International Journal of Scientific Research in Computer Science and Engineering
Vol.**12**, Issue.**4**, pp.**32-47**, August **2024**
E-ISSN: 2320-7639
Available online at: www.isroset.org

Research Article

Internet of Things (IoT) and their Intrusion: Solution and Potential Challenges

Danial Haider[1*], Tehreem Saboor[2], Aqsa Rais[3]

[1]Dept. of Avionics Engineering, Air University, Islamabad 44000, Pakistan
[2,3]Dept. of Computer Science, Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology, Islamabad 44000, Pakistan

**Corresponding Author: danialhaider112@gmail.com*

Received: 18/Jun/2024; **Accepted**: 20/Jul/2024; **Published**: 31/Aug/2024

Abstract— As we know, the cyber-attacks are merging day by day. Everything that relates to the internet has compromised with the attacks. Internet connection and their connectivity with other devices make them more vulnerable to attacks. Numerous industries, including aerial observation, wireless communication, healthcare, construction, precision farming, search and rescue, and the military, heavily rely on their usage. Moreover, these systems or networks are still exposed and have loopholes that make it welcomed to attackers to invade the system or network easily. Intrusion detection system is the system that is used to sense and also protect the network from cyber-attacks that are possible due to internet connections. This paper highlights the threat and issues that are link with the intrusion detection system in IoT domain. Also, paper emphasis on the significance or importance of the IDS in IoT. Also highlights the various IDS like signature-based IDS, anomaly-based IDS etc. Furthermore, describes and elaborates the problems that are faced with respect to each type of IDS. Finally, suggest remediation against each problem of each type of IDS to safeguard the IoT domain.

Keywords— IoT, IDS, Attacks, Challenges

1. Introduction

The software or hardware module that basically detect the malicious actions on the devices, systems or networks, thus allowing security to be maintained is called Intrusion Detection System (IDS). Network-based intrusions (NIDS) target a whole network, whereas host-based intrusions (HIDS) focus on a single computer system. NIDS are the strategies or software components that are to be deployed in a network which is used to analyse the traffic that is to be generated by hosts and devices [1]. The focus of this work is NIDSs and from now on the term IDS will indicate NIDS. The goal of an (IDS) is to identify potential threats or network intrusions. It does this by actively monitoring the network, identifying possible occurrences, and recording details about them through incident resolution. The (IDPS) is a hybrid system that combines two different systems to monitor network events and assess them for potential security policy violations or incidents. It also automates the process of doing intrusion detection and stopping to detect incidents. Figure 1 depicts the general IoT issues and their challenges.
The most intriguing developments in technology of the digital age is the Internet of Things (IoT). It has predicted that about 50 million gadgets would be connected to the internet by 2020 [1], because of the internet's ability to enable connected devices to increase rapidly every day. The aim of Internet of Things is to link the technology every device in a way that makes every computer programmable, intelligent, and more secure for human-to-human communication. Everything can directly connect with each other through networks and sensors to exchange vital information. In the future, machine-to-machine (M2M) connectivity will make it feasible. The (IoT) system gains a lot from its use in various application areas, including monitoring of environment, the smart homes, the smart industries, and the healthcare. Confidentiality, integrity, availability, and permission are significant IoT security concerns [2-3].

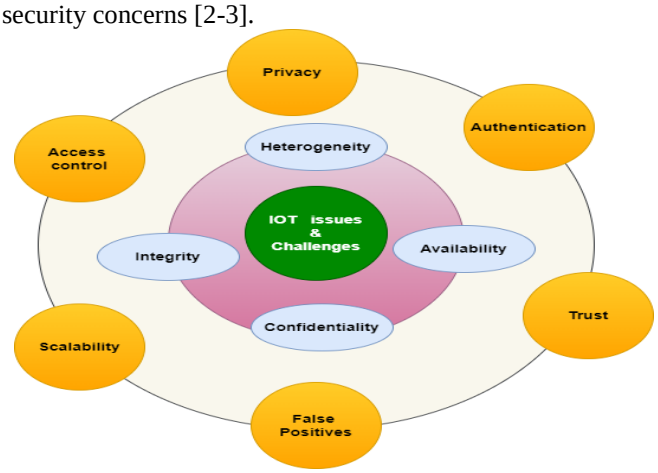

Figure 1. IoT Issues and their Challenges

© 2024, IJSRCSE All Rights Reserved

Figure 1 outlines the various issues and challenges related to the Internet of Things. The central theme of the figure is "IoT issues and challenges," surrounded by various specific concerns divided into two layers. The first layer is inner layers which deals with the diversity of devices, protocols and technologies in IoT. It also concerns about the consistent and reliable availability of IOT devices, ensuring that sensitive data transmitted and stored within the IOT system. The outer layer addresses the protection of personal information collected by the IOT devices, builds the confidence of the users and stakeholders, managing the authority to access and control IoT devices. The outer layer also deals with the incorrect identification of threats.

However, integrating real-world devices with IoT introduces a variety of cybersecurity risks into day-to-day operations. These potential assaults, which include denial of service (DoS), man-in-the-middle (MITM), and others, target key infrastructure on the Internet of Things [4]. They can infiltrate any device, and if the main server is attacked, the attacker can cause the system to crash. IDS, one of the essential tools, is vital to the IoT security framework that protects traditional and information systems to address these issues.

By creating a smart objects environment, or things, the (IoT) is a modern standard that goal is to improve the daily living through global connectivity with each other [5]. That made possible by the networking of instruments and actuators, which enables the analysis of a characteristic abundance of data to support the making of wise judgments. It is anticipated that Internet of Things technology would present hitherto unheard-of chances for human connectivity.

A future of the worldwide interconnection in which sensors and embedded devices enable a new era of internet connected gadgets to enhance our quality of life. a task renowned for being accomplished via mass data collection and analysis the Internet of Things (IoT) was born as the need for a globalized access to networks.

The security of network has long a big problem for computers. The necessity to protect sensor-based networks is perhaps more important than ever because they are utilized in many key infrastructures and applications [3-4]. Anyone must handle data securely when using IoT-based networks because of that mandate the accountable gathering and data storage, as well as concerns about individual privacy. Furthermore, anyone looking to safeguard their own legal interests or that of the police is finding that digital forensics is an indispensable instrument. As a result, accurate computer network activity tracking is essential.

Also, there are various threats that emerge and are never ignored. Figure 2 below shown the various threat in the IoT domain. Basically, attacks are the major threat in any network. There are four major attacks such as attacks on software, attacks on the network, cryptanalysis attacks, and the physical attacks. Each attack is further classified in their further branches. Software attacks comprise of viruses, worms, and logic bombs. Similar network attacks compromise of active and passive attack, which is further divided in eavesdropping, network sniffing, routing, cryptographic as the passive attacks and false node, battery exhaustion, DOS attacks are lie in the active attacks. Further cryptanalysis attacks comprise of cyphertext attacks, and MIM attacks. Last physical attacks comprise of mode jamming, micro probing, and physical damage. [6].

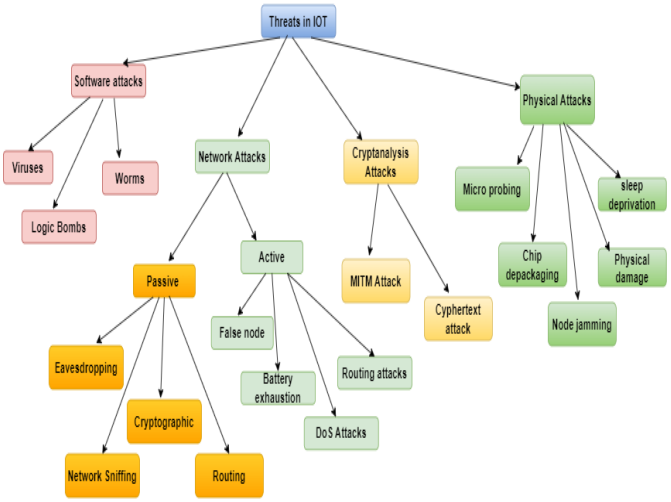

Figure 2. Threats in Internet of Things (IoT)

The figure 2 categorizes various threats in the internet of things into different types and subtypes. It is organized hierarchically showing how each category of threat branches into more specific threats. The software attacks includes the malicious programs , standalone malware and some logic bomb. The network attacks focuces on the eavesdropping, network sniffing, cryptographic, false node, battery exhaustion Man in the Middle attack and cypertext attacks. The physical attacks

In this chapter first describe some literature review , intrusion detection system, types of IDs in IoT , problems with anomaly base IDs, layer wise attacks, smart city and their attributes.

2. Related Work

The deployment and widespread adoption of IoT devices are hindered by security and privacy concerns, despite the technology's increasing popularity. Over the past thirty years, intrusion detection has grown to be a significant area of study. Researchers now have a greater understanding of security requirements and network intrusion detection.

Pietro Spadaccino and Francesca Cuomo [7] proposed a research work and the goal of this work is to assess the utilization of intrusion detection systems (IDS) in Internet of Things (IoT) networks, where edge computing is employed to facilitate the deployment of IDS. There are new issues that come up when implementing IDS at an edge environment, and solutions are suggested. P. Sanju et al. [8] proposes a hybrid met heuristics-deep learning strategy to facilitate the detection of intrusion in IoT systems. To improve intrusion detection in IoT, an ensemble of recurrent neural networks

© 2024, IJSRCSE All Rights Reserved

(RNNs) combined with an advanced met heuristics method can be used. LSTM and GRU models, which make up the RNNs, are used to identify various sorts of threats in IoT systems. In this research, fractional derivative mutation and Harris hawk optimization are used for feature selection. Sicato et al. [9] present a thorough overview of current intrusion detection systems for IoT environments, cyber-security threats issues, and problems of transparent and concerns are evaluated and explored to design an attack detection and stable network. They also present a distributed cloud architecture based on software-defined IDS, which offers a secure Internet of Things. The suggested architecture provides superior detection and accuracy compared to conventional approaches, according to an experimental evaluation. Khan et al. [8] proposed research work for the detection of intrusions and sophisticated deep learning methods have been suggested for network anomalous behaviour identification and automatic intrusion detection. The aim of this study is to offer a comprehensive examination of intrusion detection using deep learning methods that are applied by various intrusion detection systems. Public network-based IDS datasets are thoroughly examined and analysed in this review.

By giving depth analysis of existing (IDS) for Internet of Things technologies, with an emphasis on architecture kinds. After that, a suggestion for future developments in IoT-based IDS is made and assessed. Also demonstrate how the inherent shortcomings of existing approaches provide inadequate coverage of the IoT domain, making them inappropriate. The current IoT intrusion detection research must take a distinct approach in order to create a safe, reliable, and optimize the solution for the networks. It is suggested as an example to show how malicious nodes could be passively identified.

Albara Awajan et al. [10] proposed a methodology that provides solution for (IoT) devices based on (DL). To identify nasty traffic which could start an assault on linked Internet of Things devices, the intelligent system employs a four-layer deep Fully linked (FC) network architecture. To simplify implementation, the suggested system has been designed to be independent of communication protocols. Through the experimental performance analysis, the suggested system shows dependable performance for both simulated and actual invasions.

Kumar et al. implement the intrusion detection systems, a thorough examination of the security of (IoT) networks is conducted using quality of the service metrics. This is done by conducting tests and gauging the networks performance by comparing it to the available security metrics. They suggest a novel and efficient intrusion detection system (IDS) that enhances communication security by utilizing fuzzy CNN, a deep learning-based classification method. The system's primary benefits are a decrease in false positive rates, an increase in detection accuracy, and more efficient and precise detection of (DoS) attacks.

Mohy-eddine et al. [11] developed of feature selection and a K-NN classifier; to increase the accuracy (ACC) and detection rate (DR) of the IDS, we constructed the NIDS utilizing the K-NN algorithm. For the 10 features that were chosen, the suggested model retained its excellent performance while offering 99.99% ACC. Additionally, we computed the prediction time because we believe it is crucial for developing IDS for IoT. By using feature selection, we were able to drastically cut it down from 51,182.22 s to less than a minute. Comparing this unique model to earlier models that used the same dataset, there are several benefits and consistent performance.

Shah et al. [12] proposed deep learning techniques to categorize smart contracts into dangerous and non-malicious categories. Non-malicious IoT data can be stored in tamper-proof storage thanks to blockchain technology. On the other hand, a malevolent user may take advantage of the blockchain-based smart contract to lower the IoT environment's performance. The proposed system paradigm provides the recipient with an end-to-end security pipeline for the distribution of IoT data. Finally, the receiver operating characteristic (ROC) curve, classification measures (precision, recall, and F1 score), training accuracy, training loss, and other assessment metrics are considered while evaluating the suggested system model.

Trifa Sherko Othman and Saman Mirza Abdullah [13] used the most recent network flows of IoT gadgets as benign and other flows as threats from the up-to-date dataset known as IoT23. This work investigated the effects of several data preprocessing theories on the accuracy rate, including data cleansing, data coding, and SMOT theory for imbalanced data. The results of the study demonstrate that the intelligent IDS can successfully identify attacks using multiclass classification and detect assaults using binary classification.

Savanovi et al. [14] proposed a work to discover security concerns in IoT devices used for healthcare 4.0, this work optimizes machine learning techniques via a modified version of the Firefly algorithm, taking on security challenges head-on. Because metaheuristic solutions can solve nondeterministic polynomial time-hard problems (NP-hard problems) accurately and in reasonable amounts of time—two qualities that are critical for sustainable systems in any industry, but particularly in healthcare—they have aided in sustainability in several domains. A synthetic dataset created via a sophisticated configuration tool for IoT structures is used for the experiments. Additionally, several well-known machine learning models were employed, and their performance was improved by adding altered firefly metaheuristics. Shapley Additive explanations (SHAP) analysis has been applied to the best models to identify the contributing reasons to troubles that arise. Bhavsar et al. [15] develop a methodology as an Intrusion Detection System (IDS) that uses the Pearson-Correlation Coefficient - Convolutional Neural Networks (PCC-CNN) deep learning model to identify anomalies in the network. Important features from linear-based extractions and convolutional neural networks are combined in the PCC-CNN model. It carries out multiclass classification for diverse assault kinds in addition to binary classification for anomaly detection.

© 2024, IJSRCSE All Rights Reserved

Three publicly accessible datasets—NSL-KDD, CICIDS-2017, and IOTID20—are used to assess the model. To assess the model performance, we first train and test five different PCC-based ML techniques: SVM, LR, linear discriminant analysis, KNN and classification and regression tree. Across the three datasets, we obtain the best comparable accuracy of 98%, 99%, and 98% from the KNN and CART models, respectively [16].

3. Intrusion Detection system

IDS stands for Intrusion Detection System. Basically, it is a security tool or software that was designed for the monitoring the network activities for all malicious or suspicious behaviour [17]. Therefore, particular goal of an IDS is to help in detection and responding of the unauthorized access, misuse, or other security events. Intrusion detection system and their types are depicted below in Figure 3.

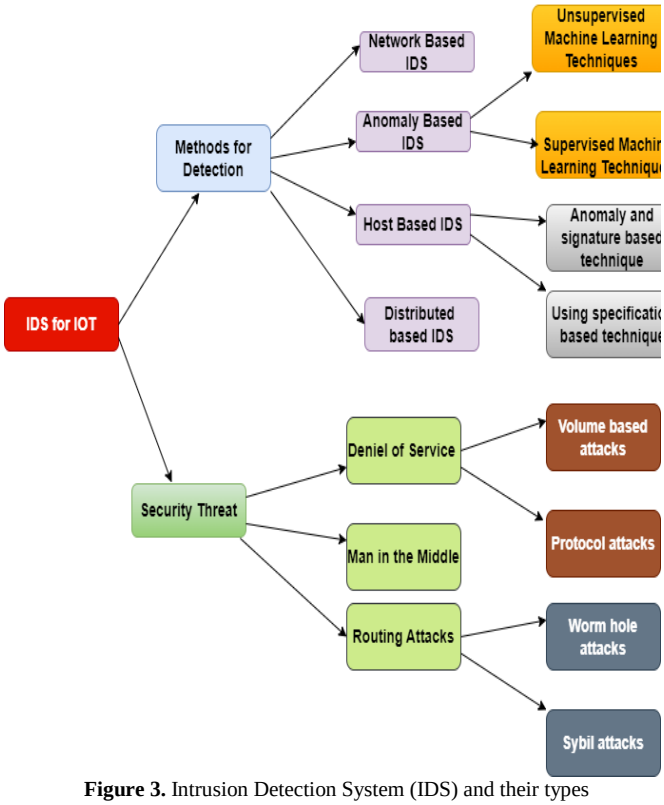

Figure 3. Intrusion Detection System (IDS) and their types

The figure 3 illustrates the different methods for the detection of intrusion specially designed for the IoT, along with the types of security threats they addresses and emphasizing the use of machine learning techniques for the detection of anamolies and the importance of both network based and the host based detection system.

4. Signifigance of Intrusion Detection System

Below mentioned are some key points related about IDS and their significance:

4.1 Anomaly Detection: IDS is responsible for observation the state of the system and the network in order to determine different patterns of behavior. In this regard, identification of the potential security breaches or intrusions helps to searches the deviations from the typical behavior within the system [18]. The process of creating a baseline of typical behavior and identifying any deviations from that baseline is what is known as anomaly-based detection.

4.2 Detection Based Signature: Signature-based detection is some other method that intrusion detection systems (IDS) might use in add-on to anomaly detection. That particular method pertains matched patterns or signatures of known attack. With the help of the activity of a database that has specify signatures that are related to particular kinds of attacks.

4.3 Network and Host-based IDS: Intruder detection systems (IDS) can be separated into two categories: such as (NIDS) and (HIDS). While HIDS focusing on the events that was occur on single computers or hosts, whereas, (NIDS) study about the traffic on network for unethical activity.

4.4 Real-time Monitoring: Real-time operation, intrusion detection systems (IDS) modify the prompt determination of expected security breaches. This observation in real time scenarios is help in order to instantly respond to and mitigate any security concerns that may arise.

4.5 Incident Response: It is achievable in the intrusion detection system (IDS) to transfer warnings or notifications to security administrators when identify an expected security breach. These particular notifications consist of information about the nature of the problem, which assists administrators in respond in a well-timed and efficient manner.

4.6 Prevention and Mitigation: IDS do not forbid attacks on its own; rather, it is a primary component in the process of early detection. However, it is realizable for security teams to come with actions regarding prevention or similar generate the mitigation strategy to reduce the impact of a security incident if they are capable to get early detection.

4.7 Compliance: As concern of all-encompassing security strategy, the adoption of (IDS) is needful by a number of regulatory frameworks and industry standards. Organizations that work in industries or manage delicate data are often necessary to follow with these standards in order to continue their operations.

4.8 Continuous Monitoring: The intrusion detection system (IDS) offers uninterrupted monitoring that will which aid the organizations in maintaining situational awareness with respect to the security of their networks and systems [19]. Keeping this constant attention is absolutely necessary in light of the constantly shifting landscape of cybersquatting threats.

© 2024, IJSRCSE All Rights Reserved

4.9 Forensic Analysis: In addition to render real-time monitoring, intrusion detection systems (IDS) use in conducting forensic investigation by followed a security breach policy. Information that is adjacent to events have been detect is logged by it. This information can be highly helpful in gaining an understanding of the nature of an attack and weakening overall security measures.

5. Types of IDS in IoT

Following discuss are the types of IoT. The detail Summarize the Types of IDS, their Associated Problems and Remediation as stated below in Table 1.

5.1 Signature Base IDS

Based on particular patterns discovered in network traffic, like the number of bytes, 1s, or 0s, the signature base IDS assist in the identification of several dangers. Furthermore, it bases its detection on the known dangerous instruction sequence of the infection. The problem with Signature Based IDS.

5.1.1 Problems with Signature Base IDS

- **Limited to Known Signatures:** Signature-based IDS has only detected threats for which they have predefined signatures. When it comes to fresh or zero-day assaults that haven't been previously discovered and recorded, they are useless.
- **False Positives:** These systems may generate false positives, indicating an attack when there isn't one. This can occur if legitimate traffic matches a signature or if the signature is overly broad.
- **False Negatives:** There is a expectation of false negatives, that occurs when intrusion detection system fails to determine a genuine attack. Their occurrence phenomenon guide in the scenario when attackers hide their operations through the use of evasion techniques, encryption, or other methods.
- **Update Dependency:** Regular updates are helpful for signature databases that incorporate new signatures for newly revealed threats easily. If the system is not quickly updated, there is a expectation that it will fail to consider the most recent threats.
- **Encrypted Traffic:** That type of system have difficulty in the dealing with communication that was encrypted since they are incapable to inspect the list of encrypted packets. The efficiency of signature-based systems decreases as the amount of communication that takes place across encrypted channels increases.
- **Resource Intensive:** The process of doing packet inspection and matching against a large signature database can be resource-intensive, that can evidence to possible performance concerns, especially in environments with a high volume of traffic.
- **Evasion Techniques:** Evasion strategy can be used by attackers to circumvent signature-based detection technologies. Among the various strategy utilized to modify the expression of their attacks include fragmentation, polymorphic code, and other techniques.
- **Limited Anomaly Detection:** It is possible that signature-based intrusion detection systems are not well-equipped for the detection of abnormal behavior due to their essential focus is on established attack patterns. Due to this restriction, they are less effective against assaults which are unique or clever and do not have a signature that has been distinct upon beforehand.
- **Complexity of Signatures:** The process of processing signatures which are accurate and particular for each and every attack can be difficult. As a phenomenon of this, definite signatures may be excessively wide, that result in false positives, or excessively particular, and also might origin versions of known attacks to be missed.
- **Dependency on Protocol Knowledge:** An in-depth knowledge of network protocols is necessary for signature-based IDS. It is a challenging for an (IDS) to effectively identification of malicious activities if it does not have enough information about specific protocols or if it comes across enforcement that are not standard.

5.1.2 Solution of Signature Base IDS

- **Anomaly Detection using ML:** It helps in the implementation of Artificial intelligence algorithms for anomaly detection. Also, ML models can acquire the normal behavior of the network and determine deviations from this baseline. Anomalies, which may signify as the harmful threats, can be flagged for encourage research.
- **Deep Learning for Pattern Recognition:** It guide in the consumption of various deep learning algorithms, like as neural networks, for more innovative pattern recognition. DL models can automatically learn complex patterns and features from network data easily, rising the system's power to detect intelligent and previously unseen attacks.
- **Behavioral Analysis with ML:** Machine Learning for the analysis of the behavior help to allow the IDS to alter to evolving threats by learning from past data. ML models can easily recognize changes in user and system behavior that may point malicious activity easily.
- **Zero-Day Threat Detection:** ML and DL models can be skilled to identify zero-day threats by learning from the behavior of normal and anomalous network activities. These models help in the can generalization of the patterns on the far side known signatures, also help to discover novel attacks.
- **SSL/TLS Decryption with ML:** Machine Learning algorithms with SSL/TLS decryption easily analyze the content of encrypted traffic. ML models can determine patterns or anomalies within encrypted communications, sanctioning the detection of threats that may be hidden within secure channels.
- **Federated Learning for Decentralized Training:** Federated Learning are implemented to train models across distributed environments without centrally pooling sensitive data. That particular approach

© 2024, IJSRCSE All Rights Reserved

allows organizations to cooperate on improvement of the IDS models without sharing raw network data.

- **Continuous Learning:** Continuous learning execution enable in ML and DL models help to regulate upgradation and retraining of the models to easily adapt towards the changes in network behavior and the develop threat landscape. Also, assist to maintain the effectiveness of the IDS over time.
- **Ensemble Learning:** The techniques ensemble learning was used to combine the guesses from multiple ML or DL techniques. Also, this aid in the enhancement of the whole accuracy and robustness for the intrusion detection system by giving leveraging against diverse models.
- **Transfer Learning:** This learning is applied to give the leverage for the per-trained models within specific tasks. Models are trained on large datasets, for general security features can be fine-tuned for the organization's specific network environment, also, reduced the need for extended labeled data.
- **Feature Engineering for DL:** In feature engineering, invest in the extraction of relevant features from raw network information before stimulation it into DL models. Furthermore, Well-designed feature representations can importantly alter the performance of deep learning-based intrusion detection.
- **Reducing False Positives with FL:** Federated Learning to join forces to reduce false positives crosswise multiple organizations. FL permit organizations to share insights on false positives without exposing raw data, and support collective learning and betterment.
- **Adaptive Models with ML/DL:** Adaptive models that can dynamical adjustment towards the changes in the network environment. ML and DL techniques can be configured to monitor and accommodate the shifting patterns of normal and malicious behavior in a continuous manner.

5.2 ANOMALY BASED IDS

Anomaly-Based (IDS) in the discourse of IoT (Internet of Things) that are focusing on to identify the deviations from normal to discover expected security threats. Alternatively of relying on predefined attack signatures, anomaly-based IDS found a baseline of normal activity and create alerts when discovered behaviour significantly that pervert from this baseline. So, that particular approach useful for detection of novel or antecedent unexplored attacks.

5.2.1 Problems with Anomaly Base IDS

- **False Positives:** As we know, anomaly-based IDS may bring up forth false positives by drooping normal or authorized behavior as anomalous. Furthermore, this may lead towards the occurrence of the system that want an accurate baseline or if there are abrupt alteration in network patterns due to legitimate reasons.
- **False Negatives:** Also, on the flip side, there is a hazard of false negatives in the scenario where the IDS neglect to detect a real attack due to the poisonous conduct that closely resembles normal patterns or the system neglect to accept subtle anomalies**.**
- **Complex Baseline Establishment:** The creation of accurate baseline of normal behavior for a system or network can be challenging. Systems can exhibit variations in behavior due to cause such as system upgrades, changes in user behavior, or variations in network traffic.
- **Adaptation to New Threats:** The Anomaly-based systems struggle to adapt to new and emerging threats quickly. Therefore, they rely on historical data for the establishment of normal behavior, that may proceed within time for the recognizance and adapt to new attack techniques.
- **Noise and Irregularities:** Anomaly detection systems are effort with distinguishing between intentional malicious activities and irregularities caused by temporary issues, configurations, or non-malicious circumstance. This can lead to unneeded alerts or false alarms.
- **Scalability Challenges:** The complexity and volume of network traffic are going to increase with time, anomaly-based systems can aspect scalability challenges. To Analyze large datasets in real-time definite quantity significant computational resources, also maintain the performance can be a interest of domain.
- **Insider Threats:** It is challenge to find anomalies in the Anomaly-based systems and to differentiate between poisonous actions by external attackers and those of legitimate users with privileged access, particularly if the anomalous behavior is subtle.
- **Dynamic Environments:** Are basically environments that happening regular changes, like as dynamic cloud-based infrastructures, which are the present challenges for anomaly-based detection. The system necessarily to adapt to this modification and incessantly update its perceptive of normal behavior.
- **Tuning and False Positive Mitigation:** The Anomaly-based IDS often require fine-tuning to cut down false positives. Therefore, achieving the right balance between sensitivity to observe threats and particularity to prevent false alarms can be a delicate process.
- **Encrypted Traffic:** As similar to signature-based systems, anomaly-based IDS may also aspect challenges with encrypted traffic. Therefore, If the system cannot examine the content within encrypted packets, it might ignore possibly malicious activities.

5.2.2 Solution of Anomaly Base IDS

- **Behavioral Analysis with ML:** Basically, the implementation of the ML algorithms helps to analyze and learn the regular activity of network traffic. However, these models can help in the detection of deviations from the learned baseline, and also help to observe anomalies that may indicate actual intrusions.
- **Deep Learning for Complex Pattern Recognition:** Particularly neural networks, repeatedly learn difficult patterns and attribute from network data. DL models excel at capturing complex relationships, to enhanced the uncovering of sophisticated and develop threats.
- **Dynamic Thresholds with ML:** It also employ Machine Learning algorithms to dynamically alter anomaly

© 2024, IJSRCSE All Rights Reserved

detection thresholds that are based on the develop network environment. This adaptability aid in the reduction of false positives and negatives by explanation for changes in normal behavior.

- **Handling Class Imbalance:** It helps in the dealing of class imbalance issues which are inherent in anomaly detection by using different Machine Learning techniques which are robust to imbalanced datasets. Furthermore, techniques like oversampling, under sampling, or using algorithms are studied for imbalanced data which aid in the improvement of the model performance.
- **Feature Engineering for DL:** In feature engineering, its aids in the extraction of relevant features from raw data before input it into Deep Learning models. As, well-designed representation of the feature can importantly modify the performance of DL based systems.
- **Unsupervised Learning for Novelty Detection:** Unsupervised learning techniques helps in the detection of novel invisible anomalies easily. Therefore, Unsupervised learning models, like as clustering algorithms, easily identify the patterns which are deviate from the normal behavior without relying on labeled training data.
- **Adaptive Models with ML/DL:** Adaptive ML and DL models are continuously learning and modify to occurrence in network behavior. Also, these particular models can dynamically modify their agreement of normal and abnormal patterns, up their ability to discover emerging threats.
- **Ensemble Learning:** Ensemble learning techniques and predictions combine with the multiple Machine Learning or Deep Learning models. Also, ensemble methods can improve the whole accuracy of detection of the anomaly by gaining leveraging towards the diversity of respective models.
- **Transfer Learning:** Basically, transfer learning gives a significant leverage towards the per-trained models for the detection of the anomaly. Furthermore, models that are trained on general network behavioral features can be fine-tuned for particular organizational contexts, and reduction of the need of extended labeled data.
- **Federated Learning for Decentralized Anomaly Detection:** Federated Learning helps in the Implementation and training anomaly detection models crosswise distributed environments without centrally pooling delicate data. This approach allows organizations to cooperate on rising anomaly detection without sharing raw network data.
- **Context-Aware Anomaly Detection:** Basically, integration of ML/DL models with features that are related to context-aware to enhance anomaly detection. Also, models that are helpful in the circumstance of network activities can differentiate between normal variations and actual security threats easily.
- **Reducing False Positives with FL:** Federated Learning collaboratively help in the reduction of false positives crosswise multiple organizations. It also enables organizations to assets insights on false positives without exposing raw data, promoting collective learning and betterment.

5.3 Behavior Base IDS

A Behaviour-Based (IDS) in the context of the (IoT) focusing on observation and analysing the behaviour of devices and systems within an IoT network to observe abnormality that may inform regarding security threats.

5.3.1 Problems with Behaviour Base IDS

- **False Positives:** Behavior-based IDS also create false positives by flagging normal user behavior as anomalous. Also, this can occur if the system disappoints to accurately model and interpret the legitimate activities of users and systems.
- **False Negatives:** Besides, there is a risk of false negatives in the scenario where the IDS fails to detection and identification of malicious activity due to the recognize issue or acquire attack patterns. Attackers can adjust their behavior to fend off detection.
- **Baseline Challenges:** The establishment of a true baseline of normal behavior can be difficult, particularly in dynamic environments. Changes in user roles, system configurations, or network conditions lead to inaccuracy in the baseline, which impact the system's ability to determine anomalies.
- **Insider Threats:** Behavior-based systems also help in the struggle to separate between legitimate actions by authorized users and malicious actions, especially in the context of insider threats where individuals with authorized approach may abuse their privileges.
- **Complexity and Customization:** Furthermore, behavior models which are represent normal and abnormal action can be complex and time-consuming. However, customization for particular environments or industries may be necessary, and this particular operation can be resource-intensive.
- **Adaptation to New Threats:** Also, behavior-based systems have certain limitations in adaption of rapid evolving threats. Furthermore, if the system is not on a regular basis update to realize new attack techniques, it may miss emergent threats.
- **Scalability Challenges:** As we know, analyzing and associate behavior across large and dynamic networks are intensive in terms of computationally. Scaling behavior-based IDS to manage high volumes of data, as well maintain the real-time analysis can be challenging.
- **Overhead and Performance Impact:** As we know, continuous monitoring of behavior leads towards the introduction of some level of overhead, that can impact the system in terms of their performance, particularly in high-traffic environments. Also, balancing the requirement for monitoring with system performance is critical.
- **Dynamic Environments:** Frequent changes, like as those using cloud-based infrastructures or dynamic scaling within the environments, can lead towards the situation for behavior-based systems. Besides, these systems demand to adjust rapidly towards the changes in network topology and user behavior.
- **Complex Attack Techniques:** As we know, advanced attackers state sophisticated techniques to imitative normal

© 2024, IJSRCSE All Rights Reserved

behavior and circumvent detection. Also, behavior-based systems out the effort for the identification of the subtle deviations from the norm in such cases.

- **Contextual Understanding:** Context of activities is crucial in terms of Understanding and assessing behavior. Also, behavior-based IDS face objection in inaccurately rendering activities without adequate context that lead towards the expected misinterpretations.

5.3.2 Solution of Behaviour Base IDS

- **Machine Learning for Behavior Modeling:** Artificial intelligence models help in the modelling of the normal behavior within the network. This regard training models to recognize patterns that are associated with typical network activities, make it easier to determine abnormal that might point malicious behavior easily.
- **Unsupervised Learning for Anomaly Detection:** Unsupervised learning techniques, like as clustering or auto-encoders help to detect different anomaly in network behavior. Whereas, unsupervised learning is not relied on labeled data that make it desirable for distinguishing deviations without predefined signatures.
- **Sequential Pattern Analysis with DL:** DL algorithms, especially (RNNs) or (LSTM) networks easily deploy for serial pattern analysis. Deep learning acquiring dependencies and patterns in the sequence of network events, that enhanced the detection of complex attack scenarios easily.
- **Feature Engineering for DL:** Feature engineering is able to extract relevant features from raw network data before in putting it into DL models. As well, well-designed feature corresponds significantly and aid in the improvement of the performance of DL behavior analysis.
- **Dynamic Learning with ML/DL:** ML and DL models are dynamically adapting towards the modification in the network environment. These models should continuously learn and update their understanding of normal and abnormal behavior to improved detect emerging threats.
- **User and Entity Behavior Analytic (UEBA) with ML:** Machine Learning algorithms for User and Entity Behavior Analytic are easy to implement. Also, by analyzing patterns of user and entity behavior, the system can discover abnormality that point compromised accounts or insider threats.
- **Contextual Analysis with ML/DL:** ML and DL models which consider only contextual information during the analyzing the behavior. Whereas, understanding the context of network activities, like as time of day, user roles, and specific applications, aid in the improvement of the accuracy of threat detection.
- **Adversarial Machine Learning Defense:** Defenses against adversarial attacks in ML models are easy to Integrate. Adversarial machine learning techniques have purpose to betray models, and integrate defenses that can help in the enhancement of the robustness of behavior-based IDS against such attacks.
- **Federated Learning for Collaborative Detection:** Federated learning to enable collaborative behavior analysis across distributed environments without sharing raw data are easy to implement. Also, Federated Learning able the organizations to amend the accuracy of IDS models while keep data privacy in concerns.
- **Explain ability in DL Models:** Transparency and interpretability in DL models are easily integrated. As well, understanding of why a DL model flag have behaviors as abnormal is critical for security analysts to make informed decisions and inquire incidents.
- **Continuous Learning with FL:** Federated Learning for continuous learning in a decentralized manner. Federated Learning allows models to alter during the involvement of the threat landscapes and dynamic network conditions by giving leveraging insights from dual organizations without sharing sensitive data.
- **Ensuring Model Fairness:** Fairness concerns in ML/DL models are address by considering the factor of carefulness evaluate and mitigate biases. Biases in models are led to disparities in the perception of malicious behavior, and it's crucial to ensure equitable treatment crosswise various user groups.

5.4 Heuristic-Based IDS

The Heuristic-Based (IDS) in the context of the (IoT) uses heuristics and rules to identify potentially malicious activity within an IoT network. While signature-based systems depend on well-known attack patterns, heuristic-based intrusion detection systems use widely accepted heuristics to identify suspicious activity.

5.4.1 Problems with Heuristic Base IDS

- **False Positives:** The Heuristic-based IDS might generate false positives, fading normal behavior as the malicious due to the integral uncertainty in defining heuristics. This can lead to unnecessary alerts and it can be a noteworthy problem, as it may be result in squandered time and money looking for potential threats.
- **False Negatives:** The false negatives can appear when the system has not be able to detect real attacks because of the heuristics are not inclusive enough or fail to adapt to new attack patterns.
- **Dynamic Environment:** The Heuristic-based IDS might struggle in the dynamic environments where the system's behavior changes over time. It can be difficult to modify algorithms to account for changing network conditions and novel attack techniques.
- **Imperfect Context:** The Heuristics are naturally relied on definite patterns or rules to identify attacks. They may lack the ability to analyze the broader context of an event, possibly omitting more complex or situation-specific attacks.
- **Resource Intensive:** While depending on the difficulty of the heuristics, the system capacity requires the important computational resources. This may have an effect on the IDS's overall functionality and scalability.
- **Over fitting:** The over fitting arises when the heuristics are also specific to the training data and fail to generalize well to new, unseen data. As a result, a system may function effectively against recognized threats but poorly against new ones.

© 2024, IJSRCSE All Rights Reserved

- **Maintenance Challenges:** By keeping the heuristics up to date can be a stimulating task. The new threats emerge; the heuristics must be updated frequently to remain effective. Security professionals must continue working on this, which could cause delays in responding to new attacks.
- **Stealthy Attacks:** To detect the stealthy and sophisticated attacks by Heuristic-based IDS may have difficulty identifying that purposefully attempt to avoid detection by imitating typical conduct.
- **Regulation Complexity:** The technique of fine-tuning heuristics to attain a balance between false positives and false negatives can be an intricate task. It also needs a better understanding of the network environment and potential threats.

5.4.2 Solution of HeuristicBase IDS

- **Machine Learning for Rule Generation:**

By the utilization of Machine Learning techniques to automatically generate and improve heuristic rules. Machine Learning can examine historical data to identify patterns revealing of malicious conduct, helping to create more operative and adaptive rules.

- **Behavioral Analysis with ML/DL:** Incorporation of ML and DL models for behavioral analysis together with heuristics. The trained models can learn usual working patterns and against the threats not covered by heuristic rules.
- **Dynamic Thresholds with ML:** The use of Machine Learning algorithms is beneficial to energetically adjust heuristic-based edges based on evolving network conditions. This type of adaptability helps in reducing the false positives and negatives also by cooperative changes in normal behavior.
- **Feature Engineering for DL:** The techniques of feature engineering can be applied to get meaningful features from raw network data before passing it into DL techniques. This method can enhance the performance of deep learning-based analysis with heuristic rules.
- **Collaborative Learning:** Implement the collaborative learning techniques to combine the fortes of heuristic rules with predictions from AI techniques. Ensemble techniques can increase overall robustness and accuracy by utilizing the variety of detection techniques.
- **Adaptive Learning with ML/DL:** Change the ML and DL algorithms that can familiarize to changes in attack techniques. In order to effectively identify new dangers, these models should be able to adapt their understanding of normal and aberrant behavior when new data becomes available.
- **Federated Learning for Collaborative Rule Improvement:** To Apply the Federated Learning to collaboratively improve the heuristic rules crosswise different environments without sharing the sensitive data. With the use of Federated Learning, businesses may improve their IDS rules as a group using knowledge from various network settings.
- **Boosted Alert Prioritization with ML:** The Machine Learning algorithms prioritize the alerts that are generated by heuristic rules based on the harshness and likelihood of an actual threat. By doing this, security analysts can spend less time on false positives and concentrate on the most important incidents.
- **Reducing False Positives with FL:** The Federated Learning can be employed for the collaboratively reduction of false positives across numerous organizations by using heuristic-based IDS. Without disclosing raw data, Federated Learning enables organizations to exchange thoughts about false positives, fostering group learning and development.
- **Regularly Updated Heuristics with FL:** The Federated Learning is also used to facilitate the sharing of updated heuristic instructions across administrations. This cooperative strategy makes it possible for heuristic-based intrusion detection systems to take advantage of collective intelligence while maintaining data privacy.
- **Adaptive Rule Tuning with ML/DL:** By Implementing the Artificial Intelligence models to dynamically tune and enhance heuristic rules that based on real-time analysis. The adaptive fine-tuning can enhance the IDS's capability to adapt to changing the attack patterns.
- **Explain ability in DL Models:** Ensure transparency and interpretability in DL models used alongside heuristics. For the understanding why a Deep Learning model take certain decisions it is difficult for the security analysts to trust and effectively use the combined detection approach.

5.5 Hybrid based IDS

In the context of (IoT), another term is Hybrid Inspection Detection System (IDS). It combines several types for the detection method to make it more comprehensive and sturdier. The goal of Hybrid IDS is to combine the strengths of multiple types, methods or a combination thereof, in order to maximize the overall effectiveness.

5.5.1 The Problems with Hybrid Base IDS

- **Complexity:**

When combining different detection techniques and technologies only adds to the complexity ofthe system. Due to the complexity of a system, such supervision and maintaining may require resources and knowledge.

- **Consumption of Resources:** More resources are often required by the Hybrid IDS as compared to a single-method IDS solutions. This may be a heavy impact system performance and scalability.
- **Combination Issues:** The integration of diverse types of intrusion detection technologies may also become challenge in the form of compatibility and interoperability. However, it ensures the seamless communication and management between different components can be a substantial task.
- **False Positives and Negatives:** While combining the multiple detection methods doesn't guarantee elimination of false positives or false negatives. The integration can occur new difficulties in tuning and calibration, potentially it leads increasing in the false alarms or missed detections.
- **Training and Maintenance:** Specific type of training and maintenance is required to every detection technique in

© 2024, IJSRCSE All Rights Reserved

the hybrid system. So, the coordination with the informs and maintenance actions across different components can be demanding.

- **Flexibility to New Threats:** The solutions to the Hybrid IDS may fight to adjust quickly to emerging and the evolving threats. When there is the possibility that one component fails in detection of a new type of attack, then the overall system may be compromised.
- **Cost:** The implementation and maintenance of a hybrid IDS is expensive. The cost of licensing, hardware, and gradually the maintenance may be greater than that of a single-method IDS solutions.
- **Scalability:** It can be difficult to scale a hybrid intrusion (IDS) to handle a growing network or more traffic. Careful planning and resource allocation are needed to make sure the system stays efficient and successful as the company grows.
- **Proficiency Requirements:** Expertise in many detection technologies may be required for hybrid intrusion detection systems. It could be difficult to find and keep qualified employees that can handle and troubleshoot the numerous components.
- **Lack of Standardization:** It is possible that defined contexts and protocols for combining various IDS components are lacking. This may impede compatibility and complicate the upgrading or replacement of individual parts.

5.5.2 Solution of Hybrid Base IDS

- **Integration and Compatibility:** Solution: ML/DL techniques can be used to develop a unified model that participates and analyzes data from different detection methods. This prototypical can efficiently integrate data from multiple sources and raise detection accuracy overall.
- **False Positives and Negatives:** Solution: Machine Learning algorithms applied to animatedly adjust the sensitivity of each finding method based on the growing threat landscape. By optimizing the system, this adaptive method can reduce false positives and negatives.
- **Complexity and Resource Consumption:** Solution: Deep Learning models can utilize that can repeatedly learn and get the useful information from the raw data, lowering the requirement for laborious manual configuration. This can increase resource efficiency and reduce system complexity.
- **Adaptability to New Threats:** Solution: Machine Learning/Deep Learning models can be implemented that has the power of learning and adapting to new threat patterns. Continually add threat intelligence feeds to the models to improve the system's capacity to adopt new threats.
- **Training and Maintenance:** Solution: The use of Federated Learning allows individual mechanisms of the hybrid system to learn from local data without sharing sensitive information. By using a collaborative learning strategy, centralized maintenance is not as necessary and distributed training is made possible.
- **Scalability Challenges:** Solution: By employing AI models that are scalable and can handle increasing amounts of data. Deep Learning models are appropriate for large-scale settings since they may be tuned for parallel processing.
- **Expertise Requirements:** Solution: Influence the DL techniques with automated separation of feature capabilities to reduce the requirement for deep knowledge in setting up and fine-tuning specific detection techniques. This may increase the system's usability for a larger group of security experts.
- **False Positive Reduction with FL:** Solution: By using the Federated Learning to collaboratively reduce false positives across different organizations. Through the exchange of knowledge regarding false positives without disclosing raw data, entities can work together to enhance the hybrid system's accuracy.
- **Threat Intelligence Integration:** Solution: Incorporation Using Federated Learning technique to share threat information data privacy while sharing intelligence across different organizations. This cooperative approach ensures that the hybrid IDS can make full use of collective knowledge with end-to-end transmission without revealing sensitive information.
- **Continuous Learning and Updating:** Solution: Through Federated Learning for continuous learning across distributed environments. If the threat landscape changes, then through learning from local data when tolerating each component of it, the hybrid system will be able to adapt without relying on centralized updates.
- **Customization and Flexibility:** Solution: By the use of ML and DL techniques allow the customization based on the specific needs of an organization. It guarantees that the hybrid IDS can be personalized to the exclusive characteristics of the network.
- **Enhanced Threat Detection with Ensemble Learning:** Solution: By the use of the ensemble learning methods to combine predictions from different methods of detection. Ensemble approaches can improve overall detection accuracy by leveraging the strengths of the individual components.

5.6 Network Based IDS

A (NIDS) is designed to check and also analyse traffic of a network for security threats within the (IoT).

5.6.1 Problems with Network Base IDS

- **Encoded Traffic:** The wide use of the encryption techniques NIDS might face the challenges in inspecting encrypted traffic. It may happen that it may fail to detect the threats hidden within encrypted infrastructures.
- **Incorrect Positives:** There is the possibility that NIDS can give false positives, mistaking normal network activity for potential threats. Reducing false positives without decreasing the accuracy of finding can be difficult through fine-tuning.
- **Incorrect Negatives:** On the other hand, the NIDS can also produce false negatives, failing to detect actual security incidents. That might be happen when the system is unable to recognize subtle or sophisticated attack patterns.
- **High Network Traffic Volume:** It may also be possible that the NIDS may struggle to keep up with the volume of

© 2024, IJSRCSE All Rights Reserved

data flowing through the network while in high-traffic environments. In this situation the performance degradation and missed detections.

- **Signature-Based Limitations:** The Signature-based detection performs better on the known attacks type. While NIDS using the same method may be less effective against zero-day attacks or sophisticated threats with novel methods that don't match existing signatures.
- **Limitations of Protocol:** While dealing with non-standard or proprietary network protocols the effectiveness NIDS can be limited in this situation. Moreover, it may scrap to analyze traffic in certain network environments, clogging its ability to detect anomalies.
- **Scalability Encounters:** The network become more complex as it grows and the scaling NIDS to effectively cover the entire network can be challenging. Confirming that the system remains reactive and accurate in large and dynamic environments needs careful planning.
- **Network Separation:** While in the context of segmented networks or those using the technologies of virtualization, NIDS might face challenges in traffic monitoring across different segments. That could result in blind spots where malicious activity goes undetected.
- **Evasion Techniques:** The Cultured attackers may employ evasion techniques to avoid NIDS. These techniques involve operating the network traffic to avoid detection, making it difficult for the system to identify the malicious activity.
- **Limited Context:** It is also possible that the NIDS often deficiencies the context of the overall system or application state. Now understanding the context of network traffic is essential for distinctive between normal and the malicious behavior.
- **Resource Consumption:** In the context of resource consumption, the NIDS can be resource-intensive, consuming important bandwidth and processing power. This may be possible that it has an impact on the overall network performance and may require substantial hardware resources.
- **Maintenance and Updates:** For effective threat detection, it is important to keep the NIDS signatures up-to-date. The system must be constantly updated to identify the latest attack patterns and vulnerabilities.

5.6.2 Solution of Network Base IDS

- **Encrypted Traffic Analysis:**

Solution: By implementing the Machine Learning/DL algorithms has power to analyze encrypted traffic patterns. The deep packet examination techniques and machine learning procedures can be used to identify irregularities or threats within encrypted infrastructures.

- **False Positives and Negatives:** Solution: The utilization of ML algorithms to energetically adjust detection edges based on the evolving network environment. DL techniques are capable of picking up complex characteristics and patterns, dropping false positives and improving the system's ability to detect subtle threats.
- **High Network Traffic Volume:** Solution: Employing the ascendable Machine Learning/Deep Learning models to optimized for processing the large dimensions of network traffic. By doing this, the NIDS can manage heavy traffic loads without compromising the accuracy of its detections.
- **Adaptability to New Threats:** Solution: Implementation of ML models that can identify to new threats by incessantly learning from updated threat intelligence feeds. Update the models frequently to identify new attack vectors and weaknesses.
- **Protocol Limitations:** Solution: The (ML) and (DL) models used to enhance the protocol analysis capabilities. By training these models to comprehend and adjust to proprietary or non-standard network protocols, the system's anomaly detection capabilities can be enhanced.
- **Scalability Challenges:** Solution: Employ distributed ML models or DL models optimized for parallel processing to address the challenges of scalability. It can improve the NIDS's scalability in expansive and intricate network environments.
- **Integration with Other Security Layers:** Solution: By combining the AI models with the other security coatings, such as the firewalls and endpoint protection systems. This cooperative strategy may offer a more complete protection against several attack avenues.
- **Threat Intelligence Integration:** Solution: By applying Federated Learning to enable the cooperative exchange of danger intelligence between several organizations without the need to provide unprocessed network data. This guarantees that a deeper comprehension of the threat landscape will be beneficial to the NIDS.
- **Resource Consumption:** Solution: The optimization of ML/DL techniques for the efficiency of resources, seeing factors like memory and dispensation power. Good models can preserve good intrusion detection while lessening the impact on network performance.
- **User and Entity Behavior Analytics (UEBA):** Solution: The combination of Machine Learning models for the UEBA to examine user and entity performance for signs of cooperation. This method improves the NIDS's capacity to identify compromised accounts and insider threats.
- **Customization and Fine-Tuning:** Solution: The employment of Machine Learning/Deep Learning models that allow for customization and the fine-tuning created on the specific network features. Because of its adaptability, the NIDS may be made to meet the specific needs of the company.
- **Reducing False Positives with FL:** Solution: By the implementation of Federated Learning to collaboratively minimize false positives across different organizations. Through the exchange of knowledge regarding false positives without disclosing raw data, entities can jointly enhance the precision of NIDS.

Table 1. Summarize the types of ids, their associated problems and remediation.

No	Types of IDS	Problems	Remediation
1	Signature Base IDS	Limited to Known Signatures. False Positives. False Negatives. Update Dependency.	Anomaly Detection using ML. Deep Learning for Pattern Recognition. Behavioural Analysis

© 2024, IJSRCSE All Rights Reserved

		Encrypted Traffic. Resource Intensive. Evasion Techniques. Limited Anomaly Detection. Complexity of Signatures. Dependency on Protocol Knowledge. Intensive.	with ML. Zero-Day Threat Detection. SSL/TLS Decryption with ML. Federated Learning for Decentralized. Training. Continuous Learning. Ensemble Learning. Ensemble Learning. Transfer Learning. Feature Engineering for DL.
No	**Types of IDS**	**Problems**	**Remediation**
2	Anomaly Based IDS	False Positives. False Negatives. Complex Baseline Establishment. Adaptation to New Threats. Noise and Irregularities.	Behavioural Analysis with ML. Deep Learning for Complex Pattern Recognition. Dynamic Thresholds with ML. Handling Class Imbalance. Feature Engineering for DL. Unsupervised Learning for Novelty Detection.
3	Behavior Base IDS	False Positives. False Negatives. Baseline Challenges. Insider Threats. Complexity and Customization. Adaptation to New Threats. Scalability Challenges.	Machine Learning for Behaviour Modelling. Unsupervised Learning for Anomaly Detection. Sequential Pattern Analysis with DL. Feature Engineering for DL. Dynamic Learning with ML/DL.
4	Heuristic-Based IDS	False Positives and False Negatives. Dynamic Environment. Limited Context. Resource Intensive. Overfitting. Maintenance Challenges. Stealthy Attacks. Tuning Complexity.	Machine Learning for Rule Generation. Behavioural Analysis with ML/DL. Dynamic Thresholds with ML. Feature Engineering for DL. Ensemble Learning. Adaptive Learning with ML/DL.
5	Hybrid based IDS	Complexity. Resource Consumption. Integration Issues. False Positives and Negatives. Training and Maintenance. Adaptability to New Threats. Cost. Scalability.	Integration and Compatibility. False Positives and Negatives. Complexity and Resource Consumption. Adaptability to New Threats. Training and Maintenance. Scalability Challenges.
6	Network Based IDS	Encrypted Traffic. False Positives. False Negatives. High Network Traffic Volume. Signature-Based Limitations. Protocol Limitations.	Encrypted Traffic Analysis. False Positives and Negatives. High Network Traffic Volume. Adaptability to New Threats. Reducing False Positives with FL.

The table 1 illustrates the different types of detection of intrusion and also highlight the different problems that are created by the intrusions. The table also focus on the solutions of different types of problems and also the improvements that can be achieved using machine learning and deep learning techniques.

6. Layer Wise Attacks

6.1 Perception Layer

The perception layer consists of sensors and actuators [20]. The sensors act as controllers by detecting their surroundings through actuators based on sensed data. Nodes also called sensors and can be targeted by node-hijacking attacks where; An attacker might either seize the node or swap it out. a malicious node. The wireless upgrade of these nodes' settings. software or firmware that allows the attacker to succeed to put in bad or wrong code in the node making problems. fake data injection attacks [21] using wrong information.

Attacks using laser, power use and timing can happen at this layer [22]. The parts of a network in an open space can be listened to by bad people when information is being sent or something similar happens [23]. IoT devices use up energy quickly. Attackers take advantage of this problem by making them lose power and causing lack of sleep. Usually, IoT device security is turned on after starting up. This gives the attacker a chance to start an attack at boot time.

Figure 4. Involvement of IoT Applications of in different fields

The figure 4 is showing the application of the internet of things in the daily of the users. The applications of the IoT devices are in the area of education, homes, grid, farming, wearable, city and health care. The use of IoT in these fields made them smart.

6.2 Network Layer

This is the layer that deals with networks sends details from the sense-checking stage for more handling to the computer part. This level is very weak against attacks that use many IoT devices. Phishing attack aim some IoT gadgets in an

© 2024, IJSRCSE All Rights Reserved

effort to at least manage a few of them [24]. In a DDoS attack, an attacker tries to flood the target with fake requests. Internet things, also known as IoT devices act like a large group of weak computers in DDoS attacks. They can create a huge number of requests to stop the target from using resources [25]. Worm-hole and sinkhole attacks are kinds of routing attacks. In these, the attacker tries to send traffic on a different path by getting into computer nodes [26].

6.3 Support Layer

The Help layer works in between Network and Application layers. This part aids in sharing resources, doing calculations and keeping data. Keeping a database safe is very important at this point. In a Man-in-the-middle attack, the bad guy takes over the broker. This gives them control of all messages sent between people [27]. The attack in the Support layer often aims to get data, so keeping information safe on databases and clouds is really important.

6.4 Application Layer.

The calling layer was the smart part of software including: ```markdown - Regular programs or apps that give helpful functions. So, it makes tasks easier and run more smoothly. Smart city, smart home and healthcare are all examples. This layer is the one that directly handles end-users, so privacy and stealing data are big worries for this level [28]. Like other levels, this one is also hit by the bad code attack. A service break attack is like a (DDoS) attack because it makes services stop working. Some people are allowed to let real users in when an attack happens, but the whole system can be attacked if this permission is taken over by bad guys. This makes stopping unauthorized access a big worry at the level where we interact with applications [29]. In a sniffing attack, the bad guy uses special tools to look at network traffic data. Confidential information can be stolen during this type of hack [30].

6.5 Session Layer

The session layer makes sure we stay connected with the user. This part checks if the user is allowed and keeps track of their connection based on that. This session layer mostly deals with managing user activities based on their confirmation and permission [31]. This is simple for any use of the app by people. The session layer adds a token-filled header to uniquely identify the session. The app can also use other information for its activities or safety.

6.6 Transport Layer

The transmitting and receiving addresses between computer components are handled by the transport layer. This level connects the start and finish points as movement headers to the data. This makes sure where the data goes. The transport layer often uses one of these two methods [32]. TCP (Transfer Control Protocol) wants data to be good instead of fast and UDP (User Datagram Protocol) chooses speed over quality in a setup that has no connection.

6.7 Data Link Layer

The data connect layer is the second to last level in a group of layers used by OSI model. The data link layer mostly sends the information [33] to the physical level. However, this layer is in charge of logical sorting and grouping [34]. Data, network structure and access must be discussed. Telling about mistakes and controlling the flow [35]. The possible attacks [36] on this layer include DDoS attack with which the network traffic becomes flooded [37]. The trusted devices become impersonate by MAC address spoofing [38].

Table 2 summarize the types of attacks on different layers of osi model.

Attack	Application Layer	Perception Layer	Network Layer	Support Layer	Data link Layer	Trans-port Layer	Session Layer
DDoS Attack	×	×	✓	✓		✓	×
Node Capture attack	×	✓	×	×	×	×	×
Malicious code Injection attack	✓	✓	×	×	×	×	×
(MitM)	×	×	✓	✓	×	×	✓
Phishing Attack	×	×	✓	×	×	×	×
Data Transit Attack	×	×	×	×	×	×	×
Routing Attack	×	×	✓	×	×	×	×
Storage Attack	×	×	✓	×	×	×	×
Sniffing Attack	✓	×		×	×	×	×
Booting Vulnerabilities	×	✓	×	×	×	×	×
Eavesdropping	×	✓	×	×	×	×	×
Access Control Attack	✓	×	×	×	×	×	×
MAC address spoofing	×	×	×	×	✓	×	×
VLAN hooping	×	×	×	×	✓	×	×
DoS attacks	×	×	×	×	✓	✓	✓
Port redirection	×	×	×	×		✓	×
TCP hijacking	×	×	×	×	×	✓	×
Replay attacks	×	×	×	×	×	×	✓
Session Termination Attacks	×	×	×	×	×	×	✓

There are number of attacks that are committed on the seven layers of ISI model and the Table 2 illustrates the different types of those attacks. Every layer might be attacked by more

© 2024, IJSRCSE All Rights Reserved

than one attack form and the most committed attack by the attacker on these layers are the DOS and DDOS attacks.

Table 3 summarize the attacks and different proposed methodology.

Attacks	Contribution	Merits	Demerits	Validation Strategy
DDoS Routing Attack	A blockchain-based architecture with the combination of blockchains in the IoT	Highly efficient and Highly robustness	All the threats are not covered	Implementation base
DDOS attack	Proposed advanced IDS by using Deep learning algorithms	Highly accurate Good for low power consumption devices	Low scalability Inefficient when the network becomes large	Simulation base
Signature based attacks DoS attack Phishing	Proposed signature pairing method for the authentication of IoT devices	Highly reliable Highly secured	High delay	Implementation base
MITM attack, DDOS attack	Proposed predefined rules to identify the attacks through web	False alarm reduction Good precision	Good response time	Simulation base
Data injection attacks	Proposed a method for the detection of false data injection attack	Highly available High robustness	Low scalability	Simulation base
Heuristic-based IDS attacks	Detection of heuristics-based IDS in IoT	Small memory usage Energy consumption is low	Robustness is low Low scalability	Simulation base
Internal and External attacks	Internal and external attacks detection	Highly accurate Computational resources usage is low	Highly complex	Implementation base

Table 3 summarize the different types of attacks that committed on the IoT environment. It also describes the different contributions that the researcher already done with following the merits and demerits. At last, it explains the validation criteria about the different methodologies that are proposed to detect and reduce the risk of attacks.

6. Conclusion and Future Scope

In this paper, a critical review of the latest paper is carried out. Also, we presented the review on various types of IDS in IoT domain. While IoT holds immense promise for the revolutionizing various sectors, its potential is accompanied by the significant security risks. The rapid pace of the IoT adoption often outstrips the development of adequate security measures, creating a persistent gap that attackers can exploit. Moreover, we discuss the significance of the IDS and their problems that are associated with each type of IDS. The IoT presents both unprecedented opportunities and significant security challenges. As IoT devices proliferate across various sectors, from healthcare to smart homes, the risk of intrusions increases dramatically. The unique characteristics of IoT such as diverse device types make traditional security measures insufficient. The intrusion detection system particularly those enhanced with ML and DL offer promising solutions by enabling real time threat detection, anomaly recognition and adaptive defence mechanism. The paper also covers many types of attacks that can be committed by the attacker on the seven layers of OSI. The research is summarized by suggesting the remediation for the problem with each type of IDS. Additionally, the dynamic nature of the IoT environments requires continuous adaption and learning to counteract evolving threats effectively. For future direction; we aim to extend the work by the consideration of the tools and other challenges that are faced by the IDs in IoT domain. Also, extend the work by considering the techniques or framework that are designed to overcome the issues and threat for the IDs in IoT system. Technological developments have the potential to alter both the economy and the planet.

Conflict of Interest
Not Applicable

Funding Source
Not Applicable

Authors' Contributions
Mr.Danial Haider researched literature and conceived the study. Ms.Tehreem Saboor involved in protocol development, gaining ethical approval, patient recruitment, and data analysis. Ms.Aqsa Rais wrote the first draft of the manuscript. All authors reviewed and edited the manuscript and approved the final version of the manuscript.

Acknowledgements
No Applicable

References

[1] Spadaccino, P., & Cuomo, F. Intrusion Detection Systems for IoT: opportunities and challenges offered by Edge Computing and Machine Learning. *arXiv preprint arXiv:2012.01174*,2020

[2] Sanju, P. Enhancing Intrusion Detection in IoT Systems: A Hybrid Metaheuristics-Deep Learning Approach with Ensemble of Recurrent Neural Networks. *Journal of Engineering Research*, 100122, 2023

[3] Sicato, J. C. S., Singh, S. K., Rathore, S., & Park, J. H. A comprehensive analyses of intrusion detection system for IoT environment. *Journal of Information Processing Systems*, *16*(4), 975-990, 2020

[4] R. Nicole, "Title of paper with only first word capitalized," J. Name Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., & Bahaj, S. A. Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible

© 2024, IJSRCSE All Rights Reserved

solutions. *Security and Communication Networks*, *2022*.Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982],2022

[5] Benkhelifa, E., Welsh, T., & Hamouda, W. A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE communications surveys & tutorials*, *20*(4), 3496-3509.2018

[6] Hassija, V.; Saxena, V.; Chamola, V. Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory. *Comput. Commun.* 2019, *149*, 51–61. [Google Scholar] [CrossRef]

[7] Khraisat, A., & Alazab, A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, *4*, 1-27, 2021

[8] Awajan, A. A novel deep learning-based intrusion detection system for IOT networks. *Computers*, *12*(2), 34,2023

[9] Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. *Computational Intelligence and Neuroscience*, *2023*.

[10] Mohy-eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. *Multimedia Tools and Applications*, 1-19,2023

[11] Shah, H., Shah, D., Jadav, N. K., Gupta, R., Tanwar, S., Alfarraj, O., ... & Marina, V. Deep learning-based malicious smart contract and intrusion detection system for IoT environment. *Mathematics*, *11*(2), 418.,2023

[12] Othman, T. S., Koy, K. R., & Abdullah, S. M. Intrusion Detection Systems for IoT Attack Detection and Identification Using Intelligent Techniques. *networks*, *5*(6),2023

[13] Savanović, N., Toskovic, A., Petrovic, A., Zivkovic, M., Damaševičius, R., Jovanovic, L., ... & Nikolic, B. Intrusion detection in healthcare 4.0 internet of things systems via metaheuristics optimized machine learning. *Sustainability*, *15*(16), 12563 ,2023

[14] Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things*, *3*(1), 5 ,2023

[15] Mahadik, S., Pawar, P. M., & Muthalagu, R. Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT). *Journal of Network and Systems Management*, *31*(1), 2,2023

[16] Heidari, A., & Jabraeil Jamali, M. A. Internet of Things intrusion detection systems: A comprehensive review and future directions. *Cluster Computing*, *26*(6), 3753-3780 ,2023

[17] Jeyaselvi, M., Dhanaraj, R. K., Sathya, M., Memon, F. H., Krishnasamy, L., Dev, K., ... & Qureshi, N. M. F. A highly secured intrusion detection system for IoT using EXPSO-STFA feature selection for LAANN to detect attacks. *Cluster Computing*, *26*(1), 559-574 ,2023

[18] Musleh, D., Alotaibi, M., Alhaidari, F., Rahman, A., & Mohammad, R. M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. *Journal of Sensor and Actuator Networks*, *12*(2), 29,2023

[19] Al Sawafi, Y., Touzene, A., & Hedjam, R.Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks. *Journal of Sensor and Actuator Networks*, *12*(2), 21,2023

[20] Otoum, Y., Liu, D., & Nayak, A. DL-IDS: a deep learning–based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3803,2022

[21] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), e4150,2021

[22] Visoottiviseth, V., Sakarin, P., Thongwilai, J., & Choobanjong, T. Signature-based and behavior-based attack detection with machine learning for home IoT devices. In *2020 IEEE REGION 10 CONFERENCE (TENCON)* (pp. 829-834). IEEE,2020

[23] Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. Perception layer security in Internet of Things. *Future Generation Computer Systems*, *100*, 144-164. 2019

[24] OS, J. N., & Bhanu, S. M. S. A survey on code injection attacks in mobile cloud computing environment. In *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 1-6). IEEE.2018, January

[25] M. Devi and A. Majumder, ''Side-channel attack in Internet of Things: A survey,'' in Applications of Internet of Things (Lecture Notes in Networks and Systems), J. K. Mandal, S. Mukhopadhyay, and A. Roy, Eds. Singapore: Springer, 2021, pp. 213–222.

[26] K. O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer, ''A survey on the security of low power wide area networks: Threats, challenges, and potential solutions,'' Sensors, vol. 20, no. 20, pp. 1–19, 2020

[27] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, ''A survey of IoT security based on a layered architecture of sensing and data analysis,'' K. Nirmal, B. Janet, and R. Kumar, ''Analyzing and eliminating phishing

[28] R. Vishwakarma and A. K. Jain, ''A survey of DDoS attacking techniques and defence mechanisms in the IoT network,'' Telecommun. Syst., vol. 73, no. 1, pp. 3–25, Jan. 2020

[29] Raoof, A. Matrawy, and C.-H. Lung, ''Enhancing routing security in IoT: Performance evaluation of RPL's secure mode under attacks,'' IEEE Internet Things J., vol. 7, no. 12, pp. 11536–11546, Dec. 2020.

[30] D. Dinculeană and X. Cheng, ''Vulnerabilities and limitations of MQTT protocol used between IoT devices,'' Appl. Sci., vol. 9, no. 5, p. 848, Feb. 2019.

[31] Tewari and B. B. Gupta, ''Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,'' Future Gener. Comput. Syst., vol. 108, pp. 909–920, Jul. 2020.

[32] Ahlawat, A. Sangwan, and V. Sindhu, ''IoT system model, challenges and threats,'' Int. J. Sci. Technol. Res., vol. 9, no. 3, pp. 6771–6776, 2020.

[33] Prabadevi and N. Jeyanthi, ''A review on various sniffing attacks and its mitigation techniques,'' Indonesian J. Elect. Eng. Comput. Sci., vol. 12, no. 3, pp. 1117–1125, 2018

[34] Tariq, N., Saboor, T., Ashraf, M., Butt, R., Anwar, M., & Humayun, M. IoT Security, Future Challenges, and Open Issues. In *Cybersecurity Measures for Logistics Industry Framework* (pp. 116-140). IGI Global. 2024

[35] Butt, M. H. F., Li, J. P., Saboor, T., Arslan, M., & Butt, M. A. F. Intelligent Phishing Url Detection: A Solution Based On Deep Learning Framework. In *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)* (pp. 434-439). IEEE. 2021, December.

[36] Butt, M. H. F., Li, J. P., & Saboor, T. A tunable and explainable attributes (TEA) for recommendation system. In *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)* (pp. 39-43). IEEE. 2020, December

[37] Mortada M. Abdulwahab, Hadeel A.Mohamed, Mutseuim A. Alameen, Mohamed A. Mosalam, Faris M.Elsadig, "Wireless Sensor Network of Monitoring Water Distribution Network Service using IoT," *International Journal of Scientific Research in Computer Science and Engineering*, Vol.11, Issue.1, pp.51-55, 2023

[38] Prabhat Bisht, Manmohan Singh Rauthan, "Machine Learning and Natural Language Processing Based Web Application Firewall for Mitigating Cyber Attacks in Cloud," *International Journal of Scientific Research in Computer Science and Engineering*, Vol.11, Issue.3, pp.1-15, 2023

© 2024, IJSRCSE All Rights Reserved

AUTHORS PROFILE

Mr.Danial Haider has done his Master in (Computer Science) from COMSATS University, Islamabad. He is currently pursing Ph.D. in (Information Security) from Air University, Islamabad. He has 03 years of teaching experience. Currently, he is working as Lecturer in the Information Technology Department. During his three years in the engineering program, he has worked on various projects, ranging from chat application to an English learning application. He has also developed several applications, including a face-tracking application in Python and a DriveWatch application, in order to find his specific domain for doing research. He has published 03 research papers in reputed journals His research area is IoT, Cryptography security.

Ms.Tehreem Saboor completed his Master (Software Enginering) from National University of Computer and Emerging Sciences, Islamabad. She is currently pursuing a Ph.D. in (Information Security) from Air University, Islamabad. she has 03 years of teaching experience. Currently she is working as Lecturer, in Computrer Science Department. She has published 03 research papers in reputed journals, 04 Conference Publications, and 02 Book Chapters. Her research area is Network Security, Bloch Chain Technology and IOT.

Ms.Aqsa Rias has done her Master in (Computer Science) from COMSATS University, Islamabad. She is currently pursing Ph.D. in (Information Security) from Air University, Islamabad. She has 03 years of teaching experience. Currently, she is working as Lecturer in the Computer Science Department. She has published 02 research papers in a reputed journals. Her research is Fog Security, Edge Computing and IOV.

© 2024, IJSRCSE All Rights Reserved