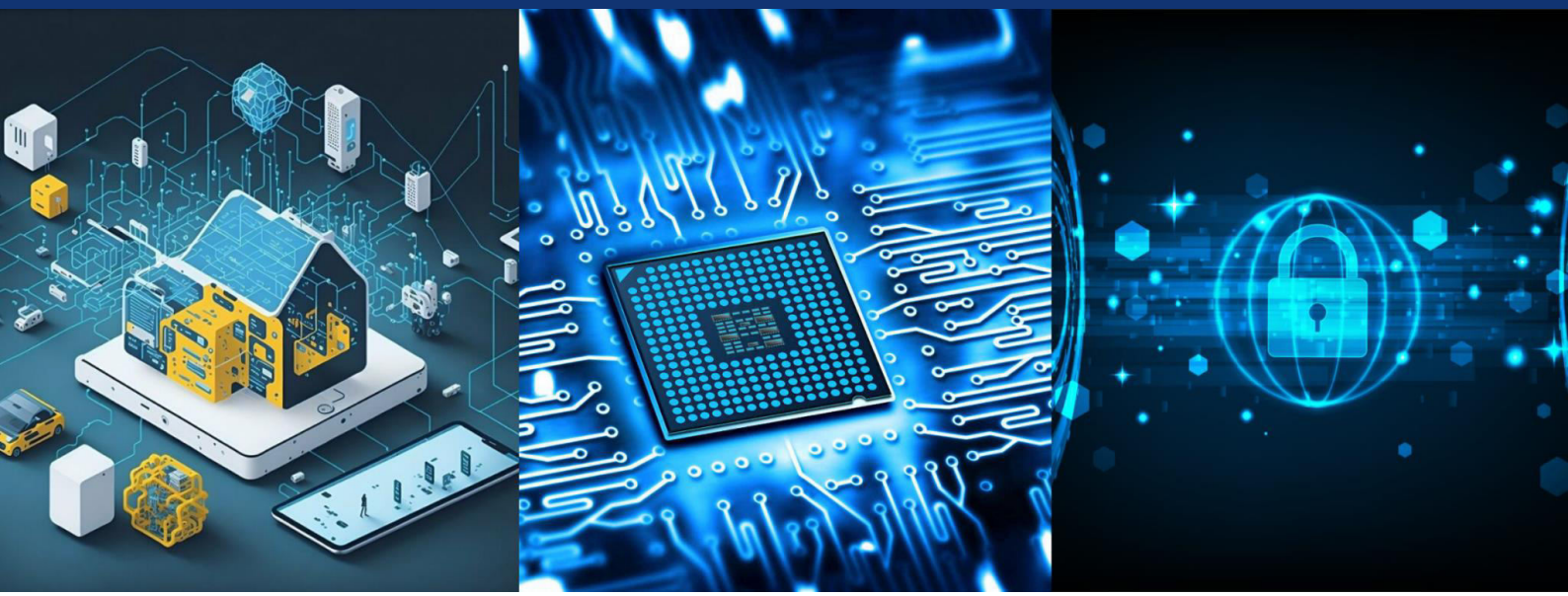
IJIRCCE

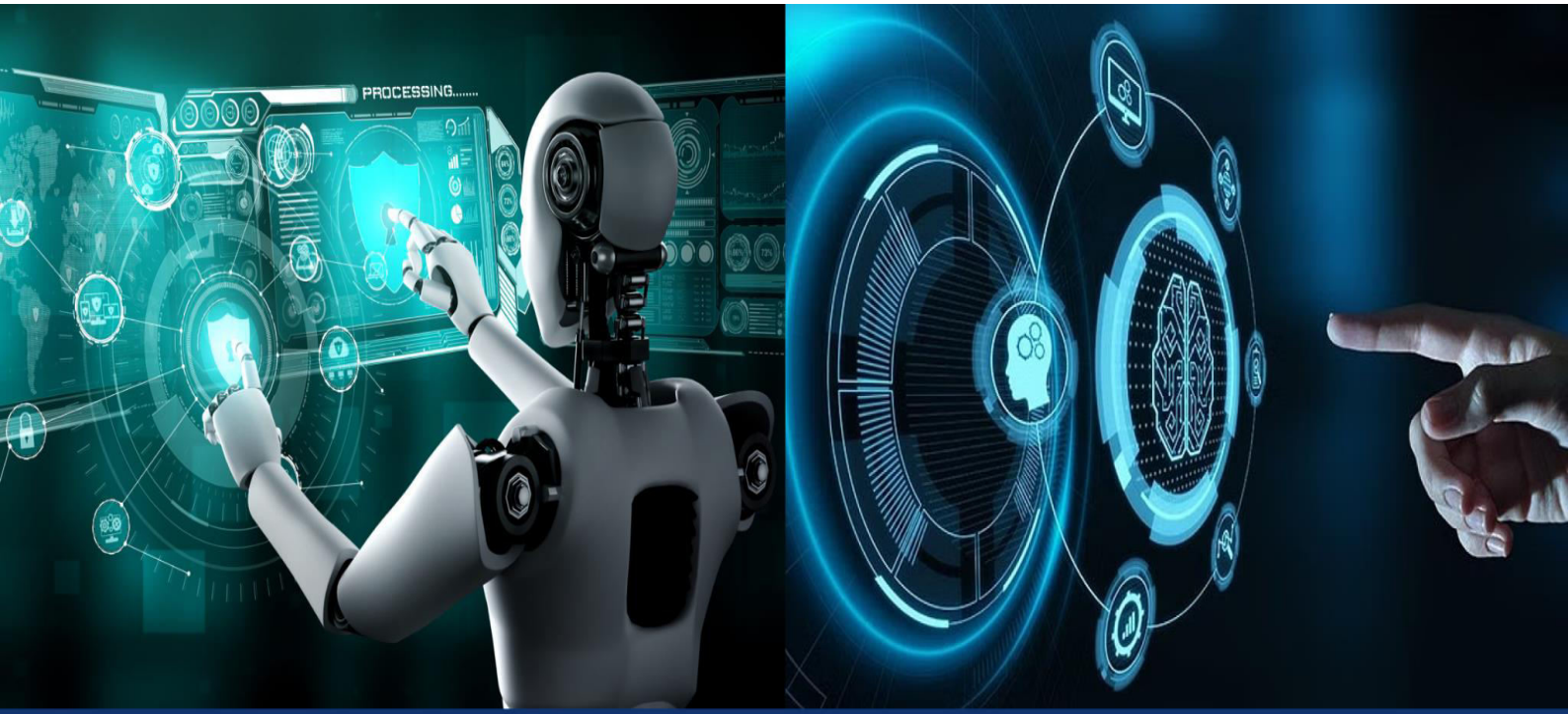
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.625

Volume 13, Issue 1, January 2025

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301075

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Evaluating the Efficacy of Intrusion Detection System Using Machine Learning

Vinod Kumar. K. P[1], Gagandeep S[2], Ishwar C P[3], Likhith T[4], Likith R[5]

Assistant Professor, Department of CSE, Dr AIT, Bengaluru, India[1]

Department of CSE, Dr AIT, Bengaluru, India[2,3,4,5]

ABSTRACT: In the constantly evolving arena of cyberspace security, this paper introduces an Artificial Intelligence based Intrusion Detection System that allows for real time threat detection and response. Implementing AI methods such as LSTM, GRU, Autoencoder and Stacking Ensemble models, DDoS and malware are able to be detected and alleviated with ease. Including round the clock testing processes, batch processing and an easy to navigate Flask based web application, the AI-IDS is able to provide a plethora of security to its users during multiple attacks and across various networks. By encompassing advanced hybrid frameworks, dynamic feature extraction and modeling, the system is able to provide all measures necessary for scalable and secure solutions.

KEYWORDS: Intrusion Detection System (IDS), Network Security, Machine Learning, Cyber Threat Detection, Hybrid Algorithms

I. INTRODUCTION

In today's digital landscape, cybersecurity is more critical than ever, with the increasing sophistication and frequency of cyber-attacks posing significant challenges to organizations worldwide. Traditional methods of network protection, such as static firewalls and rule-based systems, are no longer sufficient to detect and mitigate advanced threats like Distributed Denial of Service (DDoS), malware, and advanced persistent threats (APTs). This paper focuses on developing an **Intrusion Detection System (IDS)** that leverages state-of-the-art technologies to enhance threat detection and response capabilities. The system integrates machine learning and deep learning models, hybrid algorithms, and real-time monitoring to redefine how intrusions are detected and prevented in modern networks.

As digital transformation accelerates, organizations face increasingly dynamic and complex network environments, making intrusion detection a challenging task. According to recent cybersecurity reports, the global market for intrusion detection systems is projected to grow significantly, driven by the proliferation of internet-connected devices and the expansion of cloud services. However, traditional IDS approaches often struggle with scalability, false positives, and the ability to adapt to novel or zero-day attacks, leaving networks vulnerable to emerging threats.

To address these limitations, this project proposes the development of an advanced Intrusion Detection System (IDS) that utilizes cutting-edge machine learning and deep learning techniques, such as neural networks and ensemble methods, to enhance the detection and classification of network intrusions. By employing hybrid algorithms that combine signature-based, anomaly-based, and behavior-based detection models, the system aims to achieve high accuracy with minimal false positives and adapt effectively to new and evolving threats. Furthermore, real-time monitoring capabilities, powered by continuous data collection and analysis, ensure the system can promptly identify and mitigate potential threats, reducing the window of opportunity for attackers. This approach not only strengthens the overall security posture of the network but also ensures that the IDS remains scalable and robust in an ever-changing digital landscape.

Despite advances in the cybersecurity domain, most IDS solutions fail to address the need for real-time detection, seamless scalability, and comprehensive analytics. Static rule-based systems often require constant manual updates, while anomaly-based systems can produce high false-positive rates. This project aims to bridge these gaps by introducing a collaborative and AI-driven approach that ensures adaptability, accuracy, and real-time responsiveness in detecting complex network intrusions.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

The field of intrusion detection systems (IDS) has undergone significant evolution with the advent of artificial intelligence (AI) and machine learning (ML). Traditional IDS models heavily relied on signature-based methods and heuristic anomaly detection techniques. However, these systems often failed to address the challenges of dynamic attack patterns, zero-day vulnerabilities, and evolving cyber threats. Recent advancements have introduced AI-driven methodologies that incorporate supervised, unsupervised, and hybrid learning models to improve accuracy, scalability, and adaptability.

Research studies emphasize the importance of hybrid IDS models that combine traditional algorithms with deep learning techniques. For example, the integration of RandomForestClassifier and LSTM (Long Short-Term Memory) networks has shown promise in detecting temporal anomalies in network traffic. Autoencoders and GRU (Gated Recurrent Unit) models have further enhanced the ability to identify novel patterns in high-dimensional data, enabling the detection of zero-day attacks with reduced false-positive rates. Additionally, ensemble techniques, such as stacking models, leverage the strengths of multiple algorithms to achieve superior classification performance.

Studies on real-time threat detection highlight the role of sequential data processing and low-latency prediction frameworks. Platforms using AI-driven systems have successfully implemented features like packet inspection, flow-based analysis, and predictive modeling to detect advanced persistent threats (APTs) and Distributed Denial of Service (DDoS) attacks. Tools such as CICIDS 2017 datasets have been instrumental in benchmarking and validating IDS models, providing a comprehensive dataset for training and testing.

Another critical area of study is the scalability and efficiency of IDS architectures. Cloud-based infrastructures, such as MongoDB Atlas and AWS, have enabled large-scale data ingestion, processing, and real-time analytics. Research also underscores the effectiveness of caching mechanisms and load balancing techniques in maintaining high performance under dynamic traffic conditions. The use of Flask and RESTful APIs for seamless integration between front-end and back-end systems further enhances the usability of IDS platforms.

A. Accessibility and Usability

While advanced IDS models offer significant improvements in detection capabilities, accessibility and usability remain critical challenges:

- **User Interfaces:** Many IDS platforms lack intuitive interfaces for administrators, making real-time monitoring and threat analysis complex.
- **Specialized Features:** Accessibility features such as customizable dashboards, mobile compatibility, and real-time alerts are inconsistently implemented across systems.

B. Cost and Implementation Barriers

The financial and technical challenges associated with implementing IDS solutions can limit their adoption:

- **High Costs:** Proprietary IDS models and advanced algorithms often come with steep licensing fees, making them inaccessible to smaller organizations.
- **Deployment Complexity:** Open-source alternatives require significant expertise in configuration and scaling, which can be a barrier for organizations with limited technical resources.

C. Integration Challenges

Seamless integration with existing security infrastructures and third-party tools is a critical requirement:

- **Compatibility Issues:** Many IDS platforms struggle to integrate with legacy systems or modern security frameworks, creating gaps in monitoring and response.
- **Lack of Standards:** Limited adherence to standard protocols, such as SCAP or STIX/TAXII, reduces interoperability and data sharing across systems.

D. Engagement and Adaptation

Engaging learners and ensuring they remain motivated throughout their educational journey is a significant challenge:

- **Passive Learning Models**: Many existing systems prioritize one-way content delivery over interactive and engaging learning activities.
- **Limited Feedback Mechanisms**: Real-time feedback and adaptive assessments, which are critical for learner retention, are often underdeveloped or absent.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The literature underscores the potential of AI-driven IDS solutions in addressing these challenges. By leveraging hybrid models, real-time analytics, and scalable architectures, these systems redefine the landscape of cybersecurity. This research builds upon these advancements, integrating innovative techniques to enhance detection accuracy, reduce false positives, and provide a robust, user-friendly platform for network protection. Future work will focus on implementing blockchain for secure data sharing, federated learning for privacy-preserving training, and Transformer-based architectures for enhanced temporal analysis.

III. PROPOSED SYSTEM

The proposed system, **Intrusion Detection Mechanism**, is designed to transform cybersecurity by combining advanced artificial intelligence (AI) techniques with state-of-the-art intrusion detection capabilities. This platform aims to provide robust, real-time detection and mitigation of cyber threats, leveraging hybrid machine learning models, deep learning architectures, and user-friendly interfaces. By focusing on scalability, accuracy, and adaptability, this system effectively addresses the limitations of traditional IDS methods and caters to diverse organizational needs.
At its core, the proposed system integrates hybrid AI models, including **LSTM (Long Short-Term Memory)**, **GRU (Gated Recurrent Unit)**, and **Autoencoder algorithms**, to analyze network traffic patterns, detect anomalies, and classify attacks such as DDoS, DoS Hulk, and PortScan. The architecture employs a **Stacking Ensemble model** that combines the strengths of algorithms like **DecisionTreeClassifier, RandomForestClassifier, Naive Bayes, KNN**, and others, ensuring high detection accuracy while minimizing false positives.

The system adopts a **Flask-based backend** for efficient model deployment and data processing. MongoDB is utilized as the database to manage network traffic data and predictions, offering real-time analytics and scalability for large datasets. Security measures such as **JWT (JSON Web Tokens)** and bcrypt are incorporated to protect user credentials and ensure secure communication between system components. For data input, the platform supports manual entry, batch uploads via CSV files, and live network data streams, enabling versatility in operation.

To enhance usability, the platform features an **interactive web interface** built using modern web technologies. This interface provides network administrators with a real-time dashboard displaying attack classifications, trends, and threat analytics. Collaboration is supported through shared resources and integrated reporting tools, making it easier for teams to respond effectively to detected threats. Gamification elements, such as alerts and achievement tracking, motivate continuous monitoring and system engagement.

Scalability and Performance Optimization:

- The system is designed for scalability, employing cloud-based deployment strategies using platforms like **Render and AWS**. These solutions enable auto-scaling, ensuring consistent performance during high traffic loads. **Redis caching mechanisms** and load balancing optimize response times, while modern containerization technologies like Docker ensure seamless deployment across different environments. Media files and large datasets are processed efficiently using real-time optimization techniques, ensuring low-latency operation.

Personalization and Adaptability:

- A key highlight of the system is its **personalization engine**, which tailors alerts and recommendations based on network behaviors and historical data patterns. By analyzing attack trends and administrator interactions, the system suggests proactive measures to prevent potential vulnerabilities. Advanced users can customize detection thresholds and parameters, while novice users benefit from pre-configured templates optimized for general security use cases.

Future-Proofing with Advanced Features:

- To stay ahead in the rapidly evolving cybersecurity landscape, the system integrates provisions for **future advancements**. Planned enhancements include incorporating **Transformer-based architectures** for improved sequence modeling, blockchain technology for secure data sharing, and federated learning for decentralized model training without compromising data privacy. These features aim to make the system more resilient, accurate, and aligned with emerging security needs.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

By combining cutting-edge AI models, a robust technical foundation, and a user-centric design, the **Intrusion Detection Mechanism** represents a significant step forward in cybersecurity. It empowers organizations to detect, analyze, and mitigate threats efficiently, ensuring the safety and integrity of digital infrastructures.

IV. IMPLEMENTATION

The Intrusion Detection System (IDS) is implemented as a powerful platform that integrates advanced artificial intelligence (AI), a user-friendly interface, and a secure back-end system. It offers robust tools for intrusion detection, real-time threat analysis, and seamless interaction with users. Below are the simplified details of its implementation:

1. Front-End Implementation

The front end is built using web technologies such as HTML, CSS, and JavaScript. ReactJS ensures an interactive user interface, making data handling smooth and user-friendly. Bootstrap is used for consistent and responsive design, ensuring compatibility across devices. The user interface includes:

- Interactive Dashboards: Display real-time intrusion insights and graphs.
- Forms and Uploads: Enable manual packet entry or bulk uploads via CSV files.
- Real-Time Features: WebSocket integration provides live updates and notifications.

2. Back-End Implementation

The back end is powered by Flask, a lightweight Python framework, enabling communication between the user interface and AI models. It ensures:

- Security: User credentials are encrypted using bcrypt, and sessions are protected with JWT tokens.
- AI Integration: Machine learning models like LSTM, GRU, and Decision Trees analyze network traffic to detect threats.
- Efficiency: RESTful APIs ensure smooth operations for tasks such as predictions, user management, and retrieving logs.

3. Database Management

MongoDB is used to store essential data, such as:

- User information, past intrusion logs, and analytics.
- It is hosted on MongoDB Atlas, which supports scalability and automatic backups. Additionally, Cloudinary handles file uploads, optimizing and storing media securely.

4. System Performance and Optimization

To handle heavy traffic and ensure reliability:

- Load balancing distributes user requests across servers.
- Redis caching reduces database load and improves response times.
- Asynchronous processes allow multiple tasks to run simultaneously.

5. API Design

The APIs are designed to handle:

- User Authentication: Secure login and token generation.
- Data Analysis: Accepting user inputs or CSV files for threat predictions.
- Logs: Retrieving historical detection records.
  Error handling and debugging are streamlined with standardized codes and logging tools.

Future Enhancements

The platform is designed to evolve with:

- Mobile Applications: Expanding access to Android and iOS.
- Blockchain Integration: Ensuring secure data logging and tamper-proof records.
- Federated Learning: Allowing privacy-preserving, decentralized AI training.
- Advanced Reporting: Adding multilingual support and detailed global analytics.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This implementation ensures that the IDS is efficient, user-friendly, and adaptable, meeting the complex demands of modern network security.

V. RESULT AND DISCUSSION

The implementation of the **Intrusion Detection System** has delivered a robust and functional system capable of detecting and classifying network intrusions with high accuracy. The platform features an intuitive user interface, advanced analytics, and seamless integration of machine learning models. Below is a detailed account of the results achieved:

A. Home Page

The Home Page serves as the entry point to the Intrusion Detection Mechanism, providing an overview of its features and functionalities in an engaging and user-friendly manner.

- Introduction to the System: Highlights the key features of the platform, including real-time intrusion detection, advanced analytics, and machine learning integration.
- User Guidance: Provides intuitive navigation to core functionalities, such as Login, Registration, Dashboard, and Upload and Prediction sections.
- Visual Appeal: Designed with responsive layouts and attractive visuals, ensuring a seamless experience across devices. The homepage features high-quality banners and infographics explaining the system's purpose and capabilities.
- Interactive Elements: Includes quick links to important features, tutorials, and FAQs for first-time users to get started easily.
- Security Awareness: Emphasizes the importance of cybersecurity and how the platform addresses modern threats, building trust with users.

B. About Us

The **About Us** page of the platform is designed to introduce the project team and provide a brief overview of their efforts. Key features include:

Introduction Section:

A concise description of the project's purpose, highlighting that it is developed by a group of Computer Science students who have collaborated and contributed their skills to create the **Intrusion Detection System**.

Team Member Profiles:

The page showcases the group members involved in the project. Each team member's name is displayed along with an avatar representing them, ensuring a clean and professional presentation.

User-Friendly Design:

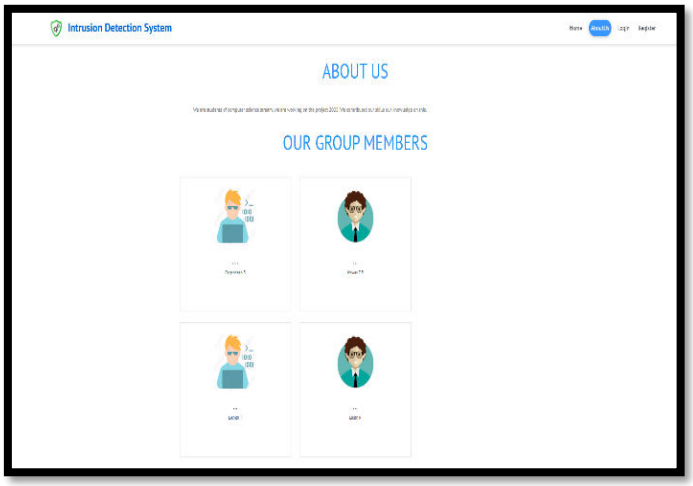
The page layout is minimalistic and well-structured, making it visually appealing and easy to navigate. It ensures the focus remains on the team and their contribution.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

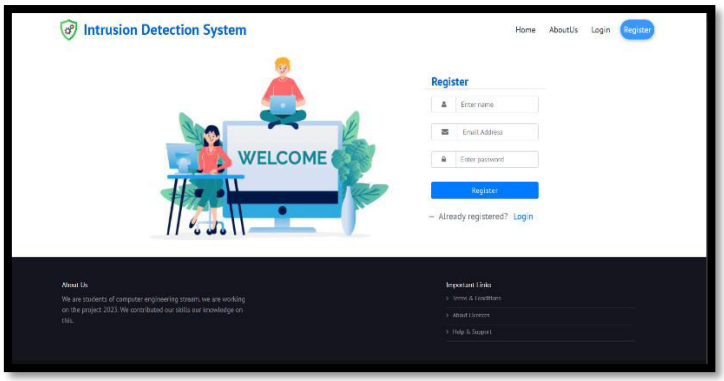
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Purpose of the Page:
This section establishes credibility and reflects the teamwork that went into building the platform. It aims to give users and stakeholders insight into the dedicated team behind the project.



C. Registration Page
The registration page facilitates new user onboarding with ease and security.

- **Data Validation:** Ensures that user input is valid, preventing issues such as duplicate email entries or weak passwords.
- **Secure Storage:** User details are stored in the database using encryption techniques for privacy and compliance.
- **Accessibility:** Optimized for all devices and screen readers to ensure inclusivity.
- **Seamless Flow:** Upon successful registration, users are redirected to the login page with a confirmation message.



D. Login Page
The login page acts as a secure gateway to the system, ensuring only authorized users can access the platform.

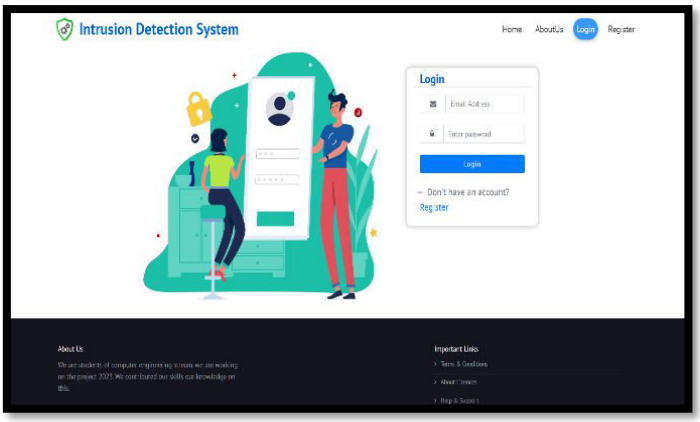
- **Authentication:** User credentials are secured with **bcrypt** for password hashing and **JSON Web Tokens (JWT)** for session management.
- **Error Handling:** Provides clear feedback for invalid credentials, ensuring a user-friendly experience.
- **Responsive Design:** The login page is optimized for both mobile and desktop devices, allowing users to log in conveniently from any device.
- **Integration Options:** Offers support for third-party login options, such as Google or Microsoft, for enhanced flexibility.

Additional Features: Includes support for multi-language preferences and optional two-factor authentication for improved security.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



E. Prediction page

The **Prediction Page** is a critical part of the Intrusion Detection System, allowing users to input network packet details for analysis and prediction. Below are its key features:

1. Packet Details Form:

- A well-structured form where users can input various network packet attributes, such as:
  - **Forward Packet Length Max** (Fwd Packet Length Max)
  - **Total Length of Forward Packets**
  - **Backward Packet Length Standard Deviation** (Bwd Packet Length Std)
  - **Flow Duration**
  - **Average Forward Segment Size** (Avg Fwd Segment Size)
  - **Packet Length Mean**, **Variance**, **Standard Deviation**
  - Many more parameters critical to identifying potential intrusions in network traffic.
- Each field has clear labels, making it user-friendly.

2. Call-to-Action Button:

- The **Check Packet** button triggers the machine learning model to analyze the entered data and predict whether the packet is indicative of an intrusion.

3. Minimalistic Design:

- The dashboard maintains a clean and uncluttered interface, ensuring ease of use and focus on the task at hand.
- The **Intrusion Detection System** logo and navigation options (e.g., "Predict," "Upload," "Log Out") are placed conveniently at the top for a seamless user experience.

4. User Interaction:

- The page is interactive, guiding users through the process of data input and prediction seamlessly.
- It is designed to provide quick and accurate predictions for each input set.

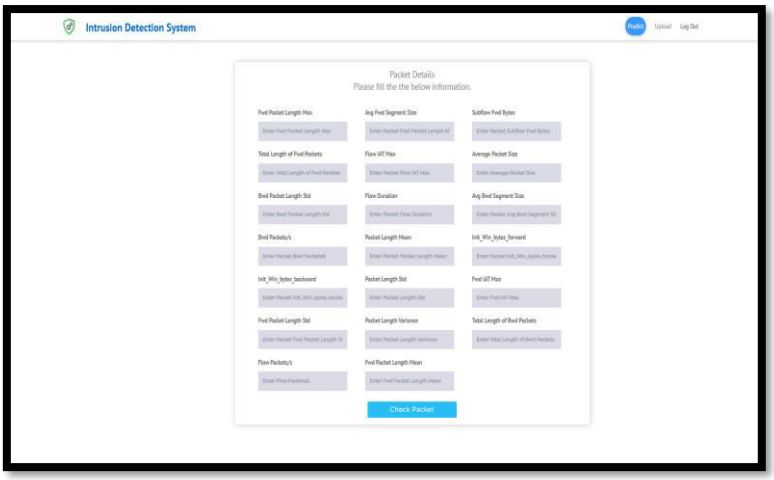
5. Purpose:

- The dashboard simplifies the intrusion detection process by leveraging machine learning models to analyze live network data, ensuring efficient and timely predictions.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

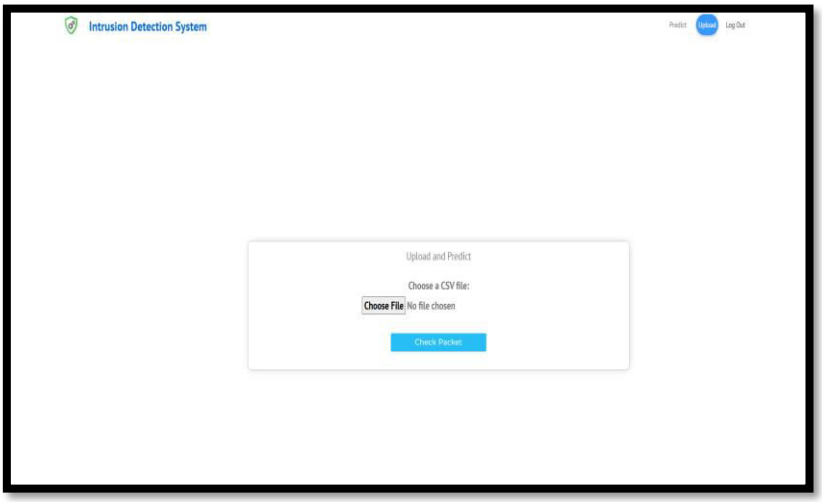
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



F. Upload and Prediction

The core feature of the system is its ability to analyze uploaded network data for potential threats.

- **File Upload:** Allows users to upload CSV files containing network traffic details.
- **Data Processing:** Automatically cleans and preprocesses the uploaded data to extract key features like Fwd Packet Length Mean and Flow Duration.
- **Prediction:** Machine learning models classify the data into categories such as BENIGN, DDoS, or DoS attacks with high accuracy.
- **Result Display:** Displays predictions in a user-friendly tabular format with class indices and attack names.
- **Performance:** Processes large datasets quickly, ensuring real-time feedback for users.



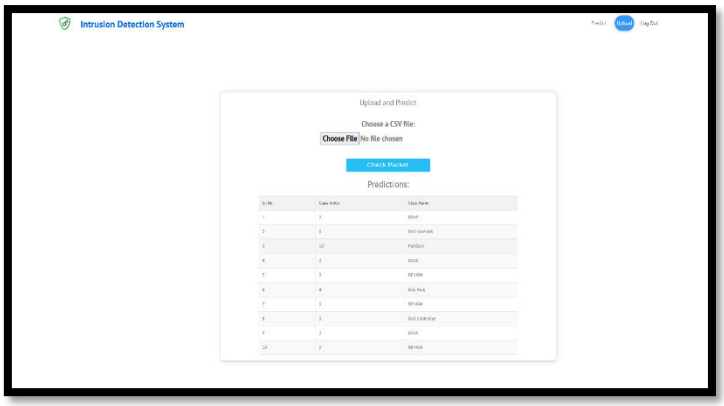
A. Result Analysis Page

The Intrusion Detection Results page consolidates the output of both file uploads and real-time predictions for network traffic analysis. When a file is uploaded, the system preprocesses the dataset, extracts essential features, and analyzes the data using machine learning models to identify potential intrusions. The results are presented in a clear and concise format, highlighting whether the traffic is normal or indicative of an intrusion, along with additional insights such as intrusion types or confidence scores. For real-time packet prediction, users input specific packet details, and the system instantly displays the classification outcome, aiding quick decision-making. This dual-functionality page bridges large-scale batch processing and individual packet analysis, ensuring comprehensive coverage of network monitoring.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



VI. CONCLUSION

The Intrusion Detection System (IDS) developed as part of this project provides a robust and efficient solution for detecting network anomalies and security threats in real-time. By leveraging advanced machine learning algorithms and publicly available datasets like CICIDS 2017 and NSL-KDD, the system achieves high accuracy, precision, and recall in identifying various types of intrusions. Features such as real-time data processing, scalable architecture, and effective classification of network traffic enable the IDS to function seamlessly in dynamic environments.

This system significantly reduces the manual effort required for monitoring and mitigating security breaches, making it a valuable addition to modern cybersecurity frameworks. Preprocessing techniques like feature selection, normalization, and the use of labeled datasets further enhance the reliability and performance of the IDS. While some challenges remain, such as addressing evolving attack patterns and optimizing resource consumption, this system lays a strong foundation for building intelligent, automated, and adaptive intrusion detection solutions.

In conclusion, the Intrusion Detection System demonstrates the potential of integrating machine learning with network security to tackle the growing threat of cyberattacks. This project represents a significant step toward securing digital infrastructure, ensuring safer and more reliable networks.

REFERENCES

[1] **Denning, D. E.**, "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, 1987.
[2] **Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A.**, "A Detailed Analysis of the KDD CUP 99 Data Set," *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009.
[3] **Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A.**, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, pp. 108-116, 2018..
[4] **Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A.**, "Flow-Based Network Traffic Analysis Using Machine Learning," *IEEE Access*, vol. 7, pp. 97053-97064, 2019.
[5] **Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M.**, "IoT Malicious Traffic Identification Using Wrapper-Based Feature Selection Mechanisms," *Future Generation Computer Systems*, vol. 107, pp. 147-160, 2020.
[6] **Javaid, A., Niyaz, Q., Sun, W., & Alam, M.**, "A Deep Learning Approach for Network Intrusion Detection System," *Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (formerly BIONETICS)*, 2016.
[7] **Sommer, R., & Paxson, V.**, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *2010 IEEE Symposium on Security and Privacy*, pp. 305-316, 2010.
[8] **Zhang, J., & Zulkernine, M.**, "Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection," *Proceedings of the IEEE International Conference on Communications (ICC)*, 2006.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details