Intrusion Detection System for IoT

S.Jayalaxmi , S.Siddharth
Department of Computer science
Bhavans Vivekananda College
of Science Humanities and Commerce
Sainikpuri, Secunderabad

ABSTRACT

The Internet of Things (IoT) has emerged as a transformative technology, interconnecting numerous devices and enabling seamless data exchange for various applications. This interconnectedness has revolutionized industries, enhancing efficiency and convenience for users. However, the proliferation of IoT devices has also introduced unprecedented security challenges, posing significant risks to data integrity, user privacy, and system reliability. This study highlights the importance of security in IoT deployments and the imperative need for effective protective mechanisms. With the increasing number of IoT devices connected to networks, traditional security measures are insufficient to thwart sophisticated cyber threats. Hence, robust security strategies must be integrated into IoT architectures from the outset to safeguard against potential vulnerabilities. One such critical security tool that plays a pivotal role in fortifying IoT networks is Intrusion Detection System (IDS). By continuously monitoring network activities, IDS identifies and responds to suspicious or malicious behavior, enabling early detection of potential threats. This proactive approach empowers IoT administrators to thwart attacks in real time, mitigating the extent of damage caused by cyber intrusions. The integration of an efficient IDS within IoT networks not only bolsters cyber security but also helps maintain data integrity and ensures uninterrupted operations. This study examines the significance of security in IoT and delves into the pivotal role of IDS as a formidable defense mechanism to protect IoT networks from evolving cyber threats.

Keywords—Intrusion Detection System, Cyber threats, Internet of Things, Network.

I. INTRODUCTION

The use of connected digital equipment has developed into a valuable instrument for the prosperous market of today. In this technologically advanced day, easy and comfortable living is essential. Everything from food to fashion, quick money to financial transfers, and dictionaries to gadgets is accessible with just one click.

It is inconceivable to imagine a world without digital communication services. The dependency has resulted in the storage and retrieval of data material from the publicly accessible internet cloud, which is aiding hackers and cybercrime. An intelligent detection system is required to gather information about the suspected attack, take appropriate action, and secure the active environment to safeguard the data, system, and network.

Every day, thousands of websites and web applications encounter network breaches, some of which can be seen in news blogs. Depending on the prompt response and protection tactics employed, the network beach can result in dangerous damage to the business and the data of the customers. Computer networks have in fact evolved into a crucial technological requirement for improving effective, adaptable, and efficient communication as well as for resolving difficult administrative and scientific issues in company by maximizing output and resources.

II. NEED OF SECURITY

A. **Importance of Security in Various IoT applications**

Given the wide and connected world that the Internet of Things (IoT) presents, security is of the utmost significance. The hazards connected with data breaches, privacy violations, and cyber-attacks are becoming more obvious as IoT devices spread across a variety of industries, from healthcare and transportation to smart homes and industrial automation (1). IoT implementations must include robust security measures in order to secure sensitive data, user privacy, and the integrity of crucial systems. IoT may realize its full potential and drive innovation and game-changing applications across many industries by completely addressing security problems (2). This will improve productivity, convenience, and general quality of life for people and businesses alike.

Addressing intrusion activities in the IoT sector requires a multi-faceted approach that combines technological solutions, industry standards, and user awareness. Some of the problem-solving solutions (3) to avoid intrusion activities in the IoT sector include:

- Two factor authentication and end-to end encryption
- Regular firmware updates with security patches to address vulnerabilities.
- Network Segmentation to reduce the impact of security breach.
- Secure boot and device identity to ensure authenticate and authorize device-to-device communication.
- Intrusion Detection and Prevention Systems to mitigate suspicious activities in real-time.
- Data Encryption and Privacy Controls helps to manage data-sharing preferences.
- Industry Standards and Certifications to demonstrates a commitment to security best practices and build trust.
- User Education and Awareness to create strong passwords and recognizing phishing attempts.
- Secure Supply Chain Management prevent the introduction of compromised or counterfeit components.
- Continuous Security Monitoring and Incident Response helps in real-time threat detection, immediate response with mitigation methods.

By integrating these problem-solving solutions, the IoT sector can fortify its defenses against intrusion activities and create a safer and more resilient ecosystem for the seamless integration of IoT devices and applications.

B. **Security services and Security Mechanisms**

This section represents various methods and techniques used to establish and maintain a secured connection, each service has a unique protection property, all these properties are discussed in this section. Confidentiality is a security service that safeguards data against unauthorized access or violating the privacy protocols this is implemented with data encryption. Data authorization is the process of specifying user id and password and data authentication is checking the credentials of the user. Integrity is the assurance that the message is unaltered, reminds the user with an alert message when violated. Data availability is a service that checks the protocols should not break data services, ensures 24*7 availability of data. A security mechanism is a protocol, method, or tool designed to implement a security service. More than one method is used for a selected service based on the complexity of the threat (4). Various security services with the most suitable mechanisms are shown in Table-1.

Table 1 Relationship between Security services and Security Mechanisms.

Service	Encryption	Digital personal evidence	Accessing the Control	N/W protection with padding	Packaging control	Matriculation
Authentication		☑	☑			
Data Integrity		☑	☑			
Confidentiality	☑	☑		☑	☑	☑
Non -Repudiation		☑				
Availability		☑		☑		

Table-1 represents primary security services and the mechanism to implement these. Digital signatures or (digital evidence) are used for authentication, which limits the services only for legitimate users for the verification of credentials in the data exchange process. Data integrity is implemented using a digital signature, access control tools, and encryption techniques that hide the content with crypto algorithms (5). Traffic/Network padding is a mechanism that adds extra patterns to the packet transferred in the network for maintaining confidentiality. Notarization (matriculation) is the procedure of using the third party to assure certain properties of data exchange and maintain confidentiality. Data is available is focused on legitimate users implemented with access rights, digital signature, and traffic padding mechanism where the original data is available (6).

III. INTRUSION DETECTION SYSTEM

Security attacks may be a threat from an external intruder or abuse of data or illegal access by an internal user. These attacks are not handled by the primary security systems (7). Though the firewall provides initial security, IDS is the extended solution for detecting and preventing malicious activities with immediate alerts and taking necessary actions accordingly. Different intruders are Masquerader, Misfeasor, and Clandestine users. Increasing internet threats creates a hazard for digital users which is not easily identified by regular firewall protection (8). "An Intrusion-Detection Model in 1986" by Dorothy E focused on a real-time model of ID with an expert system based on a theory to identify the abnormal pattern from stored patterns in the audit record (9). Apart from regular anti-virus protection, additional quality of analyzing the data with predefined rules to control and compare the flow in the network for a known or unknown intrusion is the primary quality of the initial IDS model (9). IDS creates a security block between the firewall and the host system connected to the router and database and communicated with the global network. The detection model is depended on two principles: one anomaly detection (behavior deviation), and second signature detection (pattern deviation). The detection process matches the rules with existing patterns or the behavior then raises an alert by sending the report to the security officer.

A. **IDS for IoT**

The major need of an Intrusion Detection System (IDS) for IoT cannot be overstated, given the ever-growing landscape of interconnected devices and the associated security risks. As the IoT ecosystem expands, it becomes vulnerable to a wide range of cyber threats and attacks, which could compromise data integrity, user privacy, and overall system reliability. An IDS plays a pivotal role in enhancing the security posture of IoT networks by actively monitoring and analyzing network activities in real-time. By detecting and alerting administrators about suspicious or anomalous behavior, IDS enables swift responses to potential threats, helping to thwart cyber-attacks before they can cause significant damage (10). The proactive nature of an IDS is essential in the dynamic IoT environment, where new threats continuously emerge, and traditional security measures may prove insufficient. By deploying an effective IDS, IoT deployments can fortify their defenses and ensure the safety and integrity of data and devices, instilling confidence in users and fostering the continued growth and adoption of IoT technologies.

B. **Advantages and Disadvantages of IDS**

The intelligent detection system has numerous advantages, considering some as identification of suspicious invasion, continuous monitoring of network traffic, system activities, behavioral patterns, and communication transactions. IDS effectively prevents network damage by matching the attack with the previous attack. It categorizes the difference between baseline behavior and ongoing activity and builds the potential to detect previously unknown types of attacks. This provides a user-friendly interface for easy security management systems and reported generation. At the same time IDS has some loopholes which affect the security system and make it a choice for protection. Pointing out some as a failure in detecting the source of the attack which results in blocking the whole network. Swayed to false positives results, heavy processing overhead, lack of accurate categorization, difficult to train in highly dynamic environments, hard to identify an

unknown attack, intermediate actions cannot be performed, more vulnerable to network security evasion techniques (11).

C. **Classification of IDS**

IDS encompass various methodologies to detect and prevent potential cyber threats within computer networks, it is categorized based on usage, method of detection and area used given in Figure 1. Anomaly-based IDS focuses on identifying abnormal patterns or behaviors that deviate from established baselines. It continuously monitors network or host activities, flagging unusual occurrences that could indicate potential intrusions. In contrast, signature-based IDS relies on a database of known attack patterns or signatures to identify and block specific malicious activities. When an incoming data packet matches a signature in the database, the system triggers an alert or takes appropriate action to prevent the attack. Host-based IDS (HIDS) operates on individual devices or hosts, monitoring and analyzing system logs and activities for signs of unauthorized access or malicious activities specific to that host. On the other hand, Network-based IDS (NIDS) focuses on monitoring and analyzing network traffic to detect suspicious patterns and potential threats across the entire network. Anomaly-based IDS is adept at detecting previously unknown or zero-day attacks, while signature-based IDS is effective against known and established attack patterns. HIDS offers a more granular view of host-level activities, while NIDS provides a centralized and network-wide perspective. Together, these different types of IDS play a crucial role in enhancing the overall security posture of computer networks and IoT environments, allowing organizations to proactively detect and respond to potential intrusions and protect their valuable assets and data (12).

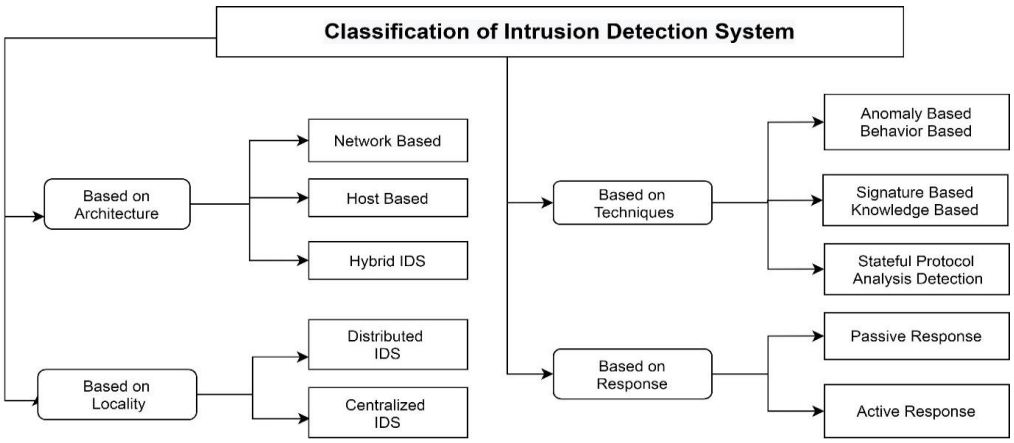

Figure 1: Classification of Intrusion Detection System

Based on the location IDS is analyzed in centralized and distributed networks. Analyzing the data with a fixed number of locations by connecting to the host system is the process of centralized IDS. This helps to monitor the

behavior of connecting hosts on the network traffic for correlation, analysis, and aggregate with standard detection algorithm. Whereas combining multiple IDS over a large network area with a central server to control and coordinate the detection process is considered as distributed IDS. Each monitoring unit is equally distributed with a centralized task for analysis. This type of IDS is used for peer-to-peer architecture. This works with logical independent components located on each workstation which are divided based on the events and actions executed. The communication manager is responsible to establish a connection between host and LAN monitors and collect data records sent to the expert system if any abnormality is found (10). The expert system which is based on specific protocols reports the details to System Security Officer (SSO) for taking relevant actions. Because of the growth of the internet, distributed working conditions, and dependency on a server this gained much popularity compared to other detection systems. At the same time, these systems are facing new problems in analyzing and identifying the intrusion with the formation of massive data (10) in the cyber world. Each category has its advantage based on the area and application used for implementing it. Focusing on this a comparative analysis on centralized and distributed IDS is shown in Table-3.

Table 2: Decentralized IDS vs. Centralized IDS

Property	**Distributed IDS**	**Centralized IDS**
Scale and extendibility	Scale a larger number of hosts and extended as needed.	Fixed with limited components.
Fault-tolerant rate	High in the distributed state.	Low as a centralized state.
Storage	Difficulty for storage, and recovery.	Easier to recover after a crash.
Load distribution	Lower load for systems, extra load for the monitoring system.	No-load on the system, high load assigned for a host with analysis task.
Reconfiguration method	Dynamic reconfiguration of each component without affecting other IDS.	Only monitoring systems are reconfigured and restarted.
Execution procedure	Harder comparatively as multiple components are connected.	Easy for executing a small number of components.

D. **IDS based on techniques**

Anomaly Based Intrusion Detection (AIDS):IDS is a technique implemented for detection by network-level and host level IDS, which is based on standard rules to monitor and identify ambiguity issues. The technique is implemented in two phases one being a training phase- building a normal structure and the second a testing phase to compare the profiles created in the current traffic with the training phase data. If the behavior patterns are matching with previous patterns, then no anomaly is generated but in other cases, a trigger is raised with an alarm indicating the unauthorized access (13). Anomaly detection is a fundamental approach in cybersecurity used to identify and address unusual patterns or behaviors that deviate from the expected norm within a system. To resolve anomaly attacks effectively, a combination of machine learning, statistical, and data mining techniques is employed. Machine learning algorithms, such as Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Isolation Forest, are commonly utilized for their ability to learn from historical data and detect novel anomalies. Statistical methods, such as Gaussian distribution modeling and time series

analysis, play a crucial role in identifying deviations from the usual patterns. Data mining techniques, including clustering and association rule mining, are utilized to uncover hidden patterns and correlations within data, aiding in anomaly detection. Hybrid approaches that integrate multiple techniques, such as ensemble methods and hybrid models, further enhance the accuracy and robustness of anomaly detection systems. By leveraging these diverse techniques, cybersecurity professionals can proactively detect and mitigate anomaly attacks, safeguarding networks, IoT devices, and critical data from potential threats given in Figure 2.

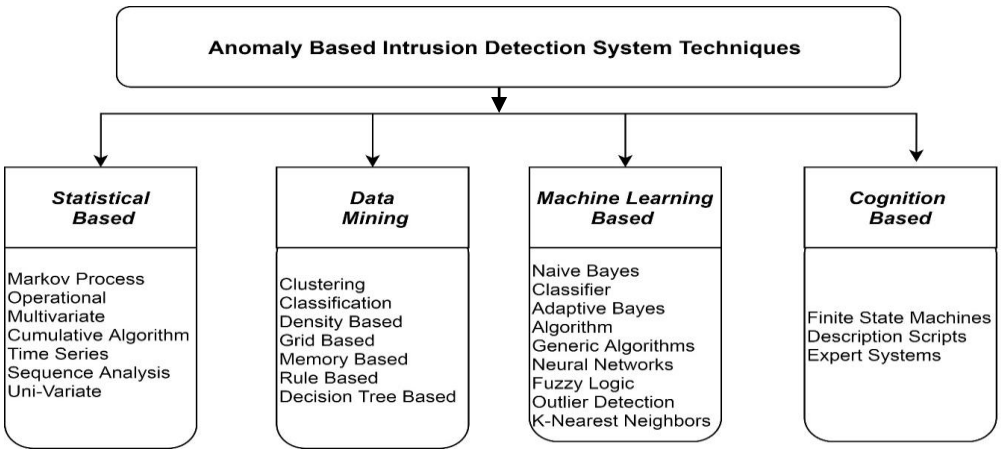

Figure 8: Classification of Anomaly Intrusion detection system.

Figure-2: Categorization of anomaly-based IDS

When deviations are discovered, statistical tests are run on the training data to determine the deviation and analyse it with a numerical value (as a score) for the transaction. When the event count reaches the threshold value IDS triggers an alarm (14). These techniques are classified into operational, threshold metrics, time-series model, sequence analysis and cumulative algorithms, etc. One of the best qualities of this method is to detect zero-day attacks; no prior knowledge is required on the patterns; the data of attacks are sniffed by the behavior pattern and analyze the deviation. The most popular method in detecting DoS attacks which are dynamic and dangerous.

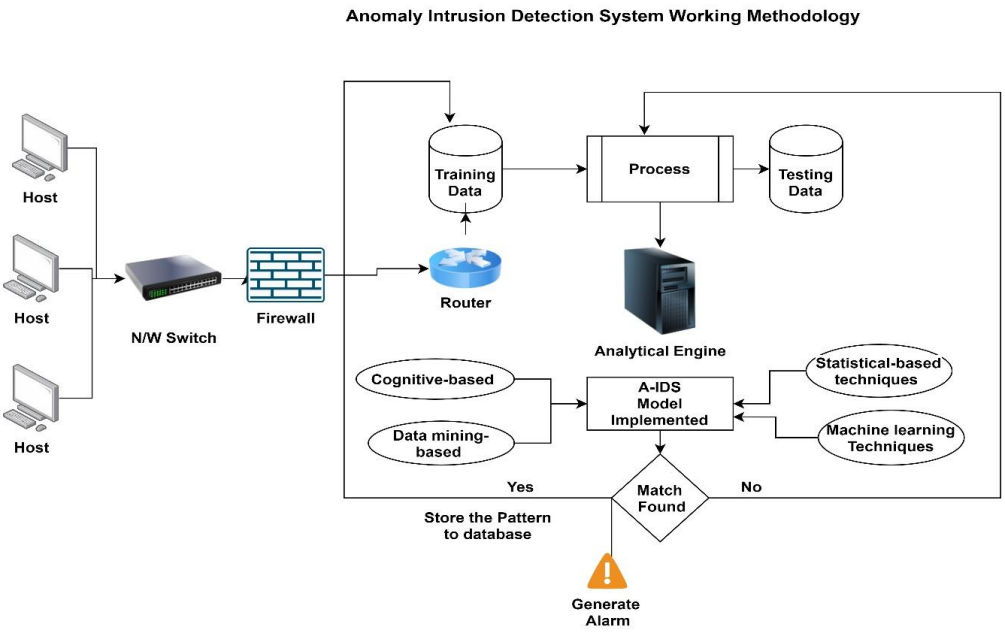

Figure-3: Anomaly Intrusion Detection System Working Process

Cognitive IDS techniques: Anomaly technique creates training data by extracting knowledge from the occurred attacks by maintaining the information about each attack with detailed analysis. The experiments conducted by various researchers proved effective with reduced false alarm rates, and take instant remedial action on the intrusions happened. Data mining-based techniques: Statistical and knowledge-based techniques are used to analyze and detect intrusion based on data mining methods. This identifies the inside attacks by classifying the current and previous patterns from the dataset. Some of the popular methods in this category include clustering, classification, rule base decision tree, etc. This method can handle huge data models by comparing each instance of the testing phase to training. The major drawback of the data mining-based approach is the requirement of high storage as it works with bulk data. Identifying abnormalities as clustering by-products are not suitable for anomaly detection (15). A schematic representation of AIDS functionality is shown in Figure-3.

Machine learning-based techniques combined with automatic learning techniques for training and testing data models to improve performance. SVM is used for both classification and regression analysis to analyze the zero-day attacks. The major disadvantage of current IDS models is the analysis with outdated(old) databases and long training time. But at the same time flexibility, data independence and adaptability are the advantages of this model (15). AIDS has more demand in detection as it compares previous and new attacks from defined normal traffic patterns with real-time data to identify suspicious activity. But lack to define perfect normal patterns in this dynamic situation (where each new pattern is generated within seconds) and reduce the time-consumed for training the model (16).

Signature Based Intrusion Detection System (SIDS): Signature-based IDS identifies unauthorized action which is suspicious and harmful to the system or network using a set of known patterns. Patterns include the sequence of bytes in network traffic or any attack which is known or recorded in the database. The main function of this system is to comparing these patterns of movements and actions with defined signatures patterns to find malicious activity within a selected time (17). Figure-4 represents the detailed process of signature-based detection. When an intrusion occurs, the details are recorded and sent to the security officer, some set values are reordered and formed as a signature, these values are used to compare with real-time attacks, and alert when deviated. Comparatively, this is an easy method to develop and understand if the patterns are available. Domain

used, Internet protocol address, and the routing protocol used is identified before the detection procedure is easy. The primary downside of this method is that it overlooks recently begun assaults owing to a lack of signatures. Additionally, because it is dependent on regular expressions, it is readily bypassed. Attacks by a worm, virus, or intrusion created by human behavior are ignored.

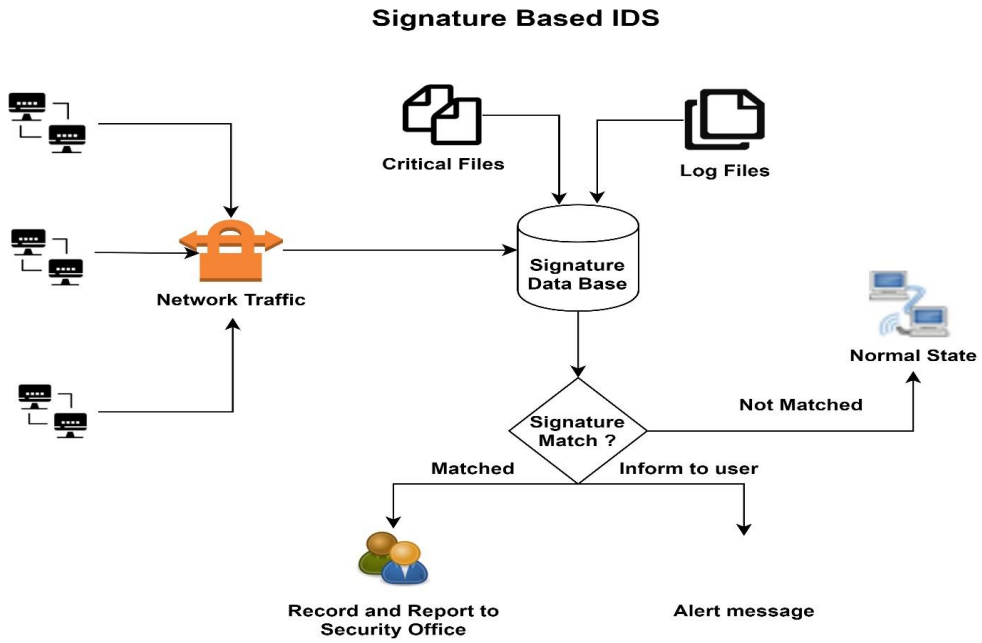

Figure 4: Working process of Signature-based IDS.

New signatures are been created to handle the new attacks based on multiple assumed values to improve the model efficiently. If the CPU load for analyzing the signature is more than the maximum bandwidth of the packets may be dropped. To avoid this data should be spliced and combined after analysis, but this increases complexity and cost. Moreover, the false positives rate will be higher if the count of signatures searched are more. This method of detection has a lot of advantages as it detects all know attacks with less computational resources. This is identified as the simplest method for creating, recording, and implementing defined patterns. If the signature is not available and the attack is raised the database is updated with attack information for the next identification (18). This method fails in identifying the zero-day error because of irregular updates of signatures. If the attack is not available in the database it is considered as a normal signature and the variations are ignored. This is a time-consuming process that requires huge storage space for keeping the

track of attack patterns. A smart attacker can implement minor changes and bypass the detection method by changing the identity. Signatures are created with string patterns each string is combined with a common prefix and corresponding set of patterns. This algorithm has deterministic and non-deterministic search variants. A non-deterministic machine layer travels from the root node and failure pointers are added thereon till the longest prefix of that node. Whereas the deterministic is a straightforward transaction implementation method. Internet attacks are more dynamic to establish a well-formed secured environment with signature IDS. However, a customizable, replicable, and expandable dataset for learning and combating advanced attackers should be developed. Many algorithms are been proposed to check the validity and existence of the system for a long period using the latest techniques. (18)

E. **Intrusion Detection and Prevention System**

A virtual security system with defined patterns for detection and prevention for handling cyber intrusion activities. IDS monitors the system and the IPS controls the system. This is a part of the network which is used to monitor and compare the data flow (bi-directional) and monitor the data packets traveled in the network. Analyzing the network or system for any suspicious activities recording in the form of state, signature, or behavior and testing the match from stored audit database and raise alert notification if any deviation occurs is the main function of IDS (19). A regular security detection system to handle cyber-attacks will monitor the network traffic or the host system for suspicious actions as violating the security policy, execution of unauthorized malware applications, and port scanning and generate a report. At the same time analyzing the packets and identifying the suspicious event comparing with the database and if match found restricting them into the network traffic is the function of Intrusion Prevention Systems. Both detection systems are software applications that reside in the same place read and compare network packets with stored attacks in the database. The implementation process is different in IDS and IPS. IDS only identifies the attack and waits for human instruction as to what action to be taken, whereas IPS is a passive method to control the process, identify the intrusion and reject the packets based on defined protocols. This is also used to identify unsafe data packets and drop them in the network before reaching the target (20). IPS is divided into multiple categories based on the implemented area and performance, and technique used. Some of them are NIPS -Network-based Intrusion Prevention Systems (NIPS) like NIDS with the technical difference of stopping the intrusion events on the network using defined signatures. NBA- Network Behavior Analysis similar to NIPS used to prevent intrusion activities in the network area but implemented with anomalies detection protocols. This technique requires a training phase to identify normal behavior and a testing phase for comparison. This is used in stateful protocol analysis, which is executed with a pre-defined baseline norm instead of learned during the training phase. HIPS -Host-based Intrusion Prevention Systems installed on host system similar to HIDS but provide attention to each host connected in the network. Another unique prevention method especially to avoid the doubtful event for a wireless network area is WIPS Wireless-based Intrusion Prevention Systems (WIPS), basically implemented with two components as integration and overlay monitoring. The overlay technique is used to monitor the radio frequencies with installed devices near access points and the integrated monitor using self APs that combine both results in hybrid monitoring. Some of the unique functions of IPS are targeting network or host TCP session. Record and update the details of the attack, reconfigure the firewall protection to prevent attacks of a

similar type, rectify the network or host area to replace or remove any suspicious data after the attack from files by repackaging, deleting header and attachment information (20), etc. The conjunction between IDS and IPS systems is shown in Figure-5.

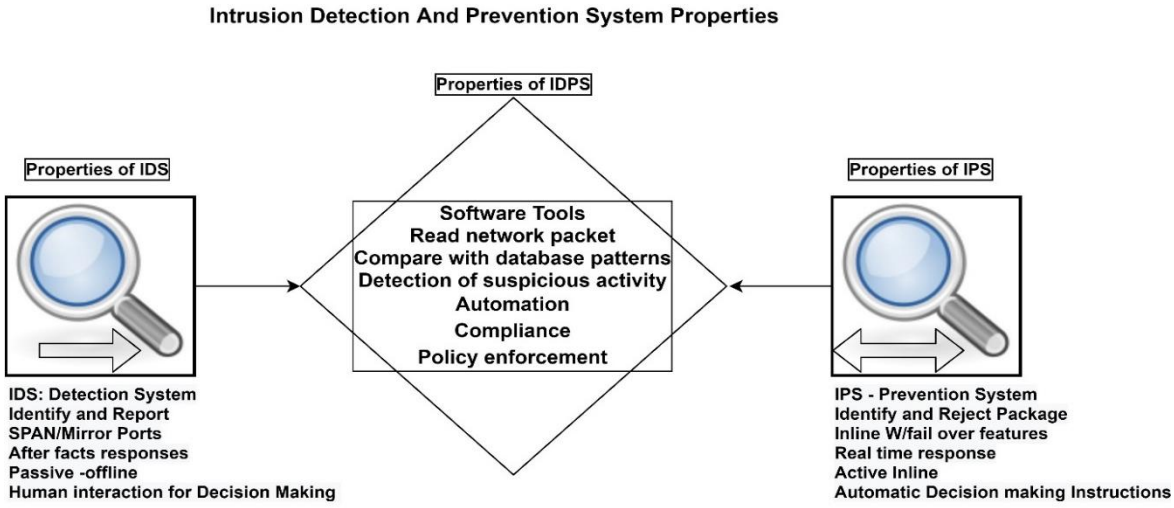

Figure:5 : Properties of IDS and IPS

IDS is a better inquest tool for computer security incidents that respond and report the investigation team. IDPS is effective only if the database is up to date to handle the zero-day error. The database should be updated or prepared for adjustments when a new attack breaches whose signatures are not available in the security database. Commercial market show curiosity on the combined system than the detection alone as Unified Threat Management (UTM) technology. This can detect and prevent intrusions in network and system. Next-Generation Firewall is implemented these days which reacts within a short time and protect most criterial area and application of network.

IV. SECURITY SERVICE RELATED TO IDS

Security Services**:** Protecting the system from vulnerable issues and save the data from intruder attempts is the primary task of the security system. A service is a process in which security is provided to protect the system and its resources. This is also considered as a communication service that improves the protection for information transfer and processing for a specific host of networks to avoid security threats with a selected mechanism. The impact of IDS on security services is summarized in Table-3

Table 3: Impact of IDS with various Security services

Security Service/IDS	Violation of service by the intruder	HIDS	NIDS	Method of Intrusion

Authentication	A. *Masquerade - legitimate user misuse other credentials*	Monitor the Host Credentials – detect abnormal activity	Monitor the Network Patters – packets, header, sender and receiver Information	Signature-based detection and Anomaly Detection (by matching with Auditing data)
Authorization	B. *Misfeasor- user trying to utilize unauthorized data/ services*	Analyze the limitations and services given to the user if violated raise and alert.	Monitor the log files, IP address, Packet Information of the user, and analyze if any unauthorized attempt is implemented.	Anomaly-based IDS check the behavior and analyze the traffic pattern
Data Confidentiality	C. *Clandestine user - utilize supervisor credentials to misuse confidential data.*	Monitor network pattern use Traffic flow to control the privacy	Implementation of Routing Control to mislead the intruders and avoid intrusion.	State full protocol analysis (match the signatures of patterns of usage)
Non-repudiation	Observe the regular records of data transfer to identify the general pattern.	Store the proof of data transfer include sender and receiver information to avoid nonrepudiation	Record the traffic information and report to audit (As sender and receiver IP address, method of sharing, protocols used, pattern analyzed)	Necessary for all IDS methods to first check this information
Auditing	Try to manifest the audit data by showing themselves as legitimate users (leads for the generation of false-positive alerts)	Obligatory to generate a report after an attack and update the audit database to control such in future		All the Methods of IDS check the audit database to match (Signatures, patterns, behaviors) and report abnormal activity.

V. SUITABLE IDS FOR VARIOUS IOT APPLICATION

Each of these IDS solutions given in Table 4 can be tailored to specific IoT application areas, providing essential security measures to protect data, devices, and infrastructure from cyber threats and potential intrusions.

Table 4: Detection solutions for various IoT implementation areas.

IOT APPLICATION	IDS SOLUTION
Smart Homes	For IoT-based smart homes, IDS solutions like Snort and Bro can be deployed to monitor network traffic and detect anomalies, such as unauthorized access attempts or unusual device behavior.
Industrial IoT (IIoT)	In industrial settings, IDS solutions like Suricata and Zeek can be utilized to monitor network communications, detect potential cyber threats, and protect critical infrastructure from attacks.
Healthcare IoT	Security Onion and OSSEC can be implemented to safeguard sensitive patient data and medical devices from unauthorized access and malicious activities.
Smart Cities	AIDE and Prelude can be deployed to detect and prevent cyber-attacks on city-wide infrastructure, ensuring the safety and security of citizens.
Connected Vehicles	CANary and CARIDS can be utilized to monitor in-vehicle networks and detect any anomalies that could lead to safety and security risks.
Agricultural IoT	Suricata and Snort can be used to monitor and protect farm machinery, sensors, and data from potential cyber threats.
Wearables and Health Monitoring	OSSEC and Zeek can be employed to safeguard sensitive health data and ensure user privacy.
Energy and Utilities IoT	Security Onion and Bro can be utilized to monitor critical infrastructure and detect any suspicious activities that may pose a threat to the energy grid.
Retail IoT	AIDE and Suricata can be implemented to protect customer data, monitor point-of-sale systems, and detect potential data breaches.
Environmental Monitoring	Prelude and Security Onion can be utilized to ensure the integrity of environmental data and detect any anomalies that may affect the accuracy of collected information.

VI. OPEN RESEARCH PROBLEM

1. Changing the behaviour of the network or a host is very hard to identify. What if an intruder changes his behaviour constantly and pretends like a legitimate user?

   Reason: An integrated technique ->Detection in such cases is a quite hard task but the framework for a model to update the database with known signatures combining with behaviour pattern can help to identify the intruder by matching one or other condition.

2. Machine learning algorithms are excellent for testing is it the same in the practical implementation?

   Reason: Most used method of machine learning is KNN and SVM both the methods were compared and tested in multiple research papers but ended with expensive computation complexity will increase as the data increase, which is impractical for an IDS application.

3. Change in size of cluster impact the distance between the variable and points. The small (normal) clusters which are very near to the deviation point are considered as anomalous then what is the accuracy of the detection method?

   Reason: Clustering technique classify and break the datasets into smaller units called clusters and label the dataset for identifying the normal and abnormal actions, and when sorted for testing with the deviation techniques based on the the distance may be labelled as the abnormal cluster.

4. Any IDS model with Systematic Intrusion detection using the integrated technique with max accuracy and the least false rate is available?

   Reason: Many research models are exploring but with multiple qualities, a new model should be invented with super intelligent technique.

5. The anomaly cannot trace dynamic behaviour and signature cannot handle zero-day-attack how to ensure the best IDS method?

   Reason: Integrated technology can merge the techniques of the IDS and result in embed products. Research is still in process.

6. Supervised learning is based on labelled data. Is it capable of labelling the current day attack for detection purposes?

   Reason: Labelling technique is used to categorize the datasets. Time and Cost factors increase if the dataset size is increased.

7. How to identify intrusion with limited resources and limited memory size?

   Reason: Analysing the intrusion consume more memory to store all the signatures, and take much processing time

for detection, so selecting a data set with only specific attributes for testing, but if the changing behaviour of the

intruder is not considered in the selected dataset. Identification is impossible.

8. The study has focused on soft computing and genetic algorithm with ANN. Is there any combined tool for GA and ANN applications?

Reason: Artificial neural network help think and identify the behaviour paters as the human brain and Generic

algorithm a search-based technique based on natural science, there is no much research exposure in this area.

9. Is this available? Updated database with dynamic configuration techniques to maintain Host and Network device details and defined patterns for matching the audit file and eliminate the zero-day- error.

Reason: The default dataset used for testing and training process ins KDD Cup 99 a very reliable and Old dataset. If

possible, developing a dataset with new attacks can solve many problems.

10. Is Any model available to reduce human dependency and automate the decision-making process?

Reason: Intrusion prevention system can take actions against the attacks when identified, but the action some time

results in breakdown of the system both the intruder and the victim, IDS help to detect the suspicious

activity but fail in taking automatic action.

11. Connect the world with connected devices is the market trend, IoT is a wireless connected service to interlink and connect the component for the best service. Enormous devices deploy massive pressure on wireless security.

Reason: Many research articles were describing and defining the vulnerabilities caused bythe wired network,

exposure in wireless in limited, and have a future research scope.

12. Is there any Standard and efficient Detection Model for IoT with a machine learning technique?

Reason: Dynamic structure of IoT, with vast data elements, create multiple security issues, a single solution to detect and prevent threats is not possible because of its heterogeneous device connectivity.

VII. CONCLUSION

The growing connectivity of devices in various sectors, such as smart homes, industrial environments, and healthcare, increases the potential attack surface, making robust security measures essential. Throughout this article, we have explored the diverse threats faced by IoT applications, ranging from data breaches and unauthorized access to device manipulation and disruption of critical services. To address these challenges, the implementation of Intrusion Detection Systems (IDS) emerges as a crucial component of an effective security strategy. IDS solutions actively monitor and analyze network and host activities, enabling early detection of suspicious behavior and potential cyber intrusions. Among the various security solutions available, IDS proves to be the best suitable option for IoT environments due to its ability to detect both known and unknown threats, fostering a proactive approach to security. By integrating IDS into IoT deployments and complementing it with other security measures, organizations can create a safer and more resilient IoT ecosystem, safeguarding

sensitive data, protecting device integrity, and ensuring the seamless functioning of IoT applications in an increasingly interconnected world.

REFERENCES

[1] RM Gomathi, G Hari Satya Krishna, E Brumancia, and Y MisticaDhas. A survey on iot technologies, evolution and architecture. In 2018 International
Conference on Computer, Communication, and Signal Processing (ICCCSP), pages 1–5, " ", 2018. IEEE, " ".

[2] Mario Frustaci, Pasquale Pace, Gianluca Aloi, and Giancarlo Fortino. Evaluating critical security issues of the iot world: Present and future
challenges. IEEE Internet of things journal, 5(4):2483–2495, 2017.

[3] Gary Mullen and Liam Meany. Assessment of buffer overflow based attacks on an iot operating system. In 2019 Global IoT Summit (GIoTS), pages
1–6, " ", 2019. IEEE, " ".

[4]Vij, C. and Saini, H., 2021, October. Intrusion detection systems: Conceptual study and review. In *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 694-700). IEEE.

[5] Challa, S., Das, A.K., Odelu, V., Kumar, N., Kumari, S., Khan, M.K. and Vasilakos, A.V., 2018. An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. Computers & Electrical Engineering, 69, pp.534-554.

[6] Lazarevic, A., Kumar, V. and Srivastava, J., 2005. Intrusion detection: A survey. In Managing cyber threats (pp. 19-78). Springer, Boston, MA.

[7] Northcutt, S. and Novak, J., 2002. Network intrusion detection. Sams Publishing.

[8] Lazarevic, A., Kumar, V. and Srivastava, J., 2005. Intrusion detection: A survey. In Managing cyber threats (pp. 19-78). Springer, Boston, MA.

[9] Yuan, B., Jia, Y., Xing, L., Zhao, D., Wang, X. and Zhang, Y., 2020. Shattered Chain of Trust: Understanding Security Risks in {Cross-Cloud}{IoT} Access Delegation. In 29th USENIX security symposium (USENIX security 20) (pp. 1183-1200).

[10] Fotouhi, M., Bayat, M., Das, A.K., Far, H.A.N., Pournaghi, S.M. and Doostari, M.A., 2020. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Computer Networks, 177, p.107333.

[11]Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A., 2018. Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, pp.108-116.

[12] Hamed, T., Ernst, J.B. and Kremer, S.C., 2018. A survey and taxonomy of classifiers of intrusion detection systems. Computer and network security essentials, pp.21-39.

[13] Nyangaresi, V.O., 2023. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. *Ad Hoc Networks*, *142*, p.103117.

[14] A Sanila, Byomakesh Mahapatra, Ashok Ku. Turuk. "Performance Evaluation of RPL protocol in a 6LoWPAN based Smart Home Environment" , 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), 2020
.

[15] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G. and Vázquez, E., 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, 28(1-2), pp.18-28.

[16] Aljawarneh, S., Aldwairi, M. and Yassein, M.B., 2018. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, pp.152-160.

[17] PlsJayalaxmi, Rahul Saha, Gulshan Kumar, Mauro Conti, Tai-Hoon Kim. "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey" , IEEE Access, 2022
[18] Teal, D.M., Cisco Technology Inc, 2002. Intrusion detection system and method having dynamically loaded signatures. U.S. Patent 6,477,651.

[19]Scarfone, K. and Mell, P., 2007. Guide to intrusion detection and prevention systems (idps). NIST special publication, 800(2007), p.94.

[20] El-Taj, H., Najjar, F., Alsenawi, H. and Najjar, M., 2012. Intrusion detection and prevention response based on signature-based and anomaly-based: Investigation study. International Journal of Computer Science and Information Security, 10(6), p.50.