IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204132 |

BLOCKING DNS ATTACKS USING BLOCKCHAIN

Bandaru Bhavana, Ravula Surya Narayana, Donthineni Akshitha, Meenakshi Simha
Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, India
Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, India
Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, India
Assistant Professor, Department of Computer Science and Engineering, Anurag University, Hyderabad, India

ABSTRACT: Cybersecurity is becoming a major worry for everyone in today's technologically advanced and interconnected world, including individuals, businesses, and governments. Our increasing reliance on digital platforms and systems has resulted in an expansion of the threat landscape and a wide range of security concerns. Transport Layer Certificates offer authentication and encryption for client-server communication. They are not, however, impervious to all forms of attacks, including DDoS assaults, insider threats, and application-layer flaws. One could get a false sense of security if they only rely on TLS certificates. This study uses blockchain technology to provide a novel way of combating URL redirection assaults. The project's goal is to improve DNS security and resilience against a variety of attack vectors, such as DNS cache poisoning, by utilizing the decentralized and tamper-resistant features of blockchain technology.

Keywords: VSCode , SHA-256, proof of work(POW)

I.LITERATURE SURVEY

[1] An Binh Tran, et.al.[11]stated Regerator in the research work that is a Registry Generator for Blockchain. The registry can be defined as a list related to the data recorded by an authorized person. There are the needs to secure the Registries for data integrity as well as for the availability. The security is required to make the connection of one to other registries. Building registries on a block chain influences key properties related to the Blockchains. Here the data integrity, immutability as well as the availability is considerable.

[2] Harry Halpin, et.al.[12] wrote on security and privacy of Blockchain. The Blockchain is one of the most enthusiastic bursts related to activity. It is necessary that the issues related to the security and privacy must be resolved. Therefore they discussed on block chain. In 2018,Mahdi H. Miraz, et al.[13]discussed the Apps related to the Blockchain and Cryptocurrency. When a new transaction is add to chain, all participants provide the validation to this transaction. It is made to apply an algorithm to verify the transaction. The accurately meaning of "valid" is defined using the Blockchain system which varies among the systems.

[3] Mohamed Amine Ferrag, et.al.[14]presented a comprehensive survey on protocols of the Blockchain. In addition, the researchers also stated the review on application domains related to the Blockchain technologies. In 2018, Carmen Holotesc, et.al.[15]described Blockchain technology to understand it properly. They made the exploration of Blockchain technology as well as its platforms. They also discussed the existing global as well as the governmental initiatives.

II.PROPOSED METHOD

Figure 2 shows the proposed system model. The detailed operation illustrated as follows:

Step 1. Input Certificates: This likely represents the starting point of the research. Input certificates refer to the digital certificates that need to be validated or verified. These certificates could be various types such as educational diplomas, professional certifications, or any other forms of digital credentials.

Step 2. Certificate Issuance and Verification System: This component suggests the existence of a system responsible for issuing and verifying digital certificates. In the context of the research, it's important to examine how this system currently works and identify its strengths and weaknesses.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204132 |

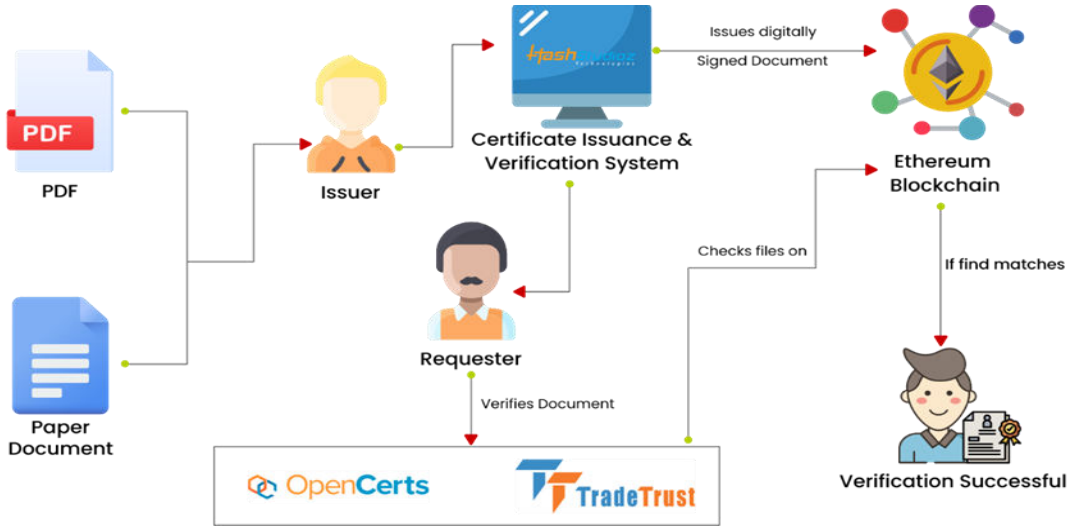


Fig 2. Proposed System model.

Step 3. Ethereum (Blockchain): Ethereum is mentioned as the blockchain technology that is likely being proposed or utilized in the research. Ethereum is a popular platform for developing blockchain-based applications. In this research, it's important to explain how Ethereum is used to enhance the security and efficiency of the certificate validation process.
Step 4. Requester: The "requester" is likely a user or entity that initiates the certificate validation process. In a blockchain-based system, this could be someone who wants to verify the authenticity of a digital certificate.
Step 5. Verification Results: This component indicates the outcome of the certificate validation process. It's essential to understand how the blockchain-based system generates and communicates verification results, including whether a certificate is valid or not.

III.OVERVIEW OF TECHNOLOGY

Python and Tkinter (GUI Development): The graphical user interface (GUI) is developed using Python and the Tkinter library. Python is a versatile programming language known for its simplicity and readability. It is well-suited for developing the user- friendly interface through which users submit and validate certificates. Tkinter, as a standard GUI library for Python, simplifies the creation of interactive interfaces. This combination of Python and Tkinter ensures that users can comfortably interact with the blockchain system.
Cryptographic Hashing (SHA-256): Cryptographic hashing is a fundamental technology used in the project to calculate digital signatures for domain certificates. Specifically, the SHA-256 hashing algorithm is employed to generate unique digital signatures based on certificate contents. These digital signatures are essential for ensuring the authenticity and integrity of submitted certificates.
Permissioned Blockchain Network: The project operates on a permissioned blockchain network. This network configuration enables control over who participates and maintains the blockchain. This permissioned approach aligns with the project's goals of security and trust, as only trusted entities are involved in the maintenance of the system.
Implementation
The project is a practical demonstration of how blockchain technology can be applied to enhance the trust and security of a domain name system.the project combines the graphical capabilities of Tkinter with the security and immutability of a blockchain, implementing custom block and blockchain classes to handle domain certificate transactions. The use of SHA-256 for digital signatures and the PoW algorithm for block mining ensures the integrity and security of the system, while file handling enables data persistence.

Packages

Tkinter (GUI Package): Tkinter is Python's standard GUI library and is used to create the graphical user interface for this project. It provides tools for creating windows, buttons, text fields, labels, and other GUI elements. The project uses Tkinter to build a user-friendly interface for users to interact with the system.
hashlib (Hashing Algorithm): The hashlib package is used for cryptographic hashing. In this project, the SHA-256

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204132 |

(Secure Hash Algorithm 256-bit) is employed to calculate digital signatures for domain certificates. SHA-256 is a widely recognized and secure hashing algorithm used for its ability to produce unique hash values for input data.

Modules : Block and Blockchain (Custom Modules): These custom modules are implemented for the blockchain functionality of the project. They include the following:

Block Class: The Block class defines the structure of a single block in the blockchain. It includes fields for the block index, a list of transactions, a timestamp, and the hash of the previous block. The class also contains methods for computing the block's hash and verifying proof of work.

Blockchain Class: The Blockchain class defines the blockchain itself. It manages a list of blocks, including the genesis block, and handles various blockchain operations, including adding new transactions, mining new blocks, and verifying the blockchain's integrity.

File Handling (Pickle): The project uses Python's pickle module for saving and loading the blockchain object to/from a file named "blockchain_contract.txt." This allows the system to persist the blockchain even after the application is closed and reopened.

Graphical User Interface (GUI): The graphical user interface created using Tkinter provides a user-friendly way to interact with the system. Users can input domain certificate information, save certificates with digital signatures, verify certificates, and view the blockchain's status through the GUI elements, including text fields, labels, buttons, and a text display area. The project utilizes data structures such as lists and dictionaries to manage transactions, blocks, and the blockchain.

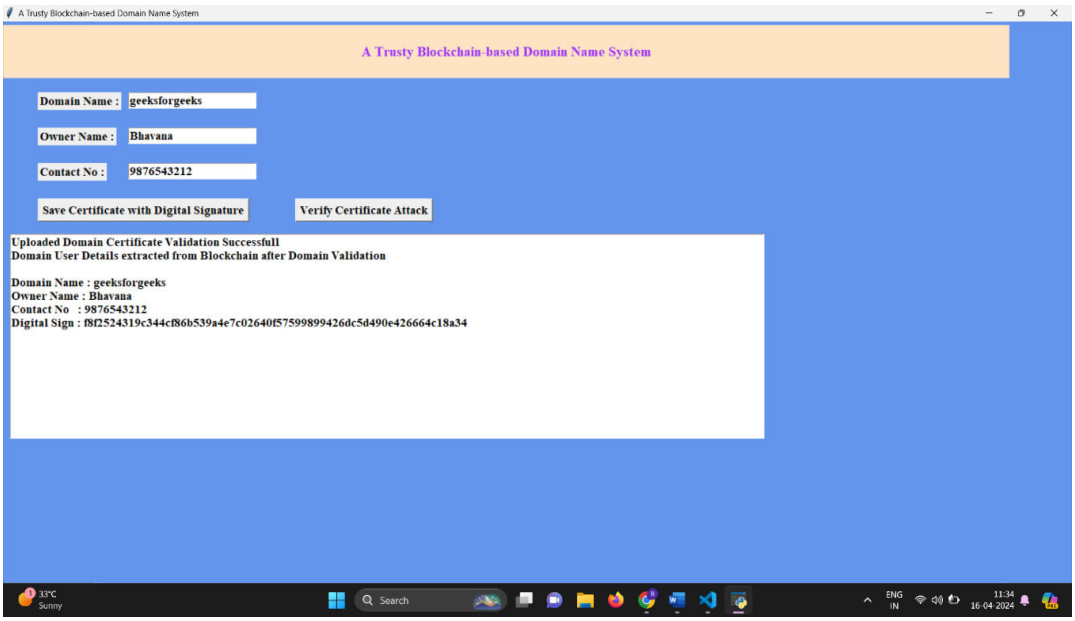
I.A TRUSTY BLOCKCHAIN BASED DNS GUI

International Journal of Innovative Research in Computer and Communication Engineering

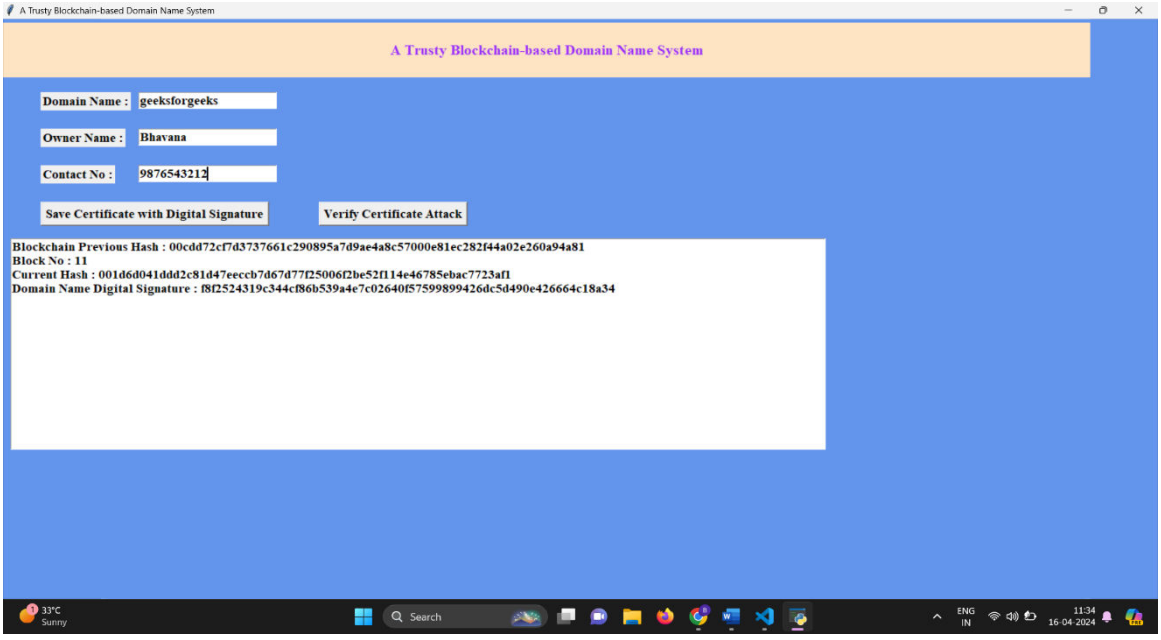
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204132 |



2. Storing certificate and domain name in the blockchain



3.Certificate Verification

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204132 |

4. SSL Certificate for sit

IV.CONCLUSION

Finally, the use of blockchain technology to improve DNS security is very promising in the ongoing fight against DNS threats. Although the Domain Name System is a fundamental component of the internet, creative solutions are required due to its susceptibility to different types of cyberattacks. With its reputation for being decentralized and impervious to tampering, blockchain proves to be a powerful tool in mitigating these weaknesses. Through an examination of the fundamental ideas behind blockchain technology and its useful uses to protect DNS infrastructure, we unearth a potent defense against DNS attacks. DNS transactions are more secure and resistant to manipulation when smart contracts, decentralized identity management, and public/private key infrastructure are included.

REFERENCES

[1] V. Ramasubramanian and E. G. Sirer, "The design and implementation of a nextgeneration name service for the Internet," in Proc. ACM SIGCOMM, 2004.
[2] B. Benshoof, A. Rosen, A. G. Bourgeois, and R. W. Harriso, "Distributeddecentralized domain name service," in Proc. IEEE IPDPSW, May 2016.
[3] S. Gourley and H. Tewari, "Blockchain backed DNSSEC," in Proc. ICBISIT, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details