by the represented voter of the constituency

3.2 Client Side Deployment:

The client side components which interacts with the whole component side of the client interaction. The client is the person who takes on the system for the e-casting of their respective votes. The Client side server which acts the client end for the respective client to cast their vote. In the client end, the device which is taken for the casting of the vote is taken into consideration, In this sector. The sectored e-voting device is authenticated by the various authentication process for the successful casting of the data authentication protocol.

The client side component is connected to a temporary database and centralized server. The temporary database which holds the data which consist of the data consistency which receives the user data from the various type of the voting devices and is stored in the temporary database where the temporary database is connected to the routing protocol which has established its manipulated connection with the centralized database.

The centralized server which has its internal and active connection with the cloud server through makes an efficient way to make the data which is being generated from the client side device.

A commendable e-voting framework must perform the vast majority of these undertakings while consenting to an arrangement of benchmarks built up by administrative bodies, and should likewise be able to bargain effectively with solid prerequisites related with security, precision, respectability, quickness, protection, auditability, availability, cost-adequacy, adaptability and environmental supportability.

Electronic voting innovation can incorporate punched cards, optical output voting frameworks and specific voting booths (counting independent direct-recording electronic voting frameworks, or DRE). It can likewise include transmission of tickets and votes by means of phones, private PC systems, or the Internet.

3.3 Security Implementation

By using the XEX tweakable block cipher concept[1] the two keyed permutation [2]over $M=\{0,1\}^n$, $E:K_1 x\ M \rightarrow M$ and $G: K_2 x\ M \rightarrow M$. Two keys $K_1 \in K_1$ and $K_2 \in K_2$ can be dependent or independent. Specifically, we consider tweak consisting of two parts,

$I \in M$ and $j \in J$ $((i,j) \in T = M \times J)$

The encryption is written as:

$T \leftarrow f(j, GK2(I))$
$PP \leftarrow P \oplus T$
$CC \leftarrow EK1(PP)$
$C \leftarrow CC \oplus T$

Key Scope: Data encrypted by a particular key, divided into equal-sized data units. The key scope is identified by three non-negative integers: tweak value corresponding to the first data unit, the data unit size, and the length of the data

Tweak Value: The bit value used to represent the logical position of the data being encrypted or decrypted with XTS-AES.

Audit-without-downloading: To allow TPA (or other clients with the help of TPA) to verify the correctness of cloud data on demand without retrieving a copy of whole data or introducing additional on-line burden to the cloud users

3.3.1 Verification-correctness: To ensure there exists no cheating CSP that can pass the audit from TPA without indeed storing users' data intact

3.3.2 Privacy-preserving: To ensure that there exists no way for TPA to derive users' data from the information collected during the auditing process

3.3.3 High-performance: To allow TPA to perform auditing with minimum overheads in storage, communication and computation, to support statistical audit sampling and optimized audit schedule with a long enough period of time.

Here it provides the information for the client to know how the security is provided to the user data which is retrieved from the cloud storage and those data how it is transmitted to the client as per the request which is forwarded by the client. The XTS-AES algorithm gives the basic definition for the encryption and decryption of the data from the Cloud Storage to the Client Module. The first main advantage in this paper is the client burden is reduced to half on the basis of client do not have to provide the security manually and physically to the possessed data. Second is data security that defines that the data are encrypted with the SSL format through which there would be secure transformation of the data, the Key is also optimized on this proposed method that through which the key length used for the encryption and decryption will be less.

IV. ALGORITHMIC VIEW OF THE PROPOSED SYSTEM

Server Side View

Input: User = U
Input Software =S
Verification Database = DB
User Credentials (Aadhaar Card =a, Fingerprint Authentication=b, Location=c, and Data=D)
Output: Successful Authentication
{Access Permission =Y}
{Access Denied = X}

Start S,
Input I= (a, b, c, d) →S
Where S sends the I to Z
If I→Z
Then check the Data → DB
Return (Access Permission) =Y

Else
Check the Nearest Value N→DB
If N→DB
Then
Return (Access Permission) =Y
Else
Return to Step 2 for Re-Verification
If I≠Z
Return (Access Denied) =X
Stop

Client Side View

Input: Voting Device =V
Encryption = E
Temp DB = TDB
Key = Key 1→A
Key 2→B
Key Distribution Center = KDC
Cloud Server= CS
Routing Server=RS
Centralized Voting Server=CVS

Output: Secure Casting and Storing the Vote

Start V
User After Success Verification from Server Side obtains the Y
Enter Y→V
then
Cast the Vote V(x) →V
Encryption
V(x) →Enc (key a, key b)
send
Key (a, b) → KDC (kdc (a), kdc (b))
Casted Vote
V(x) → TDB1
TDB1(V(x)) →RS
RS(V(x) →CVS
CVS(V(x)) →CS

The Counting of Vote is retrieved by the counting system which takes the two keys from the Key Distribution center and verifies it for the proper authentication and then the decryption is happen for the vote counting.

V. CONCLUSION

This paper solves the efficient framework based system for the e-voting protocol procedure. E-Voting framework is one of the developing method for innovation for competitors making their supportable choice for the possibility for they to be chosen. The entire framework is partitioned into two fundamental area with one on the customer side correspondence and another on server side correspondence. The entire framework which involves Mobile Devices as the Voting Devices are associated with their separate servers. For the benevolent validation a one of a kind confirmation convention called Single Token Authentication Protocol (STAP) is being made with the particular tokens through which the client is given a likely shot for the voting once. Once the Vote is being threw for the bolstered ones the session token terminates. Singular design which involves the customer and server activities is exhibited for the straightforwardness being used of the general execution. The test yield which involves all the individual consequences of the proposed design.

REFERENCES

[1]. Mavridis I., Pangalos G., "Security Issues in Mobile computing Paradigm". 1997, http://www.researchgate.net.
[2]. Erik Olson and Woojin Yu, "Encryption for Mobile computing", 2000.
[3]. Wendy Chou, "Elliptic Curve Cryptography and Its applications to Mobile Devices,2000.
[4]. Limor Elbaz, "Using Public Key Cryptography in Mobile Phones", White Paper,Discretix Technologies Ltd., Advancedsecuritysolutions for constrained environments, October 2002.
[5]. Dharma P. Agrawal et al., "Secure Mobile Computing", S.R. Das, S.K. Das (Eds.): IWDC 2003, Springer-Verlag., LNCS2918,pp.265-278.
[6]. WHanping Lufei and Weisong Shi, "An Adaptive Encryption Protocol in Mobile Computing", Wireless/Mobile NetworkSecurity,Springer, 2006.
[7]. WWWWAbhishek Kumar Gupta, "Challenges of Mobile computing", Proceedings of 2nd National Conference on Challenges&Opportunities in Information Technology RIMT – IET, Mandi Gobindgarth, March 29, 2008.
[8]. S. Krishna Mohan Rao and Dr. A Venugopal Reddy, "Data Dissemination in Mobile Computing Environment", BIJIT–BVICAM's International Journal of Information Technology, Bharati Vidyapeeth's Institute of Computer applications and Management (BVICAM),New Delhi, Vol. 1, No. 1, January 2009.
[9]. M. Razvi Doomun, and KMS Soyjaudah, "Analytical Comparison of Cryptographic Techniques for Resource-Constrained WirelessSecurity", International Journal of Network Security, Vol.9, No.1, July 2009, pp. 82–94.
[10]. Jayaprakash Kar & Banshidhar Majhi, "An Efficient Password Security of Multi-Party key exchange protocol based on ECDLP",International Journal of Computer Science and Security (IJCSS), Vol.1, Issue 5, Sep. 2009.
[11]. Mooseeop Kim et.al., "Design of Cryptographic Hardware Architecture for Mobile Computing", Journal of Information Processing Systems, Vol. 5, No. 4, Dec. 2009.
[12]. Bruno P.S. Rocha et. al., "Adaptive Security protocol selection for mobile computing", Journal of Network and Computer Applications 33,2010, pp. 569.

[13]. Sathish Alampalayam Kumar, "Classification and Review of Security Schemes in Mobile Computing", Wireless Sensor Network, June 2010, 2, pp.419-440.
[14]. Sameer Hasan Al-Bakri, Gazi Mahabubul Alam et. al., "Securing peer-to-peer mobile communications using public key cryptography:New security strategy", International Journal of the Physical Sciences Vol. 6(4), Feb. 2011, pp. 930-938.
[15]. Rahat Afreen and S.C. Mehrotra, "A Review on Elliptic Curve Cryptography for Embedded Systems", International Journal of ComputerScience & Information Technology Vol. 3, No 3, June 2011
[16]. Helena Rifa-Pous and Jordi Herrera-Joancomarti, "Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices", Future Internet 2011, 3, 31-48; doi: 10.3390/fi3010031, ISSN 1999-5903, www.mdpi.com/ journal/futureinternet.
[17]. Jagdish Bhatta and Lok Prakash Pandey, "Performance Evaluation of RSA Variants and Elliptic Curve Cryptography on HandheldDevices", IJCSNS International Journal of Computer Science and Network Security, Vol. 11, No. 11, Nov. 2011.
[18]. K. Sathish Kumar et. al., "An Experimental Study on Energy Consumption of Cryptographic Algorithms for Mobile Hand-Held Devices",International Journal of Computer Applications, Vol. 40, No.1, Feb. 2012. 19. Masoud Nosrati et. al., "Mobile and Operating Systems", Computing: Principles, Devices World Applied Programming, Vol. 2, Issue 7,July 2012.
[19]. Ravinder Singh Mann et al., "A Comparative Evaluation of Cryptographic Algorithms", Int. J. Computer Technology & Applications, Vol3(5), Oct. 2012, pp. 1653-1657.
[20]. Giripunje et al., International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 5, May 2013,pp. 704-713.
[21]. Ameya Nayak, "Android Mobile Platform Security and Malware Survey", IJRET: International Journal of Research in Engineering and Technology, Vol. 02 Issue 11, Nov. 2013.

Bimal Kumar " A Security Implementation for Thearchitectural Approach on E-Voting System" International Journal of Engineering Research and Applications (IJERA), Vol. 09, No.04, 2019, pp. 74-79