 ISSN: 3107-6513

# Intrusion Detecion System

Mr. S. Manoj[1], Ram prasad.A[2], Vishal.N[3]
[1]Assistant Professor, Department of Computer Science with Cognitive Systems,
Sri Ramakrishna College of Arts and Science, Coimbatore, Tamilnadu, India.
[2,3]Students, Department of Computer Science with Cognitive Systems,
Sri Ramakrishna College of Arts and Science, Coimbatore, Tamilnadu, India.
ramprasad22082005@gmail.com, Vishalnallathambi19102005@gmail.com

**Abstract:**

With the rapid growth of computer networks and internet-based services, securing systems from cyber threats has become a major challenge. Traditional security mechanisms such as firewalls are not sufficient to detect all types of attacks, especially internal and unknown threats. An Intrusion Detection System (IDS) plays a crucial role in identifying malicious activities by continuously monitoring network traffic and system behavior.

This project focuses on the design and development of an Intrusion Detection System that detects unauthorized access, misuse, and abnormal activities in a computer system or network. The proposed system analyzes incoming data using predefined rules and anomaly detection techniques to identify potential intrusions. When suspicious activity is detected, the system generates alerts and stores detailed logs for further investigation.

The developed IDS reduces manual monitoring effort, improves detection accuracy, and enhances overall system security. The system is simple, efficient, and suitable for academic and small-scale organizational environments. Future enhancements include the integration of machine learning techniques and real-time alert mechanisms to improve detection of advanced cyber-attacks.

## 1.INTRODUCTION:

An Intrusion Detection System (IDS) is a security mechanism designed to monitor network traffic or system activities to identify malicious actions, policy violations, or abnormal behavior. The primary purpose of an IDS is to detect intrusions in real time and alert system administrators so that appropriate preventive or corrective measures can be taken. Unlike firewalls, which mainly block unauthorized access, an IDS focuses on identifying both internal and external threats that may bypass existing security controls.

IDS works by analyzing network packets or system logs and comparing them with known attack signatures or normal behavior patterns. Based on this analysis, the system can classify activities as normal or suspicious. Intrusion Detection Systems are broadly classified into Network-based IDS (NIDS) and Host-based IDS (HIDS), each serving a specific role in securing information systems.

The implementation of an Intrusion Detection System enhances the overall security posture of a network by providing early detection of attacks, minimizing damage, and improving incident response. This project focuses on designing and developing an efficient IDS that can accurately detect intrusions, reduce false alarms, and ensure the confidentiality, integrity, and availability of system resources.

## 2.LITERATURE SURVEY:

Intrusion Detection Systems (IDS) have been a vital research area in cybersecurity for decades. The increasing number and complexity of cyberattacks have driven researchers to develop more effective techniques for detecting unauthorized access and malicious activities within networks and systems.

Early work in intrusion detection focused on **signature-based detection**, where patterns of known attacks are stored in a database and incoming traffic is compared against them. Notable systems such as **Snort** and **Bro (now Zeek)** demonstrated practical effectiveness in real-time network traffic inspection by matching predefined signatures. However, signature-based IDS have limitations in detecting **zero-day**

**attacks** and novel threats, as they can only recognize patterns already present in their databases.

To overcome these limitations, researchers explored **anomaly-based detection** approaches that establish normal behavior models and flag deviations as potential intrusions. Techniques including **statistical analysis**, **state-based models**, and **machine learning** have been widely used. For example, Denning (1987) proposed an early model of statistical anomaly detection that calculates deviations from established norms, enabling detection of unknown attacks. Researchers have applied clustering algorithms such as **K-means**, **Self-Organizing Maps (SOM)**, and classification methods like **Support Vector Machines (SVM)** to differentiate between normal and malicious activities.

With advancements in artificial intelligence, **machine learning-based intrusion detection** has gained substantial attention. Works by researchers such as Ahmed et al. (2016) and Vinayakumar et al. (2019) demonstrated that supervised learning models, including **Decision Trees**, **Random Forests**, and **Neural Networks**, can improve detection accuracy. Deep learning models such as **Deep Neural Networks (DNN)** and **Recurrent Neural Networks (RNN)** have also been employed to capture complex patterns in network traffic, offering better performance for large datasets.

## 3.EXISTING SYSTEM:

In the existing system, network and system security is mainly ensured using traditional security mechanisms such as **firewalls, antivirus software, and signature-based Intrusion Detection Systems (IDS)**. These systems are designed to protect networks by defining predefined rules and known attack patterns. Firewalls control incoming and outgoing network traffic based on security rules, while antivirus software detects and removes known malware using signature databases.

## 4.PROPOSED SYSTEM:

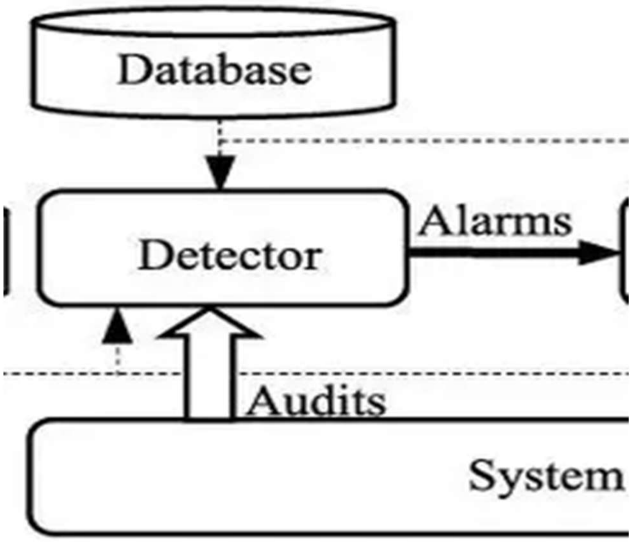
The proposed system introduces an **intelligent and efficient Intrusion Detection System (IDS)** designed to overcome the limitations of traditional security mechanisms. This system focuses on accurately detecting both **known and unknown attacks** by analyzing network traffic and system activities using advanced detection techniques.

Unlike the existing signature-based systems, the proposed IDS adopts an **anomaly-based and hybrid detection approach**. It monitors network packets in real time, extracts relevant features, and compares them with normal behavior patterns. Any significant deviation from normal behavior is identified as a potential intrusion. This approach enables the system to detect **zero-day attacks and previously unseen threats**.

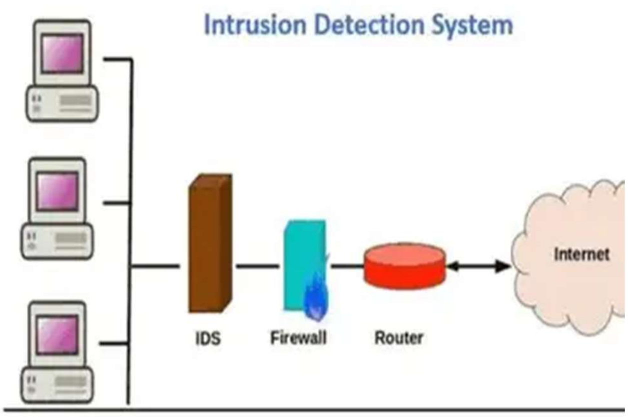
The proposed system can integrate **machine learning algorithms** to improve detection accuracy and reduce false positives. By training the model using historical and real-time data, the IDS can learn attack patterns and continuously adapt to new threats. Classification techniques such as Decision Trees, Random Forests, or Support Vector Machines can be used to classify network activities as normal or malicious.

Additionally, the system provides **real-time alerts and detailed logs** whenever suspicious activity is detected. These alerts help system administrators take immediate action to prevent damage. The proposed system is designed to be **scalable, flexible, and efficient**, making it suitable for modern high-speed network transferred data is collected ,stored and analyzed using Thing speak application. Thingspeak is one of the recently developed application in the field ofIoTfor analyzing data transferred by wireless sensor networks.

## *5.BLOCK DIAGRAM:*



## *6. CIRCUIT DIAGRAM:*




## *7. WORKING PRINCIPLE:*

The working principle of the Intrusion Detection System (IDS) is based on continuous monitoring, analysis, and detection of suspicious activities within a network or system. The system operates by observing network traffic or host activities and identifying potential intrusions in real time.
Initially, the IDS **captures network packets or system log data** from the monitored environment. This data is collected through packet sniffing tools or system sensors without interrupting normal network operations. The captured data is then forwarded to the preprocessing stage.

In the preprocessing phase, the raw data is **filtered and converted into a suitable format** for analysis. Important features such as source IP address, destination IP address, port numbers, protocol type, packet size, and time interval are extracted. Noise and irrelevant data are removed to improve detection accuracy.

**HARDWARE CONFIGURATION**

1. Processor: Intel Core i3 / i5 or higher
2. RAM: Minimum 4 GB
3. Hard Disk: 250 GB or above
4. Network Interface Card (NIC)
5. Keyboard
6. Mouse
7. Monitor

**SOFTWARE CONFIGURATION**

1. Operating System: Windows / Linux
2. Programming Language: Python / Java
3. Database: MySQL / MongoDB
4. Web Server: Apache / Tomcat
5. IDS Tool / Framework: Snort / Custom IDS
6. IDE: VS Code / Eclipse

## 9. COMPONENT DETAILS:

**1. Data Collection Component**
The Data Collection component is responsible for continuously monitoring the network or host environment to gather relevant data required for intrusion detection. It captures incoming and outgoing network packets, system logs, user activities, and application-level events. This component uses sensors or packet sniffing tools to collect data in real time without disrupting normal system operations. Efficient data collection ensures that no critical information related to malicious activity is missed.

**2. Preprocessing Component**
The Preprocessing component prepares the collected raw data for effective analysis. It removes irrelevant, duplicate, and noisy data that may affect detection accuracy. This component also handles missing values, normalizes data, and converts it into a standardized format. By cleaning and structuring the data, preprocessing improves system performance and reduces false detection rates.

**3. Feature Extraction Component**
The Feature Extraction component identifies and extracts significant attributes from the preprocessed data. These attributes include source and destination IP addresses, port numbers, protocol types, packet size, flow duration, and frequency of requests. Selecting relevant features reduces computational complexity and plays a crucial role in accurately distinguishing between normal and malicious activities.

**4. Detection Engine**
The Detection Engine is the core component of the Intrusion Detection System. It analyzes extracted features using various detection techniques such as signature-based detection, anomaly-based detection, and machine learning-based detection. Signature-based methods compare activities with known attack patterns,

while anomaly-based methods detect deviations from normal behavior. Machine learning techniques enable the system to learn from historical data and improve detection accuracy over time.

**5. Knowledge Base / Signature Database**

The Knowledge Base stores predefined attack signatures, detection rules, and trained machine learning models. It acts as a reference repository for the detection engine. Regular updates to the knowledge base allow the system to recognize newly discovered attacks and adapt to evolving threat patterns. This component is essential for maintaining the effectiveness of the IDS.

**6. Decision Component**

The Decision component evaluates the results produced by the detection engine and determines whether the observed activity is normal or malicious. It applies threshold values and classification rules to minimize false positives and false negatives. Accurate decision-making ensures reliable intrusion detection and avoids unnecessary alerts.

**7. Alert and Response Component**

When an intrusion is detected, the Alert and Response component generates real-time alerts and notifications for system administrators. Alerts may be displayed on dashboards, sent via email, or logged in monitoring systems. In some implementations, this component can also initiate automated responses such as blocking suspicious IP addresses or terminating malicious sessions.

**8. Logging and Reporting Component**

The Logging and Reporting component maintains detailed records of all detected intrusions and system activities. Logs include timestamps, source details, attack type, and response actions. These records are useful for forensic analysis, compliance auditing, and improving future security policies. Reports generated from logs help administrators understand attack trends and system vulnerabilities.