Survey of IOT Cyber Security in Network Intrusion Detection Systems

Rishika*, Yogendra Maravi **, Nischol Mishra*, Jitendra Agarwal****

School of Information Technology, RGPV, Bhopal

Abstract- The internet of things based application is rapidly growing in current scenario. Many of the users are using the internet services. The cyber world includes the information technology, computer etc based services. Many of the protocols, technology make improvement in the cyber world. The security is important concern in the cyber based services. The Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) is primary system to detect and prevent cyber security. This paper includes the survey of IOT cyber security in the NIDS.

Index Terms- IOT, Cyber, NIDS, HIDS, Security

I. INTRODUCTION

This article presents review of Information and communication technology (ICT) progressions have adjusted the whole processing worldview. Because of these enhancements, various new channels of correspondence are being made, one of which is the Web of Things (IoT). The IoT has as of late arisen as state of the art innovation for establishing shrewd conditions. The Web of Clinical Things (IoMT) is a subset of the IoT, where clinical hardware trade data with one another to trade touchy data. These advancements empower the medical services business to keep a more significant level of touch and care for its patients. Security is viewed as a critical test in at all innovation's dependence in light of the IoT. Security hardships happen attributable to the different potential assaults presented by assailants. There are various security concerns, for example, remote seizing, and pantomime, refusal of administration assaults, secret key speculating, and man-in-the-center. In case of such assaults, basic information related with IoT network might be uncovered, changed, or even delivered difficult to reach to approve clients. Accordingly, it ends up being basic to defend the IoT/IoMT environment against malware attacks [1][2]. An exhaustive report with a test examination of united profound learning approaches for network safety in the Web of Things (IoT) applications. In particular, we initially give an audit of the unified learning-based security and protection frameworks for a long time of IoT applications, including, Modern IoT, Edge Registering, Web of Robots, Web of Medical services Things, Web of Vehicles, and so on Second, the utilization of unified learning with blockchain and malware/interruption recognition frameworks for IoT applications is examined. Then, at that point, we audit the weaknesses in united learning-based security and protection frameworks [3]. Independent control frameworks are progressively utilizing AI advancements to deal with sensor information, settling on convenient and informed choices about performing control capacities in view of the information handling results. Among such AI advances, support learning (RL) with profound brain networks has been as of late perceived as one of the attainable arrangements, since it empowers learning by communication with conditions of control frameworks. In this work, we consider RL-based control models and address the issue of transiently obsolete perceptions frequently caused in powerful digital actual conditions. The issue can frustrate expansive receptions of RL techniques for independent control frameworks. In particular, we present a RL-based strong control model, to be specific protocol, that takes advantage of a progressive learning structure in which a bunch of low-level strategy variations are prepared for old perceptions and afterward their learned information can be moved to an objective climate restricted in ideal information refreshes [4].

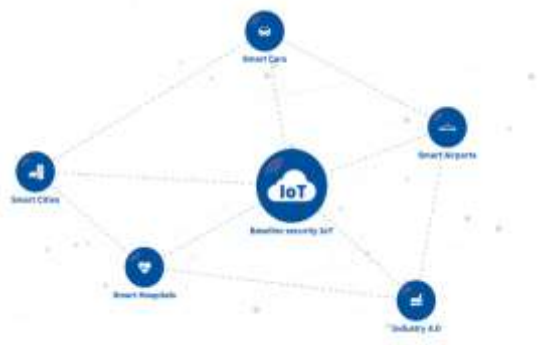

Figure 1: IOT smart infrastructure security

AI calculations are viable in a few applications; however they are not as much fruitful when applied to interruption identification in digital protection. Because of the great aversion to their preparation information, digital locators in view of AI are helpless against designated antagonistic assaults that include the bother of starting examples. Existing safeguards accept unreasonable situations; their outcomes are disappointing in non-antagonistic settings; or they can be applied distinctly to AI calculations that perform inadequately for digital protection [5]. Web of-Things (IoT) gadgets and frameworks will be progressively designated by cybercriminals (counting country state-supported or associated danger entertainers) as they become an indispensable piece of our associated society and environment. Notwithstanding, the difficulties in getting these gadgets and frameworks are compounded by the scale and variety of organization, the speedy digital danger scene, and numerous different elements [6]. The learning for the advanced

wellbeing. The conventional validation frameworks are defenseless against the dangers of absent mindedness, misfortune, and burglary. Biometric verification is has been improved and turned into the piece of day to day existence. The Electrocardiogram (ECG) based verification strategy has been presented as a biometric security framework appropriate to check the distinguishing proof for entering a structure and this examination accommodates concentrating on ECG-based biometric validation methods to reshape input information by cutting in light of the RR-stretch [7]. Distributed computing has been broadly applied in various applications for capacity and information investigation undertakings. In any case, cloud servers drew in through an outsider can't be completely trusted by different information clients. Subsequently, security and protection concerns become the fundamental deterrents to utilize AI administrations, particularly with different information suppliers. Furthermore, some new rethinking AI plans have been proposed to save the security of information suppliers. However, these plans can't fulfill the property of public unquestionable status. In this work, we present an effective protection safeguarding AI plot for quite some time suppliers [8].

Figure 2: Cyber security [google image]

Digital protection with regards to large information is known to be a basic issue and presents an incredible test to the exploration local area. AI calculations have been proposed as contender for taking care of huge information security issues. Among these calculations, support vector machines (SVMs) have made momentous progress on different arrangement issues. Nonetheless, to lay out a successful SVM, the client needs to characterize the appropriate SVM arrangement ahead of time, which is a difficult undertaking that requires master information and a lot of manual exertion for experimentation. In this work, we form the SVM setup process as a bi-objective improvement issue in which precision and model intricacy are considered as two clashing targets [10].

.

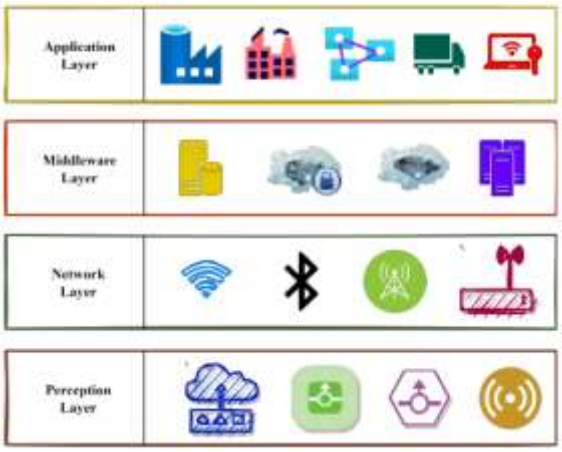

Figure 3: Multi-tier structure of IIoT

Table 1: Consumer IoT and Manufacturer IIoT [21]

Manufacturer IIoT	Consumer IoT
Works large scale networks.	Related with small scale networks.
Focuses on industrial domains by application, service and devices	Focuses on general usage area such as individual usage, smart objects.
Requires not only Wi-Fi connection but also cellular connection type.	Requires Wi-Fi connection and configuration to transmit data.
Device and services have long life period.	Device and services have short life period.
Designed for manufacturing areas to provide resource efficiency and management.	Designed for consumer areas by applications and services.
Requires higher bandwidth generally.	High bandwidth is not necessary.
Used in industrial and professional service domains.	Covers covers a wide range of industries and users.
Require high levels of precision and accuracy to provide efficiency and reliability.	Quality is not depending on directly precision and accuarcy.
Energy harvesting is a promising approach.	Not guarantee energy and resource efficiency.
Focuses on data processing and decision making.	Focuses on data collection and transmission.

II. REVIEW OF LITERATURE

H. Hou et al.,[1] presents framework is assessed on the notable benchmark informational index NSL-KDD for examination with other existing strategies. The exploratory outcomes exhibit that contrasted and existing beginning of-the-craftsmanship strategies, our framework has better recognition execution for various kinds of cyberattacks. What's more, the low-recurrence network assault types have higher arrangement precision and a lower misleading discovery rate.

Y. K. Saheed et al.,[2] present review is to show how a profound repetitive brain organization (DRNN) and managed AI models (arbitrary woodland, choice tree, KNN, and edge classifier) can be used to foster a proficient and successful IDS in the IoMT climate for ordering and determining surprising digital dangers. Preprocessing and standardization of organization information are performed. Following that, we improved highlights utilizing a bio-enlivened molecule swarm calculation. On the standard information for interruption discovery, an intensive assessment of examinations in DRNN and other SML is performed. It was laid out through thorough testing that the proposed SML model beats existing methodologies with an exactness of 99.76%.

M. A. Ferrag et al.,[3] present At long last, we give an exploratory examination of unified profound learning with three profound learning draws near, in particular, Intermittent Brain Organization (RNN), Convolutional Brain Organization (CNN), and Profound Brain Organization (DNN). For every profound learning model, we concentrate on the presentation of brought together and unified learning under three new genuine IoT traffic datasets, specifically, the Bot-IoT dataset, the MQTTset dataset, and the TON_IoT dataset. The objective of this article is to give significant data on combined profound learning approaches with arising innovations for network protection. Furthermore, it exhibits that combined profound learning approaches beat the work of art/incorporated forms of AI (non-unified learning) in guaranteeing the protection of IoT gadget information and give the higher exactness in distinguishing assaults.

G. Yoo et al.,[4] In doing as such, we utilize an auto encoder-based perception move conspire for methodicallly preparing a bunch of adaptable control approaches and a collected model-based learning plan for information effectively preparing an undeniable level orchestrator in an order. Our examinations show that rocorl is hearty against different states of disseminated sensor information refreshes, contrasted and a few different models including a cutting edge POMDP technique.

G. Apruzzese et al.,[5] present a unique procedure for countering antagonistic annoyances focusing on interruption identification frameworks in view of arbitrary timberlands. As a reasonable application, we coordinate the proposed safeguard technique in a digital locator breaking down network traffic. The trial results on huge number of named network streams show that the new locator has a twofold worth: it beats cutting edge identifiers that are likely to ill-disposed assaults; it displays strong outcomes both in antagonistic and non-ill-disposed situations.

M. Saharkhizan et al.,[6] presents plan a methodology utilizing progressed profound figuring out how to distinguish digital assaults against IoT frameworks. In particular, our methodology incorporates a bunch of long transient memory (LSTM) modules into an outfit of locators. These modules are then combined utilizing a choice tree to show up at an accumulated result at the last stage. We assess the viability of our methodology utilizing a genuine informational index of Modbus network traffic and acquire an exactness pace of more than close to 100% in the discovery of digital assaults against IoT gadgets.

S. - K. Kim et al.,[7] The General Presentation (Over powered) as a recently proposed exhibition measure is the consolidated exhibition metric of different validation measures in this review. The exhibition of the proposed framework utilizing a disarray network has been assessed and it has accomplished up to 95% exactness by minimal information investigation. The Amang ECG (amgecg) tool compartment in MATLAB is applied to the mean square mistake (MSE) based upper-range control limit (UCL) which straightforwardly influences three verification execution measurements: the quantity of acknowledged examples, the precision and the Over powered. In light of this methodology, it is observed that the Over powered could be boosted by applying a UCL of 0.0028, which shows 61 acknowledged examples inside 70 examples and guarantees that the proposed validation framework accomplishes 95% precision.

A. Hassan et al.,[8] The proposed plot permits all members in the framework model to freely check the accuracy of the encoded information. Besides, a unidirectional intermediary re-encryption (UPRE) plot is utilized to decrease the high computational expenses alongside various information suppliers. The cloud server implants clamor in the scrambled information, permitting the examination to apply AI strategies and safeguard the security of information suppliers' data. The outcomes and analyses tests exhibit that the proposed plot can decrease computational expenses and correspondence overheads.

Y. Xin et al.,[9] With the advancement of the Web, digital assaults are changing quickly and the network safety circumstance isn't hopeful. This review report depicts key writing studies on AI (ML) and profound learning (DL) strategies for network examination of interruption location and gives a concise instructional exercise portrayal of every ML/DL technique. Works addressing every strategy were listed, read, and summed up in light of their worldly or warm relationships. Since information are so significant in ML/DL strategies, we depict a portion of the generally utilized network datasets utilized in ML/DL, examine the difficulties of utilizing ML/DL for online protection and give ideas to explore bearings.

N. R. Sabar et al.,[10] presents a clever hyper-heuristic structure for bi-objective enhancement that is autonomous of the issue space. This is whenever that a hyper-heuristic first has been produced for this issue. The proposed hyper-heuristic system comprises of a significant level technique and low-level heuristics. The undeniable level procedure utilizes the hunt execution to control the choice of which low-level heuristic ought to be utilized to produce another SVM arrangement. The low-level heuristics each utilization various guidelines to successfully investigate the SVM design search space. To address bi-objective advancement, the proposed system adaptively incorporates the qualities of decomposition and Pareto based ways to deal with rough the Pareto set of SVM designs.

Y. Wang et al.,[11] Misleading information infusion digital actual danger is a normal trustworthiness assault in current shrewd matrices. Nowadays, information scientific techniques have been utilized to alleviate misleading information infusion assaults (FDIAs), particularly when huge scope brilliant frameworks produce enormous measures of information. In this work, a clever information logical strategy is proposed to identify FDIAs in light of information driven worldview utilizing the edge setting calculation (MSA). The exhibition of the proposed strategy is shown through reenactment utilizing the six-transport power network in a wide region estimation framework climate, as well as exploratory informational collections. Two FDIA situations, playback assault and time assault, are examined. Exploratory outcomes are contrasted and the help vector machine (SVM) and counterfeit brain organization (ANN). The outcomes demonstrate that MSA yields better outcomes as far as identification precision than both the SVM and ANN when applied to FDIA discovery.

F. Wang et al.,[12] this work investigates the chance of allowing the specialist to gather expected objectives through activities over space with numerous items, utilizing the momentary award to allot credit spatially. A past strategy, consideration gated RL utilizes a multi-facet perceptron prepared with backpropagation, yet it is inclined to nearby minima ensnarement. We propose a quantized consideration gated part RL (QAGKRL) to stay away from the neighborhood minima transformation in spatial credit task and sparsify the organization geography. The test results show that the QAGKRL accomplishes higher effective rates and more steady execution, demonstrating its strong translating capacity for more modern BMI assignments as expected in clinical applications.

A. J. Smith et al.,[13] Reverse Code Engineering (RCE) to detect anti-debugging techniques in software is a very difficult task. Code obfuscation is an anti-debugging technique makes detection even more challenging. The Rule Engine Detection by Intermediate Representation (REDIR) system for automated static detection of obfuscated anti-debugging techniques is a prototype designed to help the RCE analyst improve performance through this tedious task. Three tenets form the REDIR foundation. First, Intermediate Representation (IR) improves the analyzability of binary programs by reducing a large instruction set down to a handful of semantically equivalent statements. Next, an Expert System (ES) rule-engine searches the IR and initiates a sense-making process for anti-debugging technique detection. Finally, an IR analysis process confirms the presence of an anti-debug technique. The REDIR system is implemented as a debugger plug-in. Within the debugger, REDIR interacts with a program in the disassembly view. Debugger users can instantly highlight anti-debugging techniques and determine if the presence of a debugger will cause a program to take a conditional jump or fall through to the next instruction.

M. Guri et al.,[14] Modern malicious programs often escape dynamic analysis, by detecting forensic instrumentation within their own runtime environment. This has become a major challenge for malware researchers and analysts. Current defensive analysis of anti-forensic malware often requires painstaking step-by-step manual inspection. Code obfuscation may further complicate proper analysis. Furthermore, current defensive countermeasures are usually effective only against anti-forensic techniques which have already been identified. In this work we propose a new method to detect and classify anti-forensic behavior, by comparing the trace-logs of the suspect program between different environments. Unlike previous works, the presented method is essentially noninvasive (does not interfere with original program flow). We separately trace the flow of instructions (Opcode) and the flow of Input-Output operations (IO). The two dimensions (Opcode and IO) complement each other to provide reliable classification. Our method can identify split behavior of suspected programs without prior knowledge of any specific anti-forensic technique; furthermore, it relieves the malware analyst from tedious step-by-step inspection. Those features are critical in the modern Cyber arena, where rootkits and Advanced Persistent Threats (APTs) are constantly adopting new sophisticated anti-forensic techniques to deceive analysis.

M. Hirabayashi et al.,[15] Vision-based object detection using camera sensors is an essential piece of perception for autonomous vehicles. Various combinations of features and models can be applied to increase the quality and the speed of object detection. A well-known approach uses histograms of oriented gradients (HOG) with deformable models to detect a car in an image. A major challenge of this approach can be found in computational cost introducing a real-time constraint relevant to the real world. In this work, we present an implementation technique using graphics processing units (GPUs) to accelerate computations of scoring similarity of the input image and the pre-defined models. Our implementation considers the entire program structure as well as the specific algorithm for practical use. We apply the presented technique to the real-world vehicle detection program and demonstrate that our implementation using commodity GPUs can achieve speedups of 3x to 5x in frame-rate over sequential and multithreaded implementations using traditional CPUs.

Lin Wang et al.,[16] A number of shocking cyber-attacks have happened in recent years, and the damage they have caused has led to the emergence of cyber-security as a consideration when designing embedded systems. Software vulnerability and physical attack are the most severe threats the system face. This work provides information about hardware designed to monitor potential intrusions and incidences of unauthorized access. Crucially, it can also trace execution patterns and cryptographic schemes in relation to memory authentication. The automated compiler extracts the intrusion detection model and covers the important instructions with cipher text at the compile time. At runtime, the proposed hardware monitors the instructions that change program trace and access memory data, which ensure the process and data follow the permissible behavior and resist the potential attacks. The security analysis shows that the proposed techniques can recognize and eliminate a wide range of common software and physical threats with low performance penalties and minimal overhead.

R. Tao et al.,[17] Application features such as port numbers are used by network-based intrusion detection systems (NIDSs) to detect attacks coming from networks. System calls and the operating system related information are used by host-based intrusion detection systems (HIDSs) to detect intrusions towards a host. However, the relationship between hardware architecture events and denial-of-service (DoS) attacks has not been well revealed. When increasingly sophisticated intrusions emerge, some attacks are able to bypass both the application and the operating system level feature monitors. Therefore, a more effective solution is required to enhance existing HIDSs. In this work, we identify the following hardware architecture features: instruction count, cache miss, bus traffic and integrate them into a novel HIDS framework based on a modern statistical gradient boosting trees model. Through the integration of application, operating system and architecture level features, our proposed HIDS demonstrates a significant improvement of the detection rate in terms of sophisticated DoS intrusions.

K. A. Bowman et al.,[18] Microprocessor clock frequency (FCLK) is traditionally determined based on maximum supply

voltage (Vcc) droop and temperature specifications. Since typical usage patterns usually run at nominal Vcc and temperature, these infrequent dynamic variations severely limit FCLK. The concept of timing-error detection and correction to explore the effectiveness of resilient circuits in eliminating Vcc and temperature FCLK guardbands as well as exploiting path-activation probabilities to maximize throughput (TP).

N. R. Yang et al.,[19] The energy consumed in instruction fetching accounts for a significant portion of total processor energy consumption. Energy consumption as well as performance should be considered when designing high performance embedded processors. In this work, we present a hardware-based loop detection technique to reduce the energy consumption in the instruction fetch unit (instruction cache and branch prediction logic) for high performance embedded processors. The proposed instruction fetch unit reduces the energy consumed in the instruction cache by replacing the accesses to the large main instruction cache with those to the small selectively accessed cache (SAC). It also reduces the energy consumed in the branch prediction logic by reducing unnecessary accesses to the branch prediction logic. We evaluate the proposed design using a simulation infrastructure based on SimpleScalar and CACTI. Simulation results show that the proposed technique reduces the energy consumption in the instruction cache and the branch prediction logic by 20% and 24% on the average, respectively. Moreover, the proposed scheme shows little performance loss compared to the traditional scheme.

S. Koohi et al.,[20] Real-time video transmission is considered as an important means for information distribution. One major application of it is e-learning, which requires real-time video processing and transmission. On the other hand, the process of cut detection is a fundamental component in automatic video browsing, indexing, searching, retrieval, and archiving. This work introduces a new video cut detection technique that uses dominant lines and angles extracted from edge information of the video contents. To the best of our knowledge, it is the first works done for cut detection in e-learning application. This method is compatible with our application requirements and has a low complexity and high speed. We have compared the performance of our proposed method against three established techniques and have evaluated the results using different video sequences.

III. IOT INTRUSION DETECTION SYSTEMS TECHNIQUES

The IoT Interruption is characterized as an unapproved activity or movement that hurts the IoT biological system. For instance, an assault that will make the PC administrations inaccessible to its real clients is viewed as an interruption. An IDS is characterized as a product or equipment framework that keeps up with the security of the framework by recognizing vindictive exercises on the PC frameworks. The primary point of IDS is to distinguish unapproved PC utilization and vindictive organization traffic which is preposterous while utilizing a customary firewall. This outcomes in making the PC frameworks exceptionally defensive against the noxious activities that compromise the accessibility, respectability, or secrecy of PC frameworks.

A. Signature-based intrusion detection systems (SIDS)

Signature interruption location frameworks (SIDS) use design matching procedures to track down a referred to assault; these are otherwise called Information based Recognition. In SIDS, matching techniques are utilized to track down a past interruption. As such, when an interruption signature matches the mark of a past interruption that as of now exists in the mark data set, an alert sign is set off. For SIDS, the host's logs are reviewed to observe arrangements of orders or activities which have recently been distinguished as malware. SIDS has likewise been named in the writing as Information Based Discovery or Abuse Recognition. Customary strategies for SIDS experience issues in distinguishing assaults that length different parcels as they inspect network bundles and perform matching against an information base of marks. With the expanded refinement of current malware, separating mark data from different bundles might be required. With this, IDS needs to bring the substance of prior parcels also. For making a mark for SIDS, by and large, there have been a few strategies where marks are made as state machines, formal language string designs or semantic circumstances.

B. Anomaly-based intrusion detection system (AIDS)

Helps has drawn in a great deal of researchers due to its element to beat the constraint of SIDS. In Helps, a typical model of the conduct of a PC framework is made utilizing AI, measurable based or information based techniques. Any huge deviation between the noticed conduct and the model is viewed as an irregularity, which can be deciphered as an interruption. This sort of strategy chips away at the way that pernicious conduct is not quite the same as commonplace client conduct. The conduct of unusual clients that separates from the standard conduct is characterized as an interruption. There are two stages in the advancement of Helps: the preparation stage and the testing stage. In the preparation stage, the typical traffic profile is utilized to gain proficiency with a model of ordinary conduct. In the testing stage, another informational index is utilized to foster the framework's ability to sum up to beforehand inconspicuous interruptions. Helps can be sub-arranged in light of the strategy utilized for preparing, for example, factual based, information based and AI based.

The primary benefit of Helps is the capacity to distinguish zero-day assaults on the grounds that perceiving the strange client movement doesn't depend on a mark information base. Helps sets off a risk signal when the inspected conduct goes amiss from ordinary conduct. Moreover, Helps has various advantages. To begin with, they can find inside malignant exercises. Assuming an interloper begins making exchanges in a taken record that are unidentified in the average client movement, it makes a caution. Second, it is trying for a cybercriminal to perceive what a typical client conduct is without delivering a ready as the framework is developed from redid profiles.

C. Machine Learning based Technique

AI is the most common way of separating information from huge amounts of information. AI models include a bunch of rules, techniques, or complex "move works" that can be applied to observe intriguing information designs or to perceive or anticipate conduct. AI procedures have been applied broadly in the space of Helps. To extricate the information from interruption datasets, various calculations and strategies, for example, grouping, brain organizations, affiliation rules, choice trees, hereditary calculations, and closest neighbor techniques are used.

Some earlier examination has analyzed the utilization of various strategies to assemble AIDSs. Analyzed the presentation of two element determination calculations including Bayesian organizations (BN) and Characterization Relapse Trees (CRC) and consolidated these strategies for higher exactness.

Procedures of component determination utilizing a mix of element choice calculations like Data Gain (IG) and Connection Characteristic assessment. They tried the presentation of the chose highlights by applying different order calculations like C4.5, guileless Bayes, NB-Tree and Multi-facet Perceptron. A hereditary fluffy rule mining strategy has been utilized to assess the significance of IDS highlights. NIDS by utilizing the Arbitrary Tree model to further develop exactness and diminish the misleading problem rate.

Different AIDSs have been made in view of AI procedures as displayed in Fig. 4. The primary point of utilizing AI strategies is to make IDS that requires less human information and further develop exactness. The amount of Helps which utilizes AI procedures has been expanding over the most recent couple of years. The fundamental target of IDS in light of AI research is to distinguish examples and fabricate an interruption discovery framework in view of the dataset. For the most part, there are two classes of AI strategies, regulated and unaided.

IV. Intrusion Detection System

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms. [1]

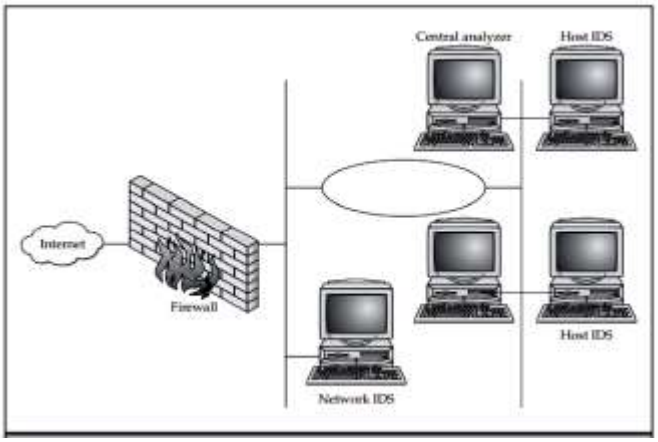

Figure 4: A simple active defense architecture

IDS types range in scope from single computers to large networks.[3] The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of an NIDS. It is also possible to classify IDS by detection approach. The most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Another common variant is reputation-based detection (recognizing the potential threat according to the reputation scores). Some IDS products have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system.[4]

Intrusion detection systems can also serve specific purposes by augmenting them with custom tools, such as using a honeypot to attract and characterize malicious traffic detailed investigation and analysis of various machine learning techniques have been carried out for finding the cause of problems associated with various machine learning techniques in detecting intrusive activities. Attack classification and mapping of the attack features is provided corresponding to each attack. Issues which are related to detecting low-frequency attacks using network attack dataset are also discussed and viable methods are suggested for improvement. Machine learning techniques have been analyzed and compared in terms of their detection capability for detecting the various categories of attacks.

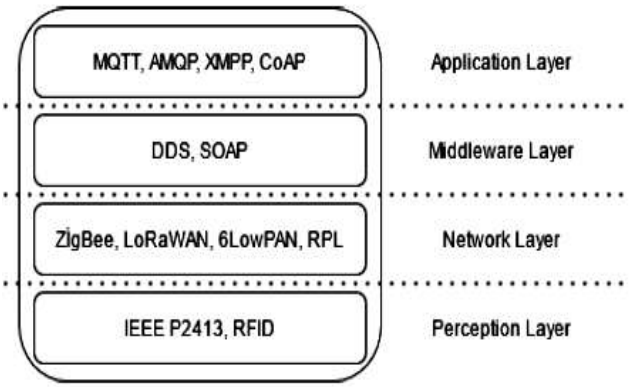

Figure 5: IIoT protocols by layer

Table 2: Consumer IoT and Manufacturer IIoT in terms of Security [21]

Manufacturer IIoT	Consumer IoT
The damage probability depending on data manipulation can be higher.	The damage probability depending on data manipulation can be lower due to working area.
Works on local network.	Works on general network.
Can benefit from fog computing services to provide security.	Can benefit fog computing services due to application and determined storage method.
Due to low latency requirement, lightweight protocols is needed.	Low latency is not a priority as IIoT.
Depending on high volume data processing and transmission, data loss probability is higher.	Due to limited data processing and transmission, data loss probability is lower.
Since process-specific customized protocols can be developed in the Operational Technologies (OT), standard security solutions may be insufficient.	Known security solutions can be implemented due to uses the standard TCP/IP stack.
Uses protocols such as Modbus, Ethernet/IP, DNP3, and Profinet and these are rarely uses authentication, authorization or encryption methods.	Known authentication, authorization or encryption methods can be implemented due to usage of the standard protocols
Data backup is needed due to high data volume and provide data integrity.	Due to a relatively limited data volume, high storage spaces are not required.

Network Intrusion Detection Systems

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. [8]It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulating network intrusion detection systems. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the design of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS, often referred to as inline and tap mode, respectively. On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

NIDS can be also combined with other technologies to increase detection and prediction rates. Artificial Neural Network based IDS are capable of analyzing huge volumes of data, in a smart way, due to the self-organizing structure that allows INS IDS to more efficiently recognize intrusion patterns.[9] Neural networks assist IDS in predicting attacks by learning from mistakes; INN IDS help develop an early warning system, based on two layers. The first layer accepts single values, while the second layer takes the first's layers output as input; the cycle repeats and allows the system to automatically recognize new unforeseen patterns in the network. This system can average 99.9% detection and classification rate, based on research results of 24 network attacks, divided in four categories: DOS, Probe, Remote-to-Local, and user-to-root.

A. Host Intrusion Detection Systems

Host intrusion detection systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

B. Detection Method

Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.[14] This terminology originates from anti-virus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is difficult to detect new attacks, for which no pattern is available.

C. Signature-based

In Signature-based IDS, the signatures are released by a vendor for its all products. On-time updating of the IDS with the signature is a key aspect.

D. Anomaly-based

Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid

development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model. Since these models can be trained according to the applications and hardware configurations, machine learning based method has a better generalized property in comparison to traditional signature-based IDS. Although this approach enables the detection of previously unknown attacks, it may suffer from false positives: previously unknown legitimate activity may also be classified as malicious. Most of the existing IDSs suffer from the time-consuming during detection process that degrades the performance of IDSs. Efficient feature selection algorithm makes the classification process used in detection more reliable.

E. Intrusion prevention

Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPS have become a necessary addition to the security infrastructure of nearly every organization.

IDPS typically record information related to observed events notify security administrators of important observed events and produce reports. Many IDPS can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.

F. IDS Placement

The placement of Intrusion Detection Systems is critical and varies depending on the network. The most common placement being behind the firewall on the edge of a network. This practice provides the IDS with high visibility of traffic entering your network and will not receive any traffic between users on the network. The edge of the network is the point in which a network connects to the extranet. Another practice that can be accomplished if more resources are available is a strategy where a technician will place their first IDS at the point of highest visibility and depending on resource availability will place another at the next highest point, continuing that process until all points of the network are covered.

If IDS is placed beyond a network's firewall, its main purpose would be to defend against noise from the internet but, more importantly, defend against common attacks, such as port scans and network mapper. IDS in this position would monitor layers 4 through 7 of the OSI model and would be signature-based. This is a very useful practice, because rather than showing actual breaches into the network that made it through the firewall, attempted breaches will be shown which reduces the amount of false positives. The IDS in this position also assists in decreasing the amount of time it takes to discover successful attacks against a network.

V. CONCLUSION

The network intrusion system prevent the cyber world form the various attack. There are various techniques based on the artificial intelligence, machine learning and deep learning, which can able to handle the attack prediction. This paper present the review of the cyber security using machine and deep learning techniques. In the future take some suitable dataset based on the KDD from the machine learning repository and apply the classification algorithm.

REFERENCES

[1]. H. Hou et al., "Hierarchical Long Short-Term Memory Network for Cyberattack Detection," in IEEE Access, vol. 8, pp. 90907-90913, 2020, doi: 10.1109/ACCESS.2020.2983953.

[2]. Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms," in IEEE Access, vol. 9, pp. 161546-161554, 2021, doi: 10.1109/ACCESS.2021.3128837.

[3]. M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke and L. Shu, "Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis," in IEEE Access, vol. 9, pp. 138509-138542, 2021, doi: 10.1109/ACCESS.2021.3118642.

[4]. G. Yoo, M. Yoo, I. Yeom and H. Woo, "rocorl: Transferable Reinforcement Learning-Based Robust Control for Cyber-Physical Systems With Limited Data Updates," in IEEE Access, vol. 8, pp. 225370-225383, 2020, doi: 10.1109/ACCESS.2020.3044945.

[5]. G. Apruzzese, M. Andreolini, M. Colajanni and M. Marchetti, "Hardening Random Forest Cyber Detectors Against Adversarial Attacks," in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 4, no. 4, pp. 427-439, Aug. 2020, doi: 10.1109/TETCI.2019.2961157.

[6]. M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. -K. R. Choo and R. M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8852-8859, Sept. 2020, doi: 10.1109/JIOT.2020.2996425.

[7]. S. -K. Kim, C. Y. Yeun and P. D. Yoo, "An Enhanced Machine Learning-Based Biometric Authentication System Using RR-Interval Framed Electrocardiograms," in IEEE Access, vol. 7, pp. 168669-168674, 2019, doi: 10.1109/ACCESS.2019.2954576.

[8]. A. Hassan, R. Hamza, H. Yan and P. Li, "An Efficient Outsourced Privacy Preserving Machine Learning Scheme With Public

Verifiability," in IEEE Access, vol. 7, pp. 146322-146330, 2019, doi: 10.1109/ACCESS.2019.2946202.
[9]. Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 35365-35381, 2018, doi: 10.1109/ACCESS.2018.2836950.
[10]. N. R. Sabar, X. Yi and A. Song, "A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security," in IEEE Access, vol. 6, pp. 10421-10431, 2018, doi: 10.1109/ACCESS.2018.2801792.
[11]. Y. Wang, M. M. Amin, J. Fu and H. B. Moussa, "A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids," in IEEE Access, vol. 5, pp. 26022-26033, 2017, doi: 10.1109/ACCESS.2017.2769099.
[12]. F. Wang et al., "Quantized Attention-Gated Kernel Reinforcement Learning for Brain–Machine Interface Decoding," in IEEE Transactions on Neural Networks and Learning Systems, vol. 28, no. 4, pp. 873-886, April 2017, doi: 10.1109/TNNLS.2015.2493079.
[13]. A. J. Smith, R. F. Mills, A. R. Bryant, G. L. Peterson and M. R. Grimaila, "REDIR: Automated static detection of obfuscated anti-debugging techniques," 2014 International Conference on Collaboration Technologies and Systems (CTS), 2014, pp. 173-180, doi: 10.1109/CTS.2014.6867561.
[14]. M. Guri, G. Kedma, T. Sela, B. Carmeli, A. Rosner and Y. Elovici, "Noninvasive detection of anti-forensic malware," 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE), 2013, pp. 1-10, doi: 10.1109/MALWARE.2013.6703679.
[15]. M. Hirabayashi, S. Kato, M. Edahiro, K. Takeda, T. Kawano and S. Mita, "GPU implementations of object detection using HOG features and deformable models," 2013 IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), 2013, pp. 106-111, doi: 10.1109/CPSNA.2013.6614255.
[16]. Lin Wang, Xiang Wang, Zichen Zhou, Qinghai Liu and Hao Yang, "Architectural-enhanced intrusion detection and memory authentication schemes in embedded systems," 2010 IEEE International Conference on Information Theory and Information Security, 2010, pp. 221-224, doi: 10.1109/ICITIS.2010.5688775.
[17]. R. Tao, L. Yang, L. Peng, B. Li and A. Cemerlic, "A case study: Using architectural features to improve sophisticated denial-of-service attack detections," 2009 IEEE Symposium on Computational Intelligence in Cyber Security, 2009, pp. 13-18, doi: 10.1109/CICYBS.2009.4925084.
[18]. K. A. Bowman et al., "Energy-Efficient and Metastability-Immune Timing-Error Detection and Instruction-Replay-Based Recovery Circuits for Dynamic-Variation Tolerance," 2008 IEEE International Solid-State Circuits Conference - Digest of Technical Works, 2008, pp. 402-623, doi: 10.1109/ISSCC.2008.4523227.
[19]. N. R. Yang, G. Yoon, J. Lee, I. Hwang, C. H. Kim and J. M. Kim, "Loop Detection for Energy-Aware High Performance Embedded Processors," 2008 IEEE Asia-Pacific Services Computing Conference, 2008, pp. 1578-1583, doi: 10.1109/APSCC.2008.66.
[20]. S. Koohi, M. Babagoli, T. Lotfi and S. Kasaei, "Video cut detection in E-Learning applications," 2007 9th International Symposium on Signal Processing and Its Applications, 2007, pp. 1-4, doi: 10.1109/ISSPA.2007.4555325.
[21]. Aykut Karakaya, Ferhat Arat "A Survey on Security Requirements, Threats and Protocols in Industrial Internet of Things" International Journal Of Information Security Science, Vol.10, No.4, pp.138-152.

AUTHORS

First Author – Rishika, M.Tech Scholar, School of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, guptarishika6@gmail.com
Second Author – Yogendra Maravi, M.Tech, School of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, yogendra@rgtu.net.
Third Author – Nishchol Mishra, Ph.D., School of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, nishchol@rgtu.net.
Fourth Author – Jitendra Agrawal, Ph.D., School of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, jitendra@rgtu.net

Correspondence Author – Rishika, guptarishika6@gmail.com.