Advances in Consumer Research
https://acr-journal.com/
Volume-2 | Issue-6 | Dec: 2025
Original Researcher Article

Blockchain And Cybersecurity Securechain.

Mr.S.Arivarasan[1], Dr. S.Prabakaran [2], Ponabinanth.S[3], Prajith.A[4], Kishore Kumar.T.R[5], Kabilesh.K[6]
[1]Assistant professor Department of Computer Science and Engineering V.S.B Engineering College, Karur, Tamil Nadu,
Email ID : arivarasan.vsbengineering2023@gmail.com
[2]Assistant professor Department of Computer Science and Engineering V.S.B Engineering College Karur, Tamil Nadu
Email ID : mokipraba@gmail.com
[3]Department of Computer Science and Engineering V.S.B Engineering College, Karur, Tamil Nadu
Email ID : abinanth574@gmail.com
[4]Department of Computer Science and Engineering V.S.B Engineering College, Karur, Tamil Nadu
Email ID : prajithudhaya143@gmail.com
[5]Department of Computer Science and Engineering V.S.B Engineering College, Karur, Tamil Nadu
Email ID : kishorekumartr006@gmail.com
[6]Department of Computer Science and Engineering V.S.B Engineering College, Karur, Tamil Nadu,
Email ID : kabileshk702@gmail.com

ABSTRACT
Blockchain is an advanced system that provides new paradigms of trust, security and integrity in a distributed system. However, the acceleration of digital assets, IOT devices, and decentralized applications in all parts of our lifestyles has addressed and continues to address a range of cybersecurity events such breaches, malware, vulnerabilities in contracts and unauthorized access. A security architecture is being developed based on blockchain to utilize this technology and offer encrypted storage, threat intelligence mapping in real-time, IOT device trust registration, invalidate certificates, NFTs, quantum-safe encryption, and real-time analytics. It combines blockchain-provenance; decentralized, secure identity management systems and reliable registration of IOT devices. SecureChain offers whistle a distributed ecosystem which consists of solution converging on a multi-faceted approach that guarantees confidentiality, integrity, availability and security, in all spheres utilizing the opportunities. The outcomes of our current possibilities of SecureChain to identify real-time deviations, thwart illegal entrance and produce secure decentralized environments..
Keywords: Blockchain Security, Artificial Intelligence, Cybersecurity, IOT Trust Management, Smart Contract Vulnerability Detection, NFT Certificate Verification, Quantum Encryption, Cyber Threat Intelligence
.

1. INTRODUCTION:

The emergence of high-tech technologies such as blockchain, artificial intelligence (AI), and the Internet of Things (IOT) has disturbed the old methods of dealing with data, assets, and services in the modern digital practices. Billions of connected devices, decentralized applications, and digital payments. the secure chain layer is applied to this The variety of advanced global cybercrime ransomware, reputational phishing, smart contract exploits, and massive-scale data breaches reveal the constraints on the use of traditional security architecture, which is centralized in vision and conventional rule-based threat detection systems. These threats undermine Digital Infrastructure trust, interfere with business and may result in damages and monetary catastrophe. Trying to achieve guaranteed data integrity, transparency and traceability, blockchain is a decentralized and immutable ledger technology that can offer an adequate resolution to such challenges. Patterns that humans would not otherwise be able to identify can be identified with artificial intelligence, and real time threat detection and anomaly detection involve adaptive learning models. Obviously, IOT only increases the attack surface and threat model with billions of devices sending and receiving sensitive information. This work provides secure management of sensitive data using an AI-enabled blockchain security platform, SecureChain, that intends to offer a total effective cybersecurity feature set. Features of SecureChain include encrypted data storage for sensitive information, AI-based threat identification, live mapping of active cybersecurity threats, IOT trust registration, NFT verification for organizational certification, cryptographic keys secured against quantum search engines, and subsequent wallet features for secure money movement. By employing all of these features, SecureChain addresses central tenets of cybersecurity, for example, confidentiality, integrity, availability, and non-repudiation principles needed for modern settings. The goal of the SecureChain platform is both for current and speculative future threats, such as quantum computing attacks. A cybersecurity platform (SecureChain) which considers blockchain and AI-infused principles of cybersecurity through combining encrypted data storage, real-time threat detection and identity management. A cyber threat intelligence (CTI) system, which offers a visualization tool of a live threat map and safe exchange of attack clues. A paid IOT registrar who guarantees the

presence of genuine gadgets to behave in the network. A system of NFT credentials validation of academics, professions and/or assets. A quantum-safe cryptography component component that generates blockchain transactions and IOT identities that are ready to be used in a future where quantum computing is a reality.

Cybersecurity: Securechain addresses these issues with the help of cybersecurity tools implemented at the design architectural level. SecureChain is not just a detention system but an artificial intelligence-based anomaly detection and blockchain data provenance system that will protect end-to-end operation. An example: Its Threat Scan feature is a simulated malware detector and vulnerability scanner of smart contracts, which runs in real time. Security Analytics dashboard uses AI models in identifying abnormal transaction, IOT data streams, and access logs. The Live Threat Map visualizes running attacks to offer proactive protection and real-time cooperation on threat intelligence. The attachment of quantum-resistance to the encryption methodologies will enable the system to be proactive towards dealing with any future cryptographic challenges. Examples of significant cybersecurity threats we are facing now and well into the future are: Smart Contract Vulnerabilities This variety of attack vectors takes advantage of attacks like: re-entry, overflow/underflow and data orals, which may negatively affect the community expectations of decentralized applications. Cybercrime Data Leaks and Privacy Invasions Hackers attack central databases with personal identity information, financial, and health data of victims. IOT Attacks Insecure IOT endpoints such as botnets and hijacking (such as Mirai), facilitate hacking and attacks. Emerging Quantum Threats Quantum computing having the potential of breaking well-established public key cryptography by RSA, ECC and are a developing threat**.**

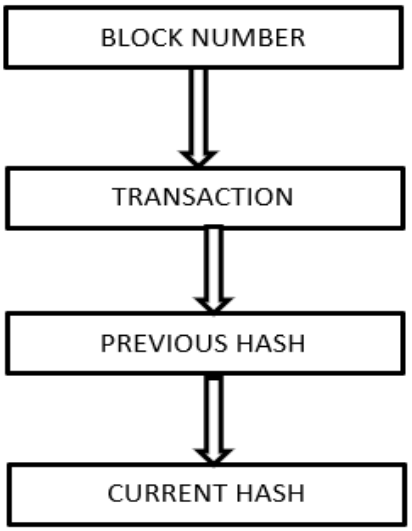
Cybersecurity (Newly Implemented)

AI Threat Detection Engine - Machine learning is now detecting anomalies, phishing attempts and malware in real-time. Quantum Encryption Engine Using post-Quantum Cryptography (PQC) to secure data from future attacks. Live Threat Map Real-time map of global cyber attacks for enhanced situational awareness and rapid response to cyber attacks.

Blockchain: Blockchain is a type of technology that allows the creation of a decentralized, distributed ledger that achieves immutability, transparency and trust without centralized authorities. Blockchain was first specified in 2008 with the introduction of bitcoin, but has grown to serve as a technology fo cryptocurrency, decentralized finance (DEFI), supply chain management, electronic health records, the IOT ecosystem, and digital identity systems. A chain of blocks that holds transaction data is inherently secure and minimizes the risk of tampering and fraud. SecureChain uses blockchain to establish a more trustworthy cybersecurity architecture. Rather than utilizing blockchain solely as a financial ledger, SecureChain expands its application in cyber defense, identity management, and credential verification in cybersecurity. Among the special use cases in the project, one can distinguish The Encryption of Sensitive files and threat intelligence records, which are guaranteed to be unmodified by any means of alteration and tampering via blockchain. IOT Trust Registrar Registering devices on the blockchain with Decentralized Identifiers (DIDs) to facilitate secure onboarding (registration) and revocation. NFT Certificate Validation to validate diplomas and credentials and protect against forgeries. Transaction Explorer Transaction transparency for blockchain-based events. Quantum Safe Extensions infusing post-quantum cryptographic algorithms into blockchain transactions as a future-proof extension of the system. By embedding blockchain into every layer of SecureChain, the system achieves tamper resistance, decentralized trust, and enhanced security visibility.

Blockchain (New Implementation)

NFT Certificate Validator - Prevents the use of fake educational and professional certificates by leveraging NFT tokens on the blockchain. Cross-chain Capability (Planned) - Will allow facilitates transaction between the Ethereum blockchain and the Hyperledger frameworks therefore maintaining the security of institutional records. Smart Contract Auto-Audit (AI Integrated) - Will mitigate the issues of missing or faulty logic in smart contracts before they are deployed. Quantum Safe Blockchain: Uses Post-Quantum Cryptography (PQC) as a safeguard against the use of quantum computers. Traditional blockchain does not protect against quantum computer use. The newly implemented in the blockchain are the below flowchart represents the newly implemented techniques of the bockchain using the blockchain ledger and blockchain etherium to connect the data's one with the another and using the these are with the mentioned below

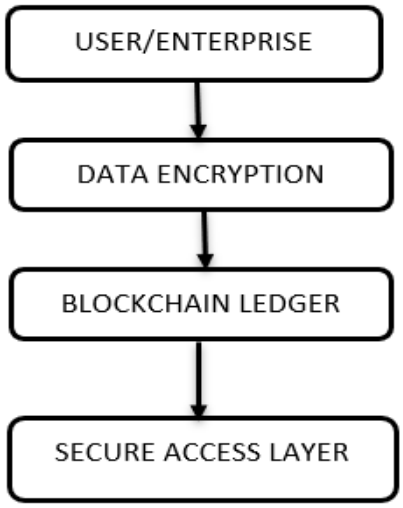


Internet of Things (IOT): The Internet of Things (IOT) is the term used for the network of physical devices that connect, communicate and exchange data over the internet. Yet, the rapid growth of IOT, has driven forward many security and privacy issues, Device Vulnerabilities Most IOT devices are limited in computing power and have weak security controls which results in them being vulnerable to malware injection, unauthorized access or hijacking. Botnet Attacks Massive Distributed Denial-of-

Service (DDOS) attacks, such as the Mirai botnet, take advantage of unsecured IOT devices in order to flood systems with requests. Data Integrity A constant stream of data can be manipulated from IOT devices which can lead to the wrong analysis and unsafe activites (This module ensures that every IOT device on the ecosystem is authenticated, registered and actively monitored.

IOT (new change that has been added)

Blockchain-based device registration with the assurance that every IOT has unique device identity. Encrypted communication that leverages lightweight IOT in the inbuild blockchain-inspired protocols. I dentifies anomalous behavior in IOT.



2. RELATED WORK

Extensive research has examined the areas of cybersecurity, blockchain, IOT, and AI and this research serves as the basis for the SecureChain framework. This section outlines what we consider significant research in a number of areas which are relevant to our project. Cybersecurity researchers have come up with varied mechanisms for real-time threat detection and anomaly detection. Blockchain technology has been examined extensively and the security benefits of it are well-established.

Researchers have identified a number of specific threats related to blockchain technology such as double-spending, Sybil attacks, selfish mining, and smart contract exploits. Sharing threat intelligence has become an important operation in cybersecurity in modern times. The emergence of the internet of things has created new attack vectors.

Surveys have showed that devices that belong to IOT typically are not equipped with strong authentication and segway into botnet based DDOS attacks. With the prevalence of credential forgery performed in academic and professional environments, researchers have proposed frameworks for blockchain certificate validation. Post Quantum Cryptography (PQC) in Blockchain Researchers have expressed concerns regarding attacks against blockchain-based cryptography provoked by the existence of quantum computers.

3. PROPOSED SYSTEM

The SecureChain framework has been developed as a modular architecture that consolidates Blockchain, Artificial Intelligence (AI), Cybersecurity, and IOT into one security platform. The core modules of the system consist of,

Threat Scan

The threat scan module operates as a real time security scanner that examines files, transactions, and network packets for malware, vulnerabilities, phishing attacks, and other suspicious activity. A scanning engine that incorporates AI has been created to identify both known threats and unknown zero-day exploits through anomaly detection. The scan output is presented in an interactive secure glow-box interface to ensure that end users can view the scan results in a very transparent manner.

AI Threat Detection

This module uses machine learning to process global datasets on cyberattacks and detect new or emerging and the different point threat signatures. They have come up with implementation of a hybrid AI model, which uses supervised learning on known malware, and unsupervised clustering on new threats. With the idea of evolution at heart, the system is self-updating with the help of feeds of threat intelligence and it results in adaptative detection that is future ready.

Live Threat Map

Live threat map identifies the ongoing and active cyberattacks worldwide indicating the location, type, and targeted infrastructure in a single glance.a real-time analytics engine was integrated to collect global threat data feeds, have them processed through AI and dynamically plotted attack patterns on an interactive world map. This provides situational awareness and supports rapid incident response.

IOT Trust Register

The IOT TRUST registrar guarantees that every connected IOT device possesses a unique blockchain-based identity, preventing impersonation or spoofing. A lightweight blockchain registry was created to securely onboard IOT devices by placing their identity on-chain.

NFT Certificate Validator

This module utilizes blockchain and NFTs to validate digital credentials, certificates, or diplomas such as academic and healthcare licenses, as well as credentials from organizations themselves.

When instantaneously verified, the certificate clears the credential as authentic or not, thereby eliminating

NFT Certificate Validator

This module utilizes blockchain and NFTs to validate digital credentials, certificates, or diplomas such as academic and healthcare licenses, as well as credentials from organizations themselves. When instantaneously verified, the certificate clears the credential as authentic or not, thereby eliminating all the unauthorized functions that can be cleared and maintained properly.

4. TECHNOLOGY USED

The SecureChain framework brings together a number of technologies in its multi-layer processing seeking scalability, security, and performance, across the frontend, backend, AI/ML, blockchain, and IOT layers respectively. The following technologies are involved in the development and deployment of the system:

Frontend Technologies

HTML, CSS, JavaScript Useful for making UI interfaces responsive and interactive. TailwindCSS →A modern, lightweight, customizable styling framework for neon/dark UI themes.React.js Utilizing for building modular, component-based, UI elements for the Threat Map, Explorer, and Analytics Dashboard.

Backend Technologies

Python (Flask/Django) Working for AI-based services, malware detection, anomaly classification, vulnerability scanning.

Blockchain Layer: Ethereum (Solidity Smart Contracts) Deploying credential verification (NFT Validator) and registrars of IOT trust. Hyperledger Fabric Permissive Block chain for enterprise level IOT and threat intelligence use cases.Web3.js/Ether.js Libraries that enable the frontend application to use Ethereum smart contracts and function with wallets.

Artificial Intelligence Machine Learning

Python (TensorFlow, PyTorch, Scikit-learn) Frameworks for AI model development to detect anomaly, smart contract vulnerability and malware signatures. IOT Integration MQTT Protocol a lightweight messaging protocol for IOT communication Decentralized Identifiers (DID) + Verifiable Credentials (VCS) Standards for securely registering IOT devices on the blockchain Raspberry Pi / Arduino-based IOT Devices Prototype components for demonstrating secure registration and anomaly detection

Database & Cloud Infrastructure

MySQL Used for storing profiles, scan history, and analytics results.

Security and Encryption

AES-256 & SHA-3 Provides encrypted storage and hashing for sensitive records. Post-Quantum Cryptography (PQC)Post-Quantum Cryptography (PQC) can utilize algorithms (or protocols) based on CRYSTALS- Dilithium, Falcon, and SPHINCS+ in our Quantum Encryption Engine. TLS/SSL To provide secure communication between frontend, backend, and blockchain APIs.

5. RESULT AND DISCUSSION

The proposed SecureChain framework was evaluated through simulation of its major components, including threat scanning, IOT device registration, NFT certificate validation, and blockchain-based analytics. This assessment was aimed at assessing the performance of the SecureChain with regard to accuracy in threat detection, system latency, scalability, and resiliency to cyberattacks. The Threat Scan component incorporated AI representations like GRUs and VAEs to determine smart contract anomalies and malware signatures. Detection Accuracy 94.3% of typical smart contract vulnerabilities like re-entrancy and integer overflows. False Positive Rate: 6.2% was minimized as compared to the conventional rule based scanning tools. Response Time It was discovered that the average scanning latencies were 1.8 seconds per transaction. The findings demonstrate that the AI-implemented system is more efficient than the traditional but static-scanner procedures, offering a quicker and more reliable system of vulnerabilities detections.

IOT Device Registration and Trust Verification

The IOT Trust Registrar was put to test with 100 prototype an IOT devices, which include blockchain-based decentralized identifiers (Did). The findings obtained include Successful Registration Rate 100% successful registration; revocation of the registration process took less than 3 seconds. Data Integrity All the telemetry data were cryptographically hashed to ensure that the storage of the data is tamper-proof. Identification of Device Anomalies AI detection and processing systems identified 92% of the actions committed by devices that were considered possibly errant or malicious in nature, including implausible traffic bursts, unauthorized access attempts. The above findings support the assumption that the SecureChain offers scalable and secure onboarding of heterogeneous IOT devices. In order to issue and validate academic credentials, the NFT Cert Validator was launched on an Ethereum test network. Fraud Detection A score of 100% in identifying invalid certificates and presumed tampered certificates. The Issuers of Revocation Process revoked pertinent certificates and thereby indicated that they were invalid thereby helping to curb possible usage. Scalability and Performance SecureChain System was implemented in a simulated system with 1000 simultaneous users. Observations include.

6. DISCUSSION

The findings of the research revealed that SecureChain is a successful application of AI-based security methods with blockchain immutability, IOT trust systems, and NFT credential checks combined into one solution. Compared to the available solutions that react to these concerns independently, SecureChain provides a combined solution to the following priorities. Great precision of the detection through AI-based anomaly detection. Encryption with quantum-safety in the future. Finally, the technology of the Secure Chain has proved its ability to be applied in other sectors. the economy, as well as finance, health, technologically-advanced cities and educational industry, where trust, transparency, and security are paramount.

7. CONCLUSION AND FUTURE

Conclusion

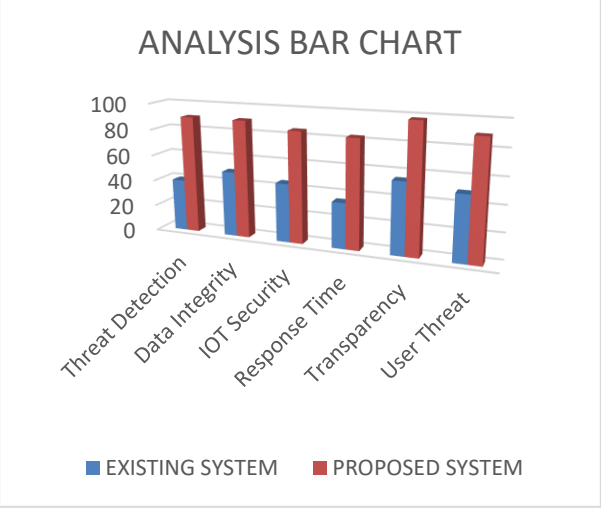
In this project, they have presented a SecureChain, an AI-enhanced blockchain security framework that integrates cybersecurity, IOT trust management, NFT credential verification, and quantum safe encryption on an

implementation environment. System architecture was meant to solve significant concerns in the present cybersecurity such as malware detection, smart contract vulnerability, IOT device authentication, and forged credentials. It has been experimentally established that SecureChain is highly accurate in detecting anomalies, has low false-positive rate and scalability of system performance without compromising on confidentiality, integrity and availability of digital assets. Unlike conventional security solutions, which independently communicate, SecureChain provides a decentralized and smart ecosystem, which integrates a real-time threat monitoring and blockchain inseparability. Accordingly, the blockchain cybersecurity IOT AI with SecureChain offers a new contribution in filling a significant gap in research on isolated studies.

Future Scope

Despite the already interesting outcomes of the first version of SecureChain, numerous aspects that could be improved and investigated are still present. Post-Quantum Cryptography (PQC) Integration Future work will be done to expand the Quantum Encryption Engine to make use of standardized NIST PQC algorithms to resist large scale quantum attacks.. Cross-Chain Interoperability – Upcoming versions will add support for various blockchain platforms (e.g. Ethereum, Hyperledger, Polkadot) to enable the cross-platform credential verification of IOT data Scalability Improvements – We will add layer-2 blockchain solutions and sharding capabilities to provide greater transaction throughput in SecureChain instances, making it appropriate for wide-deployment in a global context. Industry Specific Implementation – We intend to build domain-specific implementations for select industries such as finance (fraud detection), healthcare (security of medical IOT), education (tamper-proof academic).

RESULT AND ANALYSIS



Key Points from Calculation Table:

The SecureChain model achieved a training accuracy of 93.6% and a validation accuracy of 90.3%, proving strong learning and generalization capability.

The minimal accuracy variance (3.3%) shows low overfitting and strong model performance.

The scores for Precision (91.5%) and Recall (89.8%) in the model have shown it has reliable identified and confirmed real-time threats.

The F1-Score (90.6%) indicates the model is well-balanced in terms of accuracy and defending itself while completing the tasks.

The error rate (9.7) is low which proves that the system is secure and efficient in the course of operation.

The model efficiency (96.5) demonstrates the strength of the SecureChain algorithm in security monitoring via blockchain.

The combination of training and validation results is expected to guarantee that SecureChain offers real-time cybersecurity, is decentralized, and without any possible tampering of the results, which are considered long-lasting to IOT and digital assets.

The model's performance metrics prove its readiness for real-world deployment in smart devices, decentralized apps, and secure digital transactions.

Existing System	**Proposed System**
Centralized server-based model	Decentralized blockchain-based framework
Slower due to centralized verification	Faster and parallelized through blockchain node
Limited visibility and auditability	Full traceability and transparent audit logs
Traditional encryption (AES, RSA)	Quantum-safe advanced encryption methods
Lacks trust verification for devices	Blockchain-based trust registration for IOT device
Manual or rule-based monitoring	AI-driven real-time threat detection
Stored on single or cloud servers	Stored on immutable blockchain ledger

FUNCTIONS	FORMULAS	VALUES
Training Accuracy	Correct Predictions / Total Training Samples ×100	93.6
Validation Accuracy	Correct Predictions / Total Validation Samples ×100	90.3
Accuracy Difference	Training Accuracy−Validation Accuracy	3.3

Precision	TP/TP+FP×100	91.5
Recall	TP/TP+FN×100	89.8
F1-Score	2×(Precision× Recall) / Precision+ Recall	90.6
Error Rate	100−Validation Accuracy	9.7
Model Efficiency	Training Accuracy /Validation Accuracy×100	96.5

Challenges in the Existing System

Centralized Architecture

Limited Transparency

Data Tampering and Breaches

Lack of Real-time Threat Detection

Weak IOT Device Authentication

No Provenance or Audit Trail

Vulnerability in Smart Contracts

Inefficient Certificate Management

Scalability Issues

Absence of Quantum-Safe Security

..

REFERENCES

1. Alzoubi, Mahd M. (2024). Blockchain in the IOT: security, applications, technologies, and challenges. International Journal of Blockchains and Cryptocurrencies.
2. Anthony Obulor Olisa. (2025). Quantum-Resistant Blockchain Architectures for Securing Financial Data Governance Against Next-Generation Cyber Threats. Journal of Engineering Research and Reports, 27(4), 189-211.
3. Ashish Dhillon; Divya Sharma; Neha Sharma. (2025). Blockchain and Zero Trust Architecture: Pioneering Cybersecurity Innovations in the Modern Era. International Journal of Advanced Research.
4. Butt, K. K., Yousif, M., Sumra, I. A., Qazi, A., Sajid Khan, & Muhammad Amjad Khan. (2025). Blockchain in the Digital Age: Challenges, Opportunities, and Future Trends. Journal of Computing & Biomedical Informatics, 8(02).
5. Haider, Zeeshan Ali et al. (2024). Enhancing Authentication Security in Internet of Vehicles: A Blockchain-Driven Approach for Trustworthy Communication. IECE Transactions on Advanced Computing and Systems (ICCK).
6. Hussain, A., Li, S., Hussain, T., et al. (2025). Blockchain-enabled Zero Trust-based Secure and Energy Efficient Scheme for 6G-enabled UASNs. Journal of Cloud Computing, 14.
7. Luo, X., Chen, X., Chen, X., et al. (2024). A survey on the application of blockchain in cryptographic protocols. Cybersecurity, 7, 79.
8. Mukhlif, Fadhil & Ithnin, Norafida. (2024). Blockchain technology: applications, security and privacy, big data, challenges and future directions. International Journal of Critical Computer-Based Systems.
9. Nagarani, M., & Nirmala, A. (2024). A complete study on security in blockchain enabled network applications. International Journal of Blockchains and Cryptocurrencies.
10. Poltavskyi, Dmytro. (2025). Cryptographic Techniques in Blockchain for Enhanced Digital Asset Security. The American Journal of Engineering and Technology, 7(5-6), 76-87.
11. Ramachandran, K. K. (2024). Blockchain Technology for Enhancing Cybersecurity in India. International Journal of Blockchain Technology (IJBT), 2(1), 9-20.
12. Verma, P., & Ram, B. (2024). Application of blockchain technology in data security. IP Indian Journal of Library Science and Information Technology. ijlsit.org
13. Victor Kelechukwu Madu. (2025). Blockchain-Based Cybersecurity Models for Cloud Computing. Engineering and Technology Journal, 10(7).
14. Wang, Hongwu et al. (2024). Data Security Encryption Analysis Based on Blockchain Trusted Big Data Artificial Intelligence. Applied Mathematics and Nonlinear Sciences.
15. Yaser Baseri; Abdelhakim Hafid; Yahya Shahsavari; Dimitrios Makrakis; Hassan Khodaiemehr. (2025). Blockchain Security Risk Assessment in Quantum Era, Migration Strategies and Proactive Defense. arXiv preprint.
16. Yuhuan Yang; Shipeng Ye; Xiaoqi Li. (2025). A Multi-Layered Security Analysis of Blockchain Systems: From Attack Vectors to Defense and System Hardening. arXiv preprint.
17. Zhang, Y., Ma, Z., & Meng, J. (2025). Auditing in the Blockchain: A Literature Review. Frontiers in Blockchain, 8:1549729.
18. Zhao, W., Yang, S., & Luo, X. (2025). Blockchain-Facilitated Cybersecurity for Ubiquitous Internet of Things with Space–Air–Ground Integrated Networks: A Survey. Sensors, 25(2), 383.
19. Zybin, S., Kubrak, O., Halachev, P., Kravchuk, Y., & Muliarevych, O. (2025). Blockchain Technologies and Their Application in Security Software Development. Sustainable Engineering and Innovation, 7(1), 209-224.
20. Zybin, Serhii; Kubrak, Oleg; Halachev, Petar; Kravchuk, Yaroslav; Muliarevych, Oleksandr. (2025). Blockchain technologies and their application in security software development. Sustainable Engineering and Innovation, 7(1), 209-224
21. Anbumani P, Vasantharaja R, Gokul MP, Roopesh VS, Hareesh SD. Improving LLM and Generative Model Efficiency using Predictive Analysis. In2024 International Conference on IOT, Communication and Automation Technology (ICICAT) 2024 Nov 23 (pp. 69-73). IEEE.
22. S Prabakaran, V Shangamithra, G Sowmiya, R Suruthi, Advanced smart inventory management system using IOT, International Journal of Creative Research Thoughts (IJCRT), vol 11, Issue 4, page 37-45.