Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/6/20230797

The impact of security and privacy threat modeling on blockchain-enabled-electronic voting system

Maheshwari V and Prasanna M

School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India.

prasanna.m@vit.ac.in

Abstract. Blockchain is a decentralized, distributed ledger that records transactions between two parties. A blockchain-based software system is a new and innovative approach to software engineering that uses blockchain technology. This approach has several advantages over traditional software engineering approaches, including improved security and transparency. The most common software engineering approaches are waterfall, agile and hybrid models. Each of these has its strengths and weakness. A blockchain-based system has the advantage of being more secure and transparent than any of these approaches. It also can track changes more accurately, which can improve quality control. Blockchain technologies have incredible potential but also have some problems. One problem is security and privacy issues, which brings into question the resilience of existing security and trust mechanisms. The distributed application (dApp) framework for the proposed electronic voting system is built with the help of blockchain technology in this proposal. As a result, fewer crimes has committed against sensitive data during the electoral process because of immutability, transparency and privacy. Ganache, Metamask and hashing algorithms are used to develop the dApp. The paper's strengths lie in its ability to create and analyze threat models for blockchain-enabled-electronic voting systems and to identify the types of threats using Microsoft STRIDE.

Keywords: Blockchain, Security, Privacy, Threat Model, Vulnerabilities, Software Process Model, Microsoft STRIDE.

1. Introduction

Blockchain technology's theoretical foundation has been made on the work of Bitcoin pioneers like Satoshi Nakamoto, and recent breakthroughs in cryptography have made it possible to build practical applications using this technology [1][2]. Blockchain techniques can be used to create robust, self-managing software systems. A process model can be developed that describes how the system's various components interact. Models help understand how a system behaves, and they can be used to design improved systems or to improve the performance of existing ones. A blockchain-based software system can improve the efficiency and transparency of software development processes. Eliminating the need for intermediaries can reduce costs and improve communication between developers and managers. It can use for many different purposes, but it has a vast potential for use in other industries such as finance, banking, and healthcare [3]. For example, blockchain can create more efficient ways of sharing data between parties without having to trust each other. In addition, it could use in many different sectors,

DOI: 10.54254/2755-2721/6/20230797

including social media, advertising, and e-commerce. Blockchain technology is a novel approach to software systems management. It provides a principled and transparent way to store and manage data across distributed nodes.

Hsiao et al. [4] implement a decentralized e-voting application without a trusted third party by combining blockchain technology with a secret sharing scheme and homomorphic encryption. It allows for a public and verifiable voting process without compromising voter privacy, data security, or the ability to verify votes before they are counted. Patidar et al. [5] demonstrate that the privacy, integrity, security, enormous cost, and centralization issues associated with using an antiquated paper ballot system have plagued all countries for decades. The number of problems on the move is increasing, but the number of solutions is not. Then we transitioned to electronic voting, which still didn't resolve many problems. Using Ethereum and smart contracts, they present a new framework for implementing BC in an electronic voting system. Using Ethereum and smart contracts allows us to put the Truffle framework to use, which is used to test and verify smart contracts. Connecting to Ethereum nodes is done with the help of a Google Extension called Meta-mask. The goal of Ethereum is to facilitate the creation of any kind of network, private or public, by its developers.

E-voting that is based on blockchain technology has great potential, but it needs to be made more secure and more privacy. It was determined that frameworks need improvements in relation to blockchain practical applications [6][7].The main contribution of this paper is to create and analyze threat models for blockchain-enabled-electronic voting systems and to identify the types of threats using Microsoft STRIDE [8]. It also provides instantaneously accepted, more accurate counting results while protecting voters' privacy [9].

2. Materials and Methods

2.1. Blockchain-based E-Voting System

Government officials and citizens alike are unhappy with the election outcomes, which they call unpredictable [10]. Finally, we have a better answer for the current issues plaguing the electoral contract, such as tampering, out-of-precinct voting by non-residents, slow analysis and totaling of votes, and excessive use of resources [11]. A distributed application (dApp) threat model is developed to implement the proposed electronic voting system using blockchain technology is shown in figure 3.The identified types of threats using STRIDE for blockchain e-voting system is shown in figure 4. The number of crimes involving the processing of sensitive data in the electoral contract system is reduced because of its immutability, transparency, privacy, and receipt freedom, which are all unparalleled [12][13]. Ganache, Metamask, and the provided hashing algorithm were used to build the decentralized application is shown in figure 1, figure 2. Distributed ledger technology (blockchain) could develop a trustworthy voting system [14]. All the votes would be recorded in the distributed ledger system, making it impossible to alter or forge the results [15]. As a result, voter confidentiality is maintained, and the tally of votes is completed more quickly and accurately [16].

3. Proposed Methodology

By incorporating blockchain technology, the proposed system enhances the security and confidentiality of the existing, paper-based electoral contract system [17]. The best way to prevent rigging at the polling place, during the count, or in the final tally is for everything to be open and public [18]. A block must be distributed across a blockchain for each participant to implement this functionality. Votes cast by voters are recorded as transactions in the ledger.

3.1. Proposed Privacy and Security Preserving electronic enabled voting

Step 1: Create a local ganache network; unique account creation is created for voters with blockchain Transaction IDs, Addresses and Ethereum Balance.

Step 2: The identity verification & validation process with the unique account creation id, voter proof, and Smart contract (SC) is created for the voters.

DOI: 10.54254/2755-2721/6/20230797

Step 3: Candidate Process to call vote function () of SC using voter's public key; SC pays in ETH gas to a crypto wallet

for j= candidate '1' to candidate 'n' do

check eth_balance

if eth_balance >= threshold_cost

block[j] is created // new_uservote created with Ethereum gas

else

block[j] =null // no account is created

Step 4: E-voting transaction mapping with authentication where transaction ID is created.

Step 5: If the consumption of transaction gas limit is decreased, the transaction is submitted for mining, the block is appended in the main Ethereum chain, and the vote count has increased.

Step 6: The voter button is disabled once candidates cast a vote.

Step 7: The Data flow diagram is modeled for Blockchain-enable E-voting system and identifies the threat, property violation, threat definition, severity and SDLC phase.

Step 8: The threat report is generated and its blockchain attacks is mitigated.

4. Experimental Result

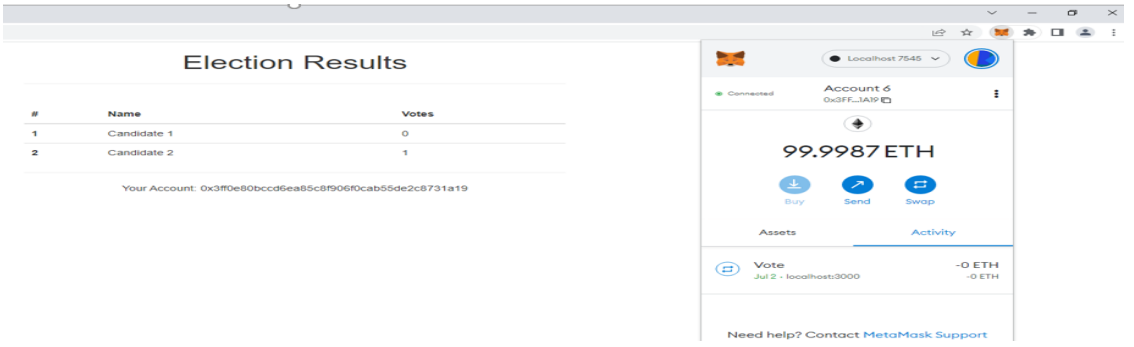

Figure 1. User Vote Successful after confirming Ethereum.

DOI: 10.54254/2755-2721/6/20230797

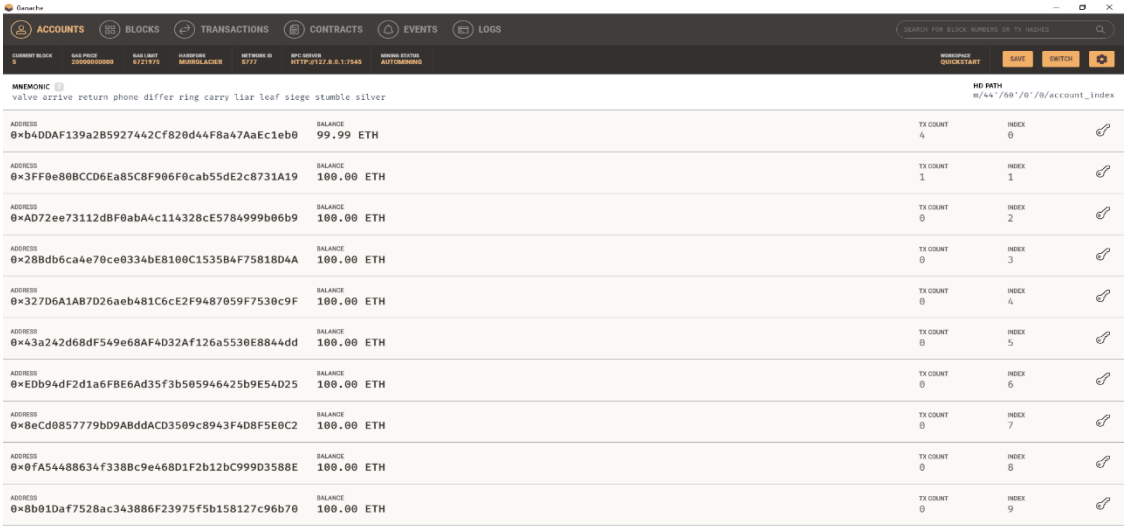

Figure 2. Transaction count increased after submitting the vote.

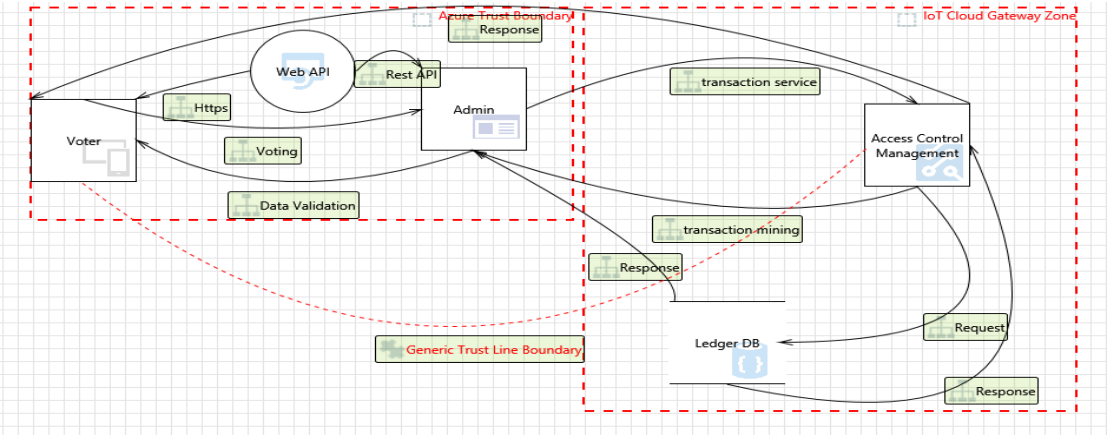

Figure 3. Threat Model for E-Voting enabled Blockchain.

DOI: 10.54254/2755-2721/6/20230797

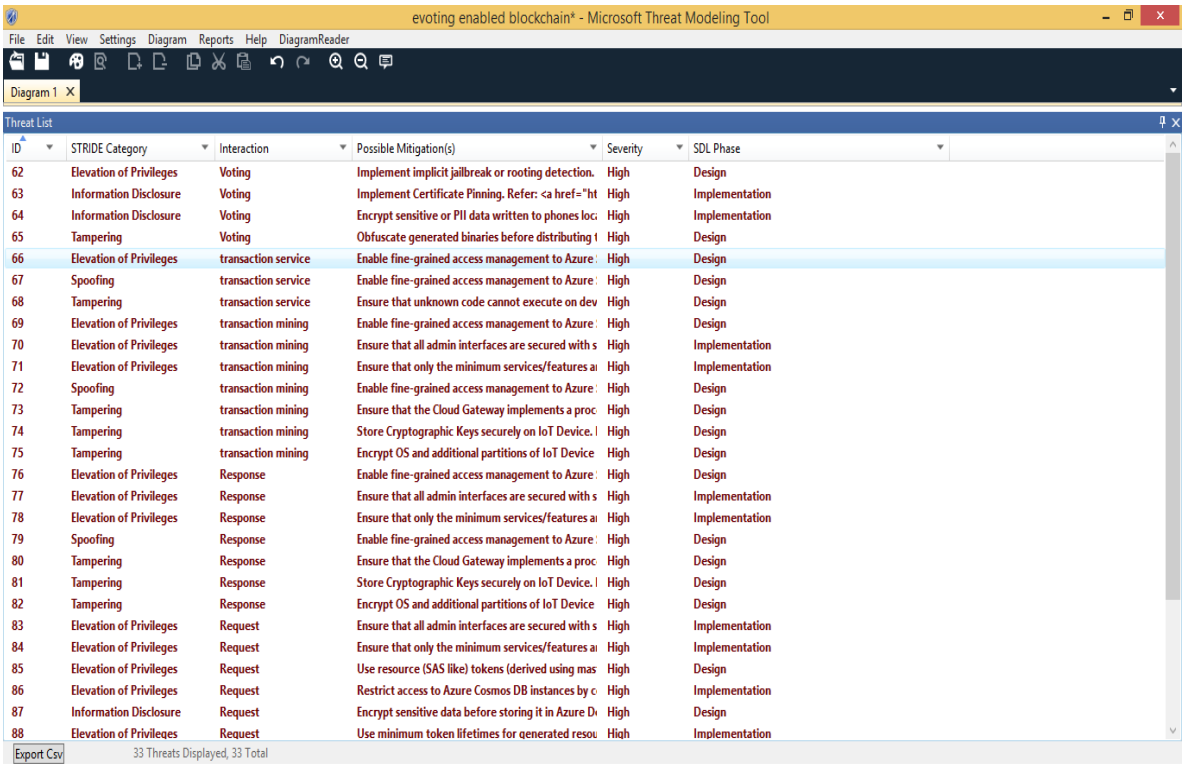

Figure 4. Threat report of STRIDE category for E-voting enabled blockchain.

5. Conclusion

In this section we will look at the security implications of blockchain technology, what it means for the future of privacy and security in the digital world and how it could be used for nefarious purposes by governments or criminals. Ever since its conception, blockchain technology has generated intense debate. Though it's used for storing data and conducting transactions safely, some people are wary of it due to privacy and security concerns. Blockchain has been used for a variety of different purposes, from digital currencies to identity management. A few people have begun to shift their attention away from the technology's potential as an asset class and towards its potential as a threat vector. The proposed threat model is to create and analyze threat models for blockchain-enabled-electronic voting systems and to identify the types of threats using Microsoft STRIDE. It also provides instantaneously accepted, more accurate counting results while protecting voters' privacy. Further, blockchain has seen use in domains disparate as a digital currency and identity management. Because of this, some have viewed the technology less as an investment opportunity and more as a security risk.

References

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 27 August 2019)

[2] Bitcoin Homepage. Available online: https://bitcoin.org/ (accessed on 17 August 2019)

[3] Moura, T., & Gomes, A. (2017, June). Blockchain voting and its effects on election transparency and voter confidence. In Proceedings of the 18th annual international conference on digital government research (pp. 574-575).

[4] Hsiao, J. H., Tso, R., Chen, C. M., & Wu, M. E. (2017). Decentralized E-voting systems based on the blockchain technology. In Advances in computer science and ubiquitous computing (pp. 305-309). Springer, Singapore.

DOI: 10.54254/2755-2721/6/20230797

[5] Patidar, K., & Jain, S. (2019, July). Decentralized e-voting portal using blockchain. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-4). IEEE.
[6] Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry, 12(8), 1328.
[7] Zhao, Z., & Chan, T. H. H. (2015, December). How to vote privately using bitcoin. In International Conference on Information and Communications Security (pp. 82-96). Springer, Cham.
[8] König, L., Unger, S., Kieseberg, P., Tjoa, S., & Blockchains, J. R. C. (2020). The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks. J. Internet Serv. Inf. Secur., 10(3), 110-127.
[9] Sathishkumar, V. E., Park, J., & Cho, Y. (2020). Using data mining techniques for bike sharing demand prediction in metropolitan city. Computer Communications, 153, 353-366.
[10] VE, S., & Cho, Y. (2020). A rule-based model for Seoul Bike sharing demand prediction using weather data. European Journal of Remote Sensing, 53(sup1), 166-183.
[11] VE, S., Shin, C., & Cho, Y. (2021). Efficient energy consumption prediction model for a data analytic-enabled industry building in a smart city. Building Research & Information, 49(1), 127-143.
[12] VE, S., Park, J., & Cho, Y. (2020). Seoul bike trip duration prediction using data mining techniques. IET Intelligent Transport Systems, 14(11), 1465-1474.
[13] Easwaramoorthy, S., Sophia, F., & Prathik, A. (2016, February). Biometric Authentication using finger nails. In 2016 international conference on emerging trends in engineering, technology and science (ICETETS) (pp. 1-6). IEEE.
[14] Easwaramoorthy, S., Thamburasa, S., Samy, G., Bhushan, S. B., & Aravind, K. (2016, April). Digital forensic evidence collection of cloud storage data for investigation. In 2016 International Conference on Recent Trends in Information Technology (ICRTIT) (pp. 1-6). IEEE.
[15] Thamburasa, S., Easwaramoorthy, S., Aravind, K., Bhushan, S. B., & Moorthy, U. (2016, August). Digital forensic analysis of cloud storage data in IDrive and Mega cloud drive. In 2016 International Conference on Inventive Computation Technologies (ICICT) (Vol. 3, pp. 1-6). IEEE.
[16] Shanthi, N., VE, S., Upendra Babu, K., Karthikeyan, P., Rajendran, S., & Allayear, S. M. (2022). Analysis on the Bus Arrival Time Prediction Model for Human-Centric Services Using Data Mining Techniques. Computational Intelligence & Neuroscience.
[17] Chen, J., Shi, W., Wang, X., Pandian, S., & Sathishkumar, V. E. (2021). Workforce optimisation for improving customer experience in urban transportation using heuristic mathematical model. International Journal of Shipping and Transport Logistics, 13(5), 538-553.
[18] Karrothu, A., Anilkumar, C., & Sathishkumar, V. E. (2022). An Escrow-Free and Authenticated Group Key Management in Internet of Things. In Smart Intelligent Computing and Applications, Volume 2 (pp. 505-512). Springer, Singapore.