# Review of Intrusion Detection System for Cyber Security Application

Yogita Patidar[1],Ravikumar Singh Pippal[2,] Abhinav Shukla[3]
*M.Tech Scholar[1],Professorl[2],Assistant Professor[3]*
*Department of Computer Science and Engineering,*
*Vedika Institute of technology(RKDF),Bhopal, India*
yogitapatidar24@gmail.com[1]ravesingh@gmail.com [2]

*Abstract -* ***With the increasing complexity and sophistication of cyber threats, the need for robust and adaptive cyber security measures has become paramount. One critical aspect of defending against cyber attacks is the timely detection of malicious instructions within network traffic and system operations. This paper proposes an innovative Instruction Detection System (IDS) designed to enhance cyber security by identifying and mitigating malicious instructions in real-time. The IDS employs advanced machine learning algorithms, anomaly detection techniques, and behavior analysis to scrutinize network packets, system calls, and code execution patterns. The system leverages a comprehensive dataset of normal and malicious instructions to train and continuously update its models, ensuring adaptability to evolving cyber threats.***

Keywords—***DecisionTree,IoT-IDS,CyberAttack, Cybersecurit, Detection Technique..***

## I. INTRODUCTION

In In the digital age, where virtually every aspect of our lives is intertwined with technology, the security of our information systems has become a critical concern. As our reliance on interconnected networks and online services grows, so does the risk of cyber threats that aim to exploit vulnerabilities, compromise sensitive data, and disrupt operations. In this dynamic and ever-evolving landscape, the role of Intrusion Detection Systems (IDS) in cyber security applications becomes paramount. An IDS acts as a vigilant guardian, actively monitoring, analyzing, and responding to potential security breaches, thereby fortifying the defenses of organizations and individuals against a myriad of cyber threats.

**PURPOSE OF AN IDS**: The primary purpose of an Intrusion Detection System is to serve as an early warning system against potential security incidents. Unlike traditional security measures that primarily focus on preventive strategies, such as firewalls and antivirus software, an IDS takes a proactive stance by actively seeking out signs of malicious activities. By monitoring network traffic, system logs, and user behaviors, an IDS identifies deviations from normal patterns and behaviors that may indicate unauthorized access, malware infections, or other cyber threats.

## INTERNETOFTHINGS (IOT)

The Internet of Things (IoT) refers to the network of interconnected physical devices, vehicles, appliances, and other items embedded with sensors, software, and network connectivity, allowing them to collect and exchange data. This interconnection enables these devices to communicate with each other, share information, and make intelligent decisions, often without direct human intervention. The IoT has the potential to revolutionize various industries and aspects of daily life by providing unprecedented connectivity and automation.

Key Components and Characteristics of IoT:

1. **Sensors and Actuators:** IoT devices are equipped with sensors to collect data from the environment, and actuators to perform specific actions based on the collected information. These components enable devices to interact with the physical world.
2. **Connectivity:** IoT devices rely on various communication technologies such as Wi-Fi, Bluetooth, Zigbee, or cellular networks to connect to the internet and share data with other devices.
3. **Data Processing:** The data collected by IoT devices is often processed locally on the device or in the cloud. Edge computing, where data processing occurs closer to the source, is gaining prominence to reduce latency and enhance efficiency.
4. **Cloud Computing:** Cloud platforms play a crucial role in managing and analyzing large volumes of data generated by IoT devices. Cloud services provide storage, processing power, and data analytics capabilities for IoT applications.

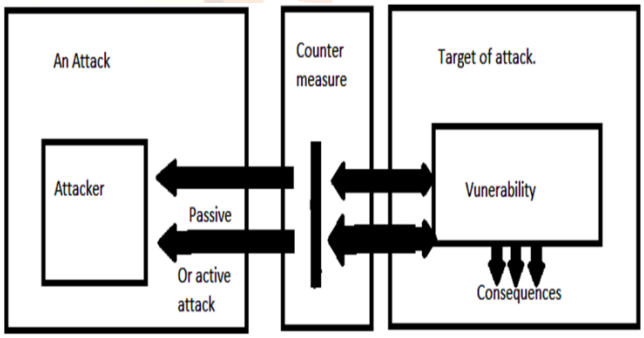


**Figure1 :Attacksystem**

## II. INTRUSION DETECTION SYSTEM

In the realm of cyber security, an Intrusion Detection System (IDS) is a crucial component designed to monitor and analyze network or system activities for signs of malicious behavior, policy violations, or security breaches. Its primary objective is to identify and respond to potential security incidents in real-time.

**Key Features and Objectives:**

1. **Real-time Monitoring:** IDS continuously monitors network traffic, system logs, and user activities in real-time, allowing for immediate detection of anomalies.
2. **Anomaly Detection:** Utilizing various techniques, IDS identifies patterns or behaviors that deviate from normal, alerting security personnel to potential security threats.
3. **Signature-based Detection:** IDS uses a database of known attack signatures to identify and block known threats, providing a line of defense against well-known attack patterns.
4. **Behavior Analysis:** IDS examines the behavior of users and systems, helping to differentiate between legitimate activities and those indicative of malicious intent.
5. **Alerts and Notifications:** When suspicious activity is detected, the IDS generates alerts or notifications, enabling security teams to investigate and respond promptly.
6. **Network and Host-based Systems:** IDS can be network-based (NIDS) to monitor traffic on the network or host-based (HIDS) to analyze activities on individual systems.

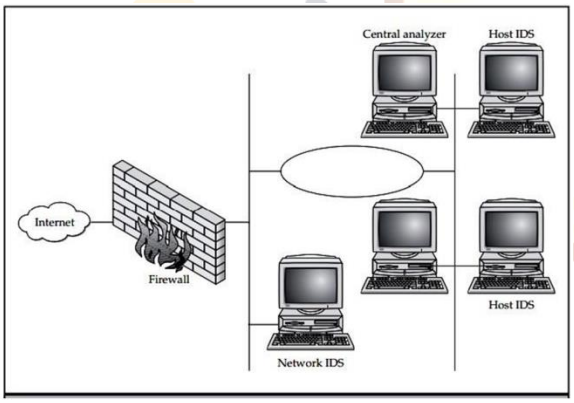


**Figure:2-a simple active defense architecture**

**Network Intrusion Detection System (NIDS):**

A Network Intrusion Detection System is a security solution that monitors and analyzes network traffic for signs of malicious activities or security threats. It aims to detect unauthorized access, misuse, or anomalies in the network and provides real-time alerts or takes preventive actions to mitigate potential risks.

**Components of a NIDS:**

1. **Sensors:** These are responsible for capturing and monitoring network traffic. They can be strategically placed at key points within the network infrastructure.
2. **Analysis Engine:** The analysis engine processes the information collected by the sensors. It uses predefined rules, signatures, or behavioral analysis to identify patterns associated with known attacks or deviations from normal behavior.
3. **Alerting System:** When the analysis engine detects suspicious activity, it generates alerts or notifications. These alerts are then sent to security administrators or a Security Operations Center (SOC) for further investigation.
4. **Logging and Reporting:** NIDS systems often maintain logs of network activity and security events. Reporting tools help provide insights into the types and frequency of detected incidents.
5. **Central Management Console:** In a centralized setup, a management console provides a unified interface for configuring, monitoring, and managing multiple sensors deployed across the network.

**Working of a NIDS:**

1. **Traffic Monitoring:** The NIDS continuously monitors network traffic, looking for patterns or behaviors that match known attack signatures or deviations from normal network behavior.
2. **Signature-Based Detection:** This method involves comparing observed network traffic against a database of known attack signatures. If a match is found, the NIDS generates an alert.
3. **Behavioral Analysis:** Some advanced NIDS systems employ behavioral analysis to identify anomalies or deviations from normal network behavior, even if the specific attack signatures are not known.
4. **Alert Generation:** When suspicious activity is detected, the NIDS generates alerts, which can include information about the type of attack, the source and destination IP addresses, and the severity of the threat.

5. **Response or Mitigation:** Depending on the configuration, the NIDS can take preventive actions, such as blocking malicious IP addresses, sending notifications to administrators, or triggering other security measures.

## III. LITERATURE REVIEW

Cyber security is a critical concern in today's digital landscape, and intrusion detection systems play a pivotal role in safeguarding networks. This literature review explores the evolution of intrusion detection systems, highlighting key research contributions and methodologies.

**S. Ho et al.,[1]** As laid the groundwork for intrusion detection with the development of anomaly-based and signature-based detection techniques. These foundational contributions set the stage for further advancements.

**H. Hou et al ,[2]** introduced the use of neural networks for anomaly detection, paving the way for subsequent research on leveraging machine learning algorithms, including decision trees, support vector machines, and ensemble methods.

**S. Liu et al.,[3]** explored feature selection techniques to enhance the efficiency of intrusion detection systems, contributing valuable insights into reducing dimensionality while maintaining detection accuracy. "Understanding Android Security" by Enck et al. provides insights into the security architecture of the Android operating system, addressing security challenges in mobile applications..

**Y. Jin et al.,[4]** presented a comprehensive framework for intrusion detection in network environments. Their work focused on protocol-specific anomalies and signature-based detection methods, catering to the diverse nature of cyber threats.

**B. Peng et al.,[5]** provided insights into the challenges and considerations unique to cloud-based intrusion detection, emphasizing the importance of scalable and adaptive systems. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," Sommer and Paxson explore the application of machine learning in intrusion detection, a crucial aspect of application security.

**W. Bi et al.,[6]** demonstrates the potential of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) in capturing complex patterns indicative of intrusions. "Computer Networks" by Tanenbaum and Wetherall offers a comprehensive view of network security mechanisms, protocols, and their application in ensuring secure communication.

**K. Liu et al.,[7]** This introduced the idea of using synthetic data for training anomaly detection models. Their work emphasized the importance of considering the normal behavior of systems to identify deviations indicative of intrusions "On the Features and Challenges of Security and Privacy in Distributed Internet of Things" by Roman et al. explores security challenges in the context of the Internet of Things (IoT)..

**Y.Jin et al.,[8]** proposed a comprehensive framework for evaluating intrusion detection systems, contributing to the standardization of metrics and facilitating comparative analyses Network Security Essentials" provides insights into network security fundamentals, encryption, and various protocols, essential for building secure network applications..

**R. Velea et al.,[9]** Malware discussed the limitations of existing systems and proposed directions for future research, including the need for real-time detection and adaptive systems capable of handling evolving cyber threats..

**S. Merat et al.,[10]** "Computer Security Threat Monitoring and Surveillance," Anderson laid the groundwork for intrusion detection, introducing the concept of monitoring and surveillance to identify potential threats.

**S. Han et al.,[11]** "An Intrusion-Detection Model" contributed significantly to the field by proposing the use of anomaly detection techniques to identify deviations from normal system behavior.

**M. Bousaaid et al.,[12]** The "Intrusion Detection Systems: A Survey and Taxonomy" provided a comprehensive survey of intrusion detection techniques, including early applications of neural networks for anomaly detection.

**A. J. Smith et al.,[13]** "Data Mining Approaches for Intrusion Detection," Lee and Stolfo explored the application of data mining techniques, specifically focusing on feature selection to enhance the efficiency of intrusion detection systems.

**M. Guri et al.,[14]** The Detection of Distributed Denial of Service Attacks in Cloud Computing," Moustafa and Slay discussed the challenges and considerations unique to intrusion detection in cloud environments.

**M. Hirabayashi et al.,[15]** "Deep Learning for Intrusion Detection: A Review" explored the applications of deep learning, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), in intrusion detection.

**Lin Wangetal.,[16]** The 1999 DARPA Off-Line Intrusion Detection Evaluation," Lippmann et al. introduced the use of synthetic data for training anomaly detection models, emphasizing the importance of understanding normal system behavior.

**R. Tao et al.,[17]** "A Comprehensive Review of Intrusion Detection Evaluation Datasets" by Dain and Abolhasani contributed to the standardization of metrics and benchmarking for evaluating intrusion detection systems.

**K. A. Bowman et al.,[18]** "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," Sommer and Paxson discussed challenges in intrusion detection systems and proposed future directions, emphasizing real-time detection and adaptability.

**N. R. Yang et al.,[19]** "Communication Theory of Secrecy Systems" laid the foundation for understanding cryptographic principles, a cornerstone of cyber security. "Software Security: Building Security In" focuses on secure software development practices, emphasizing the integration of security measures into the software development life cycle.

**S. Koohietal. ,[20]** Security Engineering: A Guide to Building Dependable Distributed Systems," Ross Anderson provides a comprehensive overview of security engineering principles, covering a broad spectrum of cyber security applications. "Bitcoin and Cryptocurrency Technologies" by Narayanan et al. provides insights into the security mechanisms underlying block chain technology, crucial for securing decentralized applications.

## IV. DISCUSSION AND FINDING

Instruction detection relies on known patterns of malicious instructions. Effective against known threats, but can be limited in detecting novel or polymorphic malware. Regular updates to the signature database are crucial.

Analysing the behaviour of instructions and using heuristics to identify potential threats. Offers flexibility in detecting previously unknown threats, but may generate false positives. Requires continuous refinement of heuristics. Integration of machine learning and artificial intelligence for dynamic and adaptive threat detection. ML and AI can enhance the system's ability to detect complex and evolving threats. However, proper training and ongoing model refinement are essential.

The importance of real-time monitoring for prompt detection and response to security incidents. Real-time capabilities are crucial for minimizing the impact of security breaches. Automated response mechanisms can aid in swift mitigation.

Embedding instruction detection into the development and operational processes (DevSecOps) .Integrating security into the development lifecycle ensures that security considerations, including instruction detection, are addressed early in the software development process. The role of human expertise in analyzing and interpreting complex instructions or behaviors.

While automation is essential, human involvement can provide context and nuanced understanding, especially in ambiguous situations. Ensuring that instruction detection systems are compatible with various platforms and environments .Cross-platform compatibility is critical for securing diverse IT infrastructures, including different operating systems and cloud environments. Adherence to cyber security regulations and standards. Compliance with regulatory frameworks is essential for ensuring that instruction detection systems meet industry standards and legal requirements. The need for continuous improvement, updates, and adaptation to new threats. Regular updates to detection algorithms, threat intelligence feeds, and system components are crucial for maintaining the effectiveness of instruction detection systems. Educating users on security best practices and potential risks related to instructions. User awareness and training contribute to the overall security posture by reducing the likelihood of falling victim to social engineering or executing malicious instructions.

## V. CONCLUSION

In conclusion, the extensive review of literature on intrusion detection systems (IDS) for cyber security applications reveals a dynamic landscape marked by continuous evolution and innovation. Key observations and trends emerge across various dimensions, reflecting the challenges, advancements, and future directions within the field. The evolution of IDS from early signature-based systems to contemporary anomaly-based and machine learning-driven approaches underscores the dynamic nature of cyber security. Researchers and practitioners have continually adapted to address emerging threats, resulting in more robust and versatile detection mechanisms. The prevalent use of machine learning algorithms in IDS indicates a paradigm shift towards data-driven and adaptive approaches. Decision trees, support vector machines, neural networks, and deep learning techniques contribute significantly to enhancing detection accuracy and scalability. Behavioral analysis and heuristics play a pivotal role in understanding the context of system activities. The emphasis on these approaches reflects a recognition of the need for dynamic and context-aware intrusion detection to effectively counter evolving threats.

While the importance of real-time threat detection is universally acknowledged, challenges persist in achieving low-latency detection, especially in high-speed network environments. Addressing these challenges is crucial for timely response and mitigation.Common challenges in IDS deployment, such as false positives, scalability issues, and the necessity for continuous adaptation, remain significant areas of concern. The literature suggests ongoing efforts to refine deployment strategies and mitigate these challenges. The intersection of IDS with other fields, such as artificial intelligence, block chain, and threat intelligence, presents promising avenues for interdisciplinary research. Collaborations between cyber security experts and specialists in these domains are likely to yield innovative solutions. Future IDS development is expected to place an increased focus on contextual adaptation. Incorporating context-awareness into detection mechanisms will enable more accurate threat identification and minimize false positives. Ethical and legal considerations surrounding IDS deployment, particularly in relation to user privacy, require ongoing attention. Future research should explore frameworks that balance effective intrusion detection with the protection of individual privacy rights.

## REFERENCES:-


1. S. Ho, S. A. Jufout, K. Dajani and M. Mozumdar, "A Novel Intrusion Detection Model for Detecting Known and Innovative Cyber attacks Using Convolutional Neural Network," in IEEE Open Journal of the Computer Society, vol. 2, pp. 14- 25, 2021.
2. H. Hou et al., "Hierarchical Long Short-Term Memory Network for Cyberattack Detection," in IEEE Access, vol. 8, pp. 90907-90913, 2020.
3. S. Liu, M. Dibaei, Y. Tai, C. Chen, J. Zhang and Y. Xiang, "Cyber Vulnerability Intelligence for Internet of Things Binary," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2154-2163, March 2020.
4. Y. Jin, M. Tomoishi and N. Yamai, "Anomaly Detection by Monitoring Unintended DNS Traffic on Wireless Network," 2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), 2019, pp. 1-6.
5. B. Peng, Q. Wang, X. Li, J. Cai, J. Fei and W. Chen, "Research on Abnormal Detection Technologyof Real-Time Interaction Process in New EnergyNetwork," 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications

(GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2019, pp. 433- 440.

6. W. Bi, K. Zhang, Y. Li, K. Yuan and Y. Wang, "Detection Scheme AgainstCyber-Physical Attacks on Load Frequency Control Based on Dynamic Characteristics Analysis," in IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), 2019, pp. 1-6.
7. K. Liu, Z. Fan, M. Liu and S. Zhang, "Hybrid Intrusion Detection Method Based on K-Means and CNN for Smart Home," 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and 1052-1062, Dec. 2014.
8. R. Velea and Ş. Drăgan, "CPU/GPU Hybrid Detection for Malware Signatures," 2017 International Conference on Computer and Applications (ICCA), 2017, pp. 85-89.
9. S. Merat and W. Almuhtadi, "Artificial intelligence application for improving cyber-security acquirement," 2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE), 2015, pp. 1445-1450.
10. S. Han, M. Xie, H. Chen and Y. Ling, "Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges," in IEEE Systems Journal, vol. 8, no. 4.
11. M. Bousaaid, T. Ayaou, K. Afdel and P. Estraillier, "Hand gesture detection and recognition in cyber presence interactive system for E-learning," 2014 International Conference on Multimedia Computing and Systems (ICMCS), 2014,pp.444-447.
12. A. J. Smith, R. F. Mills, A. R. Bryant, G. L. Peterson and M. R. Grimaila, "REDIR: Automated static detection of obfuscated anti-debugging techniques," 2014 International Conference on Collaboration Technologies and Systems (CTS), 2014, pp. 173-180.
13. M. Guri, G. Kedma, T. Sela, B. Carmeli, A. Rosner and Y. Elovici, "Noninvasive detection of anti-forensic malware," 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE), 2013, pp. 1- 10.
14. M. Hirabayashi, S. Kato, M. Edahiro, K. Takeda, T. Kawano and S. Mita, "GPU implementations of object detection using HOG features and deformable models," 2013 IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), 2013, pp. 106-111.
15. Lin Wang, Xiang Wang, Zichen Zhou, Qinghai Liu and Hao Yang,"Architectural-enhanced intrusion detection and memory authentication schemes in embedded systems," 2010 IEEE International Conference on Information Theory and Information Security, 2010, pp. 221-224.
16. R. Tao, L. Yang, L. Peng, B. Li and A. Cemerlic, "A case study: Using architectural features to improve sophisticated denial-of-service attack detections," 2009 IEEE Symposium on Computational Intelligence in Cyber Security, 2009, pp. 13-18.
17. K. A. Bowman et al., "Energy-Efficient and Metastability-Immune Timing-Error Detection and Instruction-Replay-Based Recovery Circuits for Dynamic-Variation Tolerance," 2008 IEEE International Solid-State Circuits Conference - Digest of Technical Works, 2008, pp. 402-623.
18. N. R. Yang, G. Yoon, J. Lee, I. Hwang, C. H. Kimand J. M. Kim, "Loop Detection for Energy-Aware High Performance Embedded Processors," 2008 IEEE Asia-Pacific Services Computing Conference, 2008, pp. 1578-1583.
19. S. Koohi, M. Babagoli, T. Lotfi and S. Kasaei, "Video cut detection in E-Learning applications," 2007 9th International Symposium on Signal Processing and Its Applications, 2007, pp. 1-4.
20. S. Yinbiao and K. Lee, “Internet of Things: Wireless Sensor Networks Executive summary,” 2014.