INTERNATIONAL JOURNAL OF SOCIAL Sciences and Information Technology
ISSN 2412-0294 www.ijssit.com

http:// www.ijssit.com

ELECTION RESULTS' VERIFICATION IN E-VOTING SYSTEMS IN KENYA: A REVIEW

[1*] **Charles Ochieng Oguk**
ogukcharles@gmail.com

[2**] **Jane Juma**
jjumacloy@gmail.com

[1,2] *Department of Mathematics, Statistics and Computer Science, School of Science Technology and Engineering, Rongo University*

***Abstract**: Politics is at the centre of a nation's daily life, and so are elections. There is need to project continuous, verified, and validated results simultaneously to all stakeholders. This is imperative because it not only helps in bridging the information gap from the time an election exercise is announced to the time a winner is declared, but also in shunning any probable election dispute and high temperatures that arise with suspected fraud. Provisioning of a suitable e-verification system with verifiable features goes a long way to ensure that election results are validated and thus accepted by all stakeholders. This review looked into various e-verification systems for authenticating election results.*

***Keywords**: E-voting, Electronic voting, election e-verification, validate election, voter anonymity*

Introduction

In Kenya, the importance of verification of electoral processes is emphasized in the constitution - which requires that in every election, the given electoral commission should ensure that electoral systems used be simple, accurate, verifiable, secure, accountable and transparent (Laws of Kenya, 2016). The legislation on elections requires verifiability through effective but simple approaches which are easily understood to ensure transparency. The procedure in presidential election in Kenya for example, requires that after counting the votes in the polling stations, the electoral commission shall tally and verify vote count before declaration of results and winners.

While this verifies the tally, it does not verify the count or the actual votes as cast and one cannot confirm that the votes were counted as cast. In the Kenyan manual voting, one cannot quite confirm that there is no interference as collusion by the parties can alter or mutilate votes. However in electronic voting, it is possible to connect a vote to the voter. However, this should be done without compromising the integrity, secrecy and confidentiality of the voter. Moreover, such a system should be subjected to independent auditing without compromising the integrity, secrecy and confidentiality of the voter.

Chege (2018) found that verification of results can play a vital role in detection of electoral fraud especially during casting of ballots, counting of votes and public announcement of the results. There is therefore a need for verification tools that can detect fraud with high degree of certainty in the vote tabulation as well as the counting processes by highlighting anomalies in the results. Such anomalies may suggest irregularities in the voting, counting and tallying processes. While concurring with Chege, (Omwami 2018) demonstrated that verification deters electoral fraud. However, after exploring electoral participation among young Latinos, (Popan and Hinojosa, 2017) stressed the importance of recognizing that not all discrepancies between results at the polling station and results officially released are due to fraud, but could also be a consequence of insufficient training, exhaustion and inadequate understanding of such systems among the parties involved. It however, did not focus on whether the votes are counted as cast.

By revealing certain patterns of electoral manipulation, verification approaches involving the public can deter actors from engaging in electoral fraud as the actors fear being caught. Barnes, Brake and Perry (2016) found that public involvement in verification helps in deterring fraud since when this method is made simple and understandable by the public, the actors understand they could face some sort of sanctions from informed voters for attempting to manipulate elections results.

E-verification models in electronic voting therefore, are digital systems that are used to authenticate the validity of: registered voters, votes cast, elections data transmission, vote counting, tallying, the election results as well as all the processes involved (Mwighusa, 2015). Mwighusa showed that various verification ways exist for e-voting which include: verification by the entity conducting elections like the electoral commission; third party verification, verification by voters; and verification by candidates. However, among all these types of verification, individual verification is the most desirable (Cortier & Lallemand, 2018). While verification systems for use by the commissions exist, there are cases where people do not trust the commission but rather want to confirm for themselves for example in the Kenyan disputed presidential elections and the subsequent court cases in the year 2017, where the litigants demanded the re-opening the election servers (Chege, 2018).

Further, primary goals associated with verifying election results have been emphasized in various studies. According to Birch and Muchlinski (2018), transparency and public confidence in elections can be built by improving the accountability and performance of electoral management bodies, by supporting citizens' oversight of electoral processes through simple and widely understandable verification processes. In support of this, Gastil and Meinrath (2018) analysis showed that a robust citizen oversight of elections, where voters are provided with simple but sound verification mechanisms is critical; because it can help detect electoral malpractices, and also engages citizens in democratic processes, which build trust in election outcomes. This can reduce chances of electoral disputes and violence. Conversely, e-verification systems in which citizens cannot directly verify the results, even when the systems effectively verify the results, are prone to little understanding of the verification process by electorates and a consequent lack of trust in the verification systems employed (Pimenidis, 2017).

Conrad *et al*., (2009) showed that verification helps in building confidence in electoral processes. They explain that appropriate methods to verify election results should be used to build confidence in elections, with the expectation that findings will be consistent with the official results. Chege (2018) further succinctly demonstrated that having an independent real time electoral assessment tool simple enough to be understood by voters, and which aligns with officially declared election results can build voter confidence in the election outcomes. When such verification systems reaffirm official results, they can dissuade candidates who have lost the elections from making utterances and claims of fraud, thus making them to concede defeat to the winning party without ill feelings created by uncertain results.

Verification systems can provide a valid projection of election results. According to Schnegg et al., (2014), information vacuum resulting from delayed declaration of results allow political actors, especially malicious agents to manipulate final results expectations by the public, hence creating confusion, and inciting unrest among the voters. Verification systems can project election results so fast that they can defuse political tensions by filling the information gap, and consequently neutralizing a violence probable environment.

Aguiar-Conraria, Magalhães and Veiga, (2019) highlighted that electoral verification system can build local capacity for election oversight, especially if the operation involved is simple and easy to understand even by non-system experts. While accountability of leaders to electorates remains a fundamental tenet of democracy, the study concluded that support of a more representative and participatory democratic processes is vital, especially through empowering electorates, by according them an oversight role in the electoral processes. This role can be assigned through, Kiayias, Zacharias, and Zhang, (2017) the use of verification tools that can build the capacity of not only the local groups, but also the civil society using evidence-based systems that are simple, widely understood and involves the voters.

The ultimate goal of a verification system is to validate official results in the public court of an electoral constituency (Schnegg et al., 2014). By providing an independent step by step confirmation and tabulation of the outcome, a trend informed by continuous results becomes simultaneously available to the public and the contestants as well. This helps not only in projection of results, but also in validation of the final official results. When the final tally from verification system is the same as the official results, it becomes a relief to the electoral authorities, the monitoring groups, contestants as well as the voters, thus shunning any possible cause of election results' dispute. However, such an environment can be achieved when all the stakeholders in an electoral process can adequately understand and appreciate the results verification system provisioned, (Komarova et al., 2018). In many countries, electoral systems should also allow re-opening of the e-ballot boxes in compliance with courts orders for verification, (Laksono & Agustine, 2017).

Problem statement

While e-voting systems are used in various countries and institutions, many electorates and candidates still lack trust on the systems' ability to deliver free and fair elections. Since lack of confidence among the key election stakeholders is associated by inadequate verifiability features of the systems, it is paramount to explore the election results' verification in various e-voting systems.

Objective

1. To explore election results' verification approaches in existing e-voting systems

Literature Review

Teutsch and Reitwießner, (2017) define verification as a comparison of two or more items by applying supplementary tests to ensure accuracy, correctness, and truth of the information given. Moreover, according to Kumar and Sharma (2017), when such comparisons are made through computerized systems, it becomes electronic (e) - verification. When supported and linked with the already known information that is conveniently sharable electronically, e-verification platforms offer a reference point for all the parties involved to verify the information of interest and trust the supported process, (Cortier et al., 2015).

E-Verification Models in Electronic Voting Systems

Various verification approaches in electronic voting systems exist today, wherein verification constitutes the e-voting system itself.

Scantegrity

Ganz, Bishop and Peisert (2016) explored the development of a system called scantegrity, an electronic voting system that lets voters verify that their ballots are counted, and using three-digit confirmation codes in an election. . It is an Elections' "end-to-end" verification systems that allow each voter to verify that his ballot was accurately recorded and counted. When the unique auto-generated codes map to the right candidates on the tallying portal, it does not reveal an individual voter's choice. If the code is present on the final tally web site, the system qualifies that the ballot was counted correctly. Also, on the Scantegrity ballot, each candidate position is always paired with a unique random letter. Therefore, election officials confirm receipt of the ballot by posting the letter that is adjacent to the marked position. The voting system was developed on optical scan technology by a cryptographer and researchers from the George Washington University, the University of Maryland-Baltimore, MIT, the University of Waterloo and the University of Ottawa. This verification approach however, hardly included independent logical variables such as time. A further weakness of the system is that it lacks a clear way of re-opening of the e-ballot boxes in cases of court orders, as well as complexity, low voter understanding of the verification process and lack of trust by voters.

Scratch & Vote

In their research work on Scratch & Vote (Kalchgruber and Weippl, 2010), developed an electoral e-verification model. It suggested a cryptographic voting system with least trust and least involvement of third parties. Instead, they suggested the use of representative organizations like political parties and campaign group agencies to perform pre-voting validation, notably by their presence in the polling station. Cryptographically, it sketched out a modified version of one ballot system in which voters relied on the receipts of previous voters whose digital signatures would be validated by the aforementioned external organizations for verification. The verification approach by design of the Scratch & Vote system was technically not favorable to voters. In addition, complexity of digital signatures of the previous voter receipts further impaired understandability of the verification approach even to the intended user groups. Due to its complexity, it was not well understood and remained not trusted by the voters.

A substantial study on third-party verification is by (Neumann, Olembo, Renaud, and Volkamer, 2014), which proposed the use of election websites and mobile apps accessible by voters to verify votes cast using the Helios e-voting system. In this work, third party systems provide services by which voters can verify whether their vote has been correctly marked and also stored. In operation, this was performed by showing the voter’s witness to a third-party, which then performs the cryptographic analysis and checks. However, in this scheme challenges arose in that verification could only be initiated by individual voters, but not by any third-parties like the auditors. In addition, use of third-party organizations meant that the voters' choices and passwords could be seen in other domains, due to the increasingly widespread use of modern password managers. The approach was also making voters vulnerable to compromised privacy.

New Cryptographic Voting Verifiable Scheme for E-Voting System (NCVVS)

New Cryptographic Voting Verifiable Scheme for E-Voting System (NCVVS) as presented by (Darwish & M El Gendy, 2017) was based on digital signature to implement the cryptographic protocols used to secure the communication channels to the legal users. The main target of the project was to design a more effective scheme for achieving higher security properties based on bit commitment infrastructure as well as digital signature technology. It was aimed at detecting and deterring, the improper behavior of the voter and invaliding any double votes, but facilitating the voter to prove that his vote is in correct form and maintaining voter privacy.

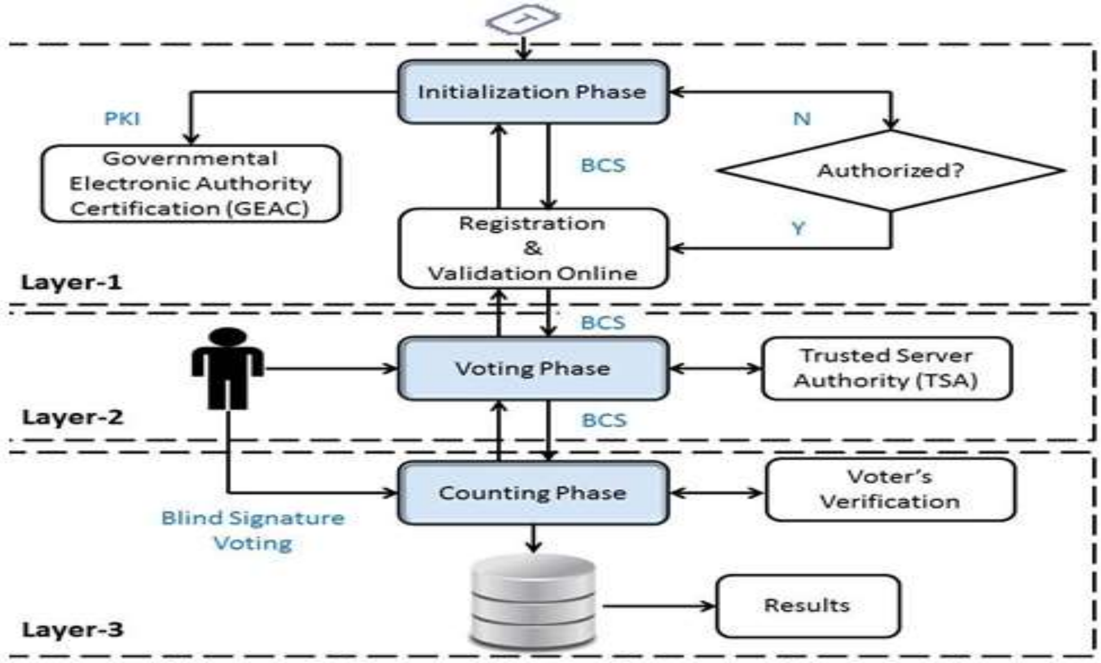

Figure 1: (NCVVS), Source: (Darwish & M El Gendy, 2017).

In operation, the NCVVS had three major layers: 1, 2 and 3 in conjunction with four phases as the initialization phase, registration of voters cum their online validation, voting and counting phases. A major contribution of the study was the presented verification process, which is only considered between voters and counting phases, where the voter unknowingly conducts blind signature voting which is ultimately reflected on the results. However, the technological complexities therein as analogous to the aforementioned reviews above which presented lack of acceptance and trust from voters as they could not understand them. Further, (NCVVS) performance results are not document hence its effectiveness may not be well established.

Crypto-voting

Fusco, Lunesu, Pani, and Pinna, (2018) project presented Crypto-voting, which is a block-chain based e-voting system, which sought to protect results and offer verifiability on the latest innovative technologies. The approach exploited the peculiarities of the block-chain technology characterized by distributed and decentralized data structures; where records exist in a chronological order called transactions. The transactions are supported by a peer-to-peer network, where it is possible to define a block in the chain as the set of information associated with each user's account only at a specific time. During transactions, all changes are recorded within a given block, whose content is used to calculate a hash. The whole chain becomes unchangeable since the hash code of a previous block forms part of the current block hash calculation.

However, the Bitcoin and Ethereum - which are the most popular block-chain systems employed, are public, implying that all transactions stored therein are publicly available; hence it is not possible to hide the data set associated with the sender and the recipient in any transaction. In support of this, Pinna, Tonelli, Orrú, and Marchesi, (2018) termed it as pseudo-anonymity because both the sender and recipient are revealed through an alpha-numeric code generally referred to as ”address” as used in tracing techniques. It was upon realization of this privacy issue, that Vote Coin, announced in 2014 and still under development, was proposed. It will be a decentralized system e-voting that exploits the privacy characteristics of Zcash in order to appreciably hide the link between voters and the voting system, (Tarasov & Tewari, 2017).

Agora voting platform for Digital democracy

Another system, albeit under development is Agora voting platform for Digital democracy (Agora Technologies, 2018), which is based on public block chain and on the sharing technologies to protect privacy of the voter. Agora uses cryptographic methods such as the El-Gamal system (Wang et al., 2018) to protect votes cast and a system called Neff shuffling, (Schaum et al., 2018) that offers protection for anonymity. The Agora voting platform was tested in one district during the March 7, 2018 general elections in Sierra Leone, and showed immutable system for vote safety, voter privacy and verifiability, (Rubtcova & Pavenkov, 2018).

Flow process

Agora voting system is made up of four technology layers while Agora's voting system proceeds in six stages;

1. During the initial configuration phase, the election administrator configures election parameters.
2. The second phase is the vote casting phase in which voters encrypt and submit their ballots.
3. The ballots are then sealed using the threshold of El Gamal cryptosystem. Before casting the vote, a locator which details the encrypted ballot is delivered to the voter. This locator helps the voter in individual verifiability.
4. The privacy phase follows, where the election authority runs all ballots via a mixing network to make the encrypted ballots cast anonymous on the Bulletin Board. This is achieved through using the Neff shuffling.
5. Once ballots have been anonymized, all the authorities collectively decrypt the ballots and publish them with decryption correctness proof, where the votes are then calculated so that the final result are published on the Bulletin Board.
6. Auditing phase comes last whereby if the election process is successfully verified, an eventual attestation is signed with the private key of the auditors.

However, according to Rubtcova and Pavenkov, system experts argued that since Agora system is based on Ethereum, which is a public block chain platform, privacy could be an issue. Besides, the local voters did not understand the complex operation process of the Swiss based e-verification system, hence lacked trust on the Agora. Apart from the one district used to test the system, the whole country conducted manual paper based voting as shown below.

S-Elect

Kusters, Müller, Scapin, and Truderung, (2016) developed s-Elect, which was a voting protocol based on additive homomorphism encryption in conjunction with two non-colluding parties aimed at preserving the essential security properties of an election such as integrity, verifiability and voter anonymity. It further involved implementation of a web front-end of the system with detailed web services architecture, database schemas, as well as the technologies for functional building blocks to aid the public in verifying election results. The voting framework operates as depicted in the figure below, where the voter connects through the internet proxy service to a broker. The broker has the front-end that provides end-to-end secure channels between the voter and some two back end servers. One server is the trustee server used for distributing sealed envelopes, while the tally server is responsible for receiving as well as counting the encrypted votes. At the cryptography level, the voting protocol is based on a three-way secure and verifiable e-voting built on Paillier's cryptosystem.

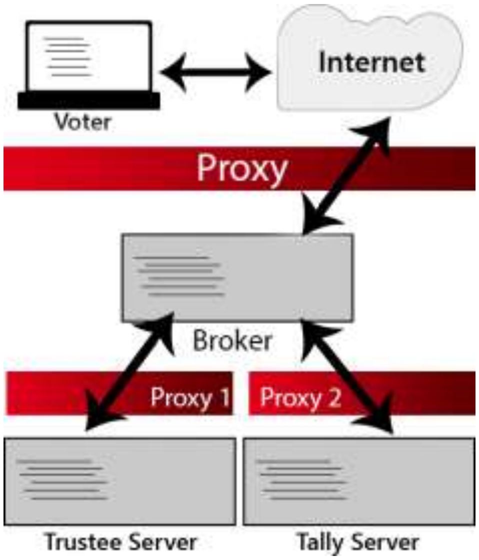

Figure 2: S-Elect, Source (Kusters et al., 2016)

The system theoretically achieved the preservation features, the essential security properties of election such as integrity, voter anonymity and verifiability of votes. However, it is established that cryptography in e-voting must be augmented with other security tools to be effective, since without this, the system may still be compromised without any signs of breaking the cryptographic protocols, (Estehghari & Desmedt, 2010). System complexity which hinder understanding among the voters was inherent in the s-Elect model. Voters were only interfaced with the internet voting system and could not understand the verification process involved, making it difficult for them to trust the system. Further, inconsistencies and complexity associated with the Paillier's cryptosystem would compromise the systems' transparency, (Cao & Liu, 2017). Moreover, the system test was only simulated with no actual voter participation to evaluate its practical performance.

Athena

Achenbach and Kempka (2015); & Smyth (2019) presented Athena, a verifiable, coercion-resistant voting model based on quadratic complexity with security equivalence of linear complexity. It further incorporated private and public key cryptography in the scheme. Universal verifiability which requires that anyone can check whether an election outcome corresponds to votes that are authorized was the major achievement of this model through it's 'verify algorithm'. The general design and operation principles also included an algorithm for tally, bulletin board, discard and ballots. These help the bulletin board to discard early votes, garbage, and unauthorized ballots as shown below. However, apart from not involving voters as a key element in the design, the verification process was made complex by the adoption of quadratic complexity and linear complexity security techniques, making the system not easily understood and trusted by the voters.

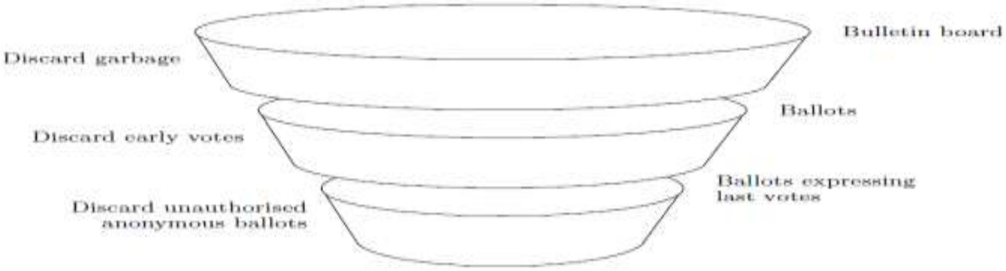
Bulletin board
Discard garbage
Ballots
Discard early votes
Ballots expressing last votes
Discard unauthorised anonymous ballots

Figure 3: Athena a verifiable coercion-resistant voting. Source: Achenbach & Kempka, C. (2015)

VoteBox

Sandler, Derr, and Wallach, (2008) developed VoteBox, through the application of cryptographic techniques and distributed systems. VoteBox, was a complete verifiable electronic voting system that combined VoteBox machines which were locally networked to allow all critical election events' broadcast and recording by every machine on the network.

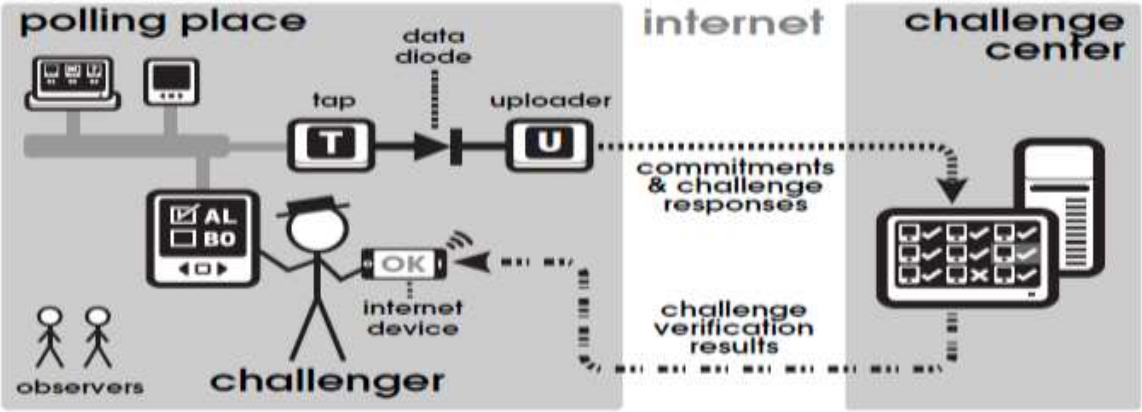

Figure 4: VoteBox, Source (Sandler et al., 2008)

The system comprises of the following components: The VoteBox network data, including encrypted votes, could be safely relayed internationally in real time, for transparency, thus allowing independent observers to validate the processes and results as it is running. It operated in the sense that as the voter advances past the review screen to the final confirmation screen, the system commits security to the state of the ballot by encrypting and publishing it. A challenger, having received the commitment in the form of encrypted ballot could then invoke the challenge function whose algorithm would be compelling it to reveal detailed contents of the encrypted ballot. In this case, a voter would simply choose to cast the ballot instead.

For verification, the polling place sends copies of all log data through a single channel to elections' central place like the headquarters, which aggregates similar data from many different election precincts and then republishes them. This way, third-parties would provide verification services to the system. While the system provided transparency to all the election stakeholders, verifiability approach did not include the voters. It was further complex and not easy to understand and appreciate, hence could not be trusted by the electorates (Coffé, 2017).

Belenios

Cortier, Gaudry, and Glondu, (2019) presented *Belenios*, a simple private and verifiable electronic voting system, which was found to be a seminal project on e-verification in electronic voting systems. The underlying cryptographic principles therein is multiple-key encryption in that encryption is based on a both public key while decryption is on a private key, which are shared between the three decryption authorities and only the final result is decrypted. Belenios ensures voter confidentiality as it makes elections transparent through the ballot box. It allows the voter to constantly check that his or her ballot (encrypted) was received in the ballot box.

This check is facilitated using a code, acting as the right to vote and issued to the voter by email. Besides protecting privacy, the system also guarantees end-to-end election verifiability. However, like the e-verification for electronic voting systems above, Belenios lacks the simplicity in the verification process, and has a capacity constraint, with a limit of 1000 voters for a single election. Further, while Cortier, Gaudry, and Glondu explcitly presented frameworks for election material generation, election key (code) generation, voting phase and tally phase, the study did not include the verification framework, thus making the vital process unclear.

Verify- Your-Vote (VYV)

Chaieb, Yousfi, Lafourcade, and Robbana, (2019) presented *verify- your-vote (VYV)*, a fully verifiable online electronic voting protocol based on blockchain. It involved cryptographic primitives based on both Identity Based Encryption (IBE) and Elliptic-Curve Cryptography (ECC) pairings to ensure authentication of the voter and that only eligible voter can vote, and also individual and universal verifiability. The verifiable voting system offers the possibility for auditing election processes and results at every stage of the election process. Once the election process and results are successfully verified, a final attestation is therefore signed with the authorities' cryptographic keys. However, for verification, each voter is required to access the blockchain system and check the existence of his counter-value in the entire list of reconstructed counter-values. Secondly, the homomorphism property of pairings is used to check accuracy of the count. However, lack of simplicity and understanding is in the protocol called ProVerif tool that only proved theoretically that the system can guarantee votes privacy, secrecy and authentication, as the system was not practically tested. Lack of simplicity on verification process and well as exclusion of voters from the verification process limits understanding and trust among the voters. Complexity in the verification is evident, as the study did not present any schematics for the verification process.

Voter Verifiable Paper Audit Trail (VVPAT)

Chandrashekar, (2017) succinctly elucidated the Voter Verifiable Paper Audit Trail (VVPAT) system as an independent printer system acting as a peripheral to Electronic Voting Machines (EVMs), for allowing the voters to verify that their votes have just been cast as they intended. VVPAT operates by generating a vote trail in form of a paper slip every time a voter casts the vote, thereby recording the party (political organizations and the contestants) to whose favour the vote has been cast. The paper slip is kept in a sealed cover, while the slip counting occurs in the VVPAT counting booths with close monitoring of the observers and direct oversight of the returning officer.

In India, for example, the balloting unit of the machine bears a list of candidates' names including their party symbols and a blue button next to it, which the voter presses to choose the candidate’s name they intend to vote for, (Pervez, 2015). Once the voter casts the vote on the electronic voting machine, the VVPAT printer peripheral generates a slip which shows the serial number, name as well as the symbol of the candidate chosen, thus serving the verifiability only for the vote cast for a very short time after casting the vote. Within 7 seconds, the VVPAT paper slip is displayed, after which it is automatically cut and dropped into a box in the VVPAT machine. This action prompts a beep sound for confirmation.

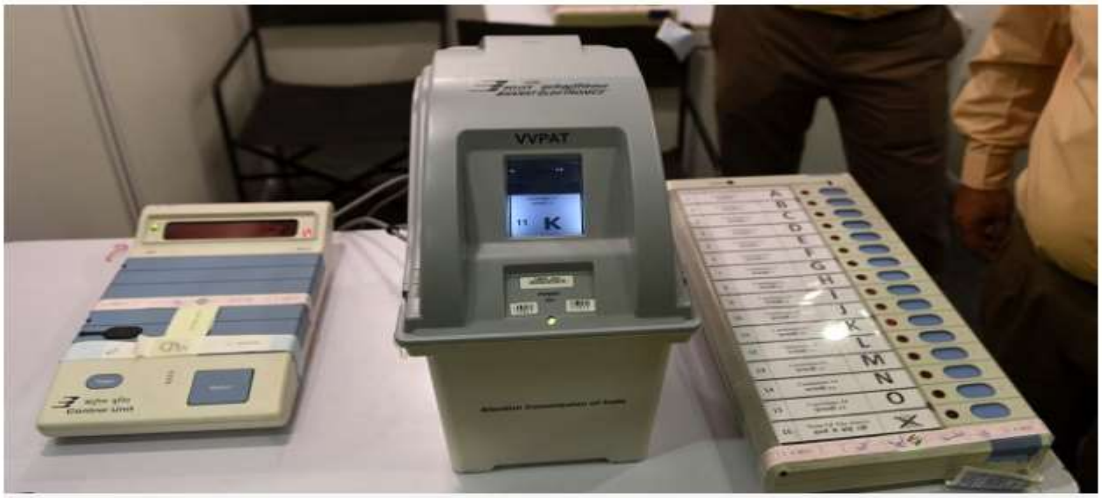

Figure 5: VVPAT attached to Electronic voting machines. Source: (Chandrashekar, 2017)

However, there have been numerous cases when the VVPAT prints wrong information creating doubts on its verification and auditing capacity. The verifiability only serves for the vote cast and for a very short time period of about 7 seconds. This however, cannot be a guarantee for any integrity in the proceeding process of voting like vote counting and tallying, (Chandrashekar, 2017). Further, being that VVPAT machines can be accessed by the election officers, who can access the collected slips and their corresponding serial matches, privacy and voter anonymity could be compromised.

The Findings

In summary, e-verification systems should not only be effective, accurate, secure (provide privacy/anonymity), accountable and facilitate both individual and universal verifiability, but should also be majorly simple with ease of understanding, involve the voters and build trust among them. Moreover, the e-voting system should provide a plausible way to re-open the e-ballot box upon court orders. However, the foregoing review indicated that while some systems presented apt models for both individual and universal verification of elections, most of the systems were vulnerable to privacy compromises and complex with technical sophistications rendering them difficult to understand by users, voters and administrators.

Helios for example, is a fairly simple protocol that voters may understand after sensitization, and then appreciate its capacity at privacy and end-to-end verifiability. S-Elect uses tracking numbers where voters can check that their vote has counted as cast. Agora is a seminal project in this perspective, however, a drawback is that while they provide an effective approach for verifiability, the cryptographic mechanisms is not understood among the voters and are also prone to breaching the voter anonymity. Further, the major limitation of the systems above is that they hardly involve the voters in the verification process. More limitations are that even those which involve the voters are found to be so complex, lacking the needed simplicity, and this makes the voters not to understand the processes involved, hence they do not trust them.

E-verification Model	**Analysis of the strength and the weaknesses**			
	Key Characteristics	**Key Technologies in use**	**strength**	**Weaknesses**
Scratch & Vote	Receipts validation of the previous voter	Digital signatures	Validation, privacy and universal verifiability	Lack of: Individual Verifiability, voter involvement, simplicity, voter understanding, trust and ballot re-opening
Scantegrity	Vote verification through unique three-digit confirmation, candidate position is paired with a unique random letter for confirmation by election officials	Optical scan technology	End to end verification, voter involvement, voter involvement	Lack of: simplicity , voter understanding , voter ability to open up the e-ballot box
RFVV	Receipt-free voter-verifiable	Blind signatures and homomorphism cryptography	Receipt-free voter verifiability, voter and universal verifiability	Lack of: privacy, voter understanding, re-opening the ballot and voter trust.
Helios	Third-party websites and mobile apps to verify votes cast	Homomorphism encryption,	Achieved verification at 80%, individual verifiability and voter involvement	Lack of: privacy, universal verifiability, voter understanding, re-opening the ballot and voter trust.
NCVVS	Security based on bit commitment infrastructure and digital signature	Digital signature	Privacy and vote integrity and verifiability	Lack of: practicality, voter understanding, re-opening the ballot and voter trust.
Crypto-voting	Distributed and decentralized transactions supported by a peer-to-peer network	Block-chain	Vote integrity and verifiability, voter involvement, individual cum universal verifiability	Pseudo-anonymity and lack of: practicality, voter understanding, re-opening the ballot and voter trust.
Agora	Public block chain and the sharding mechanism that protects the privacy of the voter	Public block-chain and El-Gamal cryptographic system	Transparency and traceability of ballot data	Lack of: real anonymity, voter understanding, re-opening the ballot and voter trust.
s-Elect	Voter connection through internet proxy service to a broker with front-end that provides end-to-end secure channels between the voter and two back end servers.	Additive homomorphism encryption	Vote integrity, verifiability and voter anonymity	Security vulnerabilities, lack of voter understanding, opening the ballot and voter trust.
Athena	Verifiable, coercion-resistant voting model based on quadratic complexity with security equivalent of linear complexity	Private and public key cryptography	Universal verifiability	Lack of voter involvement, understanding and trust. opening the ballot is difficult
VoteBox	A challenge function whose algorithm can reveal detailed contents of the encrypted ballot in real time	Distributed systems and cryptography	Strong end-to-end security guarantees to voters. universal and individual verifiability	Inadequate privacy, voter involvement, understanding and trust. opening the ballot is difficult

Belenios,	Multiple-key encryption infrastructure	Public and private key encryption	Privacy, end to end verifiability,	Limit of 1000 voters per election. Complexity, not widely understood and trusted among the voters. inability to open the ballot ox
Verify-Your-Vote	Blockchain contracts and ProVerif verification tool	Identity Based Encryption, block chain and Elliptic-Curve Cryptography	Auditing election processes and results at every stage,	Lack of simplicity, understanding and trust among voters and exclusion of voters. Not possible to open the e-ballot box. No system testing or verification schematics
VVPAT	Paper based audit trail	Nil	Ballot verifiability simple	Lack of privacy and anonymity. Cannot ensure vote integrity after the voter leaves, neither individual nor universal verifiability of election results.

Table 1: A review of relevant e-verification models for electronic voting.

Conclusion and further research

There is need for verification of results as reviewed in the foregoing sections. Most of the e-verification models have not adequately met the security, privacy, verifiability and most importantly, the elements of: simplicity, voter involvement, and voter understanding and voter trust of the verification systems. While some resultant models attempted to appreciably address the ballot verification issue just after it has been cast, the verification approaches were found so complex, with little involvement of the voters that they were inadequately understood by the voters, who in turn lacked trust in the models. Further, most of the cryptographic approaches applied lacked the provision of re-opening the e-ballot boxes as may be required by a court order for verification in cases of disputed elections. There is a need for a simple election results' verification system that is widely understood and trusted among the voters, wherein e-ballot boxes can be re-opened for verification upon court orders to improve verifiability of elections results in Kenya and world-wide.

References

Achenbach, D., & Kempka, C. (2015). Improved Coercion-Resistant Electronic Elections through Deniable Re-Voting. USENIX Journal of Election Technology and Systems.

Aguiar-Conraria, L., Magalhães, P. C., & Veiga, F. J. (2019). Transparency, Policy Outcomes, and Incumbent Support. Kyklos. https://doi.org/10.1111/kykl.12203

Barnes, A., Brake, C., & Perry, T. (2016). Digital Voting with the use of Blockchain Technology. Retrieved from https://www.economist.com/sites/default/files/plymouth.pdf

Birch, S., & Muchlinski, D. (2018). Electoral violence prevention: what works? Democratization. https://doi.org/10.1080/13510347.2017.1365841

Cao, Z., & Liu, L. (2017). The paillier's cryptosystem and some variants revisited. International Journal of Network Security. https://doi.org/10.6633/IJNS.201701.19(1).10

Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2019). Verify-your-vote: A verifiable blockchain-based online voting protocol. Lecture Notes in Business Information Processing. https://doi.org/10.1007/978-3-030-11395-7_2

Chandrashekar, K. (2017). Emerging Trends in Electoral System: Revolutionary Transformation through the Information Technology. International Journal of Trend in Scientific Research and Development. https://doi.org/10.31142/ijtsrd5968

Chege, M. (2018). Kenya's Electoral Misfire. Journal of Democracy. https://doi.org/10.1353/jod.2018.0034

Coffé, H. (2017). Citizens' media use and the accuracy of their perceptions of electoral integrity. International Political Science Review. https://doi.org/10.1177/0192512116640984

Conrad, F. G., Bederson, B. B., Lewis, B., Peytcheva, E., Traugott, M. W., Hanmer, M. J., ... Niemi, R. G. (2009). Electronic voting eliminates hanging chads but introduces new usability challenges. International Journal of Human Computer Studies. https://doi.org/10.1016/j.ijhcs.2008.09.010

Cortier, V., Eigner, F., Kremer, S., Maffei, M., & Wiedling, C. (2015). Principles of Security and Trust. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). https://doi.org/10.1007/978-3-662-46666-7

Cortier, V., Gaudry, P., & Glondu, S. (2019). Belenios: A Simple Private and Verifiable Electronic Voting System. https://doi.org/10.1007/978-3-030-19052-1_14

Cortier, V., & Lallemand, J. (2018). Voting: You Can't Have Privacy without Individual Verifiability. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS '18. https://doi.org/10.1145/3243734.3243762

Darwish, A., & M El Gendy, M. (2017). A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature. International Journal of Swarm Intelligence and Evolutionary Computation. https://doi.org/10.4172/2090-4908.1000158

Estehghari, S., & Desmedt, Y. (2010). Exploiting the Client Vulnerabilities in Internet E-voting Systems: Hacking Helios 2.0 as an Example. Helios.

Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018). Crypto-voting, a Blockchain based e-Voting System. https://doi.org/10.5220/0006962102230227

Gastil, J., & Meinrath, S. D. (2018). Bringing Citizens and Policymakers Together Online: Imagining the Possibilities and Taking Stock of Privacy and Transparency Hazards. Computer. https://doi.org/10.1109/MC.2018.2701623

Kalchgruber, P., & Weippl, E. R. (2010). Can end-to-end verifiable e-voting be explained easily? https://doi.org/10.1145/1806338.1806446

Kiayias, A., Zacharias, T., & Zhang, B. (2017). An Efficient E2E Verifiable E-voting System without Setup Assumptions. IEEE Security and Privacy. https://doi.org/10.1109/MSP.2017.71

Komarova, A., Menshchikov, A., Negols, A., Korobeynikov, A., Gatchin, Y., & Tishukova, N. (2018). Comparison of authentication methods on web resources. Advances in Intelligent Systems and Computing. https://doi.org/10.1007/978-3-319-68321-8_11

Kusters, R., Müller, J., Scapin, E., & Truderung, T. (2016). SElect: A lightweight verifiable remote voting system. Proceedings - IEEE Computer Security Foundations Symposium. https://doi.org/10.1109/CSF.2016.31

Laksono, F., & Agustine, O. V. (2017). Election Design Following Constitutional Court Decision Number 14/PUU-XI/2013. Constitutional Review. https://doi.org/10.31078/consrev223

Mwighusa, D. N. (2015). Transforming Voters Registration Paradigm in Tanzania, The Shift from OMR to BVR. International Journal of Science and Research (IJSR).

Neumann, S., Olembo, M. M., Renaud, K., & Volkamer, M. (2014). Helios verification: To alleviate, or to nominate: Is that the question, or shall we have both? Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). https://doi.org/10.1007/978-3-319-10178-1_20

Pervez, M. D. (2015). Establishing New Social Contract Across Territorial Boundaries of Pakistan is the Need of Time. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2684755

Pimenidis, E. (2017). E-Voting vs E-Trust: A test bed for e-Democracy in a World in Crisis. International Journal of Electronic Governance. https://doi.org/10.1504/ijeg.2017.10006254

Pinna, A., Tonelli, R., Orrú, M., & Marchesi, M. (2018). A petri nets model for blockchain analysis. Computer Journal. https://doi.org/10.1093/comjnl/bxy001

Popan, J. R., & Hinojosa, Y. (2017). Electoral participation among young latinos: Exploring the importance of psychological variables. Journal of Latina/o Psychology. https://doi.org/10.1037/lat0000066

Republic of Kenya. Elections Act, Subsidiary Legislation. , Kenya Gazette Supplement No. 24 of 2011 § (2016).

Rubtcova, M., & Pavenkov, O. (2018). Implementation of Blockchain Technology in Electronic Election in Sierra Leone. Proceedings of the Conference "Re-Thinking Regions in Global International Relations", Philippines 23.03.2018 - 24.03.2018.

Sandler, D., Derr, K., & Wallach, D. S. (2008). VoteBox: a tamper-evident, verifiable electronic voting system. Proceedings of the 17th Conference on Security Symposium.

Schaum, N., Karkanias, J., Neff, N. F., May, A. P., Quake, S. R., Wyss-Coray, T., … Weissman, I. L. (2018). Single-cell transcriptomics of 20 mouse organs creates a Tabula Muris. Nature. https://doi.org/10.1038/s41586-018-0590-4

Schnegg, M., Rieprich, R., & Pröpper, M. (2014). Culture, nature, and the valuation of ecosystem services in northern Namibia. Ecology and Society. https://doi.org/10.5751/ES-06896-190426

Tarasov, P., & Tewari, H. (2017). Internet voting using Zcash. Proceedings of the International Conference on WWW/Internet 2017 and Applied Computing 2017.

Teutsch, J., & Reitwießner, C. (2017). A scalable verification solution for blockchains. Url: Https://People. Cs. Uchicago