THE ROLE OF INTRUSION DETECTION SYSTEM (IDS) IN INTERNET OF THINGS (IOT) -ITS FRAMEWORK OF WORKING AND CHALLENGES

Abstract

IOT is a new emerging and modern prototype that has merged several components, internet connected to various day-to-day physical objects. IoT has become a rapidly evolving technology making a great impact on the digital world, starting from everyday home appliances to a large industrial system. It has imposed a heavy duty on the data communication through internet, high risk on information and computational complexity. Devices are affiliated with a variety of smart fields like hospital, industries and home. Devices capture more valuable information. This has led to the attention of cybercriminals to get attracted towards the IoT for exploitation of the security and gain access to the devices and the data. Despite of being trending and promising technology of the present and for the future, IoT still faces security challenges as they IoT devices increase.

The attacks on the IoT devices are increasing, because of the few drawbacks of the IoT devices like resource constraint, limited memory, low energy storage and lack in running the existing security software vulnerabilities. Cyberattacks has become very common in the IoT environment. If the attacks on the IoT devices goes unnoticed for a long time it creates many issues like inaccuracy, delay, service interruption and a huge loss.

Intrusion Detection System plays an important role in detecting any attacks on the system. It helps in preventing our system from intruders. The goal of the IDS is to monitor the entire network activity, detect for any malicious or suspicious activity and

Authors

A. Kalaivani
Research Scholar
Governement Arts College(Autonomous)
Salem, Thamilnadu, India.

Dr. R. Pugazendi
Assistant Professor
Governement Arts College(Autonomous)
Salem, Thanmilnadu, India.

trigger an alarm to the user about the attack. IDS is also undergoing so many advancements in its implementation strategies and techniques. In the last few years, the AI techniques like deep learning and machine learning has been implemented in all fields. This paper details about the Artificial Intelligence approaches (Machine learning and Deep learning) for Intrusion detection system (IDS) in Internet of Things (IoT). The complete taxonomy of IDS working, methods and the very strong datasets used are analyzed for identifying the weakness, features and to find the lacking facilities to meet the current technologies. IDS has many methods of implementing. But the anomaly –based intrusion detection system is very familiarly used in IoT. The implementation for the datasets like feature extraction, filtration, training, testing has to be performed as per the IoT environment.

Keywords: Cyberattacks IDS, deep learning, datasets.

I. INTRODUCTION

Cyber security is one of the most challenging research areas in the Information technology. Providing security becomes difficult and complicated with the tremendous growth in the emerging new technologies. IT world is full of new concepts like AI, Data science, Data Analytics and IoT. IoT is a one such technology which is very popularly known and emerging. The growth of IoT is accelerating. IoT is one of the new wearable technologies has become the hottest and busiest buzzwords.

IoT works by incorporating physical object-things and getting data exchanged among them using internet, software and sensor like devices embedded into it is making the world more evolving and trending. In spite of being the well-developed and trending technology, the challenges faced by the IoT are numerous. The cyberattacks on the IoT devices are growing.

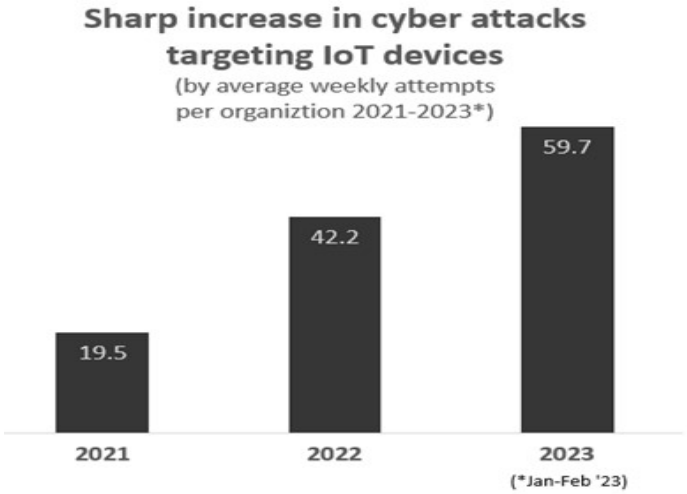


Figure: 1
Source: Checkpoint Software technologies limited

The report from checkpoint software technologies limited states that there is a sharp increase in the cyberattacks targeting the IOT devices. As the IoT is a trending buzzword, the security threats are increasing as its usage and widespread implementation is keep increasing. The attacks on the IOT devices are more because no strong security procedures are used in them [1]. Unsecure communication, device tampering, data theft are the major vulnerabilities of IoT devices.

- **The IOT security attacks are due the following surfaces as shown in figure (2)**

Figure 2: Surfaces for Security Attack

- **Devices:** The primary component for the attack is the device used in the IoT means of communication. The loopholes are present for the attackers in the memory,

firmware, default settings, weak passwords, outdated components and unsafe mechanism [2].

- **Communication Channels:** The channels connecting all the IoT devices for communication are the main place for the attacks. The procedure or the protocols used in the IoT communicating channels are not a standard one, which leads to exploit the channel.
- **Application and software:** The application and the software's which are used in the IoT world are easily vulnerable to attacks. From password cracking to the login credentials exploitation are easily done with loopholes present in the application interface and the poorly developed software.

- **The other factors for the attacks are,**
  - Lack of security software
  - Lack of cybersecurity awareness
  - Large attack surface

II. IOT IN SMART ENVIRONMENT

Today everyday life objects are connected to the technology. The IoT is the topmost ideal computing and communicating model where all the daily used objects are connected to the internet. This model works by encompassing multiple components like actuators, sensors and some knowledge-based system to obtain information from, process the same and execute the same actions on the real [3].

Now IoT has become the major part for the smart world to be done. IoT is implemented in several places like house monitoring, home appliances, transport, factories, medicine, phones, television and manufacturing.

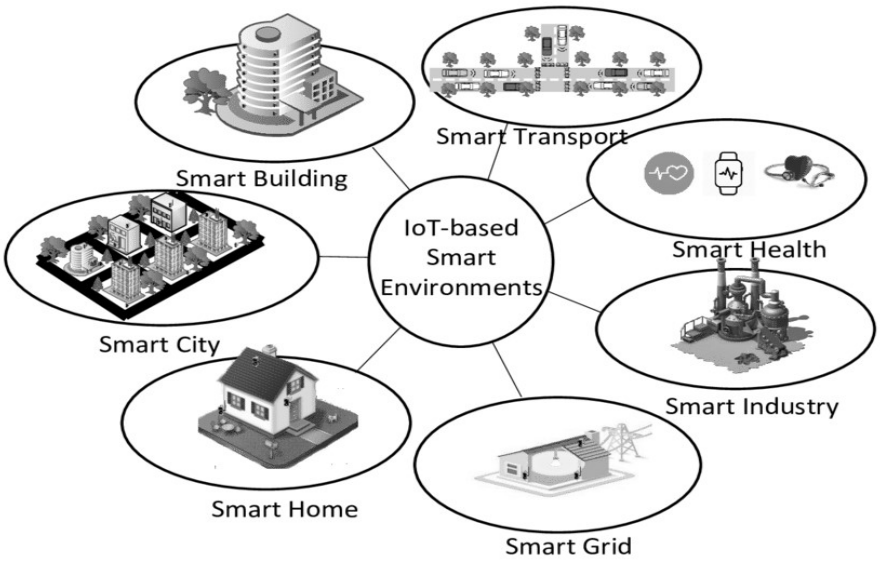


Figure: 3 [4] Iot In Smart Environment

Internet of Things (IoT) plays an important role in creating smart environments by connecting various devices and systems to improve efficiency, convenience, and sustainability. IoT technology enables the integration and communication of devices, sensors, and data to automate and optimize processes. Here are some key areas where IoT is used in smart environments.

- **Smart Homes:** smart thermostats, lighting systems, security cameras, and appliances
- **Smart Cities:** Transportation, energy, waste management, and public safety.
- **Smart Buildings:** Lighting, HVAC (Heating, Ventilation, and Air Conditioning), energy usage, and occupancy.
- **Industrial IoT:** Collect data on equipment performance, energy usage, and safety conditions.
- **Agriculture:** Monitor soil moisture, temperature, humidity, and crop health.
- **Healthcare:** monitor patient vitals, track medication adherence.
- **Environmental Monitoring:** Monitor air quality, water quality, and environmental conditions.

III. IOT ARCHITECTURE

The IOT is the interconnection of objects, sensors and internet. The data flow through the device's architecture has four important layers for the same

They are

1. Sensing Layer
2. Network Layer
3. Data Processing Layer
4. Application Layer

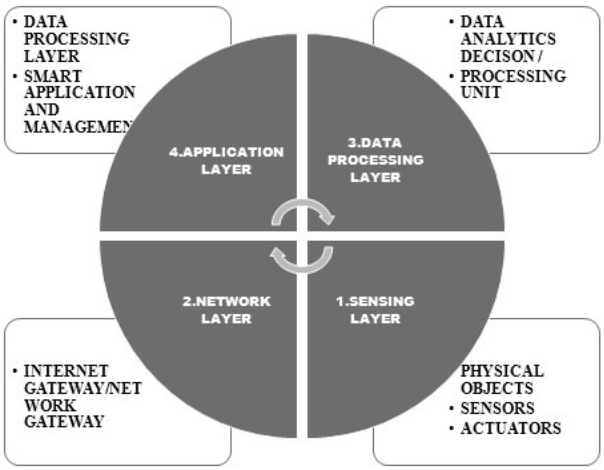


Figure: 4 Layers of IOT

IV. IOT SECURITY CHALLENGES

Developing and deploying IOT in different domain becomes a very challenging task. Few such challenges are as follows

1. **Security:** Security is a very significant concern in IoT due to the large number of devices connected and the vulnerabilities they are exposed to. No strong authentication, insufficient data encryption, lack of secure firmware updates can lead to unauthorized access, data breaches, and privacy violations

2. **Privacy:** IoT devices obtain and process sensitive personal data. Ensuring both the privacy and the user consent is a challenging task. Crucial balance between the data and the respecting the data privacy is very important.[8]

3. **Interoperability:** IoT devices faces a very challenging role when interconnected different manufacturers use different protocols and different platforms. So, maintain heterogeneous IoT world is a very complex task.

4. **Scalability:** Ensuring the all the system in IoT environment are reliable, efficient and response becomes difficult when the scalability increases.

5. **Data Management:** IoT has huge amounts of data that need to be collected, stored, processed, and analysed. So, handling data volume is crucial. Effective data management strategies like data filtering, compression, and real-time analytics are important

6. **Standards and Regulations:** Evolving IoT landscape lacks universally accepted standards and regulations. This led to fragmentation, compatibility issues, and difficulties in ensuring compliance with local regulations and industry standards.

To overcome the security challenges the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) should be implemented in the IoT devices and IoT environment.

Table 1: Different Attacks On Layers

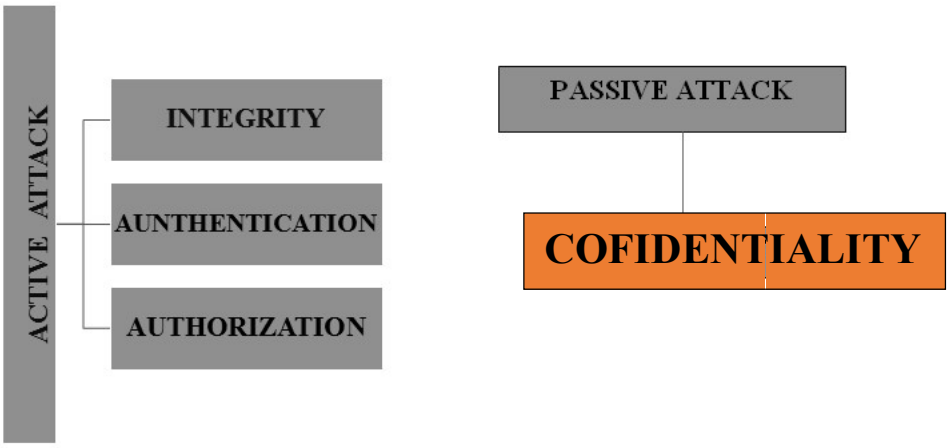
S. No	Layer name	Various attacks	Major device	Required security
1	Perception	Physical tampering, denial of service, replay attack, sensor jamming, unauthorised access.	Sensors, smart home devices, smart camera, autonomous vehicles.	Authentication, encryption and key management methods.
2	Network	Man-in-the middle, sniffing, snooping, network jamming and routing attack	Smart home hubs, IoT routers, IP cameras, smart grid devices.	Secure communication protocols, network

				access control, routing security
3	Application	SQL injection, remote code execution, device emulation, credential attack.	Smart phones, industrial control system, smart grid systems, health care devices	Authentication, secure coding, user education, firewalls, monitoring and logging

The table explains about the different types of attack on the different layers and the security mechanisms required.

V. IOT-TARGETED ATTACKS

The attacks on IoT can be active or passive attacks. The active attacks are one which disturbs the operation or working of the IoT devices. But passive attack is which monitors the IoT environment working for any vulnerabilities and use it for the future attacks. The below figure list the possible attacks on IoT environment.



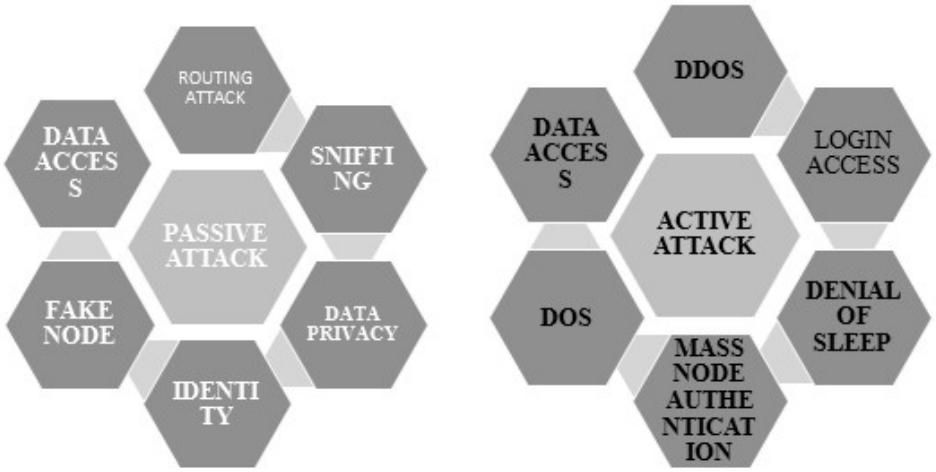


Figure 5: Types of Attack

To overcome the security challenges the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) should be implemented in the IoT devices and IoT environment.

1. **Intrusion detection system (IDS):** IDS is a security mechanism that monitors and [6] analyses network traffic or system activities to identify and respond to potential security threats, attacks and malicious activities. An intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed.

- **The following are the important reasons for implementing the IDS**
  - I)Threat Detection
  - ii)Real time monitoring
  - iii)Event correlation
  - iv)Complementing firewall
  - v)Enhancing incident response
  - vi)Detecting insider threats
  - vii) Adapting to new technology

VI. IDS PARADIGM

The term "IDS paradigm" refers to the approach or methodology used in designing and implementing an Intrusion Detection System (IDS). The Internet era has driven the need for IDSs and numerous research projects. IDSs fall into a number of different categories, or paradigms.

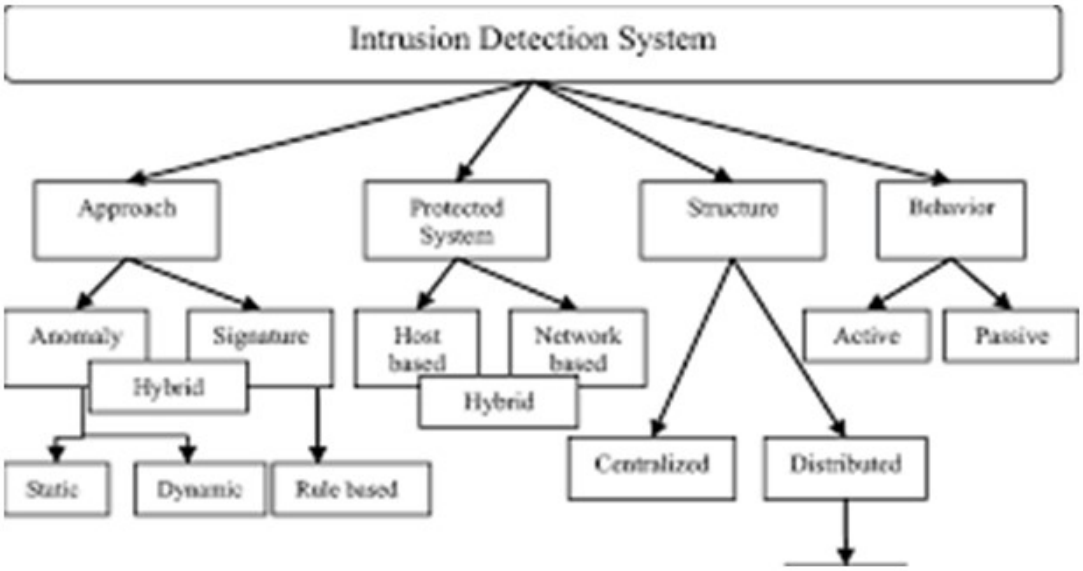


Figure 6: Taxonomies of Ids

1. **Signature Based IDS:** Signature based detection method is a best used for identifying the known threats. Itoperates by using a pre-programmed list of known threats and their indicators.

2. **Anamoly Based IDS:** Any significant deviation between the observed behaviour and the model is regarded as an anomaly, which can be interpreted as an intrusion.

3. **Host Based IDS(HIDS):** HIDS works by analysing and monitoring the internal computing, system level activities of a single system. It works on configuration, system logs, file access, sharing, modification and application usage.

NIDS is used in an overall network system or on a segment of a network to identify the attacks. Network sensors or applications are the dedicated one which is used for NIDS. It works by analysing and monitoring the activities on the network.

VII. IDS IN IOT

The IoT security is a challenging one. More researchers are concentrating towards the weak security holes. Earlier the mechanism used for the security issues are authentication, access control and encryption concepts. But all these methods are inadequate for the current digital world, where everything is trending technologies and all are AI based and cloud based. So, analysing and investigating the secure measures of IoT is a topmost higher priority for research. IDSs is one of the most promising techniques for the IoT environment and network security. IDSs is implemented in the environment of IoT to monitor,[7] analyse the packets and to give alarm monitor, analyse concentrating on the IDS deployed IoT environment is a very significant issue for understanding the security attacks.

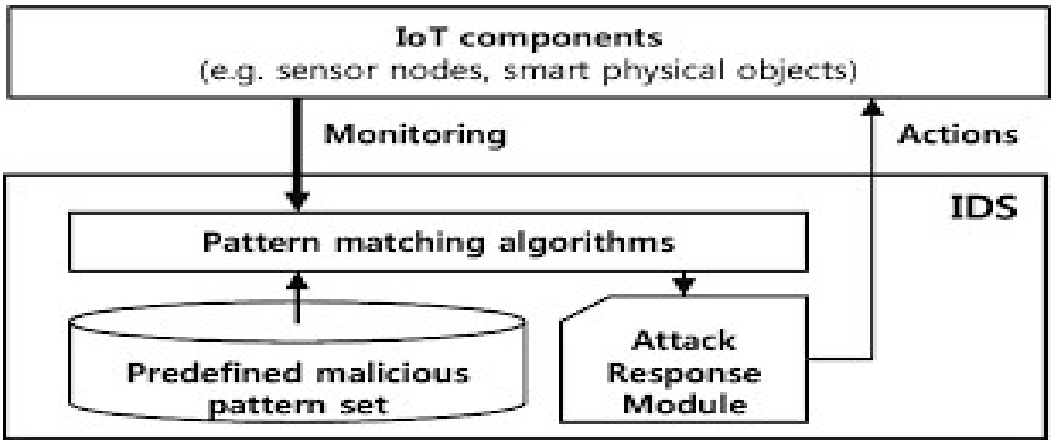


Figure: 7 Ids In Iot

An IDS is a tool which monitors and observes data in network traffic .to protect against intrusions that triggers the security of the system. In IoT environment, IDS comes in two ways,

- Host based IDS (HIDS)
- Network based IDS(NIDS)

The HIDS monitors the individual system for attack, NIDS monitors the entire network of IOT environment.

Based on the architecture deployment (placement strategy) of IDS in IoT environment it can be done in three ways,

- Centralized IDS
- Distributed IDS
- Hierarchical IDS

1. **Centralized IDS :** which monitor data from a central location. It is a type of security system which is designed to monitor and analyse network system or traffic activity in a centralized manner. Its goal is to identify and respond to suspicious activities, security breaches or attacks within an organization's network infrastructure. Some of the tasks performed are

- Centralized Management
- Centralized Data Collection
- Analysis and Alerting
- Incident Response
- Resource Efficiency

2. **Distributed IDS** are present among multiple nodes within a network. some of the tasks performed are
   - Decentralized Monitoring
   - Scalability and Resource Efficiency
   - Integration with IoT Device Management

3. **Host based IDS:** combines elements of both centralized and distributed approaches to monitor and secure IoT devices and networks, where a node will be present as alone or exists in combination of the some of the tasks performed are.
   - Local Decision-making
   - Adaptive learning and capabilities
   - Resource Optimization

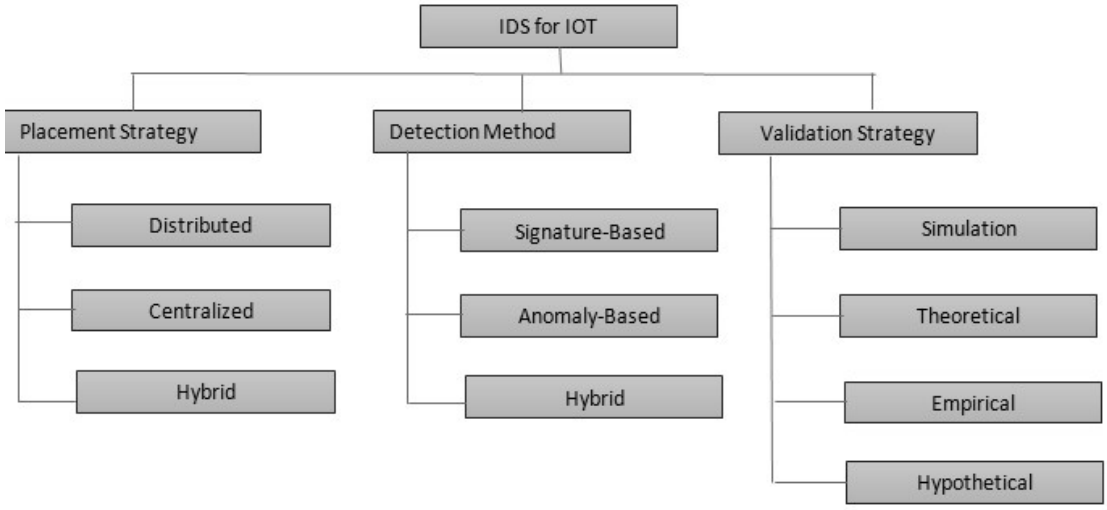


Figure 8: Ids In Iot

4. **Detection method:** Based on the detection-based method it can be signature based, anomaly based or hybrid based.

5. **The Anomaly based IDS in IOT:** In IoT environments, anomaly-based IDSs are used to monitor the behaviour of a normal network and to define a threshold [1] to detect deviations from the normal behaviour. Different techniques are used to deeply this anomaly-based IDS.To list few are:
   - Machine Learning
   - Data Mining
   - Payload Model
   - Statistical Model

- Deep learning

The deep learning techniques are the most secured and intelligent methods to use in the anomaly-based IDS in IoT.

VIII. DEEP LEARNING APPROACHES

Deep learning approaches have gained significant attention in the field of Intrusion Detection Systems (IDS) for IoT due to their ability to automatically learn intricate patterns and representations from complex data.[1]. Deep learning models like neural networks, have shown promising results in detecting and alerting security threats in IoT environments. Some popular deep learning approaches used in IDS for IoT are as follows:

1. **Convolutional Neural Networks (CNNs):** CNNs are generally used for image recognition tasks, but they are applied to analyse network traffic data in IoT. They can learn the feature automatically from raw data, making them very effective in detecting anomalies and patterns in network system.

2. **Autoencoders:** Autoencoders are used to learn to reconstruct their input data. It is an unsupervised deep learning model. In the context of IDS for IoT, autoencoders can be used to learn the normal behaviour of IoT devices and detect deviations(anomalies) from that behaviour as intrusions.

3. **Recurrent Neural Networks (RNNs):** RNNs are used for analysing time-series data, such as network logs and IoT device behaviour over time. Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) are popular variants of RNNs commonly used in sequential data.

4. **Generative Adversarial Networks (GANs):** GANs consist of generator, discriminator, two neural networks, which is trained in a competitive manner. GANs can be used to generate synthetic data that resembles normal IoT device behaviour, allowing the IDS to detect deviations from the generated samples.

5. **Deep Reinforcement Learning (RL):** Deep RL is used in the IDS of IOT to optimize the response to detected security threats. The IDS will learn to take actions to mitigate attacks based on the environment's feedback and reinforcement learning algorithms.

6. **Transfer Learning**: Transfer learning is for using the pre-trained deep learning models on large datasets and fine-tuning them on smaller datasets specific to the IoT environment. This approach can help knowledge learned from general security tasks and adapt it to the IoT context.

IX. DATASETS USED FOR IoT

The datasets play a major role in developing the model for IDS in IoT. Some of the most famous datasets which are used in IDS of IoT using deep learning approaches are,

1. Bot-IoT
2. Botnet
3. IoTID20

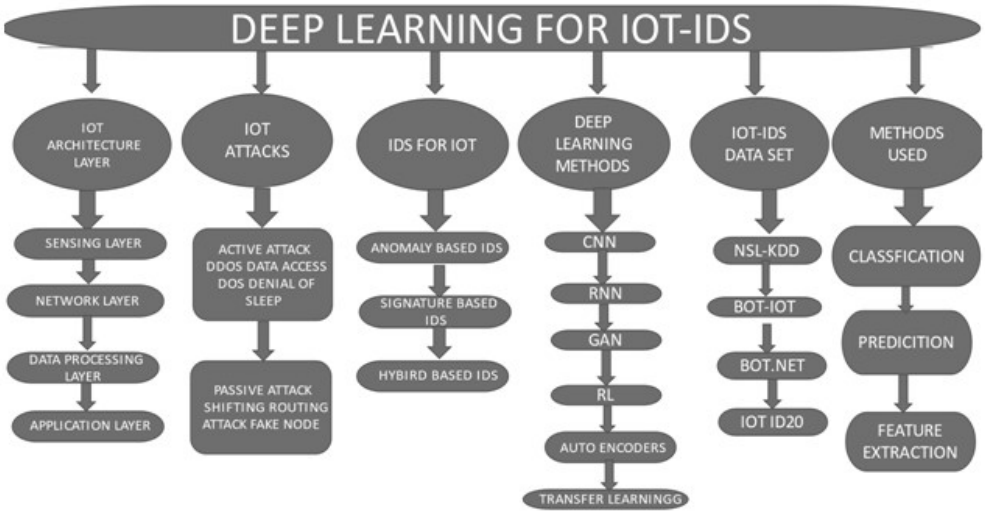
4. NSL-KDD

- **Bot-IoT he full :**This dataset is used mainly to find the botnet attacks happening. It a contains about 73 million instances. This dataset includes DDoS, DoS, OS and Service Scan, Keylogging and Data exfiltration attacks.
- **Botnet:** The Botnet dataset is an internet-connected devices-based dataset containing training and test data that include 7 and 16 types of botnet attacks. The data featured in the botnet dataset include four groups: Byte-, Packet-, Time-, and Behaviour-based.[1]

- **IoTID20:** IoTID20 consists of IoT network traffic data generated from both benign and malicious IoT devices, featuring 83 distinct network attributes. This dataset was developed using cameras, smartphones and laptops.

- **NSL-KDD:**The NSL-KDD dataset includes different types of attacks (DoS, Probe, R2L, U2R). Each attack is represented by various features extracted from the network traffic. It provides labelled data for training and testing purposes, which allows researchers to evaluate the performance of intrusion detection algorithms more effectively. This dataset is used for new intrusion detection techniques to find the new cyber-attacks

Table 2: Overall Analysis of Ids In Iot



X. CHALLENGES OF IDS IN IOT

As the IDS is a very important implementation for the secure IOT environment. Few challenges faced are as follows,

- Resource Constraints
- Network Heterogeneity
- Scalability
- Data Volume and Velocity
- Encrypted Traffic: Increasingly
- Data Integrity and Privacy
- Dynamic Network Topology
- Physical Security Concerns
- Firmware and Software Updates

XI. CONCLUSION

IoT has created a tremendous environment because of its communication process and the capacity to transform things of different application of different domains. Attackers are taking the great advantage of this tremendous approach. So, the security issue with the IoT has to be taken into high priority consideration. IDS is the strongest way of preventing the cyberattacks on the IoT devices and the environment. Different techniques are used to implement the IDS. But the deep learning approaches is at its best part. Deep learning approaches in IDS for IoT is playing a significant role to provide more accurate, efficient and exact detection of the complex and all new threats. However, they also come with challenges like significant amounts of labelled training data, computational resources, and potential adversarial attacks. The future research and development in above mentioned are essential to address these challenges and to improve the security of IoT like significant and deployment.

REFERENCES

[1] Khalid Albulayhi , Abdallah A. Smadi, Frederick T. Sheldon, and Robert K. Abercrombie" IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses", open access article under (CC BY) license .,2021[2] https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-
[2] threats-and-security-solutions
[3] Carles Gomez , Stefano Chessa , Anthony Fleury , George Roussos and Davy Preuveneers ," Internet of Things for enabling smart environments: A technology-centric perspective ", Journal of Ambient Intelligence and Smart Environments, vol. 11, no. 1, pp. 23-43, 2019
[4] https://securityboulevard.com/2022/07/7-common-internet-of-things-iot-attacks-that-compromise-security/
[5] Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang,Johari Abdullah, Farhan Ahmad, Network intrusion detection system: A systematic study of
[6] machine learning and deep learning approaches,Wileyonline library,2020
[7] Mohit Tiwari,Raj Kumar, Akash Bharti, Jai Kishan , INTRUSION DETECTION SYSTEM, International Journal of Technical Research and Applications e-ISSN: 2320-8163,pg:38-44.
[8] M. Akshay Kumaar , Duraimurugan Samiayya, P. M. Durai Raj Vincent ,Kathiravan Srinivasan, Chuan-Yu Chang, and Harish Ganesh,A Hybrid Framework for Intrusion Detection in Healthcare System using Deep learning ,open access.
[9] Satish kumar ,Sunanda Gupta , and Sakshi Arora, Research Trends in Network-Based Intrusion Detection Systems: A Review , IEEE open acess,2021.
[10] Ansam Khraisat and Ammar Alazab, A critical review of intrusion detection systems in the internet of things:techniques, deployment strategy, validation
[11] strategy, attacks, public datasets and challenges,Springer open access,2021
[12] Nancy Agarwal and Syed Zeeshan Hussain, Review Article A Closer Look at Intrusion Detection System for Web Applications,wiley publication,2018.

