Cybersecurity and Electoral Processes. An Analysis of Block Chain Enabled Biometric Voter System and Risk Control in Kenya's 2022 Electoral Process and the United States Election System Infrastructure.

John Irungu, *Anteneh Girma*

john.irungu@udc.edu anteneh.girma@udc.edu,

Department of Computer Science, University of The District of Columbia

ABSTRACT

Electoral Processes Infrastructure Security and Integrity has been an emerging challenge due to the verifiability disputes that arise in competitive elections. This is despite investments in Secure and electoral technology that meets the Confidentiality, Integrity and Availability (CIA triad) of information security. To ensure electoral infrastructure efficiency, information security and voters data confidentiality, governments have invested in Blockchain modeled technology, Biometric Voter Registration and Authentication as well as secure electronic voting mechanisms. This paper studies the Information Security issues raised in the Data Collection, Results Transmission Servers (RTS), Management in the Kenyan electoral process of 2022 where Biometric Voter Registration (BVR) Technology was used to authenticate the voter registration and a hybrid System used in voting and transmitting results. Comparatively, this paper also investigates the United States electoral voting platforms, and documented attempts to interfere with the elections Cyber Security Infrastructure through Malware Attacks and Spearphishing on State and Local Networks. The demonstrates the shows the cost and benefit of traditional data centers against block chain secured BVR and virtualized platform. To enhance electoral integrity and security, the findings recommend a proposed change in the Information Management policies and protocols in the administration of electoral hardware and software assets as well as unrestricted access for Results Transmission Audit.

Keywords: Biometric Voter Registration (BVR), Blockchain, CIA triad, Cloud Computing

1. INTRODUCTION

Cloud security can be referred as the building and hosting of secure applications in cloud environments for use and consumption [1].This amplifies the emphasis of protection of information from unauthorized access as well as provision of Confidentiality, Integrity and Availability according to NIST specifications and guidelines. A cloud environment can be either private, public or hybrid where applications and business processes are owned either solely, shared by organizations or both, respectively. The decentralization of data in cloud environment allows optimal management of information sharing and storage in an economical and cost-effective way. Computing resources in cloud can also be configured as well as scaled according to the customer's business needs and service provided. The benefits that come with the ubiquitous and rapid elastic nature makes cloud computing more business friendly to organizations.

One of the challenges that come along with cloud technology is data security breaches and vulnerabilities. As business processes and information handling infrastructure migrates to cloud, the Integrity and confidentiality of information has become vital [2] for organizations, clients as well as service providers for seamless operations and credibility, respectively. With credibility of information security for Information Communication Technology (ICT) providers being an emerging concern due to the vulnerabilities and sophistication in threats, this study evaluates the cloud security infrastructure and the management of data in Blockchain secured infrastructure. With a focus of the Kenyan and United States electoral processes as a case study, this work investigates the Biometrics Technology and information Risk Management policy challenges that may be encountered in access management of voters' data. This paper evaluates the Kenyan electoral process where policy issues in handling the Independent Electoral and Boundaries Commission were raised in 2017 and 2022 [3] general elections. Further we interrogate the merits and demerits of virtualized data centers and whether data transmission in electoral processes may be prone to Man in the Middle attacks among other vulnerabilities.

In a seemingly seamless technological process that culminated in a disputed case whereby the management of the electoral process infrastructure such a Data Servers, transmission systems and administrative rights to data logs was contracted to third parties, this case study also interrogates the Cybersecurity Governance Policies for service providers in relation to the C-I-A triad. In this evaluation we mainly focus on two institutions namely, The Independent Electoral and Boundaries Commission (IEBC) which stands for the constitutional electoral body in Kenya that is mandated to administer elections and SMARTMATIC which is an electronic voting and Technology company which was contracted by IEBC to administer the 2022 General elections using the Biometric Voter Registration System(BVR) [4]. The paper is organized as follows Section 1 is the Introduction. Section 2 highlights Related Works. Proposed works is covered in Section 3 and the paper ends with the Research Contribution and Conclusion in Section 4.

2. RELATED WORKS

Secure online voting is fundamental in ensuring that trust and fairness is guaranteed electoral processes through maintaining the Integrity and security of the process infrastructure. Srivastan [5] advocates for ensuring that the authenticity of the voters through use of technology such as Biometrics for Identity verification so as to eliminate double voting. To ensure cost effective process Srivatsan proposes an online secure voting System where voting and tally reporting is done in real time with voter's password credentials for secure casting of votes. The work shows that implementing secure technology achieves authenticity, non-traceability of votes cast and enforces confidentiality.

Yashika [6] in the paper Two-Level Biometric Security studies the voting system in India and the challenge of double registration of voters, fake voting and the disputes that arise from the integrity controversies. To eliminate the existing gaps in India voting system and improve the security of the voting process Yashika proposes the levels of voter authentication starting with Biometric registration for authenticity. Through the use of matching algorithms, the voter biometric credentials is matched with the input data for authentication before casting of the vote. This ensures 'One voter –One vote' is achieved.

2.1 DNC Malware and Spearphishing Network Attacks

In the United States electoral dispute was based on hacking or attempts to hack. According to a report [16] by the Department of Justice, in 2016 the Democratic Nation Committee experienced a malware attack when its network was penetrated and hundreds of thousands on data stolen. The attacks were malware and Spearphishing. According to the report, through Initial Access intrusion of the network was by stealing IT administrator's credentials which led to compromise of 29 computers which acted as "middle servers" which sending messages from the malware to DNC Servers.

Biometric Voter Registration Process.

The Biometric voter registration system includes the use of unique characteristics such as fingerprints, eye retina, palm prints. In the voting system, this information is used to verify a voter's identity for authentication during the casting of the ballots thereby improving credibility and verifiability of the voter's identity and the process. Automatic Fingerprint Identification Systems (AFIs) is the most commonly used biometric method of capturing, processing and biometric data in a biometric plate where matching algorithms [4] are used for verification.

In Kenya the Biometric Voter Registration (BVR) kits were used to register the voters in the 2022 General elections which form the basis of our case study. The system comprised of laptop, fingerprint scanner, and a camera to capture authentication data, in this case, something you have and Personally Identifiable Information (PII) [5]. According to the IEBC, the implementation of this technology was to ensure transparency and accountability in the electoral process which had also been disputed not only in 2017 but in the previous years of Kenya's electoral cycle.

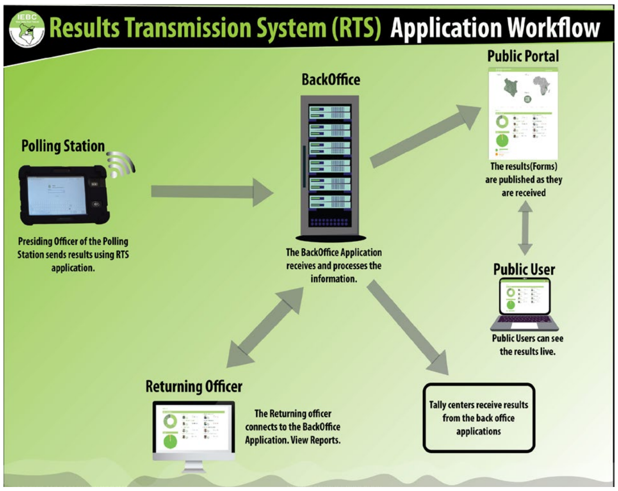

IEBC
Results Transmission System (RTS) Application Workflow
Polling Station
Presiding Officer of the Polling Station sends results using RTS application.
BackOffice
The BackOffice Application receives and processes the information.
Public Portal
The results(Forms) are published as they are received
Public User
Public Users can see the results live.
Returning Officer
The Returning officer connects to the BackOffice Application. View Reports.
Tally centers receive results from the back office applications

Figure 1. The Biometric Voter Registration System Results Transmission Model [5]

The Independent Electoral and Boundaries Commission of Kenya, stated [6] that the BVR Technology which included Biometrics Identification, maintained the CIA Triad of information security. The research looks into the IEBCs BVR Blockchain architecture and the vulnerabilities and existing gaps in administering BVR electoral processes worldwide.

International and Communications Technologies (ICT) [7]in Elections Database put the figure of countries that use BVR in their electoral processes at 25% however of the number only 9% use it electronically. The disparity may be explained by the operational costs and also legal framework in the handling and administration of the electronic votes' transmission – one of the bone of contentions in the Kenyan case when it came to sharing of Server Data logs in our case study country –Kenya.

Blockchain Technology in the Kenyan Biometric Voting System.

The merits and shortcomings of the use of decentralized infrastructure in the form of Blockchain during electoral processes are also investigated in this study. Blockchain Technology is a decentralized architecture comprising of in-built security and peer to peer techniques to enhance trust and transactions by avoiding third parties [8]. In relation to the 2022 Kenyan Biometric Voter process, the voter registers act as the public ledger with a register for each of the 46,229 decentralized polling stations in Kenya and across the globe. The candidate's data was also registered in a web-based application known as the Central Register Management System (CRMS) for validation purposes. Voter's Data was captured by the BVR was processed and integrated in the backend [9]. To eliminate double voter registration, the data was exported to a central system for data matching. The electronic voter identification using biometric ensured the legitimacy of electoral data. Each final record of the polling station was scanned as a permanent record and transmitted using the electronic and encrypted Integrated Elections Management Systems (KIEMS) to the servers for reporting [9] and tabulation intents.

Due to the decentralized nature of Blockchain technology e-voting and voter's identity authentication is made ubiquitous at any geographic location optimizing resource and logistics as well as eradicating geographical barriers. Voter data Security is also enhanced due to the record of every transaction record by a block which acts as a record book and a ledger in BVR voting and reporting system. After the transaction is completed, a block is permanently sent to the database. [10] The data recorded in the Blockchain is normally immutable. With reference to the C.I.A triad of information security, the immutability of the Blockchain ensures the Integrity of data which makes the BVR System secure. In the case of the 2022 Kenyan electoral process the ledger in the process was a form known as Form 34A which constituted a signed and approved vote tally record from each of the 46,229 decentralize poll stations.

2.2 Bitcoin nodes Concept

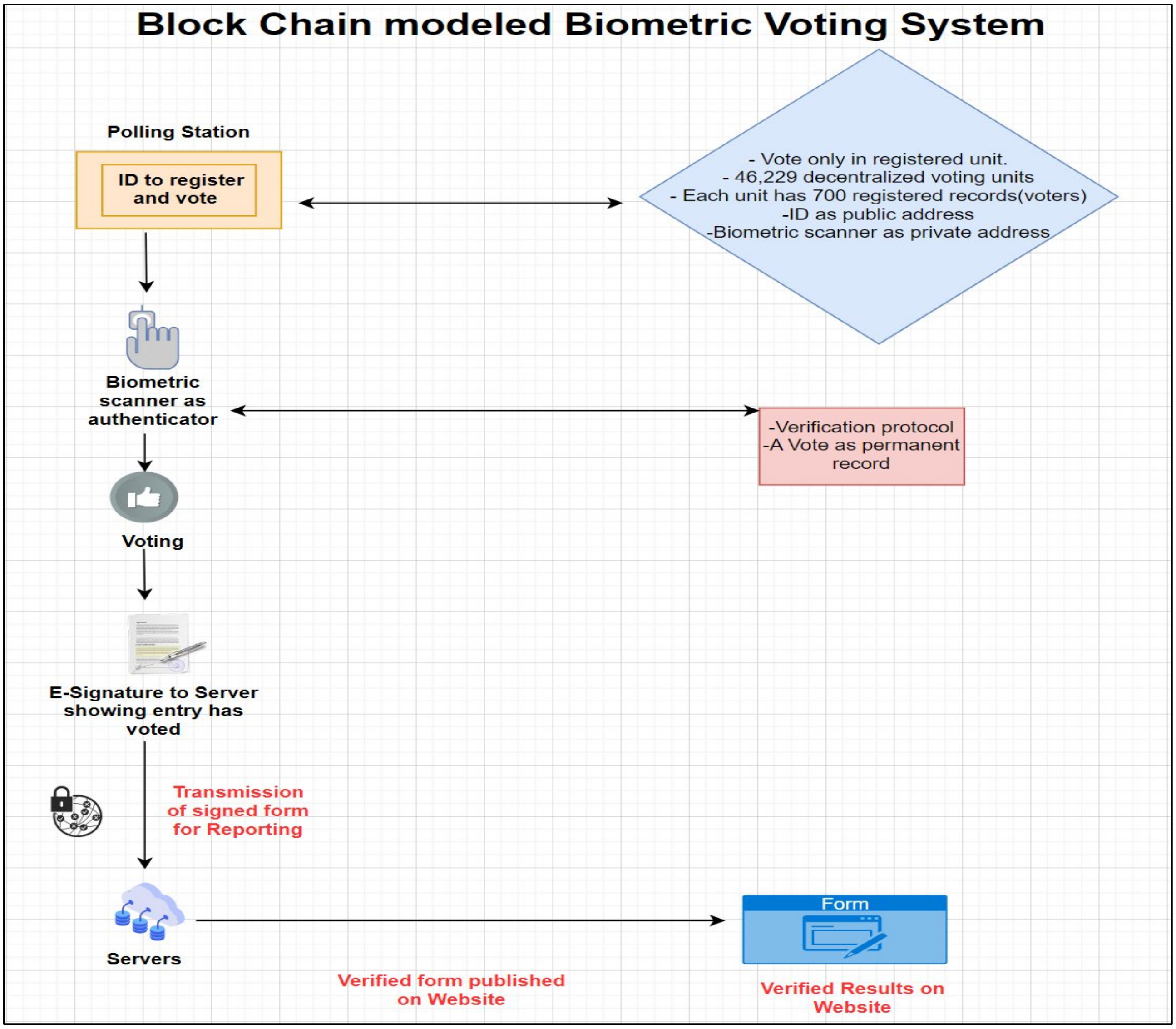
The 2022 Kenyan voting system which was a combination of both manual and electronic system of voting is argued to have borrowed its infrastructure heavily from the Bitcoin nodes concept. The 46,229 polling stations acted as Blockchain nodes where votes were recorded and signed and approved [9] as irreversible ledger. Bitcoin network has 13,812 nodes [11].The polling stations were also geo-marked within their respective networks and Biometric kits.

An encrypted Results Transmission System (RTS) was used to scan [10], upload and transmit the results uploaded form 34A from each of the 46,229 polling stations to a server. It is in the 46,229 polling stations that the Kenyan Integrated Elections Management System (KIEMS) biometric device scanned a QR-coded form and sent the copies to then IEBC servers. The signed physical form acting as a permanent record was used for verification at the Headquarters by the electoral body through cross referencing with the online form reported form on the IEBC website. The server's administration decrypted the form for display of the results in pdf form was accessible in real time on the electoral body (IEBC) website. Each polling station had 700 voters (entries) whereas one bitcoin block is one megabyte per block.

3.PROPOSED BIOMETRIC VOTING SYSTEM ADMINISTRATION

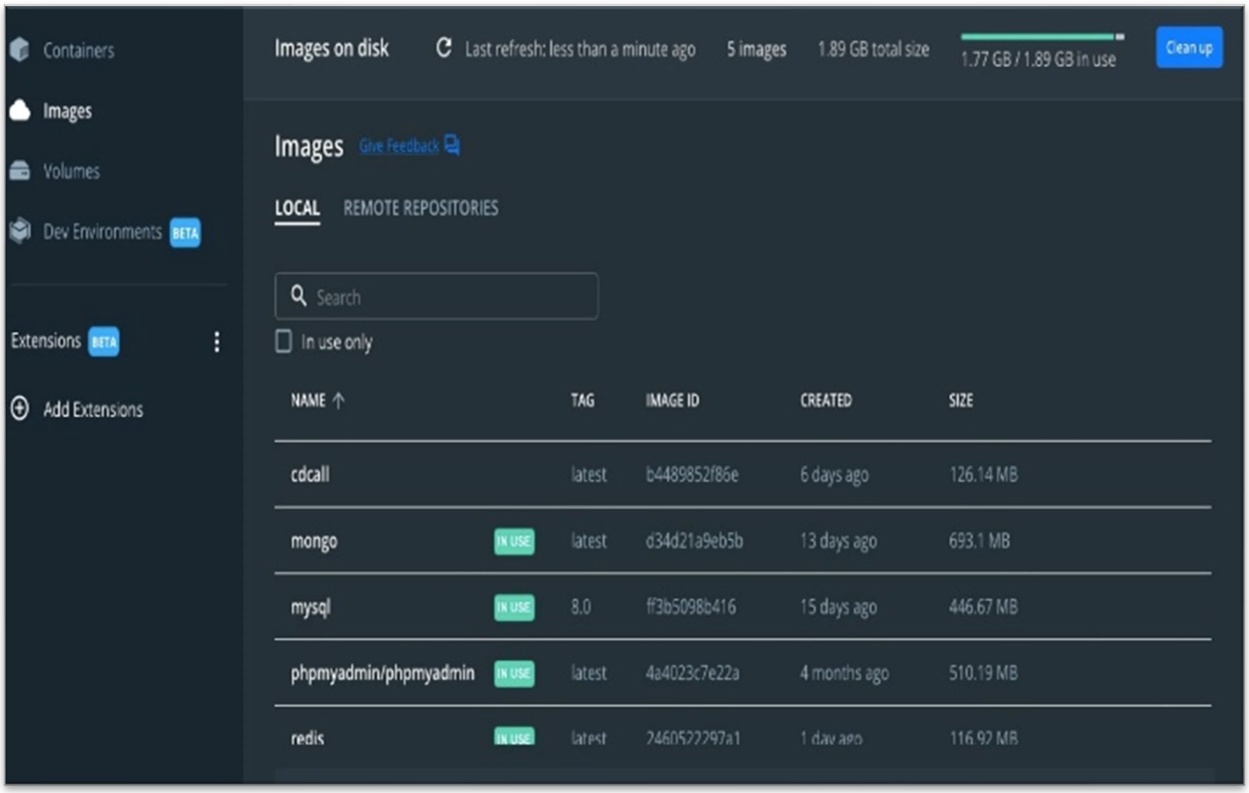
As is the case with the Kenyan electoral system and many a process in the world, technology has not been absolved [12] electoral bodies from Integrity questions as enshrined the in the C.I.A triad even where secure processes as such Blockchain are used. These can be attributed to the administrative model where different jurisdictions manage their own elections infrastructure leading to a variation of systems and complexities. In the United States, elections infrastructure is managed by states and local governments. According to the Congressional Research Service states and local governments experienced cyberattacks targeting their jurisdiction election infrastructure which led to the Department of Homeland Security Designating [13] election systems as critical infrastructure. Notably, the National Institute of Science and Technology (NIST) is responsible for certification and standards of election systems in the United States.

To mitigate vulnerabilities in the electoral systems compensation controls, software patching and


Block Chain modeled Biometric Voting System
Polling Station
ID to register and vote
- Vote only in registered unit.
- 46,229 decentralized voting units
- Each unit has 700 registered records(voters)
-ID as public address
-Biometric scanner as private address
Biometric scanner as authenticator
-Verification protocol
-A Vote as permanent record
Voting
E-Signature to Server showing entry has voted
Transmission of signed form for Reporting
Servers
Form
Verified form published on Website
Verified Results on Website

physical and procedural safeguards [12]can be implemented. However, even though the technical and procedural security measures may ensure the confidentiality of data and access of electoral results, verifiability and integrity of the results has been questioned due to the management of the electoral infrastructure. This study provides some remedies that may guarantee confidence in the handling of electoral data and always allay fears of electoral tampering.

Whereas Blockchain technology is one of the secure form of protection for data due to its desirable capability of decentralization, immutability, fault tolerance and auditability [14] the lack of a centralized data handling infrastructure by a unitary body and contracted technical expertise and technology has led to unwarranted disputes ,lack of data verifiability and autonomy in the access of information on a need basis. In the recently concluded Kenya electoral process, which was block chain secured, parts of the infrastructure such as data handling and server administration was contracted out to a vendor which led to a protracted legal battle during the audit of the elections results. In the dispute, where one of the parties requested for results transmission logs, collected data from transmission system and Images from the Servers, the vendor -SMARTMATIC- contracted by the Kenyan electoral body to manage results transmission ,citing violations of Intellectual Property Rights, denied the Kenyan Supreme Court access the images of its servers [15]. In the ICT experts Reports for the Kenya 2022 election [16], ICT experts stated that the Results Transmission System ran on One virtual Server and 7 Docker containers.



Images on disk Last refresh: less than a minute ago 5 images 1.89 GB total size 1.77 GB / 1.89 GB in use

Images

□ In use only

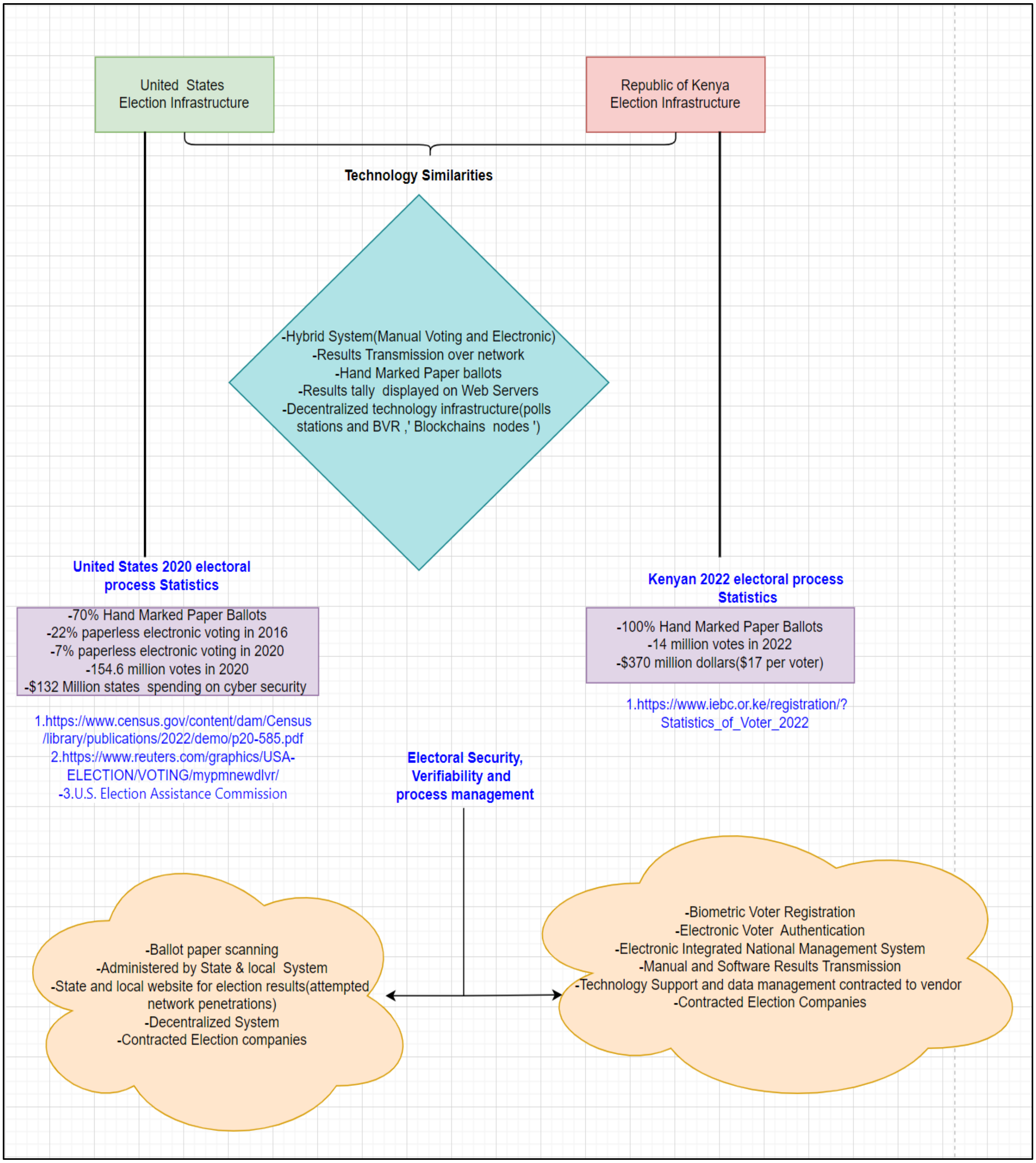
NAME ↑		TAG	IMAGE ID	CREATED	SIZE
cdcall		latest	b4489852f86e	6 days ago	126.14 MB
mongo	IN USE	latest	d34d21a9eb5b	13 days ago	693.1 MB
mysql	IN USE	8.0	ff3b5098b416	15 days ago	446.67 MB
phpmyadmin/phpmyadmin	IN USE	latest	4a4023c7e22a	4 months ago	510.19 MB
redis	IN USE	latest	2460522297a1	1 day ago	116.92 MB

Fig 2. An example of a container Image and running database applications

3.1 ELECTORAL TECHOLOGY AS INHERENTLY GOVERNMENT FUNCTION

Notably, the main causes of electoral integrity disputes in Kenya, despite secure measures for electoral infrastructure has been the issues of data handling by the contracted vendors. In two subsequent elections in 2017 and 2022, access to the Results Transmission servers (RTS) for audit in the disputed results has led to two consecutives Supreme Court litigations. In 2017 dispute, the electoral body, IEBC stated [17] that they could not give access to the RTS servers citing absolute confidentiality of usernames, passwords, IP addresses and software running applications. Although fresh orders were given by the supreme court, the IEBC only provided read only information relating to number of servers, Internal and external firewalls disclosure, password policy, password matrix, system user types, Disaster Management plan, GPS Locations of Polling Stations, Certified Copies of Penetration tests on election technology where all parties viewed transmitted results from polling stations in different geographic locations. In 2022, the vendors who managed the elections servers did not give full access of servers citing confidentiality and Intellectual property violations. In addition, the IEBC also stated the backend election transmission servers were hosted on secure oracle database and not Microsoft SQL server as stated by the petitioner. In the United States, election attempts [18] to interfere with electoral integrity technology and exploit cyber security vulnerabilities have been experienced especially on state and local networks. Just like in Kenya where security and verifiability of the election transmitted results was in Dispute, in the United States, the efficiency of ballot machines has also been called into question by disgruntled parties. With a precise focus on Technology, this study proposes administrative changes in the administration of election technology and also how these changes can lead to mitigation of electoral systems vulnerabilities through adoption of a secure centralized data handling and results reporting body.

Comparative Model of United States and Kenya Electoral Infrastructure and Security Measures.


United States Election Infrastructure
Republic of Kenya Election Infrastructure
Technology Similarities
-Hybrid System(Manual Voting and Electronic)
-Results Transmission over network
-Hand Marked Paper ballots
-Results tally displayed on Web Servers
-Decentralized technology infrastructure(polls stations and BVR ,' Blockchains nodes ')
United States 2020 electoral process Statistics
-70% Hand Marked Paper Ballots
-22% paperless electronic voting in 2016
-7% paperless electronic voting in 2020
-154.6 million votes in 2020
-$132 Million states spending on cyber security
1.https://www.census.gov/content/dam/Census/library/publications/2022/demo/p20-585.pdf
2.https://www.reuters.com/graphics/USA-ELECTION/VOTING/mypmnewdlvr/
-3.U.S. Election Assistance Commission
Kenyan 2022 electoral process Statistics
-100% Hand Marked Paper Ballots
-14 million votes in 2022
-$370 million dollars($17 per voter)
1.https://www.iebc.or.ke/registration/?Statistics_of_Voter_2022
Electoral Security, Verifiability and process management
-Ballot paper scanning
-Administered by State & local System
-State and local website for election results(attempted network penetrations)
-Decentralized System
-Contracted Election companies
-Biometric Voter Registration
-Electronic Voter Authentication
-Electronic Integrated National Management System
-Manual and Software Results Transmission
-Technology Support and data management contracted to vendor
-Contracted Election Companies

3.2 PROPOSED OPERATIONAL AND TECHNICAL CONTROL CHANGES.

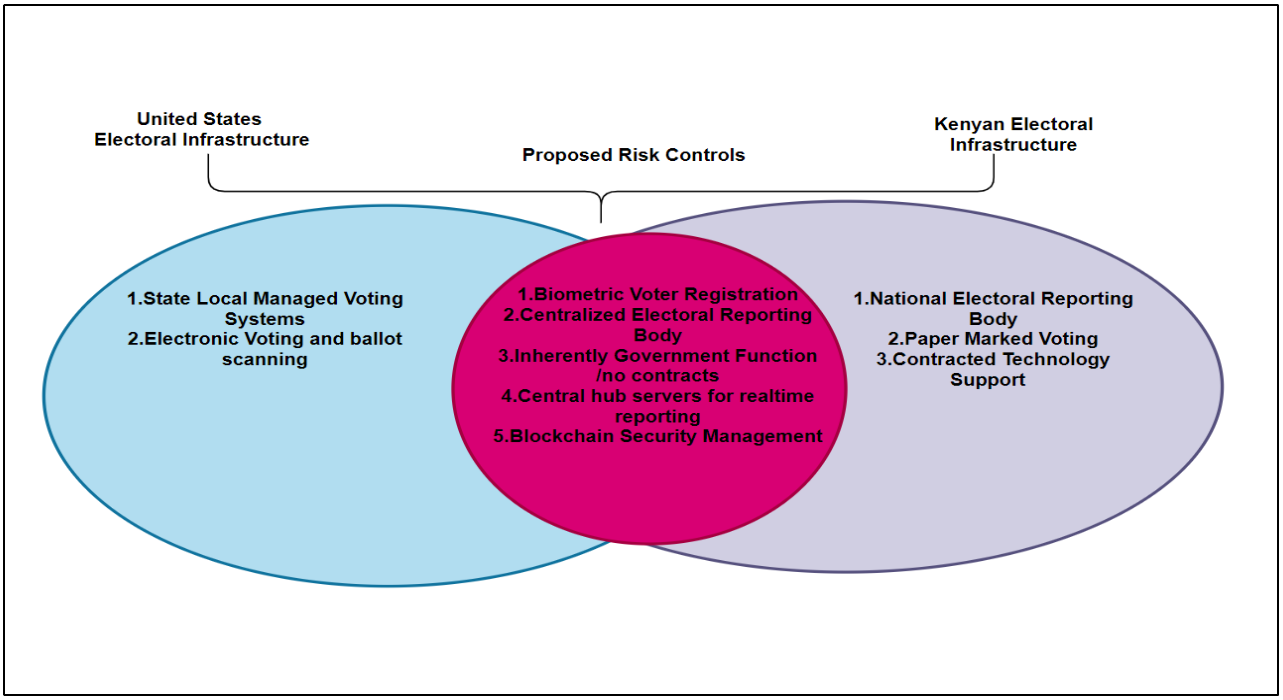

United States
Electoral Infrastructure
Proposed Risk Controls
Kenyan Electoral Infrastructure
1.State Local Managed Voting Systems
2.Electronic Voting and ballot scanning
1.Biometric Voter Registration
2.Centralized Electoral Reporting Body
3.Inherently Government Function /no contracts
4.Central hub servers for realtime reporting
5.Blockchain Security Management
1.National Electoral Reporting Body
2.Paper Marked Voting
3.Contracted Technology Support

Fig 3. Proposed Election Security Infrastructure and that United States and Kenya adopt.

To enhance the integrity of the voting process nd reduce disputes as witnessed in the United States and Kenya, the administration of the election and its security needs to be coordinated by a centralized body with full access of election data, election manager database, Biometric voter Registration and verification systems and internal network infrastructure [16]. The ownership of these rights by the electoral administering body gives full autonomy in case of judicial hearing or cyber security audit.

The above comparative model compares the United States and Kenya voting infrastructure and election administration. As seen in the model both countries share technological processes such as hybrid voting System where marking of the ballot by the voter is done physically and tally transmission to the servers and reporting is done electronically. In Kenya Biometric Voter Authentication of the voter is done before the casting of the vote to ensure 'One voter – One vote' as well as to avoid double voting. The Kenyan system also includes geo-location technology so that each voter votes in the unit and location where they were registered, even though the system reporting, and transmission is decentralized.

Once verification is done, the results transmission to the server just like the United States state government and local is transmitted through secure network to the servers for reporting.

The main difference between voting systems in Kenya and United States is the governing bodies in elections. In the United States, voting is devolved to state and local governments whereas in Kenya the authority to manage, tally and report election votes is streamlined to one national governing body. Both systems have merits and demerits due to the electoral disputes that may arise like Florida in 2002 and the 2017 and 2022 election disputes on hacking allegations and plaintiff's plea for open the results transmission servers for election results auditing.

4. RESEARCH CONTRIBUTION AND CONCLUSION.

In this study we were able to evaluate the electoral security measures of Kenya and United States elections processes and the challenges that arise from attempts to infiltrate the United States elections systems cyber security infrastructure and the lack of full autonomy by the national election body (IEBC) to manage the elections technology infrastructure hardware and software's assets such as servers in case of disputes which require security auditing. This erodes electoral trust and technical control independence. As a result, this study finds that:

1.The United States as well as other jurisdictions should adopt Biometric Voter Registration for voter Identity authentication so as to enhance voting process trust.

2.Electoral processes in Kenya and United States should adopt voting as an inherent Government Functions with no contractual practices of technology infrastructure so as to manage, the security of the elections ICT assets and have full autonomy of such as server logs audit in case of electoral dispute.

3.There is a need to use Blockchain technology as a secure way for electoral process confidentiality and networks integrity.

Bibliography

[1] Cisco, What is Information Security?, Cisco, 2022.

[2] J. Du, "Research on Enterprise Information Security and Privacy Protection in Big Data Environment," in 2021 3rd International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI), 2021, pp. 324-327.

[3] D. Miriri, "Kenya's top court to rule on hacking allegations, votes disparity in election dispute," reuters, 30 08 2022. [Online]. Available: https://www.reuters.com/world/africa/kenyas-top-court-rule-hacking-allegations-votes-disparity-election-dispute-2022-08-30/. [Accessed 28 9 2022].

[4] A. A. B. K. M. S. P. N. a. T. Z. Peter Wolf, "Introducing BiometricTechnology in Elections," International Institute for Democracy and Electoral Assistance, Stockholm ,Sweden, 2017.

[5] S. Sridharan, "Implementation of authenticated and secure online voting system," in 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2013.

[6] S. a. K. Y. a. C. A. a. J. G. Srivastva, "Two-Level Biometric Security System For Voting," in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 346-352.

[7] U.S. Department of Justice, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election, " U.S. Department of Justice, Washington D.C, 2019.

[8] IEBC, "Indepedent Electoral Boundaries and Commission," [Online]. Available: https://www.iebc.or.ke/election/technology/?Biometric_Voter_Registration_System_(BVR). [Accessed 25 09 2022].

[9] IEBC, "Biometric Voter Registration System (BVR)," [Online]. Available: https://www.iebc.or.ke/election/technology/?Biometric_Voter_Registration_System_(BVR). [Accessed 23 September 2022].

[10] International Institute for Democracy and Electoral Assistance (International IDEA), "ICTS IN ELECTIONS DATABASE," [Online]. Available: https://www.idea.int/data-tools. [Accessed 15 10 2022].

[11] N. {. Bassam}, "Chapter Twenty - Blockchain," in Distributed Renewable Energies for Off-Grid Communities (Second Edition), Boston, Elseiver, 2021, pp. 447-450.

[12] R. Kamau, "Kenyan Electoral Board Designs A Transparent Voting System That Mirrors The Bitcoin Blockchain," Forbes DIGITAL ASSETS, 11 08 2022.

[13] R. S. a. A. Alex, "A Review on BlockChain Security," IOP Conference Series: Materials Science and Engineering, vol. 396, no. 1, p. 012030, 2018.

[14] bitnodes.io, "REACHABLE BITCOIN NODES," 8 11 2022. [Online]. Available: https://bitnodes.io/. [Accessed 12 8 2022].

[15] CISA, "ELECTION SECURITY RUMOR VS. REALITY, " CYBER AND INFRASTRUCTURE SECURITY AGENCY, 8 November 2022. [Online]. Available: https://www.cisa.gov/rumorcontrol. [Accessed 15 November 2022].

[16] Brian E. Humphreys, "The Designation of Election Systems as Critical Infrastructure," Congressional Research Service, 2019.

[17] H. G. a. X. Yu, "A survey on blockchain technology and its security," Blockchain: Research and Applications, vol. 3, no. 2096-7209, p. 100067, 2022.

[18] African Centre for Open Governance, "DISOBEYING ORDERS: THE SCRUTINY OF KENYA'S ELECTORAL TECHNOLOGY," africog, Nairobi, 2022.

[19] IEBC, "Supreme Court Order on Access to RTS Server," 18 February 2019. [Online]. Available: https://twitter.com/IEBCKenya/status/1097492486560321536/photo/2. [Accessed 13 11 2022].

[20] National Intelligence Council and CIA, DHS, FBI, INR, and NSA, "Foreign Threats to the 2020 US Federal Elections," 10 March 2021. [Online]. Available: https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf. [Accessed 25 11 2022].