Digital Forensic Readiness Model for Internet Voting

Edmore Muyambo[1] and Stacey Omeleze Baror[2]
[1]DigiForS Research Group, Dept of Computer Science
[2]University of Pretoria, Pretoria, South Africa

Edmore.muyambo@tuks.co.za,
Stacey.baror@cs.up.ac.za

Abstract: Voting is an exercise of choosing a preferred candidate through a process called an election. In many countries, this exercise is a basic human right. In every election process, there are some pre-requisite processes and procedures which must be set up first. These are essential in the pre-vote-casting stage, during vote-casting and post-vote-casting stage. Electoral disagreements amongst stakeholders and parties of interest are usually experienced in each of the above-mentioned voting process stages. The main points of conflict in an election process are vote rigging and vote fraud. Failure to amicably mitigate these issues can result in a criticised/rejected election result. Therefore, this research aims to address the problem of vote rigging and vote fraud allegations in an election process. The resolution thereof is achieved through the introduction of an online based voting system which is supported by a digital forensic readiness mechanism. Online voting system gives citizens the flexibility to use internet-enabled devices such as cell phones and laptops to cast their votes in a safe, secrete and secure protocol. To address the problem of vote rigging and vote fraud, the online voting system is integrated with cyber security and vote protection mechanisms. The cyber security and vote protection mechanism is based on Blockchain algorithms. A Blockchain-based voting process is a peer-to-peer mechanism where a decentralised database is used to store data. Tokens move directly from one peer (voter) to another peer (candidate). The results are tallied by counting the number of tokens paid to each candidate. Each voter is allocated a Bitcoin token and each candidate is allocated a Bitcoin address. During vote casting, the voter transfers their Bitcoin token into the wallet of a registered candidate. At the end of the voting process, the total number of Bitcoin tokens transferred to each candidate is counted and tallied up. The wallet is loaded with only one Bitcoin token, hence there is no possibility of double voting. The model ensures vote security, anonymity, auditability, accountability, accuracy and uniqueness.

Keywords: Blockchain, Internet Voting, Electoral Data Privacy and Data Security, Cyber Security, Digital Forensic Readiness, Online Voting

1. Introduction

Voting is a process of secretly selecting an option of choice from the available options. The process thereof is called an election. Sovereign states and countries make use of the voting process to elect national leaders i.e. Presidents and/or legislators/parliamentarians.

Each country conforms to its voting mandate as stipulated in its national constitution. For example, In Zimbabwe citizens head to national polls once after every five years. The presidential terms in office are limited to two only (Makumbe, 2014). Whereas in China the presidential term limit has been dealt away with (Jiang et al.,2022). Every voting process follows a pre-set process flow. For example, in a traditional voting process, all legible voters are required to pre-register with the election administration board. The voter registration process verifies the eligibility of the voter for vote casting. The ballot paper-based voting system comes with several loopholes. These include the lack of a fool-proof vote auditing mechanism. These loopholes have been identified to be the main causes of disputed elections, vote rigging and vote fraud allegations. The traditional voting process (ballot paper-based system) can be easily manipulated to facilitate vote rigging and vote fraud as the process involves a lot of manual human activities such as ballot paper printing, ballot paper transportation, manual vote counting and results presentation (Srivastava, Dwivedi and Singh, 2018). When ballot papers are in transit to the command centre for final vote tallying, there is a high risk of getting votes tampered with as human security can be easily compromised. The manual counting process is prone to human error as well as intentional vote manipulation. This opens up a risk of announcing unverifiable and untrusted manually audited votes. Therefore, as a way of mitigating the shortcomings of the traditional (paper-based) voting system; this paper is hereby introducing the Digital Forensic Readiness Model for Internet Voting (DFRMIV). DFRMIV is an online-based technology that can be used to instantaneously flag vote rigging and vote fraud activities in an internet-based voting system. Audit trails and data logs are used to trace electronic vote movement from the polling station to the command centre data centres and the final stage of results presentation. The final results are tallied and reconciled against the votes cast. Election results are expected to perfectly tie back with the votes cast at individual polling stations. If there is any difference picked between the votes cast and the results presented the model would immediately flag a possible vote rigging activity. The DFRMIV would then accurately flag all the numerical differences picked and give a detailed view of the vote deviation.

DFRMIV makes use of some end-to-end encryption algorithms such as Blockchain to protect data integrity. Blockchain preserves vote integrity by its inability to be cracked by hackers and fraudsters. Voting transactions are stored in blocks which are in turn stacked together into a chain of decentralised node ledgers. Data stored on a centralized database through this technology cannot be altered or tampered with. Parties of interest can make use of the DFRMIV's findings to challenge an election outcome. The model's findings show valid scientific proof of any vote-tampering activities which could have happened. This makes the findings eligible for use in a court of law to challenge any vote rigging or vote fraud issues.

Therefore, the problem statement of this paper is that currently there is no digital forensic readiness process that addresses vote rigging and vote fraud issues either in the online voting process or the ballot paper-based process. The main electoral phases vulnerable to vote rigging and vote fraud are, during ballot paper printing, vote casting, ballot paper transportation, results counting and during results presentation.

This paper is structured as follows: Section 2 discusses the background and literature review. Section 3 discusses the proposed model. Section 4 collectively states discussion points. Section 5 presents the conclusion of the research and Section 6 provides a list of references used in this paper.

2. Background

As of now, majority of countries still make use of the ballot paper-based voting system (F.M.Mursi *et al.*, 2013). This means only a small number of countries have adopted the electronic voting system. Most countries reject the internet voting system sighting lack of trust in the system, its complexity and lack of operational skillset.

The ballot paper-based voting system involves a lot of manual interventions. This makes it prone to human errors, mistakes and vote manipulation. This makes the whole system vulnerable to vote rigging and vote fraud. The ballot paper-based voting system used to have the greatest trust threshold during its inception years. However, trust in the system is fast dwindling due to its vulnerability to vote rigging allegations, more so in Africa. In Zimbabwe, during the 2013 election season, the main opposition party (then) Movement for Democratic Change (MDC) claimed that some fraudulently printed ballot papers were used to illegally award the ruling party candidates some rigged votes (Magaisa, 2019). They also claimed that ballot papers used contained some tampered chemical composition which would facilitate vote rigging through a chemical process called paper chromatography. Paper chromatography is a scientific chemical reaction process that dissolves, extracts and precipitate the atomic composition of the subject matter in question (ballot paper in this case) (ROBERTS and WOOD, 1951).

Given the ever-increasing global warming challenges, a paperless based voting system would be a great gesture of embracing the fight against global warming.

Concerns in the online voting system include security issues, privacy, accountability, accuracy confidentiality and trust (Muneer and Shamail, 2013). However, all these concerns can be resolved by the digital forensic readiness framework. A well-integrated online voting system would include a series of interlinked systematic nodes that store, verify, authenticate and present a user-friendly election voting interface. (Matharu, Mishra and Chaudhary, 2014). For a smooth transition, the public would need to be imparted with online voting knowledge. This includes making it clear to voters how the system works and how vote security and confidentiality are preserved by the system in an end-to-end process. Security is a top priority in an electronic voting process (Sharkey and Paynter, 2003). The advantages of introducing a digital forensic readiness model in internet voting included vote fraud prevention, improved vote counting time and results announcement, cost efficiency and reduced number of spoiled ballots (Pawlak and Poniszewska-Marańda, 2019). To gain more community trust in the online voting system, the system must provide vote security and user identity protection. All votes cast must be audited and accounted for. Audit trails must be freely available for all to see. One of the efficient ways to meet the above-mentioned points of concern is through the use of the digital forensic readiness model in the online voting system. The digital forensic readiness model makes use of the Blockchain system to facilitate end-to-end vote security.

2.1 Blockchain System

“Blockchain is a peer-to-peer system based on a decentralised, un-tampered, open and transparent ledger that looks like a read/write database because the data stored cannot be altered” (Rabia, Sara and Gadi, 2021). The technology is popularly known for its robust security mechanism in the digital currency technology called Bitcoin. All transactions and the history of all transactions exchanged between users are stored in a grouping called a

ledger. Blockchain is not controlled by any single authority. It is sharable amongst various users. This allows everyone to check the validity of the chain. (Rabia, Sara and Gadi, 2021). It is visible to all users in it, hence transparency and auditability by any of the users. Blockchain is a safe and secure way of preserving data security. Transactions are stored in blocks which are in turn stacked together into a chain of decentralised node ledgers. Data stored on a centralized database through the means of Blockchain cannot be altered or tampered with. Hence its suitability for use in online voting systems and the digital forensic readiness model.

The Blockchain system is categorized into three groups which are, Public Blockchain (anyone can access and have visibility of transactions in the ledger), Consortium Blockchain (partially decentralised and controlled by more than one organization), Private Blockchain (managed and authorises user participation) (Rabia, Sara and Gadi, 2021).

- The public chain has open access to anyone. Everyone can access, send, receive and authenticate transactions. The mechanism which determines the block to be added to the chain is that everyone can participate and all transactions are open and anonymous. (Chen, Chen and Lin, 2020).
- A Consortium Blockchain is a partially decentralised system that is controlled by more than one organization that can act as a node.(Rabia, Sara and Gadi, 2021).
- A private chain is a completely private Blockchain. All write permissions are only held and managed by the owner. Reading permissions outside the chain may be partially restricted. The whole of the private chain is maintained by all members. This category is characterized by fast transactional speed, low cost, protection of transaction privacy and immutability. However, the degree of private chain centralization is relatively high and it is difficult to achieve consensus trust. (Chen, Chen and Lin, 2020).

Privacy and verifiability are the main aspects of internet voting. Blockchain technology can be semantically integrated with the internet voting process to provide a safe and secure online voting process. Although the Blockchain-based data encryption process is very costly, its high-end security mechanism validates the digital forensic processes.

2.2 Digital Forensic

Digital forensic is a process of answering questions about digital data's current and previous state of events (Shanmugam, 2015). This process can be initiated by digital data attack detection, policy misconduct or unauthorized digital data activities. An investigation can be live (occurs as the system is online) or dead (occurs when the system is offline). Countermeasures can be developed and deployed to eradicate system attacks. These include making use of the Blockchain system to detect data tempering activities and flag them out through authentic audit trails. The digital forensic readiness mechanism provides for an authentic, robust yet transparent vote auditing mechanism. Hence, attempted vote rigging and vote fraud activities would be detected and flagged for all parties of interest to see. Therefore, vote integrity is preserved. Direct beneficiaries of digital forensic readiness for online voting include political parties, independent candidates, electoral boards, election observers, legal services, police force and citizens at large (Gloe, Kirchner and Böhme, 2007). Each group of beneficiaries can access and use digital forensic findings as per their needs. For example, the police force can make use of the digital forensic readiness findings in their investigations to lounge an arrest. The legal services can also make use of the digital forensic readiness findings to lay charges or defend the accused. Election observers can make use of digital forensic findings to give a well-informed report to the international community on how free and fair the whole election process was. Section (3) below gives a detailed view of the proposed digital forensic readiness model. In essence, the model comprises of four main processes. These are; the vote casting process, data storage and the vote reconciliation process. After a voter casts their vote, data gets stored in the electoral board's data store and the digital forensic data store simultaneously. The vote reconciliation process would then run on top of the two data stores to compare and contrast data integrity. Any form of vote tempering would be picked up by the reconciliation process. A report would be generated and presented to stakeholders of the election process for further action.

3. Digital Forensic Readiness Model of Internet Voting

3.1 Introduction

To mitigate issues of vote rigging and vote fraud, this paper introduces the digital forensic readiness model of internet voting. The model is made up of four main layers. These are; the vote casting layer, digital forensic data store, electoral board data store and the vote reconciliation layer.

The main components of the DFRMIV's high-level view are the voting process, electoral board vote processing, digital forensic vote processing and the vote reconciliation process as shown in Figure 1 below. When a vote is cast, it goes through the Blockchain encryption technology. This technology makes sure that the vote is secure, safe and auditable. After the encryption process, votes get simultaneously stored in the Electoral Board's data repository and the Digital Forensic data repository. The Digital Forensic Readiness process would then merge the two datasets and perform a vote reconciliation process. If there are vote irregularities or vote rigging attempts, the vote reconciliation process would flag this.

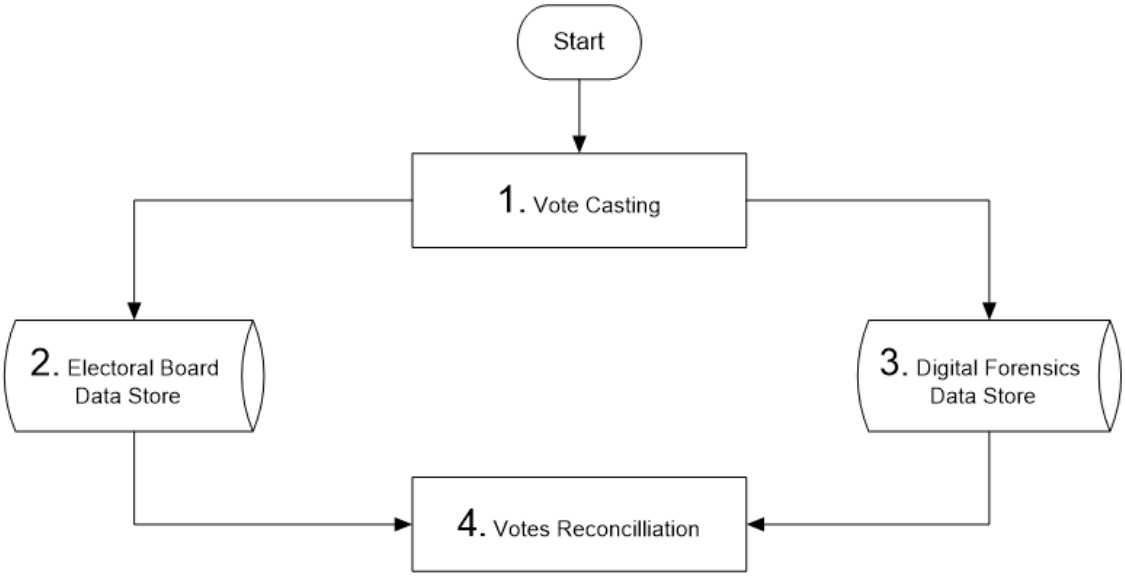

Figure 1: High-Level View of the Digital Forensic Readiness Model for Internet Voting

The Four Main Components of DFRMIV

3.1.1 Vote Casting

This is the starting point of the election process. Before vote casting, every voter is required to register to vote. On the Election Day system users would log into the voting system for the vote casting process to begin. Once the user has been successfully verified against the voter's roll and authenticated, they can proceed to the vote casting phase. The user chooses a candidate of their choice and submit the selection. When the submission process is successful the user will be automatically logged out after getting a success status confirmation and the reference number.

3.1.2 Digital Forensic Data Store (DFDS)

When votes are cast, they are simultaneously distributed into two data repositories which are the Digital Forensic Data Store and the Electoral Board Data Store. The Digital Forensic Data Store stores raw data of the votes cast. This dataset is used for digital forensic investigations which include vote rigging detection. DFDS is not government owned, it is owned by independent service providers.

3.1.3 Electoral Board Data Store (EBDS)

Vote's dataset is multicast into the DFDS and the EBDS. This means by default the two data stores should contain the same number of votes. If at one point the two contain a different number of votes, a possible vote rigging activity would have occurred. The EBDS is used by the Electoral Board for vote counting, auditing and results presentation.

3.1.4 Vote Reconciliation

This is a Digital Forensic Readiness component. Datasets from both data stores are merged and compared against each other. A difference between the datasets would mean a possible vote rigging activity has occurred. The DFRMIV would automatically detect this and flag all the numeric deviations in detail.

A detailed diagrammatic view of the above four mentioned components of the DFRMIV is shown in Figure 2, Figure 3, Figure 4 and Figure 5 below.

3.2 Vote Casting

The first stage of the voting phase is to identify the voter. After a successful user identification, the system then goes on to verify the user's existence in the voter's roll. If the user's voter registration status gets confirmed successfully they will now be allowed to log into the voting system for vote casting. Once successfully authenticated and logged in, the user can now cast their vote. As soon as the vote is cast, the encryption process (Blockchain) gets triggered automatically. This is one of the most important stages of the digital forensic readiness model as it uniquely identifies each vote and takes account of every vote cast. The system would give a success signal if the vote has been successfully captured and transferred into the secure vote repositories. If a technical error such wrong user name/password or user identification failure the system would direct these glitches to the Help Desk team for further assistance.

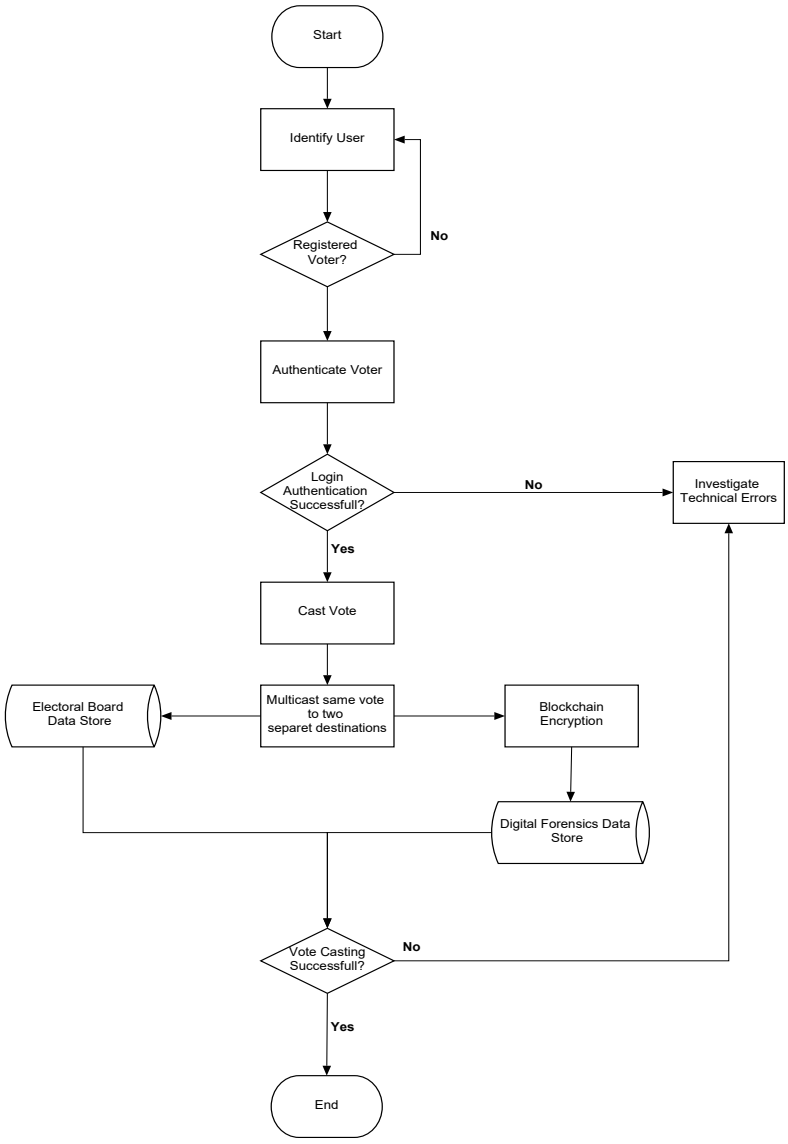

Figure 2: The Vote Casting Process

Components of the Vote Casting Process

Start: The start point of the voting process. The voter gets access to the internet voting device. This can be done either from the comfort of their home or from a polling booth with internet-enabled devices.

Identify User: The user trying to access the voting system gets verified and identified. This is a username and password verification process which is administered by the voting system. This is the first phase of user authentication and it is performed against the system user database. Access to the voting system is granted once the verification and authentication process succeeds.

Registered Voter?: After a successful system log-in, the system checks if the user is a registered voter. This is performed against the voter's roll database. A voter's roll database is managed and maintained by the election administering board.

Authenticate Voter: Once the voter's eligibility for vote casting has been verified and confirmed, the voter gets authenticated for vote casting. This is the second phase of voter authentication. This happens after verifying the user in the system and after verifying that the user is indeed a registered voter.

Voter Authentication Successful?: This is the grand authentication status. If the voter has been successfully identified and verified in all the two stages of voter administration they will then be presented with a voting page. The voting page contains all election candidates as well as the vote casting functionality. If voter authentication fails, the user would be directed to the system's help desk for authentication failure investigations.

Investigate Technical Errors: Voter authentication failures are redirected to the help desk team for further investigations.

Cast Vote: Voter gets to select a candidate of their choice from the presented options on the vote-casting screen. This is achieved by simply clicking on the candidate of choice and clicking the submit button.

Encrypt Vote Data: Soon after vote casting, the vote gets encrypted by Blockchain technology. This is a peer-to-peer process of encrypting the vote and protecting it from illegal manipulation by the way of vote rigging.

Vote Casting Successful: The system check and confirmation whether the vote casting process has completed successfully or not. If yes the process ends right there but if not then the process gets redirected to the system's help desk for vote casting failure investigations.

End: The voting is considered to be complete once the voter has successfully cast their vote. This marks the end of the entire vote casting process.

3.3 Electoral Board Data Store

After a vote has been cast, its next destination is the data repository. In this model, there are two data repositories involved. Firstly the Electoral Board Data Store (EBDS) and secondly the Digital Forensic Readiness Data Store (DFRDS). Votes are stored simultaneously in both repositories as they trickle in from the polling stations. The EBDS is owned by the state. It is used for all the vote administration and processing processes such as vote counting, report presentation and statistical data analysis.

Components of the Electoral Board Data Store Process

Start: Initiation of the vote storage process. After the voter has cast their vote, the voting system takes over the vote transmission process. This is the begging of the process where the vote cast is electronically moved from the front-end (voting application) to the back-end (database).

Cast Vote Transmission: This is an electronic movement of votes from the casting device to the data store repository through a secure internet protocol. Every vote is transmitted safely and securely through the Blockchain encryption process. The encryption mechanism secures the vote and protects it against illegal vote tampering processes such as vote rigging and vote fraud.

Vote Storage: The encrypted votes land into the data store. This can be a SQL Database (On-Premises or Cloud). The data store is also safe from illegal access and illegal data transformation process. The database is equipped with cutting-edge technology that protects the votes cast. Attempted data tampering activities with the intention of vote rigging and vote fraud are picked up and reported in data logs and audit trails.

Vote Storage Successful? A systematic check to ascertain if data has been successfully stored in the repository or not. This check confirms data integrity, anonymity, accountability and availability.

End: This marks the end of the data storage process into the electoral board data store. Successful data storage means the dataset can be accessed by authorized processes only at any time.

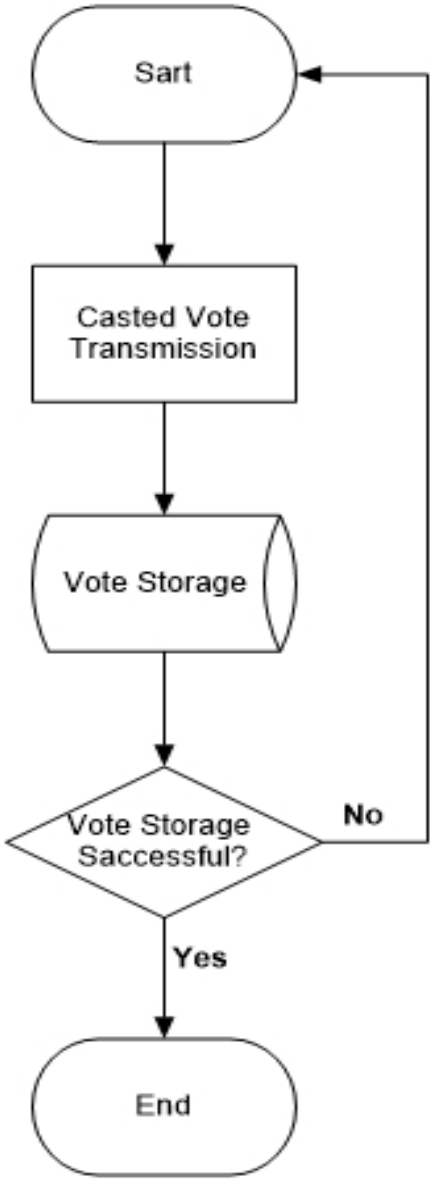

Figure 3: Electoral Board Data Store

The following section explains the Digital Forensic Readiness Data Store process. A detailed data flow process is depicted in Figure 4 below.

3.4 Digital Forensic Data Store

The capturing of data into the digital forensic data store and the electoral board's data store happens simultaneously. The digital forensic data store is not state-owned. The transmitted vote is validated against its Blockchain encryption token. The DFRMIV runs vote tempering checks on top of this data store. This is where the vote rigging attempts are automatically picked and flagged by the DFRMIV system. Data in this repository is verified, safe, authentic and auditable.

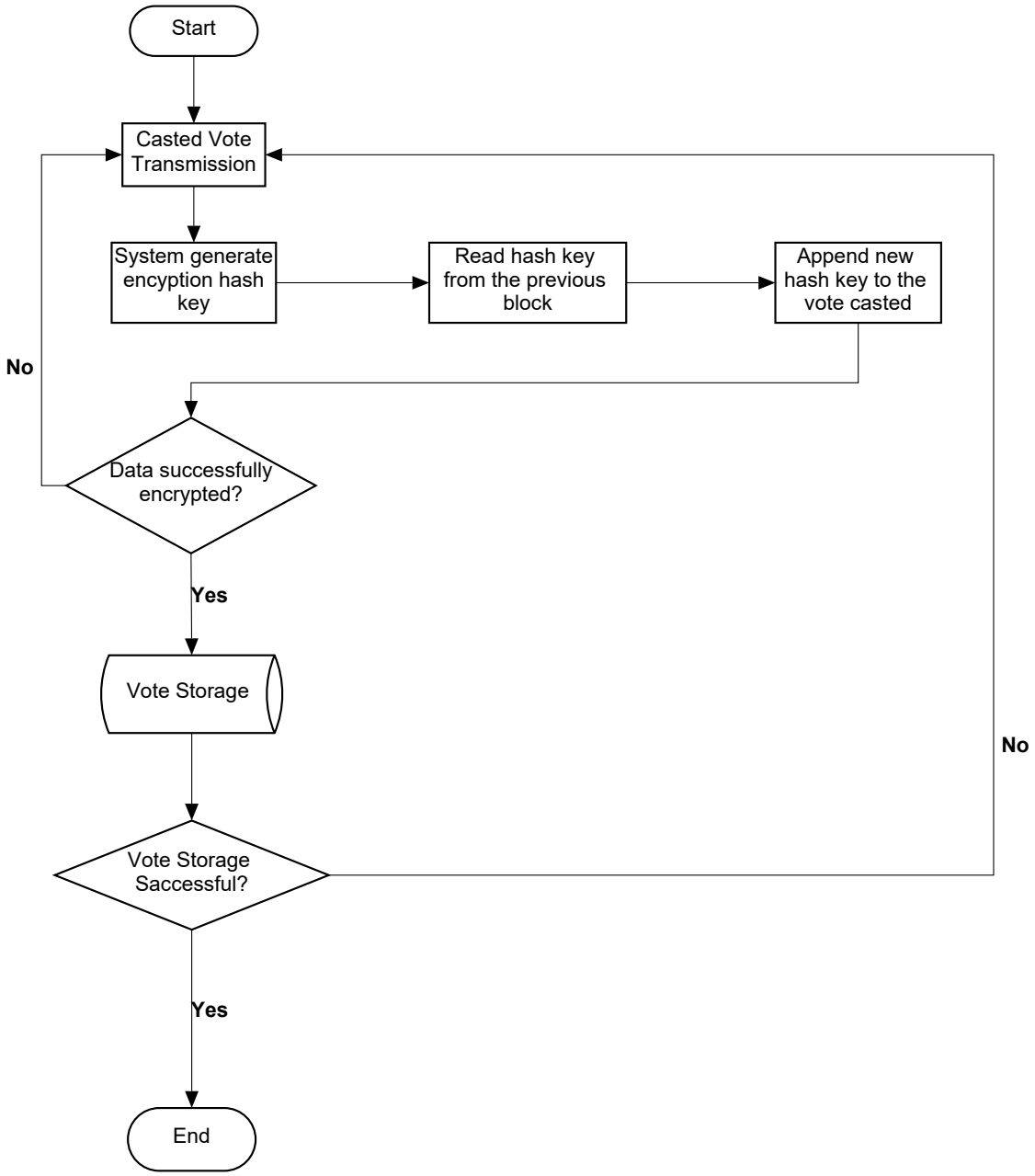

Figure 4: Digital Forensic Readiness Data Store

The stage which follows i.e. the Vote Reconciliation process relies on the Digital Forensic Readiness Data Store to reconcile the election data. Figure 5 below details more on this.

3.5 Vote Reconciliation

The vote reconciliation process references the electoral board's data store and the digital forensic data store to perform a comparison test as a way of vote reconciliation. The Digital Forensic Readiness dataset is considered to be whole, clean and un-tampered with as it went through a series of rigorous vote security mechanisms. A vote rigging flag is raised when the comparison process finds vote mismatches. All vote tempering activities are caught and flagged out at this section of the model. The two datasets are expected to be exactly the same.

A detailed report showing all vote differences and numerical variances is generated by the Digital Forensic Readiness model. Numeric mismatches and data irregularities get logged in audit log trails. The report's contents and audit logs can be referenced by all election stakeholders or beneficiaries. They can also be used in legal processes for vote rigging allegations cases.

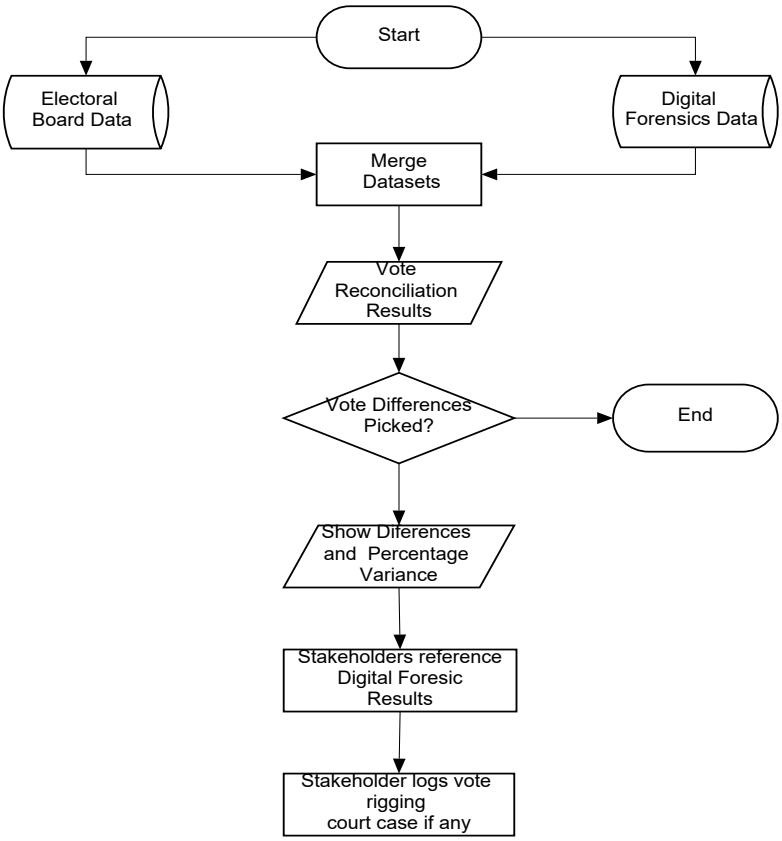

Figure 5: Votes Reconciliation

Figure 6 below shows a holistic view of the entire DFRMIV's integrated components on a lower-level view. The first block encloses the voting process, the second block encloses the data repository mechanism and the 3rd block encloses the vote reconciliation process.

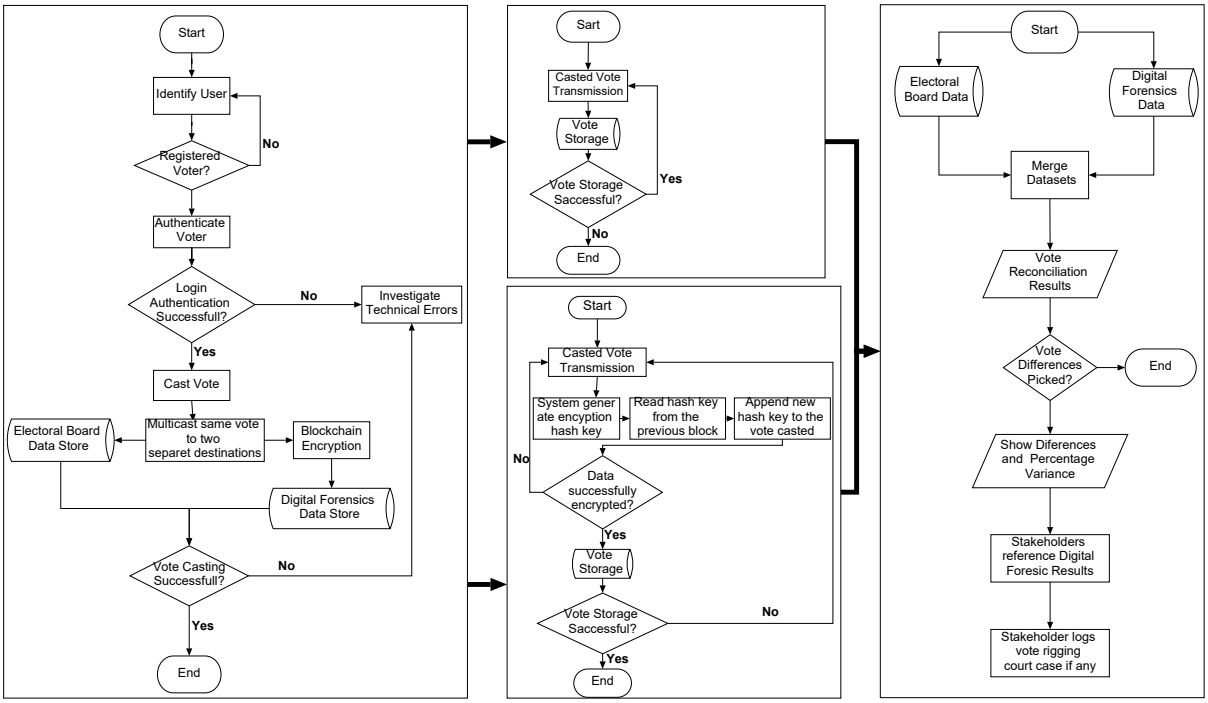

Figure 6: A holistic view of the DFRMIV

4. Discussion

Digital forensic is a scientific data investigation process that makes use of advanced mathematical algorithms to examine data integrity (Thron, Dirnberger and Quirchmayr, no date). Amongst them is the Blockchain technology. Blockchain makes use of advanced security mechanisms to preserve data integrity, security, confidentiality and anonymity. These characteristics make Blockchain the best fit for the development of a tamper-proof digital platform. (Wang, Yang and Hsiao, 2020). Therefore, this technology can be effectively employed in the online voting processes to address issues of electoral fraud, vote rigging and corrupt vote administration issues as it provides a transparent and clear data auditing mechanism. Digital forensic readiness model for internet voting is a scientific concept that is foolproof to vote tampering activities such as vote rigging and vote fraud. When the vote is cast, the Blockchain encryption process executes and protect election data from unauthorised access. This guarantees vote anonymity, security and voter. This is an end-to-end process therefore vote rigging and unauthorised election data tampering is not possible. Therefore, in an event of attempted vote rigging the digital forensic readiness model would flag this in form of digital reports, audit trails and/or log sheets. The digital forensic results can be used in the courts of law to prove alleged vote rigging or vote fraud offenses committed on an election dataset. In this paper, we also looked at the drawbacks of the traditional paper-based voting system. The main causes of concern are vulnerability to vote rigging and vote fraud. Through the means of introducing DFRMIV, this paper outlines how vote rigging and vote fraud can be mitigated in online voting processes. However, since only a fraction of countries thus far have adopted the internet voting system; there is still a long way to go in convincing the international community to trust and employ the DFRMIV to reduce vote rigging problems.

5. Conclusion

The study has shown that a ballot paper voting system is regularly associated with vote disputes. This emanates from loopholes and flaws found in the process, i.e., ballot paper printing, vote casting, ballot paper transportation and storage, vote counting and election result presentation. The audit process in a ballot paper-based system lacks transparency and scientific proof. As a result, the level of trust and confidentiality becomes low. In the ballot paper voting system votes can be easily manipulated and be tampered with without a solid form of trace as this is an end-to-end manual process. The integration of digital forensic mechanism with online voting systems proves to be a better substitute for the traditional ballot paper-based voting system. Its scientific and mathematical semantics make it foolproof to most vote-rigging antics. Its scientific audits can be legally used in law courts to challenge vote fraud and rigging issues.

In the future, this paper's focus is to find ways on how to get the collaboration of online voting and digital forensic to be widely accepted by a greater percentage of the world. The main aim is to eliminate the element of doubt and lack of trust in the online voting model. This would then result in a bigger positive response rate towards digital voting by the international community.

6. Acknowledgments

We would like to thank the anonymous reviewers from the *European Conference on Cyber Warfare and Security (ECCWS)* for their helpful comments. A special acknowledgement to a friend Amie Hewitt for her encouragement throughout the research period. We would also like to acknowledge Job Mbava (brother) for paper reviews at home during the time of writing.

Reference

Chen, M. Te, Chen, C. C. and Lin, T. H. (2020) 'A cryptanalysis of trustworthy electronic voting using adjusted blockchain technology', *ACM International Conference Proceeding Series*, pp. 275–280. doi: 10.1145/3418094.3418143.

Mursi, M.F., Assassa, G.M., Abdelhafez, A. and Samra, K.M.A., 2013. On the development of electronic voting: a survey. *International Journal of Computer Applications*, *61*(16).

Gloe, T., Kirchner, M. and Böhme, R. (2007) 'Can We Trust Digital Image Forensics ?', pp. 78–86.

Kong, H., Kong, H. and Kong, H. (no date) 'Your Meat is My Poison: The Surprisingly Diverging Reactions of Stock Market to the Presidential Term Limit Repeal in China* Junyan Jiang', pp. 1–50.

Magaisa, A. (2019) 'Zimbabwe: An opportunity lost', *Journal of Democracy*, 30(1), pp. 143–157. doi: 10.1353/jod.2019.0011.

Makumbe, J. (2014) 'Elections in Zimbabwe : The ZANU (PF) Hegemony and its Incipient Decline Elections in Zimbabwe : The ZANU (PF) Hegemony and its Incipient Decline', 2(1), pp. 122–139.

Matharu, G. S., Mishra, A. and Chaudhary, L. (2014) 'Integrated election voting system: A model for leveraging ICT in the Indian election scenario', *ACM International Conference Proceeding Series*, 11-16-Nove. doi: 10.1145/2677855.2677944.

Muneer, U. and Shamail, S. (2013) 'Internet voting: A smarter way to vote in Pakistan', *ACM International Conference Proceeding Series*, pp. 348–349. doi: 10.1145/2591888.2591953.

Pawlak, M. and Poniszewska-Marańda, A. (2019) 'Blockchain e-voting system with the use of intelligent agent approach', *ACM International Conference Proceeding Series*, pp. 145–154. doi: 10.1145/3365921.3365927.

Rabia, F., Sara, A. and Gadi, T. (2021) 'A survey on e-voting based on blockchain', *ACM International Conference Proceeding Series*. doi: 10.1145/3454127.3457626.

ROBERTS, E. A. and WOOD, D. J. (1951) 'A study of the polyphenols in tea leaf by paper chromatography.', *The Biochemical journal*, 49(4), pp. 414–422. doi: 10.1042/bj0490414.

Shanmugam, M. (2015) 'Intelligent Digital Forensic Data Analysis and Dynamic Encrypted Distribution Using Global Positioning System'.

Sharkey, E. and Paynter, J. (2003) 'Factors influencing the uptake of online voting in NZ', *Proceedings of CHINZ 2003: The 4th Annual Conference of the ACM Special Interest Group on Computer-Human Interaction New Zealand Chapter*, pp. 121–122. doi: 10.1145/2331829.2331851.

Simons, B. (2012) 'Internet Voting : An Idea Whose Time has Not Come', p. 4503.

Srivastava, G., Dwivedi, A. D. and Singh, R. (2018) 'Crypto-democracy: A decentralised voting scheme using blockchain technology', *ICETE 2018 - Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*, 2(Icete), pp. 508–513. doi: 10.5220/0006881905080513.

Thron, R., Dirnberger, H. and Quirchmayr, G. (no date) 'Requirements and Challenges for Digital Forensic Readiness in Industrial Automation and Control Systems', pp. 232–238.

Wang, P. L., Yang, S. H. and Hsiao, H. C. (2020) 'Hybrid-Voting: A Hybrid Structured Electronic Voting System', *The Web Conference 2020 - Companion of the World Wide Web Conference, WWW 2020*, pp. 83–84. doi: 10.1145/3366424.3382708.