Secure Online Election System

Sneha Subramanian, Saketh Kamatham

Abstract: India, the biggest democratic ruling system in terms of population utilises the Electronic Voting Machine or EVM for their general elections. Any EVM comprises of two units: The Control unit and the Ballot unit. Ongoing research has indicated many disadvantages in the system. One of the main disadvantages we encounter is that many researchers have claimed that the EVM can easily be tampered with. EVMs also encounter many physical threats. To prevent these drawbacks, we have proposed an online voting system which has counter many physical difficulties faced by the EVM. One main difficulty in the online system is the SQL Injection attack. SQL injection is messing with the database and controlling it with the help of SQL Queries. Our project focuses on the Tautology based SQL Injection attack. In this attack, a statement whose value will always be true or 1 is passed instead of username and password by the hacker. This allows access to the database which allows him/her to manipulate it. Manipulation can be of several kinds. Web based Voting is another innovation that is rising which has the possibility of countering numerous downsides looked by the EVMs. The online voting application works as any other web application. Each voter who wants to vote needs to fill all the required details and create an account on the website first. On the day of voting, when voters cast their vote, they need to sign in with their respective credentials. When the credentials match with the data from database, the voter can get to the voting page after effectively making the choice. The votes cast by the voters are sent to a separate database which is viewed in the administration side. We use stored procedures and parameterized queries to prevent the Tautology based SQL attack. If a malicious user enters any query which has a value, it will simply be passed as a parameter to the SQL statement and wont be a component of the SQL statement itself, thus rendering the stored procedure invulnerable to SQL injection attacks. We also use the Secure Hash Algorithm 256 (SHA-256). It is a type of cryptographic hash function which generates a unique 256 bit long hash key for each vote. It is a one way function and so it cannot be decrypted. This ensures that the votes are not manipulated.

I. INTRODUCTION

India is a majority rule republic nation. Hence, the way of choosing the leaders is an unquestionable requirement. India has been dependent on a reasonable, alter free and secure framework to pick its leaders. One of the primary methods of election that has been utilised in the past was the paper tally framework which had various security issues. The Election Commission of India has been utilising the EVMs (Electronic casting a ballot machines) in India for making its leader decisions since 1979 and has tackled the vast majority of the issues which emerged in the paper poll concept. The EVMs have a controller that once fabricated cannot be changed. The fundamental prerequisite is straight forwardness of the election procedure and furthermore that the procedure must be reasonable and just. The current electoral frameworks utilised in India are exceptionally viable yet certain questions arise. The proposed framework utilises advanced security infrastructure and software engineering concepts to beat challenges that emerge in the present and past frameworks.

![Fig 1: General Architecture of an Electronic Voting Machine](image)

II. PRESENT SYSTEM

In the course of recent years, different examinations have been completed with respect to the use of present day mechanism and to improve the possibilities of decisions. These examinations have pointed out different difficulties in the utilisation of the electronic castings of ballot machines making it a risk to the whole procedure of decision. An electronic casting of ballot machine is an independent machine with no association with any system which helps in assurance from control or risk. The machine mainly keeps running on batteries. It essentially has two units which are The Control unit and the Ballot unit. The Ballot Unit is used by the public to put in their votes and the Control unit is the fundamental brain of the framework which controls the whole process and stores the results also. The program which is used to run the decision framework is designed to run on a One Time Programmable smaller scale controller. When the vote is sent in the tally unit, it is safely transmitted to the control unit. Numerous researches with respect to the security of Electronic Voting have been directed and One main problem regarding this is that it does not address the privacy concerns during the election process. EVMs help in

Revised Manuscript Received on September 22, 2019

Sneha Subramanian, Computer Science, SRM Institute of Science and Technology, snehasbramanian_v@srmuniv.edu.in
Saketh Kamatham, Computer Science, SRM Institute of Science and Technology, kamathamsaketh_k@srmuniv.edu.in
maintaining the secrecy on the votes which is very essential for a totally unbiased election.

III. INDIA AND ELECTRONIC VOTING MACHINE

India is as of now the world's biggest vote based system with a total population of 1.34 billion making it the second most crowded nation on the planet. According to Statistics, before the use of electronic casting ballot machine, around 8,000 tons of paper was necessary for the general elections. Electronic casting ballot machines have supplanted the recently followed paper poll method in all types of elections since 1979. There were claims that emerged expressing that the currently used EVMs are alter capable which jeopardises the whole election process.

IV. DRAWBACKS OF THE ELECTRONIC VOTING MACHINE

The present methods of election in India uses EVMs for the voters to make their choice. As of late, use the EVMs has demonstrated that they are defenseless against a few sorts of noxious programming and assaults. This has helped the programmers control the vote check effectively. No check or confirmation of the EVMs is done before they are put into use amid elections. So regardless of whether somebody attempts to mess with its equipment or programming aspects before elections, it stays undetected and unchecked. For instance, according to a research, it is found how a little micro controller can be used to control the EVMs and change the outcomes as wanted. If infections and different noxious programming are put together then, in addition to the fact that it can manipulate the vote tally, it can also lead to loss of information. Another real disadvantage is physical harm to the machine. Different programming harm strategies executed are through infections and hacking. The back end can produce fake votes and they can’t be differentiated by the EVMs. SQL Injection is another serious issue we need to keep in check. It alludes to assaulting the database of the applications and succeeding to alter the database by using some SQL queries that can control the information. Climate also plays a role in working of the EVMs. They don’t work appropriately in regions which have high precipitation. This can make an issue in the equipment. The EVMs are defenseless against two conceivable components of hacking: The EVMs comprise of two EEPROMs. It is anything but difficult to peruse from it and control the information. A chip with Trojan is embedded into the EVMs which can change the outcomes and produce desired once. Through the EVMs a voter can never count if his/her vote is correct or not. A few nations have rejected EVMs since they are anything but difficult to alter, hard to verify and put the fairness of elections at risk.

V. RELATED WORKS

We have surveyed some of the literature papers as well as research papers through which we under-stood the issues and the counter mechanisms that could be used and we wish to apply these concepts in Secure Online Election Systems.

- Challenges the current Election Voting system by inspecting various flaws and their counter measures. To avoid tampering of votes they have used JBC control unit and DAU. It works without any fault with the correct configuration of JBC and eSlate with sufficient power supply.
- A system which is verified on both ends is used to check where voters can confirm that their votes were properly cast and noted into the election result system and also constructs a secured communication path without any third party involvement. It uses several encryption techniques without the need for an initial setup. It provides a broader picture on the complete process.
- It explains the use of a node(Selfish) for detecting intrusion in any mobile ad hoc network. It makes use of MANET technology for creating a secured election platform and avoids any intrusion. It works efficiently with any ad hoc networks and mobile networks with increases security. It provides very secure platform to carry out voting and due to this Confidentiality is retained.
- Uses various Block chain techniques and block chain-enabled e-voting (BEV) for efficient voting process. It uses various Block chains applications. Block chain is a very secure technique with high security and integrity. Only voters themselves know the information of their votes, and all ballots in the ballot box have no connection with their voters. Transparency is attained due to the transparency of block chain and the whole procedure is open to the public. Blind signature is used to preserve voter’s choices during the election.
- This paper identifies the vulnerabilities and security threats that might arise in any e-voting system. Careful analysis of all the e-voting system identifies threats like SQL injection, Malware insertion, DOS attacks etc. Each of these attacks have countermeasures to prevent the loss of data and integrity and they have been discussed.
- This paper analyses the use of various Cryptography techniques in electron-voting systems. Cryptography is a very productive way to build a very secured election system by establishing a communicational channeled transfer of the voting details. This system eliminates problem related to the secrecy of the ballot, integrity and privacy. For this purpose, Prêt à Voter is used. It is a paper ballot online voting system. There is no need for anonymous channels to secure the votes with the use of this system, and security is also provided.

VI. PROPOSED SYSTEM

The Online voting system is a kind of e-voting technique. The online voting is an electronic way of choosing the leader. This works like any other web application. In this system, every voter becomes a user. The voters cast their vote through computers. The user has to create an account on the official website and get his/her official documents verified and only then he/she can cast a vote.
The voter has to enter the One Time Password (OTP) to access the page to cast their votes. The voter's database and information related to votes is all saved in a database which can be accessed by the Election Commission alone. The database cannot be manipulated. The database which contains all the details of all the voters is secured using SHA 256 algorithm. SQL Injection is prevented by using stored procedures. Authenticity and integrity of the voters and their votes is maintained. To maintain data confidentiality while voting, Trusted Third Party can be used. TTP acts as a medium between the voter and the Election Commission to authenticate the voter to vote during elections. Without TTP, it is difficult to incorporate security and data confidentiality. During elections, the commission should not give out or expose the voter details to parties and should determine voter validity. The Election Commission should ensure that each voter gets to cast his vote only once and does not misuse it. We use the concept of multi chain to limit the number of votes that can be cast by a user to 1. This way fake vote cannot be generated and even if a user tries to generate fake votes then it won't be accepted. An other advantage of using the computers is that they are very accessible even in the most remote areas.

Fig 2 : During Voting Process

VII. SQL INJECTION AND HOW TO PREVENT IT

SQL Injection is a type of database attack which is a combination of database and web vulnerability. In this attack, the attacker uses SQL queries which may seem real and relevant to the user and might end up filling all the details. This way the hacker is able to access all relevant information. This way the hacker is able to gain control over the web application server. The kind of attack used is here is called Tautology based SQL Injection Attack. The code is programmed in such a way that the value of this statement will always be true. The statement used here is 'OR'=' (This statement will always be true.) The purpose of this attack is to access authentication pages and extract data from the database. The query used to access the database from the admin side is:(username) ' UNION ( SELECT table_name, table_schema,'a','b FROM information_schema.tables) When this query is injected, a condition converts this into a tautology. With this condition the query is true for each and every row and returns them all. This way the hacker is able to use INSERT and DELETE statements to manipulate the data and votes. There are several ways to prevent SQL injection attack. Stored procedures are smaller programs used in the main code stored in the database. Using stored procedures allow fast execution and modular programming. These stored procedures always return value 0 by default. They are created using inner join between two tables. NO COUNT ON and NO COUNT OFF are used in stored procedures. When the queries are not parameterised it becomes vulnerable to SQL Injection. We use parameterised queries and a stored procedure called sp_executesql to generate dynamically generated statements. Parameterised queries work this way:

- SQL Query is first sent.
- The database inserts username and password as values. These are stored with parameters.
- Let us enter the statement 'OR''='. Since the database knows the action of this query, if it tries to manipulate the database then the database doesn't get affected as the value of the statement this Apart from this, input validation helps provide better security along with stored procedures and parameterised queries. Limiting the access to database can improve the security. It is necessary that the hackers do not know what kinds of errors are possible so that they do not have counter-measures to these errors. It is very necessary to keep the system updated security wise and to prevent any sort of attacks. Keeping your SQL software updated to the latest version can prevent such malicious attacks. It is important to keep the database channel encrypted and we use SHA-256 Algorithm for that.

VIII. SHA-256 ALGORITHM

Block chain technology is an emerging and has gradually spread across the globe. This has increased the cyber security. It is used to guard the information we have against any kind of fraud or data theft. Block chain technology was first implemented in the first crypto currency, Bit coin. The data being added to block chain should be real and it is verified by other member of the block chain network. Complexity of the block chains increase when the size of block chain networks are bigger. The most popular algorithm used is SHA 256 which stands for Secured Hash Algorithm 256. It generates an almost unique 32 byte signature for a particular text. The algorithm is a one way encryption technique which means once the text is encrypted it cannot be decrypted again and it also has a fixed size. One iteration or cycle of SHA 256 is given by:
IX. IMPLEMENTATION

For the proper implementation of this project, we need a database which comprises of various details of all the registered voters. This database is created when all the voters register themselves on the website. The entire project consists of three modules. They are : 1) The User Module 2) The Admin Module 3) SQLi attack and prevention. Firstly, before the beginning of the entire election process, people who are eligible to vote must register themselves on the website in the new user. These details are stored in the database and by this, the user knows his/her log in credentials for voting. The new user section taken in details like name, voter ID, address, email id and phone number. Secondly, the voting page is open only on the day of voting. The user logs in into the application in the user section and is directed to the voting page. Here, his/her name is displayed which is to be confirmed by the user. Different parties participation in the election are also displayed. The user must choose their choice for the leader and click on confirm vote button. Once the vote is cast the user is automatically logged out of the voting page and an email conformation is sent to his registered email ID regarding the successful casting of their vote.

The Vote transmission channel is encrypted using the Secure Hash Algorithm 256 where, for the vote cast, a hash code is generated and it can be used during validation of vote if required. The Admin module has only a single login authority. The administrator has access to the entire voter details, status of all the voters i.e whether they have cast their vote or not, party wise voter details etc. One of the main limitations that presents itself in this project is the SQL Injection attack. SQL Injection (SQLi) is a type of injection attack enabling nefarious SQL statements to be performed. These statements control a web app SQL database. Attackers might use flaws of Malware to bypass security measures for programs. They could go about validating and approving a web page web service and regain the entire SQL material .we can use stored procedures to prevent this attack. In this project. The kind of attack used is called Tautology based SQL Injection Attack. The code is programmed in such a way that the value of the statement will always be true. The statement used here is ‘OR’ = '. The purpose of this attack is to access authentication pages and extract data from the database. The query used to access the database from the admin side is: (username); UNION (SELECT table name, table schema,a; b; FROM information schema.tables)

When this query is injected, a condition converts this into a tautology. With this condition the query is true for each and every row and returns them all. This way the hacker is able to use INSERT and DELETE statements to manipulate the data and votes. When the queries are not parameterised it becomes vulnerable to SQL Injection. Examples of non parameterized query sare: MySql Connection connection = new MySql Connection (connection String) My Sql Connection connection = new MySql Connection( connectionString); My Sql Command command = connection.CreateCommand(); command.CommandText = t; SELECT *FROM tablewhere name = ; : table Name.

For the prevention of this attack, Stored procedures are used. A stored procedure is a piece of code that is compiled and can be accessed from SQL statements . In the procedure, the servers belonging to the SQL Database run the code and returns results to the application which has called it. For several reasons, the use of stored procedures is beneficial. A stored procedure provides a significant security layer between the database and the user interface. It endorses security by controlling data access, as end users may enter or change data, but do not write procedures. Data integrity is maintained by a stored procedure because information is entered regularly. It improves efficiency as statements must only be written once in a stored procedure.
The proposed system helps in overcoming the various problems that exist in the Electronic Voting Machine and helps in keeping the voting process secure and integrated. The proposed system does not allow external hacking of database and helps keep the leader selection process fair and just.
REFERENCES


7) Noman Mohammed ; Hadi Otrok ; Lingyu Wang ; Mourad Debbabi ; Prabir Bhattacharya; “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET”; https://ieeexplore.ieee.org/document/5089330[5].