|  |  |  |  |
| --- | --- | --- | --- |
|  | **RV COLLEGE OF ENGINEERING®**  **Department of Computer Science and Engineering** | | |
| **Course** | **Network Programming and Security** | **Course Code** | **CS362IA** |
| **Team Student**  **Names and**  **USN** | 1. **MOHITH S** 2. **MANOJ KUMAR B V** 3. **NAGAPRASAD NAIK** | **1RV22CS119**  **1RV23CS407**  **1RV23CS410** | |
| **Project Title** | **Decentralised DNS System Using Blockchain and Machine Learning** | | |
| **Batch** | **B2** | | |
| **Lab Teacher Name** | **Dr. Pavithra H** | | |

**INTRODUCTION TO THE TOPIC:**

This project presents a novel approach to Domain Name System (DNS) management by leveraging blockchain technology and machine learning to enhance security, transparency, and resilience. Unlike traditional DNS systems that rely on centralized authorities, our decentralized model utilizes blockchain to distribute and securely store domain records across a peer-to-peer network. This ensures tamper-proof data integrity and resistance to censorship. To further strengthen security, the system incorporates a machine learning-based threat detection mechanism that automatically identifies and filters malicious domains, including those associated with phishing, malware, and other cyber threats. By combining decentralization with intelligent domain classification, this solution offers a robust and future-ready DNS infrastructure tailored for the evolving needs of the modern internet.

**PROBLEM STATEMENT:**

Traditional DNS systems are centralized and managed by a few organizations, making them vulnerable to single points of failure, cyber-attacks, censorship, and domain hijacking. This centralization can lead to security risks, lack of transparency, and limited user control over domain ownership. There is a need for a more secure, transparent, and censorship-resistant solution for managing domain names on the internet.

**OBJECTIVES:**

* Provide a secure and tamper-proof system for domain name management using blockchain technology.
* Eliminate single points of failure and reduce the risk of unauthorized changes in DNS records.
* Enhance user privacy and control by enabling decentralized and transparent ownership of domain names.

**METHODOLOGY:**

* **Decentralized DNS Using Blockchain:** Traditional DNS systems are centralized, making them susceptible to single points of failure, DNS spoofing, and data tampering. In our approach, blockchain is utilized to store domain-to-IP address mappings on a distributed ledger, ensuring data immutability, availability, and resistance to unauthorized modifications.
* **Domain Validation Using Machine Learning:** A custom-trained machine learning model is integrated into the system to evaluate domain names. This model analyzes each domain and classifies it as either safe or malicious, providing a proactive layer of security against threats such as phishing and malware.
* **User Interaction:** Users interact with the system through an intuitive interface where they can enter the domain name they wish to access.
* **Threat Detection via ML Analysis:** Once the domain is submitted, the machine learning model analyzes it:
  + If the domain is classified as malicious, access is immediately denied, and the user is alerted.
  + If the domain is classified as safe, the system proceeds to the next step.
* **Blockchain-Based Domain Resolution:** The application queries the blockchain ledger to retrieve the IP address and associated port number mapped to the validated domain name.
* **Response to User:** If a valid mapping exists and the domain is deemed safe, the system returns the corresponding IP address and port number to the user. If the domain is found to be malicious or no mapping exists, an appropriate message is displayed to the user.

**INNOVATION / CONTRIBUTION IN NPS**

This project contributes to the field of network programming and security by introducing a decentralized DNS system that leverages blockchain for secure, tamper-proof domain resolution and machine learning for intelligent threat detection. Unlike traditional DNS models that rely on centralized servers vulnerable to spoofing and single-point failures, this approach ensures data integrity and availability through a distributed ledger. The integration of a custom-trained machine learning model enhances network security by automatically identifying and blocking malicious domains in real-time, offering a proactive defense against phishing and malware. This combination of decentralization and intelligent filtering represents a modern, secure, and privacy-focused advancement in DNS infrastructure.

**OUTCOME EXPECTED**

The expected outcomes of this project include the successful development of a decentralized and secure DNS system that eliminates reliance on centralized servers, thereby reducing vulnerabilities such as DNS spoofing and denial-of-service attacks. The blockchain-based domain mapping will ensure data transparency, immutability, and availability. Additionally, the integration of a machine learning model will enable real-time detection and blocking of malicious domain names, significantly enhancing cybersecurity. Users will benefit from a more secure, censorship-resistant, and privacy-preserving DNS experience. Overall, the system aims to demonstrate a reliable, intelligent, and future-ready approach to DNS resolution and threat prevention.

**Signature of Lab Teacher**