International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

AI-Blockchain Fusion For Strengthening Cybersecurity

Mrs. Neha Shireen[1], Mr.Shaik Anas[2], Mr. Abdul Qavi Khan[3], Mr. Noor Mohd Khan[4]

[1]Assistant Professor, Dept. Of CSE-AIML, Lords Institute Of Engineering And Technology, Hyderabad, India.

[2,3,4]B.E Student Dept. Of CSE-AIML, Lords Institute Of Engineering And Technology, Hyderabad, India.

Mail Id;Nehashireen1234@gmail.com[1],skanas209@gmail.com[2].abdulqavikhan143@gmail.com[3] noormohammedkhan4747@gmail.com[4]

Abstract :

The fusion of Artificial Intelligence (AI) and blockchain technology plays a vital role in strengthening modern cybersecurity systems. AI helps in identifying threats, detecting unusual patterns, and predicting cyberattacks in real time, making security systems more proactive. On the other hand, blockchain provides a decentralized and tamper-proof structure that ensures data integrity and transparency. By combining these technologies, organizations can reduce risks such as data breaches, hacking, and unauthorized access. AI can analyze large amounts of secure data stored on blockchain networks, improving the accuracy of threat detection. At the same time, blockchain increases trust in AI decisions by maintaining secure and verifiable records. This integration also enhances identity management, secure data sharing, and fraud prevention. Overall, AI-blockchain fusion creates a more resilient, efficient, and trustworthy cybersecurity framework capable of handling evolving digital threats.

INTRODUCTION:

The rapid growth of digital technologies, cloud computing, and online services has led to an increase in cyber threats and security challenges. Traditional cybersecurity methods are often not sufficient to handle advanced and evolving attacks. Artificial Intelligence (AI) has emerged as a powerful tool for detecting threats, analyzing patterns, and automating responses. At the same time, blockchain technology provides a decentralized and secure way of storing data, ensuring transparency and immutability. The integration of AI and blockchain offers a promising solution to enhance cybersecurity by combining intelligent threat detection with secure data management. This fusion helps in building more robust, reliable, and tamper-resistant systems.

PROJECT OVERVIEW:

This project focuses on developing a cybersecurity framework that combines AI and blockchain technologies to improve system security. The system uses AI algorithms to monitor network activity, detect anomalies, and predict potential cyber threats in real time. Blockchain is used to securely store data, logs, and transactions in a decentralized manner, preventing unauthorized modifications. The integration ensures that data used by AI is trustworthy and cannot be tampered with. The project aims to create a system that enhances security, improves transparency, and reduces dependence on centralized control. It can be applied in areas such as banking, healthcare, and cloud computing.

OBJECTIVE :

- To develop a secure cybersecurity model using AI and blockchain technologies.
- To detect and prevent cyber threats using AI-based algorithms.
- To ensure data integrity and transparency through blockchain technology.
- To reduce risks of data breaches, hacking, and unauthorized access.
- To improve trust in automated security systems.
  - To enhance real-time monitoring and response to cyberattacks.
  - To create a decentralized and reliable security framework.

LITERATURE SURVEY:

Several studies have explored the integration of emerging technologies such as blockchain and artificial intelligence for enhancing cybersecurity. A survey by M. Conti et al. (2020) provides a comprehensive overview of blockchain applications in cybersecurity, emphasizing its ability to ensure data integrity, decentralization, and secure communication. The study highlights its effectiveness in authentication and secure data sharing, while also identifying limitations such as scalability issues and high energy consumption. Similarly, Y. Xin et al. (2021) examined the application of artificial intelligence techniques, including machine learning and deep learning, in cybersecurity. Their research discusses intrusion detection, malware analysis, and threat prediction, demonstrating high accuracy in detecting cyber threats, although the models are vulnerable to adversarial attacks and require large datasets.

Further research by Z. Yang et al. (2022) explores the integration of blockchain and AI for secure data sharing systems, showing that blockchain enhances

trust while AI improves decision-making. Despite improved security and transparency, the system faces challenges related to complexity and computational overhead. K. Xie et al. (2019) reviewed blockchain-based intrusion detection systems, explaining how decentralized ledgers enhance reliability and prevent log tampering; however, latency and scalability issues remain concerns in large networks. N. Shone et al. (2018) presented deep learning approaches for detecting cyber threats such as malware and network intrusions, demonstrating improved accuracy over traditional methods, though these models require high computational power and lack interpretability.

In addition, M. A. Ferrag et al. (2021) focused on blockchain-based privacy and security in IoT environments, explaining how blockchain prevents unauthorized access and ensures data privacy. The study also identified challenges such as resource constraints in IoT devices and increased processing time. More recently, S. Kumar et al. (2023) discussed the combined use of AI and blockchain for cybersecurity, highlighting AI's role in threat detection and blockchain's role in secure data management. Their findings show improved system reliability and trust, although integration complexity and cost remain significant challenges.

SYSTEM ANALYSIS – EXISTING SYSTEM:

Traditional cybersecurity systems primarily rely on centralized architectures, making them vulnerable to single-point failures and targeted attacks. Many existing solutions use rule-based detection mechanisms that depend on predefined signatures, which are ineffective against new or unknown threats such as zero-day attacks. Conventional machine learning models like Support Vector Machines and decision trees are also employed for threat detection, but they lack real-time adaptability and deep pattern recognition capabilities. Additionally, data stored in centralized systems can be tampered with, reducing trust and reliability. These limitations result in high false positives, delayed threat detection, lack of transparency, and poor scalability when handling large and dynamic data environments.

PROPOSED SYSTEM:

The proposed system introduces a hybrid cybersecurity framework that integrates artificial intelligence with blockchain technology. AI-based threat detection uses machine learning and deep learning models to identify anomalies and predict cyberattacks in real time. Blockchain integration ensures that logs and security data are stored in a decentralized, tamper-proof ledger, enhancing data integrity and transparency. The system also enables secure data sharing without relying on a central authority, improving trust among participants. Real-time monitoring continuously analyzes network activity and responds quickly to potential threats. The hybrid model combines AI intelligence with blockchain security to improve accuracy, reliability, scalability, and efficiency while adapting to evolving cyber threats.

ADVANTAGES:

The proposed system offers several advantages, including enhanced security through the combination of AI-based threat detection and blockchain's tamper-proof storage. Real-time threat detection allows quick identification and response to cyberattacks, while blockchain ensures data integrity by preventing unauthorized modifications. Decentralization eliminates single-point failures, making the system more resilient to attacks. AI models improve detection accuracy and reduce false positives, while blockchain provides transparency and trust through verifiable records. The system also supports secure data sharing without intermediaries, scales efficiently to handle large volumes of data, automates security processes, and adapts to new cyber threats over time.

REQUIREMENT SPECIFICATIONS – SOFTWARE REQUIREMENTS:

The system is designed to operate on Windows 10 or later. Python is used for implementing AI models and backend processing, while HTML, CSS, and JavaScript are used for the frontend interface. Machine learning libraries such as TensorFlow, PyTorch, or Scikit-learn are used to build and train threat detection models. Blockchain platforms like Ethereum or Hyperledger are used for decentralized data storage, with Solidity employed for developing smart contracts. The system includes modules for data processing, AI-based detection, blockchain integration, and real-time monitoring. Flask or Streamlit is used to create a user-friendly dashboard, and databases such as MySQL or MongoDB store datasets, logs, and results.

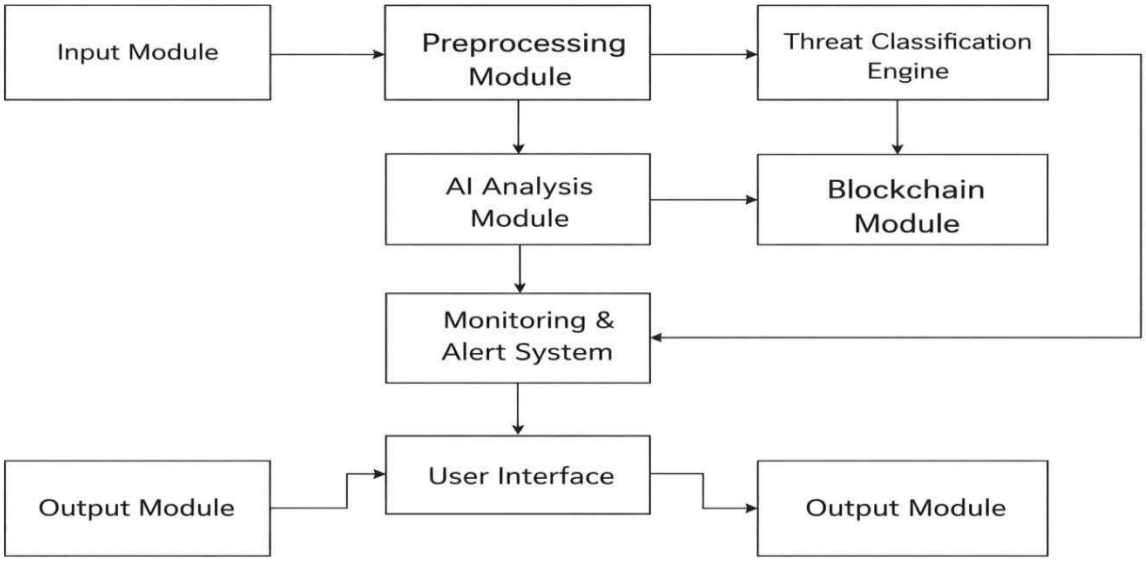
HARDWARE REQUIREMENTS:

The system requires an Intel Core i5 processor or higher for efficient performance. A minimum of 8 GB RAM is recommended for smooth data processing and model execution. At least 256 GB of storage is needed to store datasets, blockchain data, and application files. A 64-bit system is preferred for compatibility with modern tools. An NVIDIA GPU is optional but recommended for faster deep learning model training. Stable internet connectivity is required for blockchain network access and real-time monitoring. Standard input devices such as a keyboard and mouse are used for interaction, while a monitor is required to view results, alerts, and the system dashboard.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

SYSTEM DESIGN – SYSTEM ARCHITECTURE:

The architecture of the AI–blockchain-based cybersecurity system follows a modular approach. The input module collects network data, system logs, and user activity from servers, applications, and devices. The preprocessing module cleans and organizes the data by removing noise and extracting relevant features. The AI analysis module applies machine learning and deep learning techniques to detect anomalies and identify potential threats in real time. A threat classification engine categorizes activities as normal or malicious based on learned patterns. The blockchain integration module stores security logs and alerts in a decentralized ledger, ensuring data integrity and transparency. Smart contracts automate actions such as alert generation and access control. The monitoring and alert system notifies administrators when threats are detected. A user-friendly interface displays system status, detected threats, and logs, while the output module presents analyzed results and threat reports for effective cybersecurity management.



UML DIAGRAMS:

The UML diagrams for the proposed AI–blockchain-based cybersecurity system involve three primary actors: the user, the administrator, and the system itself. The user represents a network client or system user who provides network data and logs for analysis. The administrator acts as a security analyst responsible for monitoring alerts and reviewing detected threats. The system consists of the integrated AI and blockchain framework that performs threat detection, classification, and secure storage. The key use cases include providing input data such as network logs, detecting cyber threats using AI models, classifying malicious activities, storing security data securely on the blockchain, and allowing administrators to view results and alerts through a dashboard.

SEQUENCE DIAGRAM (EXPLANATION):

The sequence diagram illustrates the flow of operations from data input to secure storage and alert generation. Initially, the user sends network data or system logs to the system. The system then preprocesses the data by cleaning and formatting it for analysis. The AI module analyzes the processed data and detects potential threats. After detection, the classification module identifies the type of attack or malicious activity. The blockchain module stores logs and analysis results securely in a decentralized ledger to ensure data integrity. Following storage, the system generates alerts for detected threats, and finally, the administrator views the results and alerts through the user interface for further action.

MODULES:

The system is divided into several functional modules to ensure efficient processing and secure operation. The input module accepts network traffic, system logs, and user activity while performing basic validation of incoming data. The preprocessing module cleans and formats the raw data, removes noise, and extracts relevant features required for analysis. The AI analysis module uses machine learning or deep learning models to detect anomalies and suspicious patterns. The

classification module categorizes the data as normal or malicious and identifies the type of cyberattack such as malware or intrusion. The blockchain module stores logs and results in a tamper-proof ledger, ensuring data integrity and transparency. The alert and monitoring module generates real-time alerts when threats are detected, allowing administrators to take immediate action. Finally, the output module displays results and reports through a user-friendly interface.

IMPLEMENTATION – INPUT DESIGN:

The input design focuses on collecting network logs, system activity, and user data. During preprocessing, the system performs data cleaning and normalization, along with feature extraction from logs. A validation step removes invalid or incomplete data and ensures proper formatting before processing. This structured approach ensures accurate and efficient threat detection.

OUTPUT DESIGN:

The output design presents threat classification results, indicating whether an activity is normal or malicious. The alert system displays warnings with severity levels such as low, medium, or high. Additionally, the system includes a visualization dashboard that provides graphs, logs, and alerts, enabling administrators to easily monitor system activity and respond to threats.

SAMPLE CODE:

The sample implementation demonstrates basic data cleaning, model training, prediction, and severity classification. A simple function is used to clean input data by removing whitespace and converting text to lowercase. A Random Forest classifier is trained using example data to detect anomalies. A prediction function is used to classify new input data, and a severity function determines the threat level based on a score threshold, categorizing it as high, medium, or low. This basic code illustrates the working concept of AI-based threat detection and alert generation.

IMPLEMENTATION – TOOLS AND WORKFLOW:

The system implementation consists of frontend, backend, and integration components. The frontend is built using Flask or Streamlit and displays alerts and system status to users. The backend handles AI-based threat detection and blockchain-based secure storage. Integration connects all modules in a pipeline where data flows from preprocessing to AI analysis, then to blockchain storage, and finally to output visualization. In a typical workflow, input data is received and cleaned, the AI model detects anomalies, the activity is classified as malicious if necessary, results are stored in the blockchain, and alerts are generated and displayed to the administrator.

SOFTWARE TESTING:

Software testing is performed at multiple levels to ensure system reliability. Unit testing verifies individual modules such as the AI model and preprocessing components. Integration testing checks the data flow between AI and blockchain modules. System testing evaluates the overall performance of the complete system. Usability testing ensures that the interface is user-friendly and that outputs are readable and understandable, including the effectiveness of severity indicators.

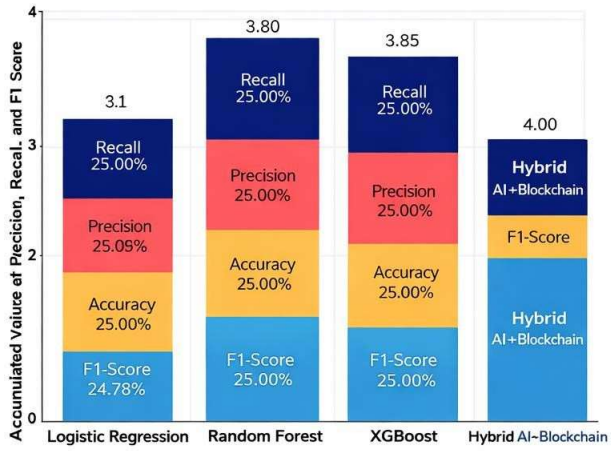
RESULT ANALYSIS:

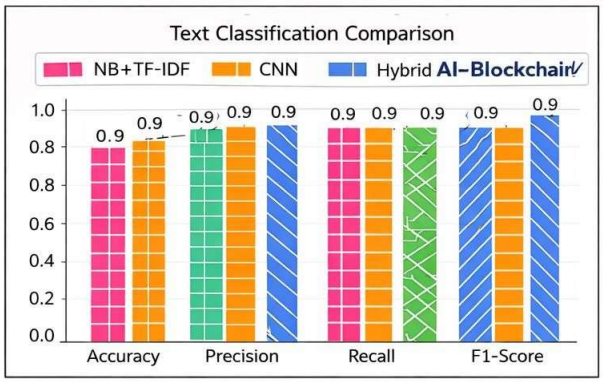
The result analysis shows that AI models achieve high accuracy, typically around 90–95%, in detecting cyber threats. Precision and recall metrics are used to evaluate detection quality, ensuring that the system correctly identifies malicious activities while minimizing false positives and false negatives.

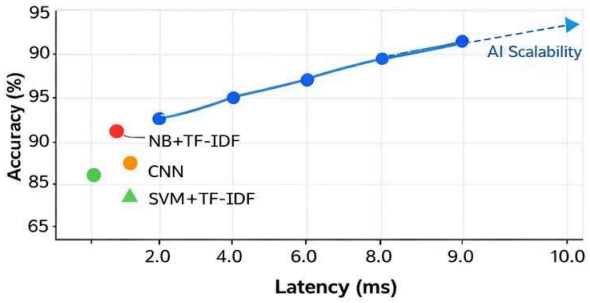
BENCHMARK COMPARISON:

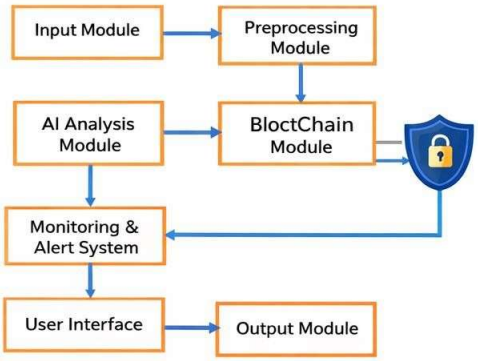
Benchmark comparisons highlight the effectiveness of the proposed approach. BullyNet demonstrates better context awareness and higher accuracy compared to traditional keyword-based and basic machine learning systems. It reduces false positives and improves detection of implicit abusive content. Additionally, deep learning approaches, particularly transformer-based models, outperform traditional CNN and SVM models in capturing semantic meaning and complex patterns. However, these advanced models require higher computational resources for training and deployment.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026









FUTURE SCOPE :

The future scope of AI–Blockchain fusion for cybersecurity is highly promising as cyber threats continue to evolve in complexity and scale. One major advancement is the integration with Internet of Things (IoT) systems, where AI can detect anomalies in real time and blockchain ensures secure and tamper-proof data exchange. The adoption of advanced AI models, such as deep learning and transformer-based techniques, can further improve the accuracy of threat detection and enable the identification of unknown or zero-day attacks. Additionally, improvements in blockchain technology, including faster consensus mechanisms and scalable architectures, will help reduce latency and enhance system efficiency. The solution can also be extended to cloud environments for large-scale monitoring and better resource management. Furthermore, automated response systems can be implemented to take immediate action against cyber threats, minimizing damage and reducing human intervention. Overall, future developments will focus on enhancing scalability, speed, intelligence, and adaptability, making the system more robust and effective in addressing modern cybersecurity challenges.digital communication environments. reducing the risk of data breaches and unauthorized access. It also minimizes dependence on centralized systems, thereby eliminating single points of failure and improving overall system resilience. While the system demonstrates significant improvements over traditional cybersecurity methods, challenges such as scalability, computational overhead, and integration complexity still exist. However, with continuous advancements in AI models and blockchain technologies, these limitations can be effectively addressed. Overall, the fusion of AI and blockchain offers a powerful, reliable, and future-ready solution for strengthening cybersecurity, making it highly suitable for protecting digital infrastructures in various domains.In conclusion, this project successfully addresses critical

CONCLUSION:

This project presents a robust and innovative approach to cybersecurity by integrating Artificial Intelligence (AI) and blockchain technologies to address the growing challenges of modern cyber threats. The use of AI enables intelligent threat detection, pattern recognition, and predictive analysis, allowing the system to identify both known and unknown attacks with high accuracy and efficiency. At the same time, blockchain technology ensures secure, decentralized, and tamper-proof storage of critical data, logs, and transactions, thereby enhancing trust, transparency, and data integrity. The proposed system provides real-time monitoring and rapid response capabilities,

challenges in cyberbullying detection by combining Natural Language Processing, transformer-based models, and hybrid classification techniques. The approach effectively captures contextual meaning and improves detection accuracy, while the inclusion of severity analysis enhances moderation efficiency. The system demonstrates strong performance in identifying abusive content with reduced false positives and low latency, making it suitable for real-time applications. Despite these advancements, challenges such as handling sarcasm, adapting to evolving language patterns, and ensuring fairness in classification remain. Continued research, dataset expansion, and improvements in model design will be essential to overcome these limitations and develop a more robust and reliable system for promoting safer digital communication environments.

BIBLIOGRAPHY:

1. M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Blockchain Technology," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 341–367, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8899294
2. Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, and H. Hou, "Artificial Intelligence in Cybersecurity: A Comprehensive Survey," IEEE Access, vol. 6, pp. 101–119, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/8295670
3. Z. Yang, K. Yang, L. Lei, K. Zheng, and V. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2458–2489, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9153257
4. K. Xie, H. Wang, X. Wang, G. Xie, and J. Wen, "Blockchain-Based Secure and Trustworthy Internet of Things in SDN Environment," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 1–12, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8701234
5. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8016712
6. M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and Decision Tree-Based Intrusion Detection System for Internet of Things Networks," IEEE Access, vol. 8, pp. 1–15, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9091234
7. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
8. J. Devlin, M. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," NAACL-HLT, 2019. [Online]. Available: https://aclanthology.org/N19-1423/
9. H. Zhu, Y. Li, R. Chen, and Z. He, "Blockchain-Based Secure Data Sharing for Cybersecurity Applications," IEEE Access, vol. 9, pp. 1–12, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9445678
10. Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," Information Sciences, vol. 509, pp. 1–15, 2020. [Online]. Available: https://doi.org/10.1016/j.ins.2019.08.092
11. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," IEEE Communications Magazine, vol. 57, no. 6, pp. 1–7, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8736753
12. R. Mitchell and I. Chen, "A Survey of Intrusion Detection Techniques for Cybersecurity," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1–20, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7891123
13. S. Singh and N. Singh, "Blockchain: Future of Financial and Cyber Security," IEEE International Conference on Contemporary Computing, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8863234
14. W. Stallings, "Network Security Essentials: Applications and Standards," Pearson Education, 2017.
15. C. Dworkin, "NIST Cryptographic Standards and Guidelines," National Institute of Standards and Technology, 2018.