TRUSTWORTHY ELECTRONIC VOTING SCHEME

P.Harini
Dept. of Computer Science and Engineering
St. Peter's College of Engineering and Technology
Chennai, India

R.Pradeeksha
Dept. of Computer Science and Engineering
St. Peter's College of Engineering and Technology
Chennai, India

R.Rishitha
Dept. of Computer Science and Engineering
St. Peter's College of Engineering and Technology
Chennai, India

Abstract— *The e-casting a ballot plot improves the presentation of the reconsidered rearranged unquestionable re-encryption and by presenting affirmation numbers that are utilized in the CN (confirmation number) based e-casting a ballot conspire. in spite of the fact that CN (confirmation number) based and R-SVRM (Revised-simplified verifiable re-encryption mix net) based had made e-casting a ballot plots progressively down to earth by excluding the zero information confirmation which requires enormous volume of calculations, still they were insufficient. In this way, the CN (confirmation number) based plans receives the RSA encryption works that were not probabilistic and commutative, along these lines it is to fulfill the basic prerequisite of decisions, as the additional arbitrary variables were important for singular votes, political race specialists must sign on votes and they should keep encryption keys.*

Keywords— e-voting, QR-code, scanner, e-casting, ballot, cloud storage, Biometrics, SMS voting, web service application, secure networks

I. INTRODUCTION

The right execution of evenhanded rights has gotten associated with the availability and strong working of bleeding edge information and correspondence advancement (ICT) Information and interchanges innovation .While present day social requests totally rely upon ICT for business, work and entertainment time works out, the use of ICT for law based dynamic is still in its beginning. To be sure, the out date creative thoughts for throwing a polling form have been blamed somewhat for lost and uncounted votes and could likewise be subject for uneven political decisions making. Countries wherever all through the world are examining e-throwing a voting form, for it makes them strike focal points over traditional paper throwing a voting form, including security for tossing votes, accuracy of checking and separating votes, choices to coordinate just in a concentrated and decentralized manner, etc. The reasons why the e-throwing a voting form advancement has not created to indistinguishable levels as known for business and unwinding time practices lies generally in a trademark nonappearance of trust and fear of electronic perils. While most countries are up 'til now conceptualizing or testing e-throwing a voting form system, three cantons in Switzerland have led the improvement of e-throwing a voting form to its full mechanical turn of events. The world is reliably in progress and improvement in development, that is the explanation we should go relating with it, to be able however much as could reasonably be expected get advantage from these upgrades.

Casting a ballot through a political race shapes a significant piece of majority rules system and for vote-based system to be feasible, the voter's investment is a key thought. Aside from voters being urged to practice this exactly right, the political decision that encourages the capacity must be believable, watertight, and liberated from inclination. Notwithstanding accommodating the methodical exchange of intensity, it likewise concretes the resident's trust and trust in an association or government when it works effectively. Society is turning out to be increasingly more web/cooperation arranged, and residents, used to the high level of adaptability in the administrations gave by the private segment and in the Internet specifically, are currently starting to set requesting norms for the conveyance of administrations by governments utilizing present day electronic conveyance strategies.

The key worries of races and substance of a democratic framework is Transparency: standard voters ought to have the option to comprehend and watch the vote throwing and checking process, even with generally ostensible training just as trust.

The usage of electronic democratic would permit expanded access to the democratic procedure for many potential voters. More elevated levels of voter interest will loan more prominent authenticity to the appointive procedure and should assist with alter the course towards voter lack of concern that is quick turning into a component of numerous popularities based social orders. It is additionally perceived that progressively conventional democratic techniques will exist for quite a while to come, so a method is expected to make these increasingly productive and coordinate them with the more up to date electronic strategies.

II. OBJECTIVE

To overcome the existing method of e-voting which uses concept like biometrics, SMS voting, etc.

III. LITERATURE SURVEY

The author in this paper [1] expressed that the democratic depended on the isolation of voting form planning and throwing. The cryptographic auditing with casting a ballot had said to be open review casting a ballot which stayed as hypothetical undertaking. Disregarding various conventions and earth-shattering advances in the field, casting a ballot on the web or through mail was normally shaky in races on account of pressure hazard. Voter gets impacted by an aggressor. Consequently, the outcome gave the advantages of cryptographically audits races.

This paper [2] described that another electronic democratic plan satisfies the security necessities. To make the vote evident, the key component is utilized which included affirmation numbers in singular votes. The linkages among voters and votes was known by incapacitating all the substances including the voters themselves. For confirmation, numerous e-casting a ballot plots broadly sent zero information evidence. This plan would be versatile and useful while the affirmation numbers accomplish the undeniable nature in the simpler manner. The perfect e-casting a ballot plans fulfilled protection, exactness, all-inclusive unquestionable status, decency, and power.

In this paper the author [3] characterized as the name recommended, the receipt freeness in mix net was believed to be hard to give electronic democratic plans. Any sort of client who was picked indiscriminately was utilized to develop a receipt, since the client can demonstrate a purchaser that how he had encoded the voting form. In extra to this, a straightforward and proficient strategy has been included to consolidate receipt freeness in mix net based electronic democratic plans by the re encryption strategies. Thus, this strategy offered association to receipt freeness.

This paper [4] expressed that the civitas was the principal electronic democratic framework that is compulsion safe, world was broadly voter undeniable and it is additionally utilized for remote democratic. It portrayed the plan and execution of civitas. The affirmation had been actualized in the plan and through security proofs and in the data stream security investigation. The Experimental outcomes gave quantitative assessment among time, cost, and security. Casting a ballot framework were said to be difficult to make reliable because they have solid, clashing security necessities. Two among them are trustworthiness and privacy. Numerous security specialists have not been persuaded about the electronic democratic, contending that affirmation in electronic democratic frameworks were too difficult to even consider obtaining and that their deployment makes the inadmissible dangers.

This work [5] expressed that the commutative and re-encryption procedures are fundamental devices for different applications as the two tasks encryption and unscrambling are acted in self-assertive request. These re encryption strategies empowered one to move data safely in a system with no information on open keys of different gatherings. Message transmission process broadly rely on the exhibition of commutative method. Chiefly it was utilized to choose whether some as of late designed commutative re encryption procedures have better activity and uncover the strategy with expanded execution. It portrayed about the three sections, out poring the significance of the commutative re encryption strategies, putting out some most recent systems alongside proposing an adjustment for making their tasks quicker, and breaking down the progression of activity in the proposed methods. It had been mostly proposed basically for trial moderate systems to affix their activity.

This method [6] delineated basic unquestionable re-encryption blend net plan which had been intended for e-casting a ballot framework. The plan fulfills all the prerequisites of decisions which incorporate protection, undeniable nature, reasonableness, and strength. It shields voters from coercers in specific situations where coercers power voters to limit from races. Voters can hide correspondence among them, and the votes can be utilized to confirm the precision of decisions. The faltered political decision results were hidden from any element. Because of the constrained activities in the stalls which in turn debilitate voters to remember total data traded among voters and political decision specialists. During the time spent tryouts, the decisions can be finished with no re-appointment process.

Security necessities designing for indicating security prerequisites of an e-casting a ballot framework as an authentic answer for e-administration portrays that the adjustments in innovation have expanded weight on e-administration to modernize the political decision process. It had been seen for quite a long while India experiences issues of long queues, touchy surveying corner and other surveying issues. The arrangement discovered was electronic constituent procedure. It was executed mostly to achieve security necessities and utilitarian prerequisites in the early periods of

e-casting a ballot. Elevated level of security was accomplished by recognizing more hints of vulnerabilities and determining security prerequisites of e-casting a ballot framework at early periods of programming improvement life cycle.

The author in this paper [8] expressed that for the cryptographic conventions, the electronic democratic is the developing social application. Over most recent two decades a tremendous measure of writing on electronic democratic had been created. Notwithstanding this a structure that orders three methodologies wherein their properties were presented. This philosophy uncovers certain distinctions in security properties between the classes and the determination remittance and future structure of casting a ballot framework. The utilization of electronic democratic can possibly diminish or evacuate undesirable human blunders.

Remote democratic was the dynamic field for the use of cryptographic procedures from the most recent two decades woman plans and frameworks. Here it introduced a diagram in creating casting a ballot plans and security models that include an assortment of imperatives to acclimate the political race trustworthiness. It additionally ordered the democratic plans dependent on essential cryptographic strategies. It analyzed the ongoing plans and frameworks against the fundamental and counter assault necessities. Such examination shows the distinction among security necessities and structure in the plans. The point was to give the specific democratic frameworks under different conditions.

In this paper [10] depicted that the arrangement of the mysterious tag depends on unknown qualifications and it was upgraded. It requires number of challengers and reactions among verifiers and certification holders. The unknown tag requires just modest number of difficulties and reactions among verifiers and rodential holders. This is because of that the plan can be effectively made sound even in environments where verifiers may do not carry on genuinely. So, the original plot has potential highlights, the verifiers must create sham difficulties, consequently for overseeing mysterious frameworks cannot be decreased. The improved mysterious tag bar the probabilistic highlights among verifiers and qualifications holders. It likewise adjusts a few structure blunders remembered for the original conspire.

In the paper the author [11] proposed that in cryptography two sorts of improvements are inspected. For the broadening of the applications have offered ascend to the new kinds of cryptographic frameworks, which limit the requirement for secure dispersion of channels and supply what might be compared to a composed mark. It recommends approach to tackle the present issues. It additionally talked about the hypotheses of correspondence and calculation to give a portion of the instruments to take care of the cryptographic issues. The advancement of the modest computerized equipment had liberated it from the structure of processing and brought the expense of high evaluation cryptographic gadgets.

The receipt freeness is a security property in electronic casting a ballot to forestall vote purchasing and selling. By changing the democratic plan proposed a proficient mix net-based receipt free democratic plan. The receipt freeness property was gotten through randomization administration given by a confided in director. The effectiveness is improved by presenting a progressively proficient mix net. Here the executive gives the both randomization and blending administration in the democratic stage. The randomization will be the polling form re-encryption, So the voting forms will be blended utilizing the proposed mix net. The mix net based democratic plan gives the receipt-freeness in a proficient way. In this plan voter needs to set up his scrambled polling form through a randomization administration gave by alter safe randomizer, so that he at last loses his insight on haphazardness. In this strategy it is utilized to give receipt-freeness.

This paper the author [13] stated that the openly evident blending plan has everlasting security towards onlookers. All the data has been distributed by the blends uncovers no data about the personality of messages distributed. The rightness of the blending procedure was measurable, regardless of whether the all specialists contrive, they cannot change the substance of the message without being recognized with likelihood. It done that by encoding the messages which are presented by Pedersen duties. Deciphering was likewise conceivable because we make an equal blend net by the equivalent blends to which open has no entrance. The private blend net uses indistinguishable changes from the open one all the while, yet utilizes the homomorphic encryption, which is utilized to send the extra data through the blend net to permit deciphering in the framework.

The author [14] expressed that casting a ballot conspires that give receipt-freeness keep voters from demonstrating their make choice. It investigated the security of the multi authority casting a ballot convention and clarified that this convention was not receipt free. In this way, it had proposed the primary sans receipt casting a ballot conspire as it will be the mystery one-way correspondence channels from the specialists to the voters, because of the open evidence. Voters can only join the single phase of the convention, understanding the "cast a ballot and go" idea. In this plan the mystery polling form casting a ballot convention were one of the most significant use of the cryptographic conventions. The most proficient mystery voting form casting a ballot convention can be arranged into the kinds of plans utilizing homomorphic encryption, plans utilizing blind marks.

This work [15] proposes that the developing notoriety of the e-government benefits, the security of customer stages and infringement of resident e-rights are of incredible concerns. So, the web casting a ballot convention had no influence over

voter side stages, the voter side stage is effectively assaulted to noxious programming will spread the security of the whole democratic convention. Thus, we proposed the ESIV convention start to finish secure web casting a ballot framework that exceptionally guarantees the voter and server-side stages security, undeniable nature, and decency. So, it utilized the java card 3 innovation as a free secure web server which was been associated legitimately to the system to send and get HTTP demands utilizing fast interface. This innovation achieves the freedom from using any confided in gadget at voter-side and gives end-end security.

In this plan, the offer gear was a hazardous assault in an electronic sale. Abe and Suzuki initially presented receipt allowed to forestall this assault. So, this plan just gives receipt-freeness to losing bidders. So, we advise that it is essential to give receipt freeness and propose another without receipt fixed offer sale conspire utilizing the homomorphic encryption system. Here our plan fulfills protection, open verifiability, and receipt-freeness for all the bidders. This plan did not depend on edge trust model however the outsider trust model will be increasingly appropriate for genuine closeout. We stretch out our plan to M+1 St value sans receipt closeout.

The author [17] expressed that the electronic democratic to take care of the issues in the lower cost of customary paper based. Numerous scientists gave their security e-casting a ballot framework. The current plans do not see to meet the prerequisites. For instance, a lot assault holder needs to allot an individual in the organization to cast a ballot by utilizing a warrant a framework ought to offer such assistance. The intermediary e-casting a ballot plot is that it can appoint an intermediary to cast a ballot. The intermediary e-casting a ballot framework will fulfill all the necessities. As the plan not exclusively can be effortlessly actualized yet in addition has less computational expense for voters to cast the voting forms.

It was recommended that conviction of simultaneous voting form approval of pressure safe, start to finish unquestionable, web casting a ballot. A focal piece of giving the intimidation opposition is that the political decision authority is to channel the phony polling form from the genuine ones in the manner that is both the private. This voting form authorization process permits voting form to be approved as they are submitted, permitting the count to be proclaimed following the surveys close. A count is significant in the pressure safe framework to offer the polling form authorization. The cobra offered the quickest counting to the related work, and it has the enlistment procedure, that we consider to be moderate. Here it has introduced the cobra as an initial move towards as it will end up being the component of compulsion safe web casting a ballot plan. It likewise gives the simultaneous voting form approval.

Electronic democratic frameworks had misused the automated democratic equipment, computer systems and cryptographic conventions to lead races. They had capacity to blend both undeniable nature and voting form effectively simultaneously. The Elections led by e-casting a ballot framework were relied upon to be effective, precise, secure, and advantageous. The issues related with e-casting a ballot framework may do not acknowledge their acknowledgment. To set up e-casting a ballot framework as a dependable instrument to lead decisions, effectively an examination has been proposed. Here it has proposed an examination of existing e-casting a ballot plots alongside their extensions and confinements.

This method [20] expressed that traditional e-casting a ballot framework replaces the paper-based procedure with an electric one at authentic democratic areas. The remote e-casting a ballot , where the voter can cast a ballot from any area, and it builds the both interest rates in the races and the clients fulfillment and it gradually process the democratic procedure and spares time. So, having a remote e-casting a ballot framework builds the security vulnerabilities. The vulnerabilities incorporate more enthusiastically client verification, probability of malignant programming on the client's gadget, arrange malevolent hubs, compulsion and vote selling. It has presented the Upvote as a helpful and certain democratic framework. The Upvote fills in as a front end to a significant number of the current customary e-casting a ballot framework, and it gives the client the advantageous democratic arrangement and which it ensures security.

The model for electronic political race contrives that incorporates a more noteworthy discussion than past work. It allowed the discussion to demand obliged voters that they vote with a certain goal in mind, or even they divulge their puzzle keys. So, it portrayed an arrangement to be impulse safe if it is infeasible for the inquiry to choose if a compelled voter agrees to the solicitations. The responsibility is to delineate and depict the as of late fortified inquiry. So, it had likewise acquainted what it has acknowledged with be the key proper security definitions for electronic arrangement of any kind. And another responsibility is that the show is no doubt secure against our formalized challenge. While the previous plans have required an untappable channel, this arrangement had continuously reasonable essential of obscure channel.

In this method the author [22] characterized as one of the best strategies for people to communicate their supposition on a subject. Electronic democratic referred the utilization of PCs or mechanized democratic types of gear to cast polling forms in a political race. E-casting a ballot performs over web and it tends to be all around acknowledged in the up and coming a long time because of the way that web assumes a significant job in the people groups lives. The DynaNotes e-casting a ballot convention tells that it is pragmatic over the web and it does not utilize any perplexing calculations, no physical suspicions as, for example, untappable unquestionable status. The product improvement requires a lot of time and cash. To

utilize all the assets, the model execution acquires significance and it gives snappy criticism about the framework.

This method [23] depicted that an all-around evident, cryptographic vote political race with solid voter protection as its essential target. It was worked around three helpful properties of casting a ballot plans and the first was been an ideal polling form mystery as it guarantees the information about the voting forms of any arrangement of voters. The subsequent one has been self-counting which throwing convention that empowers every voter to decide with high certainty have been precisely spoken to as a contribution to public count. So, the receipt, can speak to a decision for an up-and-comer with equivalent likelihood and it is empowering for vote purchasing. To make this conceivable is that totality of data that the voter uses to persuade herself regarding encoded polling form respectability incorporates transitory data that is accessible at the time just when voting form is in thrown. It has accepted that the customary democratic frameworks, here the demonstration of throwing happens in private condition that will be the pool corner. Under this plan, the conjunction with an all-around certain convention gives a start to finish irrefutable and mystery vote receipt dependent on political race convention.

In this paper the author [24] expressed that the democratic convention that ensures voters protection and accomplishes general verifiability receipt-freeness, and without specially appointed physical suspicions and procedural limitations. The plan permitted voters to cast write in polling forms and show how it very well may be for all intents and purposes actualized through voter checked voting forms. The plan permits voters to
consolidate the democratic accreditations with their picked casts a ballot and applying the homomorphic properties of certain cryptosystems.

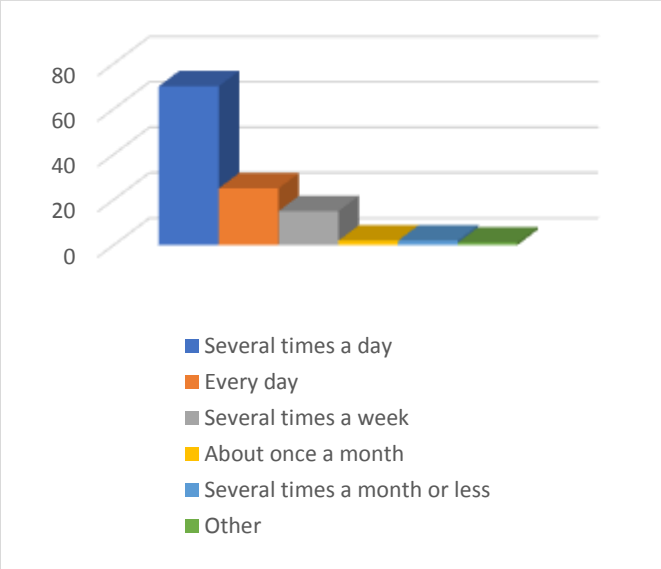
SYSTEM ANALYSIS

The purpose behind the System Analysis is to convey the short examination undertaking and moreover to develop all out information about the thought, direct and various prerequisites, for instance, execution measure and structure headway. The target of System Analysis is to thoroughly demonstrate the specific nuances for the rule thought in a minimal and unambiguous manner.

SYSTEM REQUIREMENT SPECIFICATION

The inspiration driving the System Requirement Specification is to convey the specific of the assessment undertaking and besides to develop complete information about the need, lead, and various objectives, for instance, commonsense execution, and so on. The target of Software Requirement Specification is to thoroughly decide the necessities for the item thing in a brief and unambiguous manner.

Reported Internet usage:



Internet usage by age*:

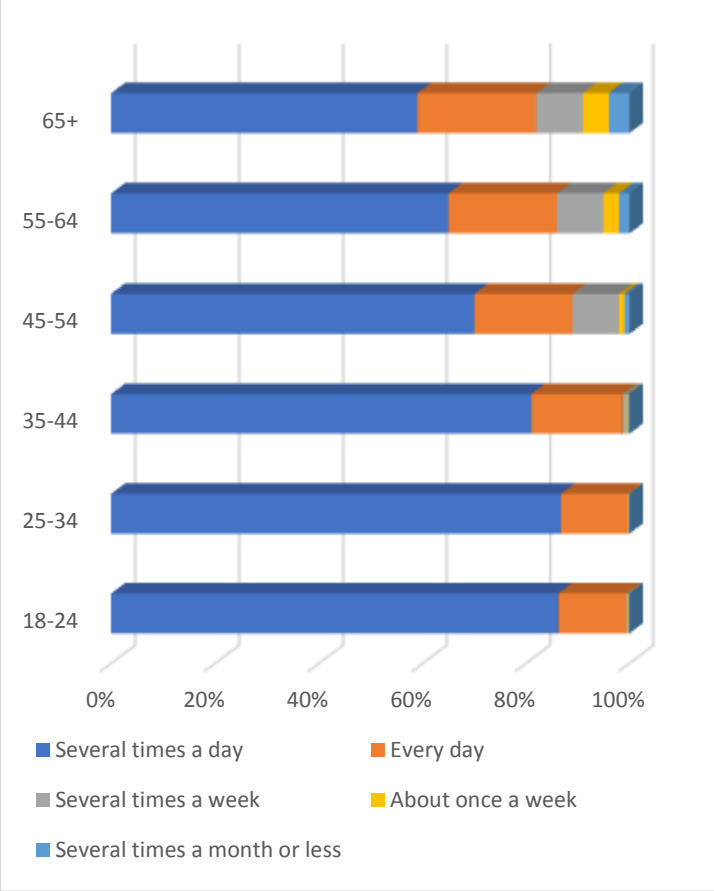


TABLE I

APPROACHES FOR AUTHOR/OBJECTIVE ANALYSIS

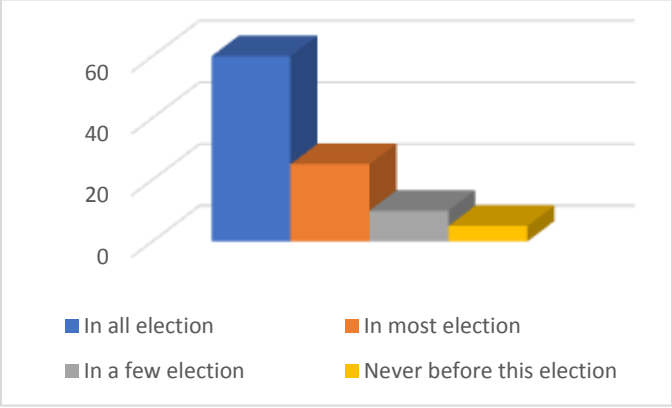
SI.NO	AUTHOR	OBJECTIVE
1	B. adidas Hermos	Casting a secret ballot based on modern web browser for the generation of validity proof.
2	K.M.R Alam	The affirmation number in singular votes includes the linkage between voters and voters themselves.
3	B. Lee	The potential strategy is considered to consolidate receipt freeness in mix net based electronic democratic plan.
4	M.R Clarkson	The prototype build to explore probability and enforces verifiability in national Elections.
5	N. Islam	The re-encryption and communicative procedures act as fundamental devices in process of task of encryption.
6	H.A. Haddad	The modification of simplified verifiable Re-Encryption and mix net SVRM developing e-voting scheme based on anonymous Tag credentials.
7	P. Salini	The determination of security prerequisites of e-casting a ballot framework at the early stage of programming life cycle.
8	K. Sampigethaya	Casting a ballot framework for future structure as in determination remittance.
9	L.Huian	The creation of ballot plans security models includes assortment of imperatives to acclimate political race trust worthiness.
10	S. Tamura	The improved mysterious tag for the probabilistic highlights among verifiers and qualifications holders for few structure blunders.
11	M.Hellman	The advancement of modest computerized equipment liberated from structure of processing for the high cryptographic gadgets.
v12	R. Aditya	The voter setup scrambled polling through randomization administration by alter safe randomizer.
13	D.Damirel	The deciphering framework, is considered for the equivalent and private blends which utilizes homomorphic encryption in voting.
14	M.Hirt	The mystery polling from casting ballot conventions will be the significant use of cryptographic convention.
15	X.Chen	A free secure webserver java3 innovation is considered confidedin gadget at voter side and gives end-end security.
16	Cheng-chilee	The intermediary e-casting is to cast a ballot and to fulfil the necessities for casting voting forms.
17	Aleksander Essex	The quickest counting ensures the safe framework of polling, as a component of compulsion safe web casting a ballot plan.
18	Md.Rokibul Alam	The commencement of examination of existing e-casting ballot plots alongside their extensions, confinements.
19	Reem abdelkader	The Upvote as a certain democratic framework for e-casting a ballot in democratic arrangement and ensures security.

20	Ari Juels	The principle formal security commitment for electronic appointment of any sort as if is pre-requisites of unknown channel.
21	O. Cetinkaya	The model execution utilizes assets, acquires significance gives snappy criticism of the framework.
22	Daniel Sandler	The customary democratic frameworks work in private condition in pool corner and the mystery vote receipt dependent on political race convention.
23	Haroid	The homomorphic properties of cryptosystem are applicable to voters to consolidate democratic accreditations with their casts a ballot in picket format.

IV. EXISTING SYSTEM

Existing System is the one wherein the biometric idea is utilized where the filtering of unique mark is finished. For certain individuals it is meddlesome, because is yet identified with criminal distinguishing proof. Voters cannot be ready to come and make their choice from their working area to local. Line framework become past the point of no return for voters to cast a ballot.

Reported voting record in past elections:



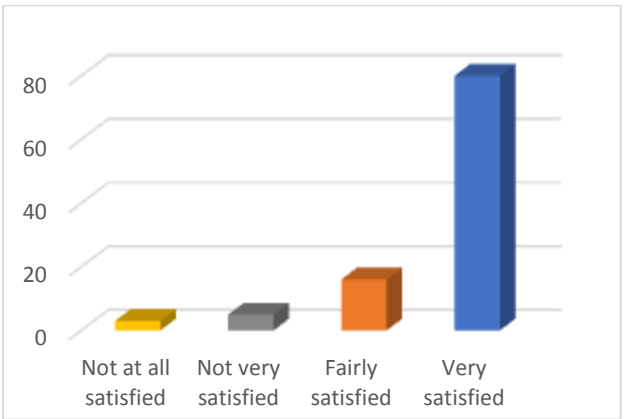
DISADVANTAGE OF EXISTING SYSTEM

- System is little bit complex
- Less security.
- Hacking voter results.
- Time Delay.
- Cost Effective.
- Time utilization is high.

V. PROPOSED SYSTEM

Framework dwells in the new idea of QR-Code and Scanner Application. Up-and-comer subtleties made to stow away in the QR-Code. Through scanner application the QR-Code is checked, and subtleties are recovered. Here there is no possibility of expanding the vote check. At that point, the democratic is performed. In the proposed framework, we are utilizing QR code for perceives picture codes utilizing PDAs to offer different types of assistance that can perceive the realness of any voter subtleties. QR code confirms vote id no by catching it through the PDA, at that point deciphers and sends it to the server for verification. This advances the chose voter id number rundown to the server and the reaction got from the server empowers the buyer to choose dependent on the voter legitimacy. At last the political race server, chairman will sift through the conclusive outcome by checking the given data with effectively wanted data.

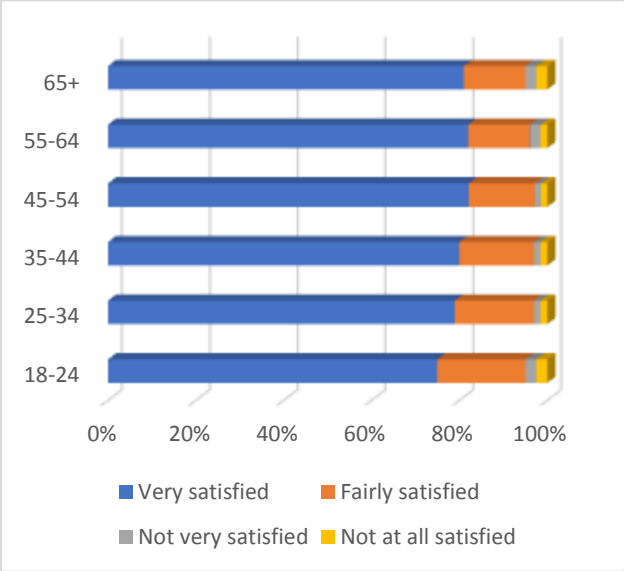
Satisfaction with the online voting process:



SI.NO	MODULES	MODULES DESCRIPTION
1	Module I	User Module
2	Module II	Election Commission Module
3	Module III	Election Commission Module

TABLE II.
APPROACHES FOR MODULE DISCRIPTION ANALYSIS

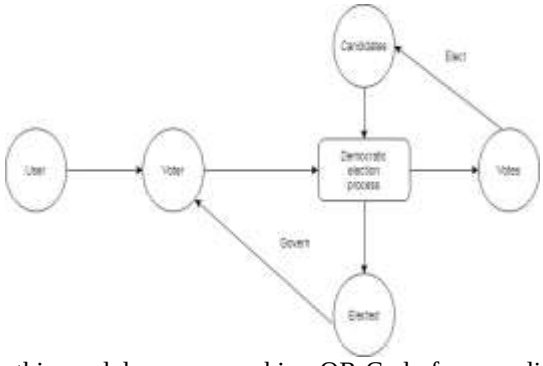
Internet voter satisfaction by age*:



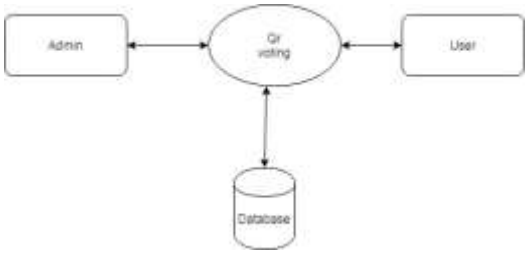
ADVANTAGE OF PROPOSED SYSTEM

- Highly made sure about and there is no way to revote.
- Scanning acknowledgment.
- Real time following of results.
- Time utilization is less.
- No chance for hacking the votes.

MODULE 1-USER MODULE



In this module we are making QR Code for encoding the data about the voter. The voter subtleties contain voter id no, voter name, DOB, Address. Each example is encoded and spoken to every module in QR Code with high contrast unique symbols QR-Code can hold data more than other scanner tags. The organization of QR Code incorporates special Finder Pattern (Position Detection Patterns) situated at three corners of the image and can be utilized to find the situating of the image, size, and tendency.

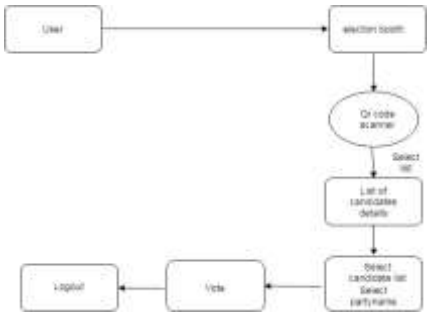


MODULE 2-ELECTION COMMISSION MODULE

This module speaks to the confirmation, which is utilized for the voter to login their subtleties for the democratic procedures. Logged voter is diverted to the scanner module. Authentication is utilized as the premise or approval deciding if a benefit will be allowed to a specific client or procedure. The approval forms are done on the webserver.

MODULE 3- ELECTION COMMISSION MODULE

This module is utilized to filter the QR-Code and read the estimation of the QR-Code inside the versatile. QR-Code is a network standardized tag intended to be perused by Smartphone. The code contains of dark modules organized in a square example on a white foundation. The data encoded might be text, a URL, or other information. If the voter chooses the applicants, the subtleties will legitimately advance to the server.



VI. CONCLUSION

In the end as the CN is acquainted with the proposed e-casting a ballot conspire which improves the exhibition of the R-SVRM based plan. Since it decreases the quantity of things in each vote structure and rejects things that incorporate data about competitors as types from vote frames, the plan gets straightforward and proficient. Additionally, it fulfills every necessity of e-casting a ballot framework, as it is supplied with highlights about protection, strength, exactness, honesty, in coercibility and decency. So as a result, the plan gets functional and versatile. Some potential future bearings of works are accessible from the current investigation. In this investigation, just stall casting a ballot is thought of. In future it may be improved with the goal that it can bolster remote democratic. Another tentative arrangement of progress is to fuse in increasingly sensible situations where numerous specialists are appropriated over better places, and numerous voters are included. This proposed system may assess with highlights of added substance and multiplicative homomorphic properties of Parlier cryptosystem.

VII. REFERENCES

[1] Aralu, U. O. "Influence of Information and Communication Technology on Digital Divide – Global Journal of Computer Science and Technology", Volume 15, Issue 3, Year 2015.

[2] Verification and validation issues in electronic voting. O Cetinkaya, D Cetinkaya - Electronic journal of **e**-government, 2007

[3] Principles and requirements for a secure e-voting system. Dimitris AGritzalis – computers and Security Volume 21, Issue 6, year 2002

[4] B. Adida, "Helios: Web-based open-audit voting" In Proceedings of 17th USENIX Security Symposium, Aug. 2008.

[5] K. M. R. Alam, S. Tamura, S. Taniguchi, and T. Yanase. "An anonymous voting scheme based on confirmation numbers." IEEJ Trans. EIS, Vol. 130, No. 11, pp. 2065-2073, 2010.

[6] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, "Providing receipt-freeness in mix net-based voting protocols," ICISC 2003, LNCS, 2971, Springer-Verlag, pp. 245–258, 2003.

[7] M. R. Clarkson, S. Chong, and A. C. Myers, "Civitas: Toward a Secure Voting System," In Proceedings of the 2008 IEEE Symposium on Security and Privacy, pp. 354-368, 2008.

[8] N. Islam, K. M. R. Alam and S. S. Rahman, "Commutative Re-encryption Techniques: Significance and Analysis," Information Security Journal: A Global Perspective, Taylor & Francis, Vol. 24, No. 4-6, pp. 185-193, 2015.

[9] S. Tamura, H. A. Haddad, N. Islam, and K. M. R. Alam, "An Incoercible E-Voting Scheme based on Revised Simplified Verifiable Re-encryption Mix-nets," Information Security and Computer Fraud, Science and Education Publishing, Vol. 3, No. 2, pp. 32-38, 2015.

[10] P. Salini and S. Kanmani, "Security requirements engineering for specifying security requirements of an e-

voting system as a legitimate solution to e-governance," International Journal of Wireless and Mobile Computing, Vol. 7, No. 4, pp. 400-413, 2014.

[11] K. Sampigethaya and R. Poovendran, "A Framework and Taxonomy for Comparison of Electronic Voting Schemes," Computers and Security, Elsevier, Vol. 25, No. 2, pp. 137-153, 2006.

[12] L. Huian, A. R. Kankanala and X. Zou, "A taxonomy and comparison of remote voting schemes," 23rd International Conference on IEEE Computer Communication and Networks (ICCCN), 2014.

[13] S. Tamura and S. Taniguchi, "Enhancement of Anonymous Tag based Credentials," Information Security and Computer Fraud, Science and Education Publishing, Vol. 2, No. 1, pp. 10-20, 2014.

[14] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, Vol. IT-22, pp. 472-492, 1976.

[15] R. Aditya, B. Lee, C. Boyd, and E. Dawson, "An efficient mix net-based voting scheme providing receipt-freeness," Trustbus 2004, LNCS, 3184, pp. 152–161, Springer-Verlag, 2004.

[16] D. Demirel and J. V. D. Graff, "A Publicly-Verifiable Mix-net with Everlasting Privacy Towards Observers," Proc. IACR Cryptology print Archive, informal publication, 2012.

[17] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," Advances in Cryptology-EUROCRYPT 2000, LNCS 1807, pp.393-403, Springer-Verlag, 2000.

[18] X. Chen, Q. Wu, F. Zhang, H. Tian, B. Wei, B. Lee, H. Lee and K. Kim, "New receipt-free voting scheme using double-trapdoor commitment," Information Sciences, Vol. 181(8), pp.1493-1502,
2011.

[19] X. Chen, B Lee, and K. Kim, "Receipt-free electronic auction schemes using homomorphic encryption," Int. Conf. on Information Security and Cryptology, pp. 259-273, 2003.

[20] K. Aggelos and Y. Moti. "Self-tallying elections and perfect ballot secrecy," Proceedings of public key cryptography, 5th international workshop on practice and theory in public key cryptosystems, LNCS, vol. 2274. Springer-Verlag, pp.141–58, 2002.

[21] R. Abdelkader and M. Youssef, "Upvote: A ubiquitous e-voting system," in 3rd FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC'12), pp. 72-77, 2012.

[22] N. Islam, K. M. R. Alam, and S. S. Rahman, "Commutative re-encryption techniques: Significance and analysis," Information Security Journal: A Global Perspective, vol. 24, no. 4, pp. 185-193, 2015. 20. S. Tamura, H. A. Haddad, N. Islam, and K. M. R. Alam, "An Incoercible E-Voting Scheme based on Revised Simplified Verifiable Re-encryption Mix-nets," Information Security and Computer Fraud, Science and Education Publishing, Vol. 3, No. 2, pp. 32- 38, 2015.

[23] C. C. Lee, T. Y. Chen, S. C. Lin, and M. S. Hwang,"A new proxy electronic voting scheme based on proxy signatures," Lecture Notes in Electrical Engineering, vol. 164, pp. 3-12, 2012.

[24] B. Adida, "Helios: Web-based open-audit voting," in Proceedings of 17th USENIX Security Symposium, Aug. 2008.

[25] L. Huian, A. R. Kankanala, and X. Zou, "A taxonomy and comparison of remote voting schemes," in 23rd International Conference on Computer Communication and Networks (ICCCN'14), pp. 1-8,2014. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions Information Theory, Vol. IT-22, pp. 472-492, 1976.

[26] K. M. R. Alam and S. Tamura, "Electronic voting: Scopes and limitations," in Proceedings of International Conference on Informatics, Electronics & Vision (ICIEV12), pp. 525-529, May 2012.