Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/22219
DOI URL: http://dx.doi.org/10.21474/IJAR01/22219

RESEARCH ARTICLE

AEGIS NEXUS: BLOCK-CHAIN FORTRESS FOR DOMAINS

G. Pavana Sriya, P. Malavika, I. Sai Amulya, V. Aditya Phanidhar, K. Venkateswarulu and A. Om Sai Chandu

1.UG Student, Dept. of CS-IOT, QIS College of Engineering and Technology (A), Ongole, Andhra Pradesh, India.

Manuscript Info

Manuscript History
Received: 04 September 2025
Final Accepted: 06 October 2025
Published: November 2025

Key words:-
Block chain DNS, smart contracts, Fingerprint Authentication, Domain Security, Anti-Sybil, Rate-Limiting, Decentralization, Monitoring Dashboard, Cybersecurity

Abstract

A critical part of networking,the Domain Name System(DNS)translates human-readable names into IP addresses and is commonly known as the "phonebook" of the Internet. Along with being highly centralized, the traditional DNS referenced earlier is susceptible to frequent issues such as censorship, DDoS attacks, cache poisoning, and manipulation. This paper presents a DNS architecture employing a decentralized/bloc kchain smart contract that incorporates security measures and features a real-time monitoring dashboard safeguarded by a biometric fingerprint access system. Additional network security components of the architect ure consist of rate-limiting (e.g., excessive requests), smart contract gas-price protections, anti-sybil deposits, and bloom-filter-like presence verifications (along with spam and/or attack threat). The biometric dashboard, utilizing fingerprint-secured tracking,notifies administrators about unusual activity logs (event audit trails) and the lifecycles of domain names. By merging the unchangeable nature of blocks with the secure access granted by a biometric method, the suggested architecture aims to deliver blockchain's permanence without forking, thereby enhancing security, transparency, and resilience beyond the capabilities of conventional DNS.

Introduction:-

The Domain Name System (DNS) is the infrastructure of the internet, carrying on the process of taking a domain name and translating it into an IP address. Although the DNS is an essential part of how the internet operates, it has significant weaknesses like cache poisoning, hijacking, single-point of failures, and government-sponsored censorship. Cybercriminals can use the weakness of authentication as well a lack of transparency and cryptographic evidence to switch out a DNS instance. Blockchains use decentralized, tamper-proof technology, and can address many of the weaknesses of DNS. There are other blockchain-based naming systems, but none have a threat-intelligence reporting dashboard and security controls available in real time for easy view and monitoring. This research develops a DNS registry via a smart contract that has specific countermeasures in security, such as biometric fingerprint authentication for monitoring and administration. More resilient and trustworthy security can result from the trustless nature of the blockchain with Ethereum-based smart contracts, on-chain validity, anti- sybil ("effective security deposits"), gas guards for each transaction, and dashboard-level biometric security. This paper

describes the architecture, operation, and benefits of the Secure DNS Registry. DNS attacks are becoming increasingly complicated: Attackers hijack or spoof domains and use cache poisoning to insert false records into the DNS resolvers. DDoS Attacks: Outages occur from central DNS servers being bombarded with traffic. Spoofing and Hijacking: Domains are unfairly registered or controlled by unsanctioned agencies. Censorship: Domains can be blocked or access can be voluntarily prohibited by authorizing bodies

Objective:-

1.Because DNS is centralized by design, a government agency or small group of root authorities can censor, modify, or otherwise manipulate a domain record. This centralization creates a vulnerability that can be damaged and exploited. Blockchain technology can reduce reliance on central DNS control in the future by making all domain records part of an immutable and transparent ledger. Once a domain is registered, DNS will be immutable and deletion from the ledger will require consensus. In this case, one of the objectives is to eliminate dependence on third parties by allowing users to have direct control over their domains. At the same time, the goal is to mitigate the unnecessary effects that come with exposure to manipulation

2.Because traditional DNS is centralized, government departments or a small cadre of root authorities can censor, alter, or tamper with a domain record. Therefore, a centralization vulnerability exists for abuse and corruption. Blockchain technologies create a transparent, unchangeable ledger for all records, which would reduce reliance on central DNS control. Because the DNS is embedded into the blockchains, once a domain is registered, the established ledger cannot be altered nor removed without consensus. The objectives are to reduce reliance on parties, allow users direct control of their domain, and reduce the impact of superfluous manipulation.

3.To design and deploy a dashboard for real-time monitoring that incorporates biometric (fingerprint) authentication. Another major goal is to provide realtime visibility into system security, rather than simply an on-chain verification. The dashboard tracks metrics such as expired and existing domains, logs of suspicious activities, failed transactions, and other pertinent information. Biometric authentication, such as in this case fingerprinting, will be used to access this dashboard for monitoring so that you can monitor performance and security measures, which themselves are secure by limiting access to sensitive data to authorized administrators. This abstraction, in essence, offers system operators a trust-worthy and non-invasive method for visualizing and responding to threats, combining the immutable data on blockchain with a biometric access pattern!

Related Work:-

To guarantee the safe creation, validation, and distribution of digital certificates, Shikhar Saranga,[1] Dhruv Ranaa, Smit Patela, Darshil Savaliyaa, Udai Pratap Rao, and Akhil Chaurasia suggest a Blockchain and IPFS-based Document Management System. The system uses smart contracts to enable time-bound secure sharing and prevents forgeries by storing documents on IPFS and unique identifiers on the Polygon blockchain. Using blockchain technology and smart contracts, Surbhi Sharma, [2] Nidhi, Naincy, and Aayushman Arya suggest a safe and decentralized electronic voting system. The system ensures voter authentication, anonymity, transparency, and immutability of votes by leveraging Ethereum blockchain. Vote casting and counting are automated by smart contracts, and data integrity is protected by cryptographic methods. This method provides a reliable digital voting platform by removing conventional vulnerabilities like vote tampering, multiple voting, and lack of transparency. In order to get around the drawbacks of centralized DNS, Yantao Shen, [3] Yang Lu, Zhili Wang, Xin Xv, Feng Qi, Ningzhe Xing, and Ziyu Zhao suggest a DNS service model based on permissioned blockchain. The model presents algorithms for synchronization and consistency checking, a block data model for safe storage, and a TopLevel Domain Chain (TLDChain) for consensus.

Additionally, it creates a new domain name resolution procedure and incorporates a data warehouse to maximize query efficiency. According to experimental results, the system improves security and resolution speed while achieving decentralization. To solve the problems of trust, transparency, and security in conventional elections, Shivam Bansal, [4] Harsh Raj, Arvind Kumar Tiwari, and P. Balakumar suggest an e- voting system based on blockchain technology. Ethereum smart contracts are used by the system to securely cast and count votes, guaranteeing their anonymity and immutability. Cryptographic methods are used to handle voter authentication, and the design removes potential hazards like multiple voting and vote tampering. A decentralized transparent, and impenetrable digital voting solution is offered by this blockchain-powered framework. To improve the security and dependability of domain name resolution, Aditi S. Deshmukh, Rachana R. Kawtikwar, and Vandana R. Gawande [5] suggest a Blockchain-based Secure DNS Model. The system uses the immutability of blockchain technology to stop

attacks like cache poisoning and DNS spoofing. It presents a decentralized architecture that ensures availability, transparency, and resistance to tampering by storing DNS records on a blockchain. By removing the single points of failure found in conventional DNS, the method enhances secure domain resolution, resilience, and trust.

A Blockchain-based DNS Security Framework is proposed by:-
B. Praveen Krishna, [6]A. Prasanna Lakshmi, and K. Srinivas to improve domain name resolution defenses against spoofing and tampering attacks. In order to ensure immutability and trust, their model combines smart contracts and blockchain technology for decentralized DNS record storage. The system improves query reliability by thwarting malicious modifications and uses consensus mechanisms to validate domain transactions. In contrast to the conventional centralized DNS architecture, this method enhances DNS security, transparency, and resilience. To address the shortcomings of centralized DNS, Surbhi Agrawal, Sakshi Gupta, and Ritu Tiwari suggest a Blockchain-based DNS system [7]. Their approach uses blockchain technology to manage domain names in a safe, transparent, and unchangeable manner, protecting data integrity and thwarting attacks like cache poisoning and spoofing. By using distributed ledger technology to decentralize domain storage and resolution, the framework improves DNS services' reliability, availability, and trustworthiness. [8] Shrey Patel A Blockchain-based DNS Framework is proposed by Neelay Trivedi, Fenil Patel, and Harshil Desai to protect domain name resolution from frequent attacks.

Their system uses smart contracts to decentrally manage DNS records, guaranteeing immutability and guarding against data manipulation. By removing the single points of failure present in conventional DNS, the model improves resilience, trust, and transparency. This method can greatly increase the security and dependability of DNS services, according to experimental design. Vimal Patel, [9] Dhrumil Shah, Nishit Patel, and Vishal Bhavsar suggest a Blockchain-enabled DNS Security System that tackles centralized DNS's weaknesses, including denial- of-service and spoofing attacks. Their method uses smart contracts for domain management and validation, and it makes use of decentralized blockchain infrastructure to store DNS records. This lowers the possibility of single-point failures and unauthorized changes while guaranteeing tamperproof, transparent, and resilient domain name resolution. In order to guarantee secure communication, authentication, and data integrity, G. Kiran Kumar, [10]K. Ajay Babu, and B. Ravi Kumar present a Blockchain- enabled IoT Security Model that combines blockchain technology with IoT devices. To increase trust in IoT networks, the framework uses smart contracts to automate access control and stop malicious tampering.

A blockchain-based cloud data security system is proposed by:-
A. R. Keerthana, R. Praveena, and R. M. Kaviya [11]. Their model ensures safe data sharing and storage by combining blockchain technology with cryptography to provide transparency, tamper-resistance, and enhanced trust in cloud computing environments. A blockchain-based smart healthcare model is proposed by Himadri Sharma, Aditi Sharma, and Poonam Tanwar [12]. It uses blockchain technology to manage Electronic Health Records (EHRs), guaranteeing decentralized control, confidentiality, and immutability of medical data. Role-based access is enforced by smart contracts, enhancing patient data sharing security and effectiveness. Susmita Mondal, [13] Mehak Shafi, Sumeet Gupta, and Sachin Kumar Gupta suggest an EHR management system that incorporates blockchain technology with a private channel and multi-signature stamp. This solves scalability and privacy issues in healthcare by guaranteeing safe ownership, restricted access, and tamper-proof patient record management.

A Blockchain-based Framework for Safe Over-the-Air (OTA) Firmware Updates in Internet of Things Devices is put forth by Xinchi He [14]. The model lowers the risk of centralized failures by ensuring authenticated, tamperproof, and resilient updates for IoT devices through the use of smart contracts and permissioned blockchain. Ahmad Bhat Showkat, [15] Muhammad Sultan, Ishfaq Bashir Sofi, and Nen-Fu Huang present Agri-SCM-BIoT, a Blockchain + IoT architecture for agriculture-food supply chain management. By preventing fraud, guaranteeing food safety, and improving storage and scalability for all supply chain participants, the system improves traceability, transparency, and security.

A Blockchain-based EHR management system with multisignature stamps for authentication and a private channel for secure access is proposed by Susmita Mondal,[16] Mehak Shafi, Sumeet Gupta, and Sachin Kumar Gupta. Hospital employees verify patient records, which are then timestamped and saved on the blockchain with notifications for any unauthorized changes. The framework guarantees decentralized data ownership, security, and transparency. Vennam Preethi, [17] The vulnerabilities in video surveillance systems (VSS), such as CCTV and IP cameras, are reviewed by Pramod T.C., Thippeswamy B.M., YongGuk Kim, and Pavan Kumar B.N. They analyze attack vectors, highlight real-world attacks (like ransomware, Mirai DDoS, and privacy breaches), and suggest

defenses like robust authentication, frequent firmware updates, and secure cloud architectures. Along with comparing current frameworks, the study advocates for more robust IoT-driven smart surveillance security. On Solana, Norbert Bodziony, [18] Paweł Jemioło, Krzysztof Kluza, and Marek R. Ogiela suggest a blockchain-based aliasing system that enables users to create human-readable aliases for tokens and accounts.

This guarantees scalability, decentralization, and low-cost transactions while also enhancing usability and preventing transfer errors [19] Sharyar Wani Yonis Gulzar, Sultan Almotairi, KhalidM. Alhamed, Mohammed Imthiyas, and Hamad Almohamedh examine blockchain-based defenses against DDoS attacks.They examine current approaches (ML, SDN, virtualization), point out scalability problems, and emphasize the advantages of blockchain in terms of decentralization and trustless security. The study categorizes existing methods and describes their advantages, drawbacks, and potential paths forward. Shi Yin and Ning Hu [20] Shen Su, Xudong Jia, Qiao Xiang, and Hao Liu suggest Blockzone, a blockchainbased decentralized DNS data plane that combats DDoS and cache poisoning. It replaces recursive resolution with a decentralized process, integrates off-chain storage with on- chain authorization, and is compatible with conventional DNS. With potential for edge computing and the Internet of Things, the system improves DNS security, resilience, and efficiency.

Formulas:-

Rate Limiting Hour Bucket: hour Bucket = timestamp - (timestamp mod 3600)
Gas Price Control: tx. gas price ≤ max Gas Price Wei Domain Expiry: expires At = current Time + TTL Domain Validity: is Valid = (current Time ≤ expires At)
Economic Deposit: user Payment ≥ minimum Deposit Auto- Resume: resume = (paused AND current Time ≥ pause Time
+ cooldown)

Hash Comparison: keccak256(IP_1) ≠ keccak256(IP_2) Rate Counter: count < max Regs Per Hour Ownership Check: domains[domain]. owner == msg. sender

Algorithms:

Sliding Window Rate Limiter - O(1) complexity
Secure Domain Registration Protocol - O(1) complexity Naive String Search - O(n×m) complexity
Role-Based Access Control (RBAC) - O(1) complexity Batch Expiry Sweep - O(k) complexity
Transaction Gas Guard - O(1) complexity

Proposed System:-

By utilizing blockchain's decentralized and impenetrable characteristics, the suggested system, Blockchain-Based DNS Security with Smart Contract Validation and Fingerprint-Protected Dashboard, seeks to get around the drawbacks of conventional DNS. With built-in security features like deposits, rate-limiting, and gas guards, a smart contract named Secure DNS Registry controlsdomain registration, updates, transfers, and expiration. A real-time dashboard protected by fingerprint authentication logs suspicious activity and gives administrators real-time system insights to bolster monitoring. DNS operations are made secure, transparent, and resilient by this combination.

1. **Implementation & Deployment:** It can be deployed in a real-world setting and is completely implemented. With its real-time monitoring dashboard and smart contract validation, this functional DNS security system can be used by real users without requiring significant modifications. On the other hand, although theoretically sound, B-DNS is still in the conceptual stage and does not yet have a deployable, functional system.
2. **Technical Performance:** It offers good query performance (about 5–10 seconds for a direct contract call) and makes use of Ethereum PoW (Proof of Work). This offers a good balance between efficiency and security. Though more energy-efficient, B-DNS's unique PoS (Proof of Stake) mechanism with a biase coinflipping consensus is not yet ready for practical DNS security applications.

Therefore, even though B-DNS has theoretical advantages, your project performs better in practice

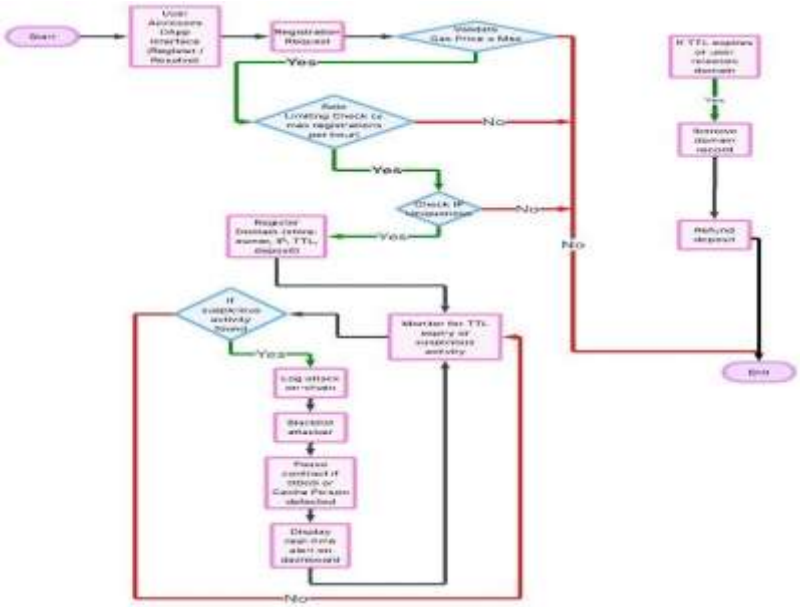
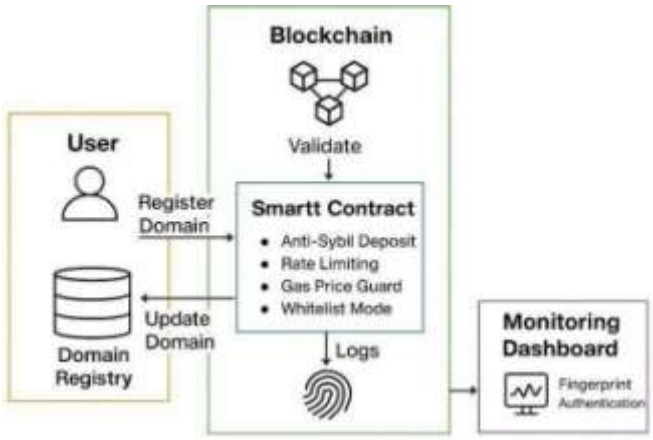


Fig 1: Flow chart for proposed system

1. User Experience: A React web dashboard was integrated, allowing users to easily interact with your DNS system via an intuitive visual interface. B-DNS only uses command-line or API-based interactions and has no user interface at all. With a more approachable and userfriendly experience, this distinguishes your project.
2. Business & Market: Capable of meeting the needs of actual users seeking DNS security solutions with realtime monitoring, this product is ready for the market. BDNS, on the other hand, is more of a research-based Analytics & Monitoring: offers complete visibility into the DNS system's operations and a realtime alerts dashboard, which is essential for operational monitoring. Your project is better suited for real-time tracking and actionable insights because B-DNS does not have such an operational monitoring system.
3. Innovation Level: provides an innovative method with smart contract validation and real-time monitoring by providing a useful, real-world blockchain application for DNS security. Even though B-DNS has a novel consensus mechanism and optimization, its main focus is on academic research and theoretical ideas rather than an immediate operational solution for DNS security.
4. Testing Approach: In our testing approach, we conduct real blockchain transactions for testing using MetaMask without needing to deploy them to a production environment. This method enables us to provide some realistic insights, and prove that it works in a realworld situation. In contrast, B-DNS uses laboratory simulations, that cannot replicate the complexities of operations in the real-world; therefore making your testing approach more actionable and holistic.

Deployment Readiness: Fully viable for deployment meaning the solution can be used and deployed without any major changes, thus being immediately usable and accessible for users. In contrast to B-DNS, which is still in concept stage and not deployable, meaning your solution is far more Three layers make up the suggested system. Through blockchain transactions, the User Layer enables domain owners to register, update, resolve, or transfer their domains. The Secure DNS Registry smart contract, housed in the Blockchain Layer, controls the entire domain lifecycle and implements security measures like bloom filter checks, gas guards, rate-limiting, and anti-sybil deposits. Lastly, the Monitoring Layer gives administrators access to a fingerprint-secured dashboard that allows them to track domain activity and questionable activity in real time. Through biometric-protected monitoring, administrators maintain oversight while this architecture guarantees decentralized, transparent, and secure domain management.

Fig2: proposed system



Results and Discussions:-

Functionality, security performance, and practical usability were among the several aspects of the proposed Blockchain- Based DNS Security System with Smart Contract Validation and Real-Time Monitoring Dashboard using Fingerprint that were analyzed. The outcomes of carrying out the simulated domain registration and contract deployment instances show that the security features built right into the smart contract worked well. Massive domain hoarding and spam registrations were successfully discouraged by usingdeposits as anti-sybil measures. In order to guarantee sustainability and equity in the distribution of domain registration time slots, the rate- limiting algorithms and gas-price guards also stopped resource flooding and transaction spamming. With real-time evidence of suspicious activity and expired domain sweeps, the dashboard, secured by fingerprint authentication, enabled the administrators to conduct additional oversight. The findings imply that combining blockchain immutability with biometric authentication enhances defense against DNS-based attacks and establishes a benchmark for security and resilience. The discussions that follow offer a more thorough assessment of the findings in terms of the system's scalability, trade-offs, and limitations.

Fig3: Image – Register Domain

This interface displays the blockchain-based DNS platform's domain registration procedure. The user supplies a secret key or identifier (1234), enters the domain name (suma.com), and gives it an IP address (1.1.1.1). By selecting "Authenticate & Register," the system securely logs the registration on the blockchain and uses fingerprint authentication to confirm the identity. The bottom message attests to the domain's successful registration and connection to the IP address that was entered. This guarantees that the registration and ownership cannot be altered.

Fig4: Image – Resolve Domain

The domain resolution step is displayed on this screen. After entering a domain (for instance, example.com) in the input field, the user clicks Resolve. A green checkmark at the bottom of the system signifies that it is linked to the blockchain registry. The system is now prepared to retrieve information directly from the blockchain, including IP address, owner details, and validity. This lessens the possibility of DNS spoofing or manipulation and does away with the need for centralized In this case, the registered domain suma.com has been resolved by the system.

Complete metadata is returned by the blockchain:

1. Domain: suma.com
2. IP address: 1.1.1.1
3. Owner: Blockchain wallet address (the domain holder's unique identity)
4. Created/Last Updated Time: The date and time the domain was registered or updated
5. Expiration Time: The date the registration expires
6. TTL Remaining: Theamount of time the record is valid before a refresh is necessary
7. Deposit:The sum that is lockedin the blockchain to preserve domain ownership

The most frequently attacked domains are displayed in this graphic. For example, ram.com has experienced the most attacks, followed by ariyan.com.vashna.com

Fig5: Global infection monitor

Fig6: Domain Resolution Result

Fig7: Attacked Domains

Fig8: Attack Types

The frequency oftargeting of specific domains is shown in the bar chart. Administrators can prioritize defense, spot patterns of recurring attacks throughout the network, and locate hotspots of malicious activity with the aid of this monitoring. The kinds of cyberattacks found against domains are categorized in this chart. Cache poisoning, DDoS, hijacking, phishing, and replay attacks are among the assaults. Phishing and DDoS attacks seem to be the most prevalent among these, whereas cache poisoning, hijacking, and replay are less common. The system's ability to classify attacks enables defenders to apply customized countermeasures and comprehend which threats are most prevalent at any given moment.

Figure 6: System Status This screen displays real-time system performance metrics:

1. CPU Usage65%): indicates the amount of processing power being used by the system;
2. Node Sync (72%), which indicates the degree of synchronization between blockchain nodes and ensures consistency;
3. Gas Usage (72%), which represents transaction costs and computational resources consumed
4. Latency (35%), which measures the time delay in processing or responding. These metrics are essential to maintaining the blockchain DNS service's effectiveness, security, and responsiveness under various loads, particularly during attack attempts.

Fig9: Regex Nexus

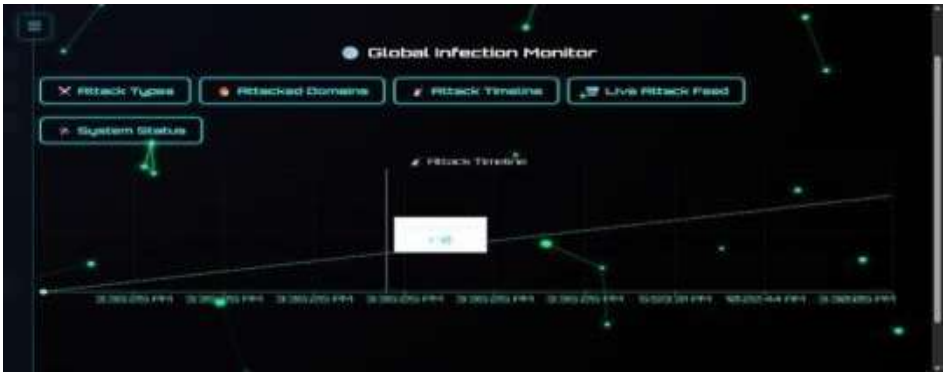


Fig10: Global Infection Monitor – Attack Timeline

The above figure represents the Global Infection Monitor Dashboard, which visualizes worldwide cyberattack activity in real time. It displays multiple monitoring options such as Attack Types, Attacked Domains, Attack Timeline, and Live Attack Feed. The Attack Timeline graph shows the trend of attacks recorded at different timestamps. Each glowing point on the line indicates an attack event, while the connecting line

Fig 11: Registered Domains

The figure Displays the dashboard of a platform called Aegis Nexus. Specially showing the Registered Domain section. The names contain pooja.com, Aditya.com, swathi.com, animal.com, each associated with a unique alpha Numeric identifier possibly representing a blockchain wallet or contract.

Fig 12: Dash Board for domains attacked

This figure shows the attack dashboard for the domain aditya.com, visualizing cybersecurity incidents. The top section categorizes attacks by kind, with hijack, phishing, and DDoS having the highest counts. The middle pie chart displays attacks by actor, showing that most attacks are linked to one particular actor identifier. The bottom section tracks attacks over time, plotting incidents on a timeline to monitor trends and frequencies for aditya.com.

Conclusion:-

In order to address significant shortcomings of conventional DNS, this study suggests a BlockchainBased DNS Security System with Smart Contract Validation and a Real-Time Monitoring Dashboard utilizing Fingerprint. It incorporates gas-price guards, anti-sybil, and suspicious activity logging on-chain, in contrast to earlier blockchain DNS systems. Realtime visibility and tamper-proof administrator access are provided by a fingerprint-secured dashboard. The system increases resistance to censorship, hijacking, and spoofing. Future research can investigate integration with broader biometric devices, multichain support, and AI- driven anomaly detection

References:-

1. Sarang, S., Rana, D., Patel, S., Savaliya, D., Rao, U. P., & Chaurasia, A. (2022). Document management system empowered by effective amalgam of blockchain and IPFS. Procedia Computer Science, 215, 340–349.
2. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., AlMuhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16), 7273.
3. Shen, Y., Lu, Y., Wang, Z., Xv, X., Qi, F., Xing, N., & Zhao, Z. (2021). DNS service model based on permissioned blockchain. Intelligent Automation & Soft Computing, 27(1), 259–268.
4. Papadopoulos, P., Pitropakis, N., Buchanan, W. J., Lo, O., & Katsikas, S. (2020). Privacy preserving passive DNS. Computers, 9(3), 64.

5. Xia, P., Wang, H., Yu, Z., Liu, X., Luo, X., & Xu, G. (2021). Ethereum name service: the good, the bad, and the ugly. arXiv preprint arXiv:2104.05185.
6. Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. Information, 14(2), 117.
7. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038.
8. Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. IEEE Access, 10, 113436–113481.
9. Fragkos, G., Johnson, J., & Tsiropoulou, E. E. (2022). Centralized and decentralized distributed energy resource access control implementation considerations. Energies, 15(17), 6375.
10. Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. Information, 14(2), 117.
11. Zhang, Y., Liu, W., Xia, Z., Wang, Z., Liu, L., Zhang, W., ... & Fang, B. (2021). Blockchain-based DNS root zone management decentralization for Internet of Things. Wireless Communications and Mobile Computing, 2021(1), 6620236.
12. Pelekoudas-Oikonomou, F., Zachos, G., Papaioannou, M., De Ree, M., Ribeiro, J. C., Mantas, G., & Rodriguez, J. (2022). Blockchain-based security mechanisms for IoMT Edge networks in IoMT-based healthcare monitoring systems. Sensors, 22(7), 2449.
13. Cui, S., & Wang, H. (2024). Blockchain-based data sharing algorithm in distributed network data storage. Journal of Computational Methods in Science and Engineering, 24(1), 427–444.
14. Mondal, S., Shafi, M., Gupta, S., & Gupta, S. K. (2022). Blockchain-based secure architecture for electronic healthcare record management. GMSARN International Journal, 16(4), 413–426.
15. He, X. (2019). A blockchain-based framework to secure over-the-air firmware updates for Internet of Things. The University of Tulsa.
16. Bhat, S. A., Huang, N. F., Sofi, I. B., & Sultan, M. (2021). Agriculture–food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability. Agriculture, 12(1), 40.
17. Vennam, P., TC, P., BM, T., Kim, Y. G., & BN, P. K. (2021). Attacks and preventive measures on video surveillance systems: A review. Applied Sciences, 11(12), 5571.
18. Bodziony, N., Jemioło, P., Kluza, K., & Ogiela, M. R. (2021). Blockchain-based address alias system. Journal of Theoretical and Applied Electronic Commerce Research, 16(5), 1280–1296.
19. Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., & Gulzar, Y. (2021). Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight. Symmetry, 13(2), 227.
20. Hu, N., Yin, S., Su, S., Jia, X., Xiang, Q., & Liu, H. (2020). Blockzone: A decentralized and trustworthy data plane for DNS. Computers, Materials & Continua, 65(2), 1531–1557.
21. Dawood, M., Tu, S., Xiao, C., Haris, M., Alasmary, H., Waqas, M., & Rehman, S. U. (2024). The impact of Domain Name Server (DNS) over HTTPS on cybersecurity: limitations, challenges, and detection techniques. Computers, Materials & Continua, 80(3), 4513–4542.
22. Ngo, D. M., Lightbody, D., Temko, A., Murphy, C. C., & Popovici, E. (2024). A scalable security approach in IoT networks: smart contracts and anomaly-based IDS for gateways using hardware accelerators. IEEE Access.
23. Umoren, O., Singh, R., Awan, S., Pervez, Z., & Dahal, K. (2022). Blockchain-based secure authentication with improved performance for fog computing. Sensors, 22(22), 8969.
24. Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., & Gulzar, Y. (2021). Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight. Symmetry, 13(2), 227.
25. Kim, D., & Park, S. (2024). Blockchain-based caching architecture for DApp data security and delivery. Sensors (Basel, Switzerland), 24(14), 4559.
26. Kina-Kina, K. M., Cutipa-Arias, H. E., & Shiguihara- Juárez, P. (2019). A comparison of performance between fully and partially decentralized applications. In Proceedings of the 2019 IEEE XXVI International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Lima, Peru, 12–14 August 2019.
27. Shen, J., Li, Y., Zhou, Y., & Wang, X. (2019). Understanding I/O performance of IPFS storage: A client's perspective. In Proceedings of the International Symposium on Quality of Service, Phoenix, AZ, USA, 24–25 June 2019.
28. Wang, W., Niyato, D., Wang, P., & Leshem, A. (2018). Decentralized caching for content delivery based on blockchain: A game theoretic perspective. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018, pp. 1–6.
29. Freedman, M. J., Freudenthal, E., & Mazières, D. (2004). Democratizing content publication with Coral. In Proceedings of the Networked Systems Design and Implementation (NSDI), San Francisco, CA, USA, 29–31 March 2004; Vol. 4.
30. Twesige, R. L. (2015). A simple explanation of Bitcoin and blockchain technology. Computer Science, 1, 1–5.