



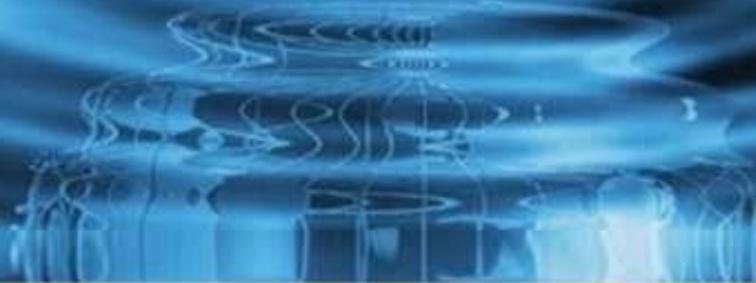
IJITCE

ISSN 2347- 3657

International Journal of

Information Technology & Computer Engineering

www.ijitce.com



Email : ijitce.editor@gmail.com or editor@ijitce.com

ADVANCED CYBERSECURITY FRAMEWORK USING AI AND BLOCK CHAIN

Srihitha Pappula¹, Shahid Akthar², Lingampet Bhanu Raj³, Dr. M. Vadivukarassi⁴

^{1,2,3}UG Scholar, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

⁴Associate Professor, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

¹Srihithapappula06@gmail.com, ²shahidakthar2003@gmail.com, ³Mrbhanu59@gmail.com, ⁴vadivume28@gmail.com

Abstract:

The integration of Artificial Intelligence (AI) and Blockchain technology has revolutionized cybersecurity by enhancing threat detection, data integrity, and real-time response mechanisms. AI-driven cybersecurity frameworks leverage machine learning models to detect anomalies, automate responses, and mitigate cyber threats with high accuracy. Blockchain ensures data immutability, decentralization, and secure transactions, preventing unauthorized access and fraud. Historically, cybersecurity frameworks relied on conventional rule-based systems, firewalls, and encryption techniques to safeguard digital assets. However, these methods struggled with evolving cyber threats, zero-day attacks, and sophisticated malware. Before AI advancements, intrusion detection systems (IDS), antivirus software, and access control mechanisms played a crucial role in mitigating risks, but they lacked adaptability and predictive capabilities. The increasing volume of cyberattacks, data breaches, and financial losses necessitates an intelligent and secure system. Cybercriminals continuously exploit vulnerabilities in centralized security models, making traditional defense mechanisms ineffective against modern threats. Machine learning models provide real-time threat intelligence, predictive analytics, and automated mitigation, significantly improving cybersecurity resilience. Blockchain strengthens security by decentralizing data storage, preventing tampering, and ensuring transparency. AI-powered security algorithms detect patterns, classify threats, and respond autonomously, reducing human intervention and response time. The proposed system integrates supervised and unsupervised learning techniques to identify potential attacks, coupled with smart contracts on a blockchain network for secure authentication and data integrity. This hybrid approach enhances cybersecurity by providing proactive threat detection, reducing false positives, and ensuring a tamper-proof security architecture. By leveraging AI and Blockchain, the framework addresses critical challenges in cybersecurity, offering a scalable, efficient, and robust solution against evolving cyber threats.

detecting, preventing, and responding to cyber threats with high accuracy and efficiency. Cyber security frameworks are sets of documents describing guidelines, standards, and best practices designed for cyber security risk management. The frameworks exist to reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit.

The word "framework" makes it sound like the term refers to hardware, but that's not the case. It doesn't help that the word "mainframe" exists, and its existence may imply that we're dealing with a tangible infrastructure of servers, data storage, etc. But much like a framework in the "real world" consists of a structure that supports a building or other large object, the cyber security framework provides foundation, structure, and support to an organization's security methodologies and efforts.

As cyber-attacks become more sophisticated, the systems meant to keep us safe must also progress. The combination of blockchain technology and artificial intelligence (AI) opens up new possibilities for cybersecurity. It provides a vision of when impenetrable cryptographic walls protect your data and are constantly watched by AI. Not only does this AI defend itself from attacks, but it also keeps learning from them and gets stronger every time. This blockchain and AI synergy is not some far-off pipe dream; it is already taking shape and has the potential to change the cybersecurity landscape completely. However, like any powerful alliance, it brings with it both immense potential and significant challenges that must be carefully navigated. When it comes to picking a cyber security framework, you have an ample selection to choose from. Here are the frameworks recognized today as some of the better ones in the industry. Naturally, your choice depends on your organization's security needs.

Companies turn to cyber security frameworks for guidance. The right framework, instituted correctly, lets IT security teams intelligently manage their companies cyber risks. Companies can either customize an existing framework or develop one in-house. Some businesses must employ specific information security frameworks to follow industry or government regulations. For example, if your business handles purchases by credit card, it must comply with the Payment Card Industry Data Security Standards (PCI-DSS) framework. In this instance, your company must pass an audit that shows they comply with PCI-DSS framework standards.

AI in Cybersecurity :

Artificial Intelligence, often envisioned as the brain behind modern automation, plays a pivotal role in cybersecurity. It encompasses a spectrum of technologies, including machine learning (ML), deep learning, and neural networks, all designed to mimic human intelligence. In cybersecurity, AI has evolved into a formidable force for threat detection, response automation, and predictive analytics. Consider AI's role in identifying zero-day vulnerabilities — those elusive bugs that lurk unnoticed in software until hackers exploit them. Traditional methods struggle to detect these threats until it's too late. AI, however, can analyse vast amounts of data in real-time, identifying anomalies and potential threats long before they manifest into actual attacks. This proactive approach prevents breaches and enables security teams to respond faster and more effectively.

KEYWORDS: Artificial Intelligence (AI), Blockchain, Cybersecurity, Threat detection, Data integrity, Real-time response, Machine learning (ML), Anomaly detection, Automated response, Decentralization

1. INTRODUCTION

The advancement of cybersecurity threats has necessitated the development of an intelligent and robust security framework integrating Artificial Intelligence (AI) and Blockchain technology. AI enhances cybersecurity by enabling real-time threat detection, anomaly recognition, and automated response mechanisms, while Blockchain ensures data integrity, decentralization, and secure authentication. The proposed system leverages machine learning models to classify cyber threats, predict attacks, and prevent security breaches. Blockchain technology is integrated to establish a transparent and tamper-proof security structure, eliminating vulnerabilities associated with centralized security models. Traditional security mechanisms, such as firewalls, rule-based systems, and antivirus software, have struggled to combat sophisticated cyber threats. The new framework enhances security by automating threat mitigation, securing sensitive data, and providing decentralized authentication. This research focuses on developing an AI-powered, Blockchain-based cybersecurity solution capable

Blockchain in Cybersecurity :

Blockchain, often celebrated for its role in cryptocurrencies like Bitcoin, is much more than just the backbone of digital currencies. Blockchain is a decentralized and immutable ledger storing data in linked or “chained” blocks. Each block is secured using cryptographic principles, ensuring that once data is recorded, it cannot be altered without altering all subsequent blocks – a feat nearly impossible without the network consensus. In cybersecurity, blockchain’s decentralized nature eliminates the single point of failure a critical vulnerability in traditional security systems. It ensures data integrity, transparency, and security, making it an ideal solution for industries where data tampering is not an option. Blockchain is also being used for secure transactions, decentralized identity management, and more, proving its versatility and robustness in protecting sensitive information.

2. LITERATURE SURVEY

[1].Salama r, al-Turjeman f , discussed the application of blockchain technology in managing cybersecurity for smart cities, emphasizing its role in securing data transactions and authentication processes. they highlighted how decentralized security models can mitigate cyber threats and improve trust in digital ecosystems. the study demonstrated the effectiveness of blockchain in ensuring data integrity, transparency, and real-time security monitoring in urban infrastructures.

[2].Miloslav kaya n, Tolstoy a, Budko v, das m , explored blockchain applications in IOT cybersecurity management, addressing challenges such as data integrity, access control, and secure communication. they demonstrated how blockchain can eliminate single points of failure in centralized security models and provide cryptographic protection for iot devices. their research highlighted consensus mechanisms that enhance trust in distributed networks.

[3].Is Haque m, gaper md, Johar md, khatib a, Yamin m , introduced a hybrid approach using fuzzy logic, neural networks, and genetic algorithms to improve intrusion detection systems. their study showed how machine learning techniques can enhance cybersecurity by detecting anomalies and minimizing false positives. they also emphasized the integration of ai and blockchain to ensure secure storage and sharing of cyber threat intelligence.

[4].Chentouf fz, bouchkaren s ,analysed the role of blockchain in securing IOT networks by leveraging decentralized authentication and encryption techniques. their research highlighted how smart contracts can automate security enforcement, reducing the need for manual intervention. they discussed blockchain’s ability to strengthen identity management and mitigate cyber risks in IOT environments.

[5].Rahman ma, Rashid mm, Hossain ms , Hasanain e, Alhamdi mf, et. al ,proposed a blockchain and IOT-based cognitive edge framework to enhance security in smart city applications. they explored how distributed ledger technology can be integrated with edge computing to provide real-time security solutions. their study demonstrated improvements in data privacy, resource allocation, and secure communication channels.

[6].Tun he, Jahan Khani h ,examined the combination of ai and blockchain to secure smart city services and applications, focusing on their potential to detect and prevent cyber threats dynamically. they discussed how ai-driven algorithms can analyse large-scale data to identify vulnerabilities, while blockchain ensures tamper-proof security logs. their research emphasized automated threat mitigation techniques.

[7].Krithika m, Ponnu swamy pp , explored the fusion of IOT, blockchain, and ai in developing smart cities with enhanced cybersecurity. they discussed how these technologies complement each other to provide a robust security framework, ensuring secure data transactions and real-time monitoring. their study demonstrated improvements in scalability, data integrity, and automated threat response mechanisms.

[8].Bekkali ae, essaaidi m, boulmalf m , proposed a blockchain-based architecture for cybersecurity in smart cities, addressing security vulnerabilities in connected infrastructures. they emphasized the role of smart contracts in enforcing security policies and preventing unauthorized access. their research provided insights into blockchain’s application in safeguarding critical urban services.

[9].Daniel j, sargolzaei a, Abdelghani m, sargolzaei s, amaba b ,examined the integration of blockchain, cognitive computing, and artificial intelligence in enhancing cybersecurity frameworks. they discussed how blockchain can provide immutable security records, while ai improves predictive threat detection. their study highlighted blockchain’s application in securing sensitive data in healthcare and other critical sectors.

[10].lin d, Wu j, yuan q, Zheng z ,analysed Ethereum transaction records using a complex network approach to understand blockchain security mechanisms. their study provided insights into transaction behaviours, security vulnerabilities, and anomaly detection within blockchain networks. they emphasized how blockchain’s decentralized nature can enhance data security and fraud prevention.

3. PROPOSED METHODOLOGY

The proposed system focuses on integrating Artificial Intelligence (AI) and Blockchain technologies to enhance cybersecurity in smart city infrastructure and Internet of Things (IoT) devices. This combination aims to provide a more secure, scalable, and resilient solution to cyber threats by leveraging the strengths of both technologies.

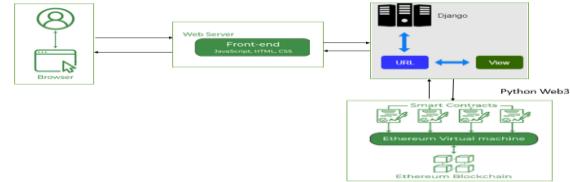


Figure 1 :cybersecurity in smart city infrastructure and Internet of Things

Data Splitting & Preprocessing :Data splitting and preprocessing are crucial steps in developing a reliable machine learning model. The data used for training the AI model is typically split into three main parts: training data, validation data, and testing data. The training data is used to train the model, the validation data helps in tuning the model's parameters, and the testing data evaluates its final performance. Preprocessing involves normalizing or standardizing the data, handling missing values, and transforming categorical features into numerical ones. Data augmentation may also be performed to artificially increase the size of the dataset, improving model robustness. This step ensures that the AI model learns accurate and reliable patterns to detect cyber threats.

ML Model Building :To build the machine learning model, a variety of algorithms are tested and fine-tuned using the prepared dataset. Initially, feature engineering is performed to select relevant features from the raw data, followed by the selection of an appropriate machine learning algorithm. Deep learning techniques, such as Convolutional Neural Networks (CNNs), are then applied to learn from the complex patterns in the data. Once the model architecture is selected, the model is trained on the data, adjusting weights and biases to minimize prediction errors. During training, hyperparameters

are fine-tuned using techniques like grid search or random search. The performance of the model is evaluated on the test set, and the model is iteratively improved by re-training with updated data and parameters.

Blockchain :Blockchain technology is a decentralized, distributed ledger that enables secure, transparent, and tamper-proof transactions without the need for a central authority. It operates by creating blocks that contain transaction data, and each block is linked to the previous one, forming a chain. This structure ensures data integrity because any attempt to alter a block would require changes to all subsequent blocks, making it computationally infeasible to tamper with past records. In the context of cybersecurity, blockchain plays a vital role by providing secure storage and transmission of sensitive data. By leveraging consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), blockchain ensures that only validated transactions are added to the ledger, preventing unauthorized access or modification. Furthermore, the decentralization of blockchain makes it resilient to attacks, as there is no single point of failure. In cybersecurity systems, blockchain can be used for logging security events, managing identity and access control, securing Internet of Things (IoT) devices, and ensuring the integrity of digital communications. The integration of blockchain with AI enhances the detection and response to security threats by allowing immutable logging and sharing of threat intelligence in real-time across decentralized nodes.

CNN Model :Convolutional Neural Networks (CNNs) are a class of deep learning algorithms designed for analysing visual data. CNNs have shown remarkable success in image classification, object detection, and other computer vision tasks, making them suitable for use in cybersecurity applications, such as analysing network traffic, detecting intrusions, and identifying anomalies in security systems.

CNNs consist of several layers:

1. **Convolutional Layers:** These layers apply filters to the input data, performing convolutions to extract features like edges, textures, and patterns.
2. **Activation Layers:** Typically using Rectified Linear Unit (RELU) as the activation function, these layers introduce non-linearity, allowing the model to learn more complex features.
3. **Pooling Layers:** These layers reduce the spatial dimensions of the feature maps, helping the model to become invariant to small translations or distortions in the input data.
4. **Fully Connected Layers:** After feature extraction, the model uses fully connected layers to flatten the output and make predictions based on the learned features.
5. **Output Layer:** The output layer produces the final classification or regression results.

In cybersecurity, CNNs can be applied to analyse network traffic, log files, or even images (in cases where visual analysis of cybersecurity data, such as detecting phishing websites, is required). By leveraging CNNs, systems can automatically detect malicious activities, identify abnormal patterns, and classify potential security threats.

User Interface :A user interface (UI) is the point of interaction between users and a software system. In the context of a cybersecurity system integrated with blockchain and AI, the UI must be intuitive, easy to navigate, and capable of displaying complex data and analytics in a user-friendly manner. Django, a Python-based web framework, is commonly used to develop dynamic and interactive web applications, while HTML and CSS are used to build and style the front-end components.

1. **Django:** Django is an open-source web framework that provides a high-level, clean, and pragmatic design for web development. It follows the Model-View-Template (MVT) architecture, making it suitable for developing robust web applications. For the integration of AI and blockchain-based cybersecurity systems, Django can be used to handle user requests, manage databases, and generate views. It also provides built-in support for user authentication, form handling, and security features, which are essential in a cybersecurity system.
2. **HTML:** HTML (Hypertext Markup Language) is the standard language for creating and structuring content on the web. It is used to define elements such as headings, paragraphs, links, images, and forms. In the context of the cybersecurity system, HTML forms can be used to gather user input (e.g., login credentials, security preferences) and display the system's output (e.g., threat analysis results, alerts, and reports).
3. **CSS:** CSS (Cascading Style Sheets) is used to style and format the HTML content, controlling the layout, colors, fonts, and responsiveness of the web pages. By using CSS, the UI can be made visually appealing and adaptable across different devices and screen sizes, ensuring a smooth user experience.

Integration and Application Development :Integration of Machine Learning (ML), Blockchain, and AI into a cohesive cybersecurity application requires careful planning and coordination between various technologies. The goal is to create a system that can automatically detect threats, record them securely using blockchain, and present actionable insights through a user-friendly interface. The integration process typically follows a sequence of steps:

Step 1: Developing the AI Model for Threat Detection The first step in developing the system is creating a machine learning model for threat detection. This involves collecting and preprocessing historical cybersecurity data to train the model. Various algorithms like CNN or Recurrent Neural Networks (RNNs) may be used to recognize patterns and detect anomalies in network traffic or system logs.

Step 2: Developing the Blockchain Technology In this step, blockchain is implemented to create a secure, immutable ledger for logging threat data, system activities, and security events. Smart contracts can be used to automate processes, such as triggering alerts when specific conditions are met, or logging data onto the blockchain for transparency.

Step 3: Developing the User Interface The user interface is developed using Django, HTML, and CSS. This interface enables users to interact with the system, view threat reports, configure settings, and analyse detected vulnerabilities. Django's back-end features are used to process requests and communicate with the blockchain and AI components.

Step 4: Integrating ML and Blockchain in the User Interface The ML model and blockchain technology are integrated into the Django-based user interface, enabling real-time threat detection and logging. The UI serves as the interaction point, where users can monitor detected threats and visualize the underlying data stored on the blockchain.

Step 5: Testing the Application The system undergoes rigorous testing to ensure that the AI model is detecting threats accurately, the blockchain is securely storing data, and the user interface is functioning as expected. Testing includes performance checks, security audits, and usability assessments to ensure the system meets all functional and security requirements.

4.EXPERIMENTAL ANALYSIS

The implementation of the Advanced Cybersecurity Framework Using AI and Blockchain involves multiple phases, including data collection, preprocessing, AI model training, blockchain integration, UI development, and deployment. The framework is designed to provide a robust, secure, and

intelligent solution to mitigate cybersecurity threats by leveraging artificial intelligence (AI) for threat detection and blockchain for data integrity and security.

Step-by-Step Implementation :

1. Data Collection and Preprocessing: Collect cybersecurity threat datasets from various sources, including network logs, malware reports, and intrusion detection system logs. Perform data cleaning, normalization, and feature selection to remove inconsistencies and improve model accuracy. Split the data into training and testing sets to evaluate the AI model's performance.

2. Development of AI-Based Threat Detection System: Train a machine learning model, such as a Convolutional Neural Network (CNN), to classify and detect cyber threats. Implement feature extraction and deep learning techniques to improve accuracy. Optimize the model using hyperparameter tuning and validation methods to ensure high efficiency.

3. Blockchain Implementation for Data Security: Develop a decentralized ledger system using blockchain technology to store threat detection logs and ensure data integrity. Implement smart contracts to automate security policies and enforce predefined rules. Integrate cryptographic hashing techniques to secure records and prevent unauthorized modifications.

4. User Interface: Design a web-based dashboard using Django for backend processing and HTML/CSS for front-end development. Enable users to view cybersecurity alerts, logs, and AI-detected threats in a real-time dashboard. Implement user authentication and role-based access control for secure interactions.

5. Integration of AI and Blockchain: Connect the AI threat detection system with the blockchain ledger to store and verify detected threats. Implement APIs or direct communication between the ML model and the blockchain network for real-time data storage and verification. Ensure seamless interoperability between the AI and blockchain components for a Testing and Evaluation. Conduct unit testing, integration testing, and performance testing to validate the system's functionality. Analyse the AI model's accuracy, precision, recall, and F1-score to ensure effective threat detection. Evaluate blockchain performance in terms of transaction speed, security, and scalability.

Description of Key Components :

1. AI-Based Threat Detection

The AI component, implemented using deep learning techniques, is responsible for analysing network traffic and detecting potential threats. A CNN model is trained on cybersecurity datasets to recognize attack patterns and classify them into different threat categories. The AI model continuously learns and updates itself based on new threat data, improving accuracy over time.

2. Blockchain for Secure Logging

Blockchain ensures that all detected threats and security logs are stored immutably. Each transaction recorded on the blockchain is verified through consensus mechanisms, ensuring that unauthorized modifications are prevented. Smart contracts automate security measures, enforcing compliance with cybersecurity protocols.

3. Web-Based User Interface

The web application, built using Django for backend processing and HTML/CSS for the frontend, provides an intuitive platform for users to monitor cybersecurity alerts. The interface allows administrators to review detected threats, manage security policies, and access blockchain-verified logs.

4. Integration of AI and Blockchain

The integration of AI and blockchain ensures that detected threats are securely recorded and cannot be tampered with. AI models predict potential security risks, and blockchain verifies and stores these events, creating a transparent and trust less security environment.

5. Security and Performance Enhancements

- **Encryption Techniques:** Data is encrypted before being recorded on the blockchain, ensuring confidentiality.
- **Scalability:** The framework is designed to handle large volumes of security logs with minimal latency.
- **Automation:** Smart contracts automate key cybersecurity functions, reducing the need for manual intervention.

Result and Description



Figure : Home Page

This is a homepage for an "Advanced Cybersecurity Framework using AI and Blockchain." It's designed with a clean and professional look, using a dark blue and gold color scheme for a tech-focused feel. It contains a navigation bar with three clear links: "Home", "User Login Here", and "New User Signup Here". These buttons guide users to the main sections of the platform.

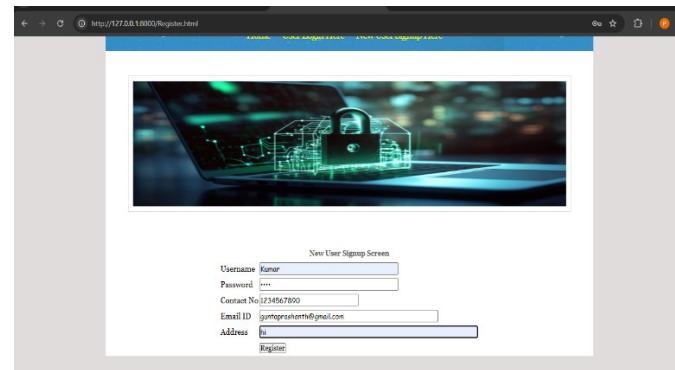


Figure : Signup Screen

The Figure Shows that it Is for a "New User Signup" screen. Let's break down its elements:

Input Fields: The form includes several input fields for users to enter their information:

- **Username:** A field to enter a username, with the example "Kumar" already filled in.
- **Password:** A field to enter a password, currently masked for security (showing "*****").
- **Contact No:** A field for a contact number, with "1234567890" pre-

filled as an example.

- Email ID: A field for an email address, with "[email address removed]" filled in.
- Address: A field for the user's address, with "hi" entered.



Figure : Login Screen

The Figure Shows that it Is for a "User Login Screen." It's a simple and straightforward design focused on the essential elements for user authentication

Input Fields: There are two prominent input fields:

- Username: A field for users to enter their username. The example "admin" is pre-filled, suggesting this might be a default or test account.
- Password: A field for users to enter their password. The password is masked with asterisks ("*****") for security.

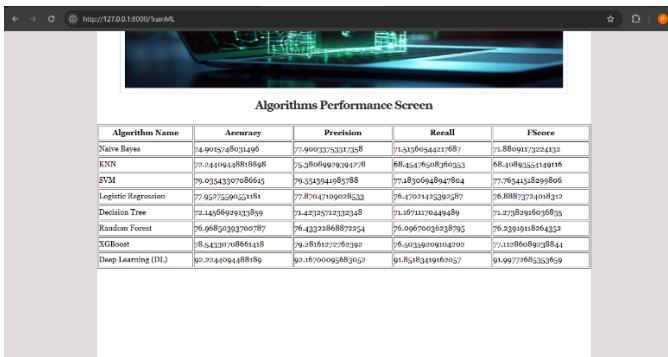


Figure : Algorithms Performance Screen

This Figure shows a table displaying the performance metrics of various machine learning algorithms. Here's a breakdown:

This image shows a table displaying the performance metrics of various machine learning algorithms. Here's a breakdown:

Title: The table is titled "Algorithms Performance Model," indicating it's a comparison of different algorithms based on their performance.

Columns: The table has the following columns:

- Algorithm Name: This column lists the names of the machine learning algorithms being compared. The algorithms included are:
 - Naive Bayes
 - KNN (K-Nearest Neighbours)
 - SVM (Support Vector Machine)

- Logistic Regression
- Decision Tree
- Random Forest
- XGBoost (Extreme Gradient Boosting)
- Deep Learning (DL)

- Accuracy: This column shows the accuracy score of each algorithm. Accuracy represents the overall correctness of the model's predictions.
- Precision: This column displays the precision score, which measures how many of the positive predictions made by the model were actually correct.
- Recall: This column shows the recall score, which measures how many of the actual positive cases were correctly identified by the model.
- F1-Score: This column presents the F1-score (or F-score), which is the harmonic mean of precision and recall. It provides a balanced measure considering both metrics.

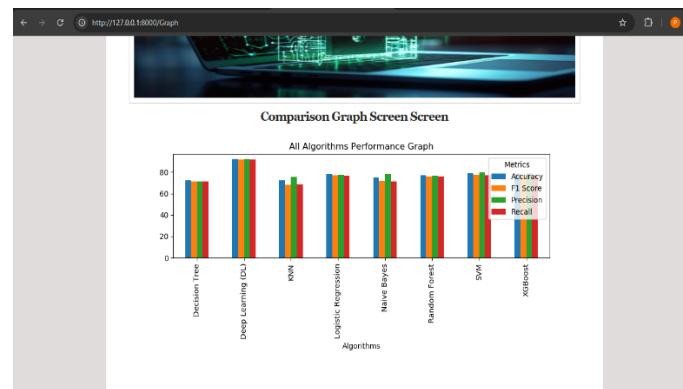


Figure : Algorithms Performance Graph

The "Comparison Graph Screen" displays a bar chart comparing the performance of various machine learning algorithms across different metrics. The graph, titled "All Algorithms Performance Graph," plots the algorithms (Decision Tree, Deep Learning (DL), KNN, Logistic Regression, Naive Bayes, Random Forest, SVM, and XGBoost) along the x-axis and the metric scores (Accuracy, F1 Score, Precision, and Recall) on the y-axis. Each algorithm has a set of clustered bars representing its scores for the four metrics, enabling a direct visual comparison of their performance. The legend, labelled "Metrics," clarifies the color-coding for Accuracy, F1 Score, Precision, and Recall. This visualization provides a clear and concise overview of how each algorithm performs in relation to the others across the chosen metrics, facilitating algorithm selection based on desired performance characteristics.



Figure : Blockchain Based Event Detection

This Figure Shows that it is for a "Post Tweet Screen," designed for composing and publishing tweets. A "Submit" button is located below the input area. Clicking this button would send the tweet to be published.



Figure: View Tweets

This Figure displays a record of tweets or posts

Username: This column displays the username of the person who posted the tweet. In the example shown, the username is "Kumar."

Tweet Post: This column contains the actual content of the tweet. The example tweet asks a question about Python data structures: "python: what is the difference between (1,2,3) and [1,2,3], and when should i use each?"

Posted Date: This column shows the date when the tweet was posted. The example shows the date as "2025-01-30."

5. CONCLUSION

The integration of Artificial Intelligence (AI) and Blockchain in cybersecurity provides a highly advanced and efficient security framework capable of addressing modern digital threats. Traditional security systems often fail to keep up with evolving cyber threats due to their static nature and reliance on centralized control. However, with AI's ability to analyse vast amounts of data in real time and blockchain's immutable ledger technology ensuring data integrity, this framework enhances cybersecurity in a transformative way. AI-powered models, such as Convolutional Neural Networks (CNNs), play a crucial role in detecting cyber threats with high accuracy by analysing patterns and anomalies in network traffic. These models continuously learn and improve over time, making them adaptable to emerging threats. Meanwhile, blockchain technology ensures that security logs and threat detection data remain immutable, preventing unauthorized modifications and ensuring a transparent and trustable system.

The proposed system provides a decentralized, secure, and intelligent cybersecurity solution that significantly reduces vulnerabilities caused by human errors or traditional security models. By integrating machine learning algorithms with blockchain smart contracts, the system can automate security measures, reducing response time to cyber threats. Additionally, its decentralized nature eliminates single points of failure, making it highly resilient against cyber-attacks.

Future Scope :

The future of AI and Blockchain-based cybersecurity is promising, with potential advancements that will further strengthen digital security systems. As cyber threats continue to evolve, AI models will require continuous updates and retraining using larger and more diverse datasets to detect new attack patterns. Future improvements in deep learning architectures, such as transformers and reinforcement learning, will enhance threat detection capabilities, making AI-driven cybersecurity systems even more intelligent and proactive.

In terms of blockchain technology, future enhancements will focus on scalability, energy efficiency, and speed. Current blockchain

implementations, such as Proof of Work (PoW), consume high amounts of energy, leading to inefficiencies. The adoption of Proof of Stake (PoS) and sharding mechanisms will enable faster transaction processing while maintaining security and decentralization. Hybrid blockchain models that combine public and private blockchains can also improve performance and security in enterprise applications.

Another promising development is the integration of AI, Blockchain, and Quantum Computing. Quantum-resistant blockchain solutions will be necessary as quantum computers become more powerful and capable of breaking traditional cryptographic algorithms. AI-powered self-healing cybersecurity systems that can autonomously detect, respond, and recover from cyber threats will revolutionize cybersecurity in critical sectors such as defence, banking, and IoT.

Additionally, the expansion of this cybersecurity framework to IoT devices will be crucial. The increasing adoption of smart devices in homes, industries, and healthcare poses significant security risks. AI-driven security mechanisms coupled with blockchain-based decentralized identity management can enhance IoT security by preventing unauthorized access and data breaches.

6. REFERENCES

- [1]Salama R, Al-Turjman F. Managing Cybersecurity in Smart Cities With Blockchain Technology. NEU Journal for Artificial Intelligence and Internet of Things. 2023;2.
- [2]Miloslavskaya N, Tolstoy A, Budzko V, Das M. Blockchain Application for Iot Cybersecurity Management. In: Essentials of blockchain technology. Chapman & Hall/CRC. 2019:141-168.
- [3]Ishaque M, Gapar Md, Johar Md, Khatibi A, Yamin M. A Novel Hybrid Technique Using Fuzzy Logic Neural Networks and Genetic Algorithm for Intrusion Detection System. Measurement: Sensors. 2023;30:100933.
- [4]Chentouf FZ, Bouchkaren S. Blockchain for Cybersecurity in Iot. In: Maleh Y, Baddi Y, Alazab M, Tawalbeh L, Romdhani I, editors. Artificial Intelligence and blockchain for future cybersecurity applications. Cham: Springer International Publishing. 2021:61-83.
- [5]Rahman MA, Rashid MM, Hossain MS, Hassanain E, Alhamid MF, et. al. Blockchain and Iot-Based Cognitive Edge Framework for Sharing Economy Services Ina Smart City. IEEE Access. 2019;7:18611-18621.
- [6]Tun VH, Jahankhani H. Using Artificial Intelligence (AI) and Blockchain to Secure Smart Cities Services and Applications. In: Jahankhani H, Bowen G, Sharif MS, editors. Cybersecurity and artificial intelligence. Advanced Sciences and Technologies for Security Applications. Cham: Springer. 2024:163-184.
- [7]Miloslavskaya N, Tolstoy A, Budzko V, Das M. Blockchain Application for Iot Cybersecurity Management. In: Essentials of blockchain technology. Chapman & Hall/CRC. 2019:141-168.
- [8]Kiruthika M, Ponnuswamy PP. Fusion of Iot Blockchain and Artificial Intelligence for Developing Smart Cities. Blockchain Internet of Things and Artificial Intelligence 2021:155- 177.
- [9]Bekkali AE, Essaaidi M, Boulmalf M. A Blockchain-Based Architecture and Framework for Cybersecure Smart Cities. IEEE Access. 2023;11:76359-76370.
- [10]Daniel J, Sargolzaei A, Abdelghani M, Sargolzaei S, Amaba B. Blockchain Technology, Cognitive Computing, and Healthcare Innovations. J Adv Inf Technol. 2017;8:194-198.