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.2024.1204103 |

Use of Chains to Block DNS Attacks

Biyyala Ramya, Chunku Saiteja, Vancha Vedhanth Reddy, Mrs. Y. Ashwini

Student, Department of Computer Science Engineering, Anurag University, Hyderabad, Telangana, India

Student, Department of Computer Science Engineering, Anurag University, Hyderabad, Telangana, India

Student, Department of Computer Science Engineering, Anurag University, Hyderabad, Telangana, India

Assistant Professor, Department of Computer Science Engineering, Anurag University, Hyderabad, Telangana, India

ABSTRACT: In today's interconnected and technology-driven world, cybersecurity has become a critical concern for individuals, organizations, and governments alike. As our reliance on digital platforms and systems grows, the threat landscape has expanded, encompassing a myriad of security challenges. Transport Layer Certificates provide encryption and authentication for the communication between clients and servers. However, they do not protect against all types of attacks, such as application-layer vulnerabilities, DDoS attacks, or insider threats. Relying solely on TLS certificates may lead to a false sense of security. This paper presents a novel approach to mitigating URL redirection attacks using blockchain technology. The project aims to leverage the decentralized and tamper-resistant nature of blockchain to enhance DNS security and resilience against various attack vectors, including DNS cache poisoning, DNS reflection attacks, and DNS hijacking. By recording the URL and IP address of a permissioned website in a blockchain, the system establishes a tamper-proof and immutable database of legitimate domain-to-IP mappings.

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

I. LITERATURE SURVEY

C. Cachin and A. Samar, "Secure distributed DNS," in Proc. IEEE/ISIP ICDSN, 2004.E. The proposed method involves creating a secure and distributed DNS system that improves fault tolerance, security, and reliability. It does so by distributing the service, avoiding single points of failure, securely storing zone secrets, and supporting secure dynamic updates. The use of state-machine replication and threshold cryptography enhances security and reliability. The method's effectiveness is validated through real- world experiments.

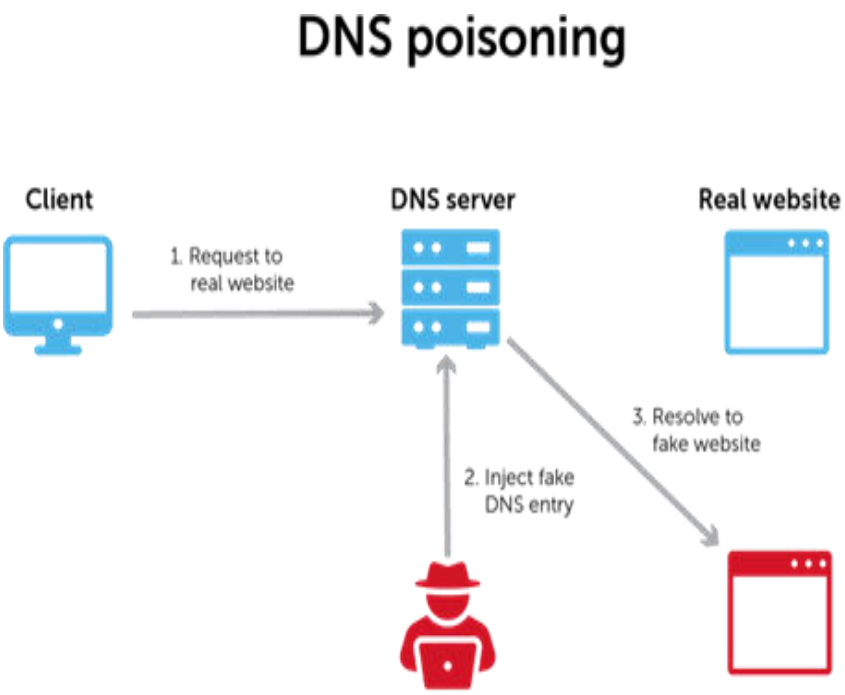
Karaarslan and E. Adiguzel, "Blockchain based DNS and PKI solutions," IEEE Commun. Standards Mag., vol. 2, no. 3, pp. 52–57, Sep. 2018 The proposed method advocates the use of blockchain technology to decentralize key management in PKIs. It highlights the importance of aligning blockchain properties with PKIs, assesses existing implementations, and identifies privacy neglect and limited evaluation as key challenges. The method concludes by providing recommendations to improve blockchain-based PKI systems, making them more privacy-aware and subject to thorough evaluation.

Z. Yu, D. Xue, J. Fan and C. Guo, "DNSTSM: DNS cache resources trusted sharing model based on consortium Blockchain," IEEE Access, vol. 8, pp. 13640-13650, 2020 the proposed method leverages consortium blockchain technology as a foundation for DNS security and credibility. It incorporates trust-based mechanisms and advanced evaluation techniques to enhance the security and reliability of DNS cache management. This model is designed to provide more reliable and trustworthy IP address assignments and DNS resolution results, while also maintaining efficiency. It is particularly valuable in a digital landscape where trust in IP addresses is a critical component of internet security.

| 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.2024.1204103 |



II. PROPOSED METHODOLOGY

The project presents a user-friendly interface using Tkinter, allowing users to interact with the system. The interface includes elements such as labels, input fields, buttons, and a text display area, making it easy for users to input data and view results.

The core of the solution is a blockchain, which is a distributed ledger known for its security and immutability. This blockchain serves as a reliable repository for domain name certificates, ensuring their authenticity and integrity.The system initializes with the creation of a Genesis Block. This first block has no previous transactions, and its purpose is to establish the foundation of the blockchain.

When a user inputs domain certificate information, such as domain name, owner name, and contact number, the system calculates a digital signature using the SHA-256 cryptographic hash. This digital signature uniquely represents the certificate's content and is added to the blockchain.

Users can save domain certificates with digital signatures. The certificate information, along with the digital signature, is added as a transaction to the blockchain. These transactions form the basis of the trust and validation process.
To ensure the security of the blockchain, the system uses a PoW algorithm. This process involves miners finding a nonce value that, when combined with the block's data, produces a hash with a specified number of leading zeros (difficulty). This PoW mechanism adds a layer of security and trust to the system, making it computationally challenging for malicious actors to alter the blockchain.

After users add transactions to the blockchain, the system mines new blocks. Mining involves solving the PoW puzzle for a new block containing these transactions. Once a valid solution is found, the new block is added to the blockchain. This ensures that the blockchain is continuously updated and secured.

Users can verify domain certificates by uploading them. The system calculates the digital signature of the uploaded certificate and compares it to the digital signatures stored in the blockchain. If a match is found, it signifies that the certificate has not been tampered with and is authentic.

| 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.2024.1204103 |

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 (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

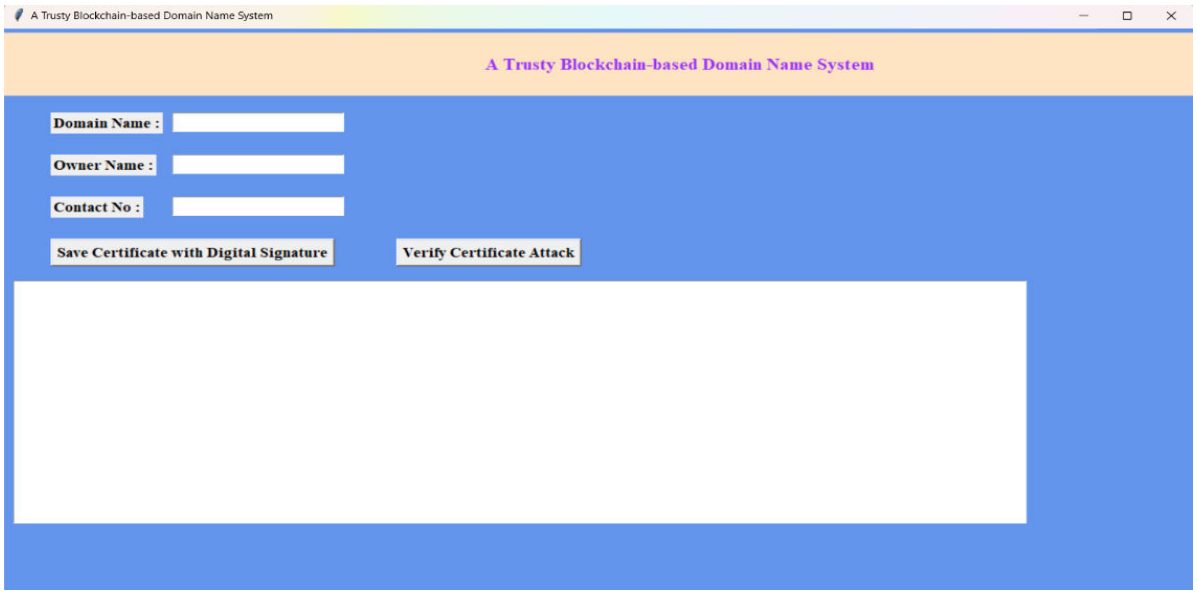
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

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

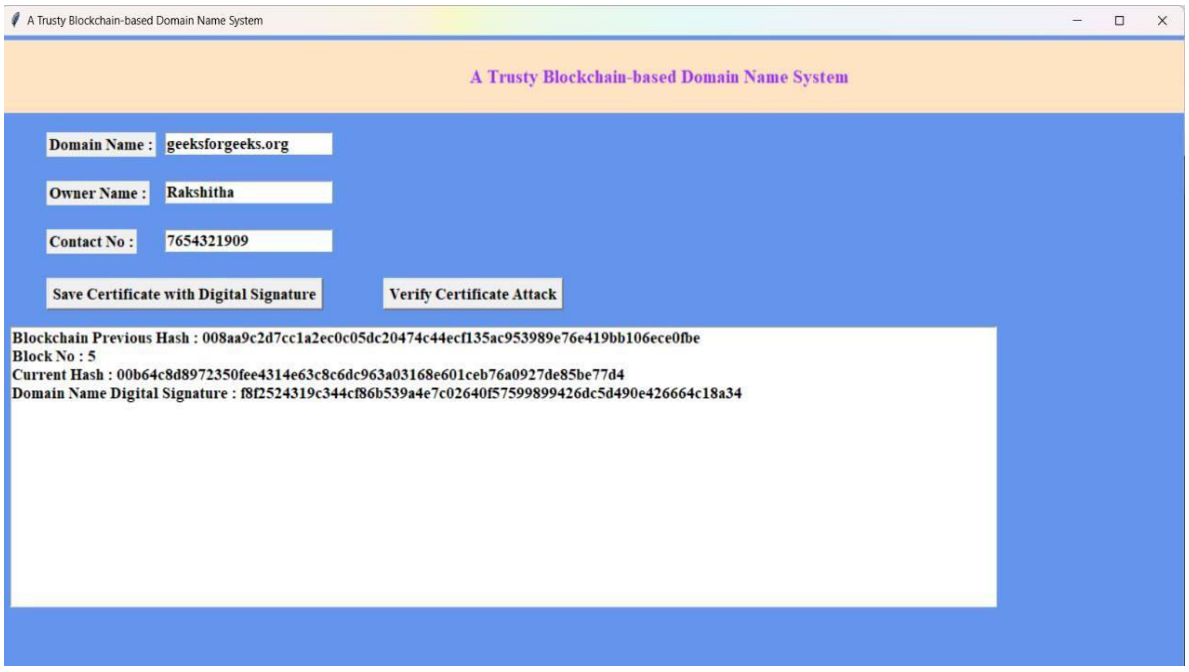
| DOI: 10.15680/IJIRCCE.2024.1204103 |

IV. RESULTS AND DECLARATION

1.A Trusty blockchain based DNS GUI



2. Storing certificate and domain name in the blockchain

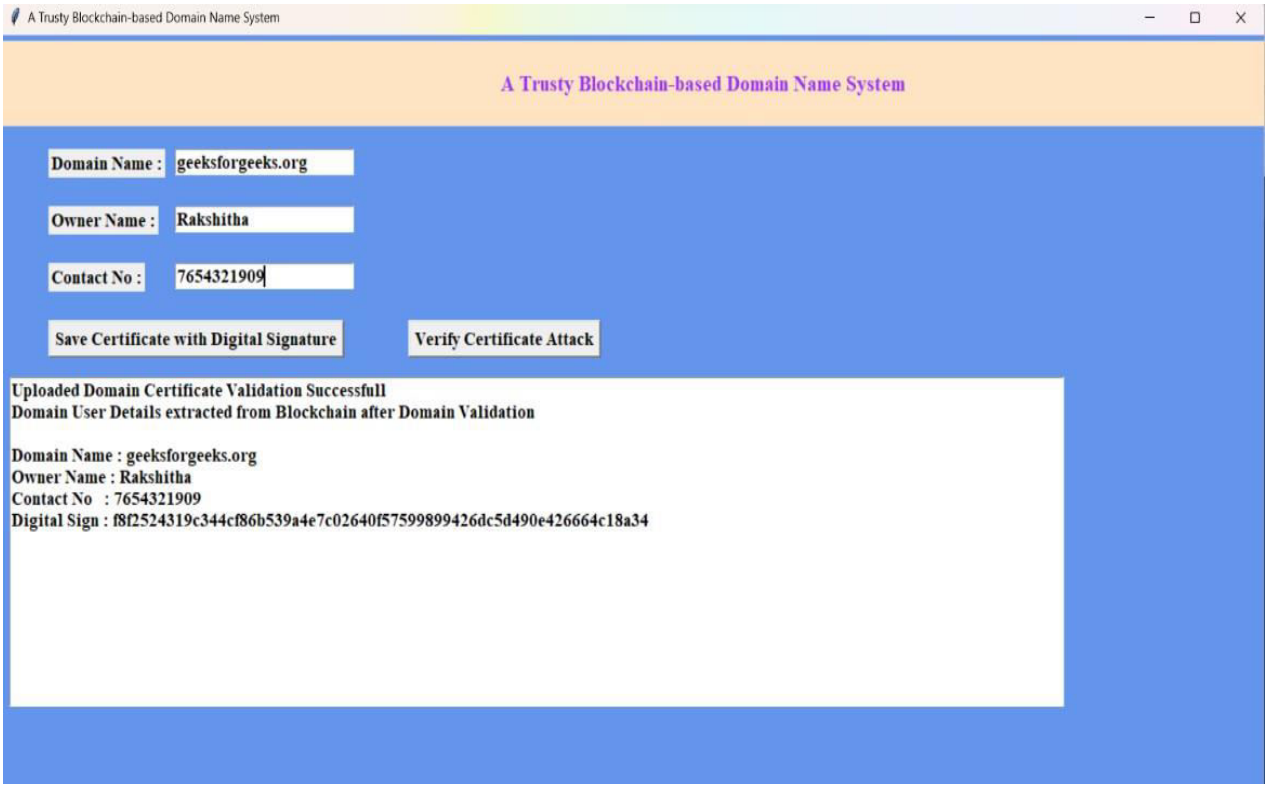


| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

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

| DOI: 10.15680/IJIRCCE.2024.1204103 |

3.Certificate Validation



SSL Certificate for sit

| 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.2024.1204103 |

V. CONCLUSION

In conclusion, the utilization of blockchain technology as a means to bolster DNS security holds great promise in the ongoing battle against DNS attacks. The Domain Name System serves as a foundational element of the internet, but its vulnerabilities to various cyber threats necessitate innovative solutions. Blockchain, renowned for its decentralized and tamper-resistant nature, emerges as a compelling tool to address these vulnerabilities.

By exploring the core principles of blockchain technology and its practical applications in safeguarding DNS infrastructure, we uncover a powerful approach to mitigate DNS attacks. The deployment of smart contracts, decentralized identity management, and public/private key infrastructure enhances the security of DNS transactions, making them resilient to manipulation

REFERENCES

1. C. Cachin and A. Samar, “Secure distributed DNS,” in Proc. IEEE/ISIP ICDSN, 2004.
2. E. Karaarslan and E. Adiguzel, “Blockchain based DNS and PKI solutions,” IEEE Commun. Standards Mag., vol. 2, no. 3, pp. 52–57, Sep. 2018.
3. Z. Yu, D. Xue, J. Fan and C. Guo, “DNSTSM: DNS cache resources trusted sharing model based on consortium Blockchain,” IEEE Access, vol. 8, pp. 13640-13650, 2020.
4. A. Har and T. V. Lakshman, “The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet,” in Proc. ACM HotNets, 2016.

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