ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Issues & Vulnerabilities Related to Online Voting and Its Mitigation

Mohammad Daud
Department of Computer Science & Engineering
Jamia Hamdard
New Delhi, India

Ihtiram Raza Khan
Department of Computer Science & Engineering
Jamia Hamdard
New Delhi, India

Abstract: Majority share of the traditional voting systems have been utilized throughout the years in races. Each of these strategies had orderly inadequacies. The current customary voting frameworks have been subjected to gross manhandle and abnormalities. Electronic voting which is rising as a contrasting option to these traditional voting frameworks, however exceedingly encouraging is not free of blemishes; remote web voting frameworks still experience the ill effects of numerous security issues which depend on the customers, the servers, and the system associations. Denial of service attack and Sybil attack still have a place with the most difficult security issues. In this paper we talk about the security issues related with remote web voting. Moreover we examine how Sybil assault can be utilized as a part of character and certifications burglary. Specifically, we look at the plausibility of running national races over the Internet. The concentrate of this paper is on the impediments of the current conveyed framework as far as the security of the hosts and the Internet itself. We infer that without fitting safety efforts, web based races can be a test.

Keywords: Sybil attack, DDOS attack, online voting.

I. INTRODUCTION

Decisions and voting are central to any agreement based society. These are the most basic elements of vote based system. Not exclusively do they accommodate the systematic exchange of energy, yet they additionally bond subjects' trust and trust in government when they work not surprisingly. Actually, the uprightness of the race procedure is essential to the trustworthiness of majority rules system itself. The race framework must be adequately strong to withstand an assortment of fake practices and should be adequately straightforward and fathomable that voters and hopefuls can acknowledge the consequences of a race.

Web has developed exponentially in the previous decade. The Internet has changed the desires of the natives around the speed and accommodation with which all taxpayer supported organizations and races ought to be conveyed. Web is being utilized for shopping, managing an account, keeping up our social and expert systems, and discovering answers to our inquiries. Each resident has voting as its crucial and the heart of each vote based system is voting. It is fundamental that the natives have confide in the voting framework. This trust is worked by giving them the certainty that each vote that they cast is being recorded covertly and furthermore is being numbered under incomparable precision and with no favoritism. The main motivation behind a race is not naming the victor, but rather likewise persuading the washouts that they have lost.

Web based voting enhances the involvement in voting by empowering a man to vote in secure way over the Internet. In an internet voting every one of the a voter needs is a PC, an electronic card peruser, their ID card and its PIN, and they can vote from anyplace on the planet. That makes voting a dauntless of savagery and that expands the rate of voting.

Web based voting enhances the involvement in voting by empowering a man to vote in secure way over the Internet. Internet voting is a future stride in the advancement of customary voting framework. A voter may confront disagreeable conditions while making choice in customary framework, for example, sick wellbeing, inaccessibility of the client, climate conditions, car influx, and so on. In another circumstance, it can happen that the voter does not have enough time to go to the surveying station to make his choice.

A. Problem Background

In the current years there are numerous writing on internet voting has been created. While internet voting has been a dynamic range of research in the current years, endeavors to grow true arrangements have recently started representing a few new difficulties.

The utilization of shaky Internet, all around archived instances of inaccurate executions and the subsequent security breaches have been accounted for as of late such as identity theft, impersonation etc. These difficulties and concerns must be settled with a specific end goal to make open trust in web based voting.

The potential advantages and dangers of Internet voting are talked about as far as seven of the center popularity based standards that shape current appointive frameworks: openness, measure up to voting power, mystery, security, review capacity ,straight forwardness ,furthermore, effortlessness. Identity theft and impersonation crimes can be occur in an online voting system. These kind of things happens in various places in the world.

B. Problem Statement

Online Voting are straightforward, alluring and simplicity to utilize. It diminishes manual endeavors and main part of data can be dealt with effectively. Be that as it may, out of every one of these elements there are a few downsides with this framework are, there can be programming disappointment issue, unreliable access of web, . Refusal of administration assaults and Sybil assault still have a place with the most difficult security issues. In addition additionally voter ought to be comfortable with web.

C. Research Objective

The primary target of this review to show how assaults like DOS, Sybil can influence the internet voting and is to show how a character can be robbery in a web based voting. Along these lines Framework ought to be completely computerized. Framework ought to give solid security highlights like making clients and allocating benefits to clients of the framework. Framework ought to be able to monitor all the point by point portrayals of the customer and the entire subtle elements of administrations offered by the customer association. Different yields (reports) ought to be accessible online at whatever time. Framework ought to have the capacity to deal with to a great degree extensive volumes of information (i.e. extensive database bolster). A safe internet voting framework where one individual can vote utilizing numerous online personalities. Eminently, this issue is right now just settled if a focal specialist, for example, the overseer of an authentication expert, can ensure that every individual has a solitary personality spoken to by one key; by and by, this is extremely hard to guarantee on a substantial scale and would require exorbitant manual consideration.

D. Scope Of Study

The scope of the study is that it will help to make a secure online voting system like an organization can develop a secure system in which voters or users get their ID along with the password. And details these credentials of the voters are saved i database of an organization. And this will act as a secure voting system, and it will help to increase the internet knowledge among the electorate. With this we can develop an advance security voting system by knowing issues and vulnerabilities of an online system. Organization can do following things:

- **E-Mails**: Organization can send the error report to an individual voter specially those who have provided wrong information.
- **E-SMS**: those voters or users which do not have an internet connections then an authority can send them SMS for verification by using two way authentication method..

It will also help to take steps to avoid the attacks (DOS,SYBIL).

This research paper also help to make online voting system more secure as we will discuss about the vulnerabilities and by remove such kind of vulnerabilities we can make online voting system:

Accessibility – With the widespread increase in the use of internet, online voting allows voters to access ballots from anywhere at any time and thus serves as an option of convenience.

Cost effectiveness – When considering costs of production involved to print, post, and mail ballots in DRE systems, Online elections are cost effective.

Security and confidentiality – If an Online voting system is properly designed with safeguards in place to assure ballot secrecy and also hides voter identity, then it can prove to be a secure system. [6]

Transparency – The chances of fraud and mismanagement of elections are eliminated if a third party runs the online election system.

Accuracy and expedience – The case of rejected, mismarked, or invalid votes are eliminated in online voting since it utilizes electronic ballots. Also, the need of manual tabulation of result is eliminated as results are automatically calculated. [4]

No Impersonation: By saving the system from attacks (Sybil, DOS) there will be less chances of impersonation in an online voting.

Moreover, unknown voting in light of mixnets can be investigated and ought to be scanned for speedier plans than homomorphic expansion as they require more encryption and decoding.

II. LITERATURE REVIEW

Just a couple of nations have tried different things with web based voting in favor of national-level decisions, web based voting is being attempted in various parts of the world as an option methods for voting in favor of the individuals who can't go to the surveying stations upon the arrival of Elections. As indicated by Trechsel and Vassil (Trechsel A. et al, 2011) Estonia credited to be a pioneer in e-administration and e-popular government and thought to be the primary nation which masterminded countrywide e-voting in 2005, 2007 and 2009.

As indicated by the examination by Nicole J. (Goodman N., 2014), in Canada more than two million chances to vote remotely were given in more than 90 nearby races of Canada.

As indicated by Michel (Chevallier M., 2009), in Switzerland the principal government ticket directed online was on September 2004. As indicated by Kristian (Gjosteen, K., 2013) web remote voting was controlled by the Norwegian government amid the 2011 nearby government decisions and a moment trial of remote voting was keep running amid the 2013 parliamentary races.

As per William J. (Kelleher W., 2013) there has been a plenitude of research and littler trials of web based voting in the USA. [1]

India presently can't seem to witness the broadband unrest, however Internet will keep on being utilized as a device that wrecks limits and democratizes the subject investment. Gujarat is the primary state in the nation to utilize Online voting utilizing innovation given by a Spain based firm named Scytl, that has as of late begun India operations. The main trial was completed in September 2010 and afterward utilized again in city races held in April 2011. The principle favorable circumstances of the Gujarat e-voting framework is the way that votes were non-traceable and genuineness of the voters being entrenched.

III. MAIN VULNARABILITIES OF ONLINE VOTING

Web based voting frameworks are helpless against assault at three noteworthy focuses:

- the server
- the customer, and
- the correspondences foundation.

Infiltration assaults focus on the customer or server straightforwardly while disavowal of administration (DOS) assaults target and interfere with the correspondences interface between the two. Each objective and assault are talked about unequivocally in the accompanying subsections.

A. The Client and Server (Voting Platform)

Entrance assaults include the utilization of a conveyance instrument to transport a vindictive payload to the objective host as a Trojan stallion or remote control program. Once executed, it can keep an eye on tickets, keep voters from throwing polls, or, much more dreadful, adjust the tally as indicated by its directions. What makes the last risk especially tricky is that it can be refined without recognition, and such security instruments as encryption and verification (e.g., secure attachment layer (SSL) and secure hypertext transport convention (https)) are inept against this sort of assault in that its objective is beneath the level of deliberation at which those security conventions work (e.g., the working framework or program). Infection and interruption location programming is likewise liable to be frail against this danger since discovery components by and large search for known marks of pernicious projects or different indications of unapproved action. These stealth assaults for the most part radiate from obscure or adjusted projects, and modify framework documents to adequately "approve" the progressions made (after which they may incapacitate assist infection insurance). The assaults could begin from anyplace on the planet.

B. The Communications Path

The interchanges way alludes to the way between the voting customer (the gadgets where the voter votes) and the server (where votes are counted). For remote voting, this way should be "trusted" (secure) all through the period amid which votes are transmitted. This requires both a verified interchanges interface amongst customer and server, and also the encryption of the information being transported to save privacy. When all is said in done, current cryptographic advances, for example, open key framework, are adequate for this last reason, expecting the measures required to run such innovations are met. Keeping up a validated interchanges linkage, be that as it may can't be ensured.

Maybe the most noteworthy risk in such manner is a disavowal of administration (DOS) assault, which includes the utilization of at least one PCs to intrude on interchanges between a customer and a server by flooding the objective with more demands that it can deal with. This activity successfully keeps the objective machine from conveying until such time as the assault stops. A refinement of this procedure is alluded to as conveyed refusal of administration (DDOS) in which programming programs called daemons are introduced on numerous PCs without the learning or assent of their proprietors (using any of the conveyance components referenced above), and used to execute an assault. In this way, an aggressor can get to the data transmission of numerous PCs to surge and overpower the expected target.

IV. AUXILLARY INTERNET VOTING VULNERABILITIES

Auxiliary web voting vulnerabilities are fundamentally through:

- Social building
- Digital partition

A. Social Engineering

In regard of decision and voting, social designing is the term used to portray assaults that include misleading voters into bargaining their security. Writing review in sociologies and humanities demonstrates that numerous voters don't take after straightforward headings. It is astonishing to discover that, for instance, when taught to circle a competitor's name, voters will regularly underline it. While PCs would appear to offer the chance to give an interface that is firmly controlled and along these lines less subject to blunder, this is counter to the run of the mill encounter most clients have with PCs. For non-PC researchers, PCs are regularly scary and new. UIs are frequently poor and make perplexity, as opposed to streamlining forms.

A remote voting plan will have some interface. The genuine outline of that interface is not the subject of this paper, but rather unmistakably there will be some interface. For the framework to be secure , there must be some path for voters to realize that they are speaking with the decision server. The foundation exists at this moment for PC security experts, who are suspicious that they could speak with a fraud, to confirm that their program is speaking with a substantial decision server. The SSL convention and server side endorsements can be utilized for this. While this procedure has its own particular dangers and pitfalls, regardless of the possibility that it is thought to be perfect, it is nonsensical to accept that normal web clients who need to vote on their PCs can be relied upon to comprehend the idea of a server authentication, to confirm the credibility of the endorsement, and to check the dynamic figure suites to guarantee that solid encryption is utilized. Actually, most clients would likely not recognize a page from a SSL association with the authentic server and a non-SSL page from a pernicious server that had precisely the same as the genuine page.[2]

There are a few ways that an aggressor could parody the genuine voting site. One way is send an email message to a client advising that client to tap on a connection, which would then raise the fake voting site. The enemy could then gather the client's certifications and as it were, take the vote. An assailant could likewise set up an association with the true blue server and bolster the client a fake site page, and go about as a man in the center, exchanging data between the client and the web server, with the majority of the movement under the aggressor's control. This is sufficiently likely to change a client's vote, paying little heed to how the application is executed.

A more genuine assault is conceivable by focusing on the Internet's Domain Name Service (DNS). The DNS is utilized to keep up a mapping from IP addresses, which PCs use to reference each other to area names, which individuals use to reference PCs. The DNS is known to be helpless against assaults, for example, store harming, which change the data accessible to has about the IP locations of PCs.

B. Computerized Partition

Remote Internet voting brings along the potential for a "computerized isolate", which can happen in two ways. There is a computerized separate between the individuals who have home PCs with Internet associations and the individuals who don't. Second, there might be a computerized partition between the individuals who have quicker get to and the individuals who have slower associations and thus bring down quality get to. Individuals with higher salaries will probably have the capacity to bear the cost of get to. Besides, get to is frequently more affordable and of higher quality in urban regions. Those with lower livelihoods and who live in rustic regions are off guard. In the western world where alter safe gadgets, for example, shrewd cards are utilized for validation, cryptographic keys can be produced and put away on these gadgets, and they can perform calculations, with the end goal that appropriate qualifications can be traded between a customer and a voting server. There are a few confinements to the utility of such gadgets. The first is that there is not a sent construct of keen card perusers in light of people groups' PCs. Any framework that includes budgetary speculation with respect to people keeping in mind the end goal to vote is unsuitable. A few people are more restricted in their capacity to spend, and it is uncalled for to diminish the probability that such individuals vote. It would, as a result, be a survey assess. This issue is additionally alluded to as advanced gap.[5]

In this manner, the expansion of Internet voting can possibly make partitions regarding numerous financial factors, in particular wage, instruction, sex, geology and race and ethnicity. These potential partitions could be hazardous for investment and portrayal.

V. SYBIL ATTACK ON INTERNET VOTING

The Sybil assault in computer security is an attack wherein a notoriety framework is subverted by fashioning characters in distributed systems. The Sybil assault has showed up in many structures in both scholarly work and in this present reality. It is an extreme and unavoidable issue in numerous ranges. For instance, it is conceivable to apparatus Internet surveys by utilizing different IP locations to submit votes, to pick up favorable position in any aftereffects of a junk letter, and is a notable and possibly significant issue in true decisions. A Sybil assault is additionally utilized by organizations that increment the Google PageRank rating of the pages of their clients, and has been utilized to connection specific look terms to sudden outcomes for political analysis. Notoriety frameworks are a typical focus for Sybil assaults counting certifiable frameworks like eBay. Spammers can utilize this assault to access different records on freeemail frameworks. Shared processing frameworks which utilize voting to check revise answers, for example, SETI@home, are likewise vulnerable to tolerating false arrangements from a Sybil aggressor. Arrange steering can be controlled at the point when a Sybil assailant seems, by all accounts, to be a wide range of portable hubs on the double. In frameworks that give obscurity between companions, for example, Tor, the Sybil assault is by and large fit for uncovering the initiator of an association and there is no guard against this assault. It additionally permits free riding in administrations in helpful record stockpiling frameworks, for example, Pastiche. Formal investigations of the assault have been done with regards to shared applications. Notwithstanding this work, there is no broad answer for the assault. Proposed arrangements most usually utilize asset testing. A wide assortment of utilizations have considered the impacts of the assault.[3]

Sybil assault involves basic significance and alarm in system security prompting many fake characters that can bring about interruption in the system. Sybil assault happens for the most part amid broadcasting and it capacities without individual check and character correlation of correspondence substances. The assailant hub can obtain numerous characters. That element in the framework can attempt to impact the Sybil assailant because of the consciousness of just others in every element by means of messages in the correspondence channel. The aggressor hubs are propelled inside and outside the course and in addition remote sensor systems. The observing hub exceptionally distinguishes the assailant hub on a unicast and in addition in a multicast situation. Here, creator proposes a validation system which can guarantee block to or moderation of security assaults on remote sensor organize.

VI. PROPOSED SOLUTIONS TO ATTACKS

We have proposed a web based voting framework with secure client confirmation by giving bio metric and watchword security to voter account, fundamentally combining mystery key with the cover picture on the premise of center picture. Approval strategies can be utilized to forestall Sybil assaults and expel disguising threatening elements. A nearby substance may acknowledge a remote character in light of a focal expert which guarantees a coordinated correspondence between a personality and an element and may even give a turn around query. A personality might be approved either specifically or in a roundabout way. In direct approval the nearby substance questions the focal specialist to approve the remote personalities. In circuitous approval the neighborhood substance depends on effectively acknowledged personalities which in turn tests for the legitimacy of the character being referred.

Authentication can also be done through SMS confirmation and two way authentication method.The most noteworthy risk in such manner is a refusal of administration (DOS) assault, which includes the utilization of at least one PCs to intrude on interchanges between a customer and a server by flooding the objective with more demands that it can deal with. This activity successfully keeps the objective machine from conveying until such time as the assault stops. A refinement of this method is alluded to as circulated disavowal of administration (DDOS) in which programming programs called daemons are introduced on numerous PCs without the learning or assent of their proprietors (using any of the conveyance systems referenced above), and used to execute an assault. In this way, an assailant can get to the data transfer capacity of numerous PCs to surge and overpower the expected target.

There are a couple of specialized measures that can be produced to halfway relieve the results of an assault - particularly in the main minutes - and some of these are very basic. For instance, you can:

- rate restrain your switch to keep your Web server being overpowered
- add channels to advise your switch to drop parcels from clear wellsprings of assault
- timeout half-open associations all the more forcefully
- drop ridiculed or malformed bundles
- set lower SYN, ICMP, and UDP surge drop limits

With individual gadgets there is dependably a probability that malignant programming is display. In the event that outlined particularly in connection to a ticket it could disturb, change or read also, impart to an outsider the voter's vote. While hostile to infection programming exists, it must be stayed up with the latest and can just secure against known issues. It is imperative here to guarantee voters know about the danger of utilizing electronic gadgets and keeping up individual information security. For instance, keeping confirmation codes mystery, not clicking suspicious connections or opening connections in unforeseen messages, what's more, properly erasing and wrecking voting data.:

There are following methods to avoid vulnerabilities:

Upgrading security with an on-request delivery model:

A Software as a Service (SaaS) based framework is, by definition, persistently refreshed as market prerequisites, security, and openness principles enhance, guaranteeing that the framework is never-endingly cutting edge. At the point when programming is keep running on obsolete innovation, security dangers are higher and item lifecycle administration staffing costs are higher. Most organizations and numerous administration associations now pick SaaS conveyance techniques for mission-basic arrangements. SaaS is the main suitable technique demonstrated to consistently expand security, dependability, and productivity, while decreasing expense.[5]

Hardware Monitoring:

All basic equipment segments ought to have robotized forms which distinguish and caution the nearness of any surprising organize activity and unapproved endeavors to get to the framework. This applies to all server, firewalls, organize switches and basic equipment segments. Suspicious movement can be signed in unchanging logs which can't be altered or changed, and triggers to ready system chairmen and IT security specialists can be designed to research at short notice.

Voter confirmation:

As talked about already, voter check gives a system for the voter to distinguish any endeavor to meddle with (control) their vote.

Uprightness checking with PBB:

This gives a component to openly demonstrate the uprightness of the race framework and to highlight any endeavor to change vote substance, erase substantial votes and include fake votes from non-qualified voters.

Blending proofs:

These numerical verifications give prove that no obstruction happened amid the basic "blending" handle and that the scrambled votes which entered the blending, are the same as those which left the blending and that no votes were erased, included or changed.

Unscrambling proofs:

These scientific confirmations give prove that no obstruction happened amid the basic decoding process and that the scrambled votes which entered the blending, are the same as those which left the decoding and that no votes were erased, included or changed.

Keeping up review trails:

The arrangement of the vital review trails and instruments are basic in the proof of the trustworthiness of any web based voting framework, which is critical to making trust in the framework.[7]

VII. CONCLUSION

The inspiration for web based voting is multi-overlay; exactness and speed of results, significantly lessened general cost and minimization of populace exchanges are the absolute most significant advantages. Up until now, because of security, innovative concerns and constraints, and in addition because of the computerized partitions, internet voting has been proposed just as an option answer for conventional race handle. Numerous web based methodologies have regularly been scrutinized for sensible and now and again demonstrated security worries because of the way that an open entomb system is constantly defenseless against programmer assaults. We have examined about how the security of web voting framework is critical and what can be the conceivable security dangers to it, disavowal of administration assaults being one of them. In spite of the fact that, there are no totally guarded procedures to oppose these assaults, yet as talked about there are sure precautionary measures which can be utilized to keep away from refusal of Denial of service attack and Sybil attack. Moreover we have tried to give solution to avoid such attacks.

VIII. REFERENCES

[1] Kelleher, W., (2013), "*Internet Voting in the USA: History and Prospects*", Western Political Science Association, Los Angeles, March 28-30, 2013, California.

[2] CyberVote consortium. Report on Review of Cryptographic Protocols and Security Techniques for Electronic Voting, 2002. Vol.1.

[3] G. Danezis, C. Lesniewski-Laas, M. F. Kaashoek, and R. Anderson. Sybil-resistant.

[4] Mercuri R (2000). Electronic vote tabulation checks and balances, Ph.D. Thesis, University of Pennsylvania, Philadelphia, PA.

[5] https://webrootsdemocracy.files.wordpress.com/2016/01/secure-voting-webroots-democracy.pdf.

[6] An Efficient Online Voting System, ISSN 2249-6645, Volume-2, Issue, July-Aug-2012, IJMER.6]

[7] https://webrootsdemocracy.files.wordpress.com/2016/01/secure-voting-webroots-democracy.pdf