Network Intrusion detection system using artificial intelligence

Clementine Mamogale - 216025117

Abstract

The rapid rise, growth, and development of new technologies that can connect and communicate with one another over the internet have increased the size of the network, which increased data transfer within the internet. Although this was made to improve our lives somehow, it comes with a huge downfall, which is the novel of attacks that are being made which poses challenges to the network securities that are used to accurately detect intrusions over a network (Ahmad et al., 2020),(Ashiku and Dagli, 2021). One tool that is widely used to detect and prevent possible intrusions over a network is the intrusion detection system (IDS). This IDS inspects traffic over the network, and it ensures the integrity, confidentiality, and availability of the network (Ahmad et al., 2020). Although it worked so well at first, hackers are on the rise, and they came up with different techniques to bypass this IDS, which they managed to do so. As a result, this tool is no longer effective because it failed on two things, which are increasing its detection accuracy rate and reducing the false alarms (Ashiku and Dagli, 2021). A new intrusion detection system that uses artificial intelligence to detect and prevent possible intrusions over a network is an alternative. This paper present and propose a Network Intrusion Detection System (NIDS) that uses Artificial intelligence architecture that will feature deep learning and machine learning techniques to develop a system that will be adaptive and be resilient to network intrusions and be able to classify attacks on a network (Ashiku and Dagli, 2021). Machine learning and deep learning can help the NIDS to learn and recognize even new or zero-day intrusions on a network and reduce or prevent the risks of compromising the network (Ashiku and Dagli, 2021). To demonstrate the effectiveness of this model, we use the old KDD+ and the new CICIDS 2017 datasets. The reason for these two datasets is because the KDD+ is widely used because it has well-known intrusions, and the CICIDS is new and has new attacks that happened recently.

Introduction

In this modern life, our daily activities are influenced by the widespread use of computer systems and information and communication technologies that can interact with one another and work or communicate with each other over the internet (Ashiku and Dagli, 2021). As much as this makes our daily activities much more interesting since it offers an interoperability solution that is so convenient to get work done with ease, it opens vulnerabilities that can be exploited on both organizations and individuals, vulnerabilities that are impossible to be managed by a human being on a real-time, hence the development of better robust network security system is needed, a system that will be able to maintain the confidentiality, integrity, and availability of data and services (Ashiku and Dagli, 2021).

Network security is recognized as one of the first layers of defense mechanism that are used to realize and defend against different attack vectors, and a network intrusion detection system is used to scan traffic on a network and identify any violation that is based on customized detection levels that are preconfigured on the network, and then report them if any violations are found. How it works is that if any intrusions are detected, they will be rejected and stopped from happening before it causes any damage to the data that is being protected, this is made possible because the network can differentiate between legitimate and non-legitimate traffic on a network based on the behavioral features of the connection that is happening (Ashiku and Dagli, 2021). Although an Intrusion detection system determines intrusions based on their features, a clear cut cannot be made from legitimate and no-legitimate connections since they cannot learn by themselves. Hence the development of an intelligent Intrusions detections system is needed, a system that will be able to learn and be able to differentiate between legitimate and non-legitimate connections that is an intrusion into the system (Ashiku and Dagli, 2021).

There are two different approaches that are by far the most dominant in the commercial and research literature which are anomaly detections which detect what is not known already, it detects new intrusions, and the other one is misuse detections which detect what is already known in the network. The misuse is one that is used mostly in our daily lives. How it works is that if a new attack is discovered, usually during the diagnostic phase after its occurrence, a human being whom he's an expert in malicious attacks will record the malicious pattern that is associated with that attack which will then be used next time to detect and recognize a new instance of the same attack (Ashiku and Dagli, 2021). This human intervention can be time-consuming and costly. To avoid such interventions, supervised computers that have learning capabilities can be used to create and register those signatures and use those newly created instances to create models that would be used to discover attacks of similar patterns (Ashiku and Dagli, 2021).

Misuse is good at discovering attacks that they are known by the system, attacks that they are programmed to know and alert on them, but then they become vulnerable to new attacks or zero-day attacks because the signatures of those attacks cannot be identified and realized as attacks and that is where the misuse becomes ineffective to identifying attacks (Ashiku and Dagli, 2021) as such, misuse results in suffering from the vulnerability of diagnosing new attacks and creations of new signatures in the long run.

Anomaly detections on the other hand, use daily instances of the normal operations of traffic to create a profile of normal traffic, and any traffic that does not fit into that profile is regarded as intrusion and gets treated like one, such as being blocked and get reported. This kind of intrusion detection system can detect attacks that are new, but then it still requires a lot of training to create those profiles of legitimate network profiles (Divyasree and Sherly, 2018). One other thing is that this kind of intrusion detection system can create high false alarms because of how it is structured, and it gets difficult to produce accurate results and keep it up to date (Ashiku and Dagli, 2021).

Although both anomaly detection and misuse detection are different in nature, they still have a similar problem, which is that they both depend on some external knowledge, which means they cannot depend on themselves to achieve their goal of identifying intrusion on a network, they have to either create some normal profile of a network or use the already created intrusion signatures to be able to identify an attack on a network. Such network security will not be a proactive active mechanism, but rather it will be a reactive countermeasure (Ashiku and Dagli, 2021). Organizations and individuals in the security of networks community over the past have been shifting towards the use of proactive defense mechanisms over-reactive countermeasure defense mechanisms (Ashiku and Dagli, 2021). As a result, a need for unsupervised network intrusion detection system is needed, and that is what this paper will be presenting. But other related works exist in the detection of intrusions over the internet.

Similar works

A very close related work is the use of Ensemble Core Vector Machine (CVM) to detect intrusions on a network. It is a data mining classifier that uses methods or algorithms that work on the concept of a Minimum Enclosing Ball basis (Divyasree and Sherly, 2018). CVM are better versions of Support Vector Machines (SVM) which are learning models that are supervised. They have algorithms that they use for learning and analyzing data for regression analysis and classifications (Ahmad et al., 2022). SVM algorithms are based on learning frameworks in statistics, hence they are taken as one of the best prediction methods. MVC being the superior version of SVM, it uses the concept of minimum enclosing ball, of which is also adopted from statistics functions. This function helps in producing false-positive rates that are less, and unlike the SVM, the CVM has a lower overhead computation. And this helps in better performance (Ahmad et al., 2022). A data mining classifier on its own will not be enough since it does not offer all desired features like an acceptable way of computation time that is less, low false-positive rates, and a high detection rate. Hence the use of Core Vector Machine as a classifier to solve the above-mentioned problems (Ahmad et al., 2022).

Another interesting field of study in intrusion detection systems is the Internet of Things (IoT) industry. Internet of Things is a new and growing technological advancement whereby the day-to-day electronics, which are from different domains, are connected to the internet and to one another. These electronics become "smart" to be able to communicate with other devices that are machine processes dependent, agriculture, healthcare, and manufacturing processes. They communicate on the internet via data sharing (Chauhan et al., 2020). Internet of Things is a system whereby people, machines, and computing devices are interconnected together on the internet. These billions of devices are embedded with technologies such as sensors and actuators that generate a high volume of data on the internet (Ahmad et al., 2022). It has been reported by fortune business insight that the Internet of Things for businesses could reach trillions of dollars by the year 2027. This shows how much IoT can reshape the future with the technology it brings.

Internet of Things brings interconnected systems that have so many benefits to our lives, but then they are also vulnerable to threats on the internet. Hence, the need for an intrusion detection system that is specifically designed for these smart devices to create a secured environment for these smart devices. Because if one is vulnerable, it automatically puts the other devices or the whole smart environment at risk (Chauhan et al., 2020). Internet of Things devices have their own specifications and protocols that they follow, protocols that are different from the rest of other computing devices. As a result, it remains a challenge to create a secured environment for these smart devices (Chauhan et al., 2020).

One reason why these smart devices are prone to cyber-attacks is because of the lack the hardware security support, and their gateways do not provide enough security features such as an intrusion detection system that will be able to detect those threats that are posed to them. Intrusion detection systems require a high computational power of which these smart devices gateways do not provide. And implementing those complicated hardware and software security features on these devices can cause these devices to misbehave or break. As a result, it brings a huge gap between

security capability and security requirements on these smart devices. Therefore, this means that these devices are prone to all these kinds of cyberattacks on the internet, such as Denial of service and spoofing attacks (Ahmad et al., 2022). There are records of these attacks that are targeting the Internet of Things all over the globe, and it shows the effect these attacks have on these devices, such as damaging the hardware of these devices, interrupting the system of these IoT, such as the Marian malicious software that ware recorded, it was the most famous attack that happened in 2017 on the Internet of Things devices. This attack affected over 300 000 Internet of Things devices, of which it further turned them into botnets that were used to create a distributed denial of service attack (Ahmad et al., 2022). Such attacks will affect the production line of organizations and having fewer devices being produced since they lack important security features. Some of the security aspects of the Internet of Things devices are:

1. **Data privacy** – it is important to secure these Internet of Things devices because if data is hacked during the transmission of data from one node to another on these devices, then the privacy or confidentiality of these data gets destroyed (Chauhan et al., 2020).
2. **The integrity of data** – during transmission of data or information, their data or information should be protected so that it does not get altered. Throughout the entire transmission, the accuracy of the data should be maintained at all times (Chauhan et al., 2020).
3. **Availability** – resources should always be available, especially for applications that are time-sensitive. The availability of resources can be affected by the denial of service attacks on these devices, hence it is important to make sure that these devices are secured and free from such attacks (Chauhan et al., 2020)
4. **Authenticity** – the Internet of Things devices should be able to provide resources to legitimate users only so that unauthorized users cannot misuse these devices for their own agenda. Legitimate end-users should be able to use the devices without any errors or disruption, and the devices should be able to realize and block the non-legitimate users.

5. **Non-denial –** the smart devices should be able to complete their duties and be able to identify and record all or only the critical actions that include data transmission or modifications so that no user will be able to deny that they have sent or received such data.

An intrusion detection system is usually deployed at the gateways of these smart devices as a mitigation security risk that will secure the network of these smart devices. How it works is that it monitors the network continuously for any malicious signs of attacks on the outgoing and incoming bounds of the network. This is not enough because it only checks the movement of the network from inside to outside and vice versa, but it does not check for the internal network traffic of these devices (Chauhan et al., 2020). As a result, the need for a deployment strategy that is distributed is needed for these smart devices, a system that will make it possible for the internal network to be integrated into gateways and routes. This will also help in decreasing the volume of network traffic within the smart devices since the traffic will be going through different routes and gateways to get to their destinations and increasing the detection accuracy of the Intrusion detection systems (Chauhan et al., 2020).

A proper solution that was proposed for these Internet of Things devices is the use of machine learning techniques that will be integrated into the intrusion detection system. Deep Neural Network (DNN) is one of the most popular techniques that are used to classify traffic on a network as either abnormal or normal classes (Chauhan et al., 2020). How this model works is that it will use an already available dataset of both normal and abnormal attack traffic, which it will use to learn and create profiles of each before it gets deployed on a live network system. This approach worked so well compared to the traditional method of identifying intrusions on a network because it can analyze and learn non-linear complex features that are most usually used in a real-world attack process (Chauhan et al., 2020).

The use of a Deep Neural Network (DNN) on a Network Intrusion Detection System (NIDS) gateway can help in achieving the goal of protecting these smart devices.

Although it is known that DNNs require high computational power, we can try to find a lightweight DNN that will use less power while producing positive results, A DNN that can be deployed and run on IoT gateways that have resource consumption that is minor such as the RAM and the CPU, that will be suitable for this small smart devices. (Chauhan et al., 2020). By having this resilient and secured connection within these networks on these smart devices, we could offer more robust connections to the cloud where the data get stored. That is, if the devices themselves have these networks embedded in them, then by default, they are secured from any attacks from either side, and hence they will be able to connect and transfer data to the cloud.

A detailed explanation of this kind of work was done that involves the designing, implementation, and evaluation of these DNN embedded NIDS on these smart devices. It is called the real guard that can be used to detect both external and internal network intrusions in real-time. In more detail, it looks at the following:

- It offers better protection for these smart devices by implementing the NIDS to the device's network gateway. This will help by increasing the detection accuracy of the system and decrease the complexity and the volume of traffic on the network, and also it will help in identifying cyber attacks on both external and internal infrastructure (Chauhan et al., 2020). For these to be a success, the newly created NIDS but be a lightweight to be able to work on these devices that are resource-constrained while maximizing the performance of identifying cyber threats. It also requires that it runs in real-time, and this can be achieved by making sure that the package processing unit is higher than the higher that the packets of the estimated arrival unit of these smart devices so that there won't be any waiting periods in between the transfer of data (Chauhan et al., 2020).
- It should be able to identify multiple attacks, and this includes groups of attacks such as distributed denial of services attacks that emerge from different sources at once. In essence, the NIDS has to be able to identify all these kinds of attacks

that might arise on the network and be able to fight or block them from happening (Chauhan et al., 2020).

- An intrusion detection system that is based on a DNN, as a Realguard system. It operates directly on the edges of the IoT's gateways. This will not only help in identifying abnormal and normal network traffics, but also it will be able to identify all these kinds of cyberattacks that might arise from within the network, such as from the already compromised devices and also from the outside networks (Chauhan et al., 2020). This is very important because the devices cannot affect one another. Each device can get affected on its own without having to involve the other smarts devices it is connected with.
- There is also a feature extraction module that works so efficiently to be able to extract features on network traffic, and the use of Dumped Incremental statistics is used to speed up the process of extracting those features from each network traffic (Chauhan et al., 2020).
- A Realguard should be able to work on resource-constrained gateways and be able to function without any problems while detecting a wide range of threats on a network while producing low false-positive rates results (Chauhan et al., 2020).
- A Docker container is finally used since it can integrate the works of Internet of Things gateways to the Internet of Things gateways. Docker supporting containers and also Junkies automation server, which is an open-source, can also be used to make sure that the system is platform-independent (Chauhan et al., 2020).

Intrusion detection in IoT taxonomy

A review was conducted on the following sections for the IDS that were proposed for the Internet of Things devices. The works are divided and classified on the following basis that is categorized as follows: validating, placements, and detection (Ahmad et al., 2022).

The placement intrusion detection strategy

- **Distributed Intrusion detection system placement strategy -** This is when every physical object has its own IDS placed on it.
- **Centralized Intrusion detection system placement strategy** – here, the IDS is placed in a centralized environment whereby it will analyze and scan every traffic that goes through the router.
- **Hybrid intrusion detection system placement strategy** – this is a combination of the two strategies that were mentioned above. This helps in getting better results because it utilizes both methods to find intrusions.

Detection methods

- **Signature-based** – this type of intrusion detection uses previously known patterns or profiles of attacks and their signatures to check, compare and fight against any attack (Ahmad et al., 2022)
- **Anomaly-based –** this is an even based kind of intrusion detection system. It uses events to find intrusions on a network. It creates profiles on normal network traffic, and if any traffic does not fall within that profile, then it gets flagged as an intrusion (Ahmad et al., 2022).
- **Specification-based** – This one works almost similar to the anomaly-based since it also uses events, but then the events here follow rules that were created by the administrators, and if any traffic does not follow those specifications, it gets flagged as an intrusion (Ahmad et al., 2022)
- **Hybrid based** – this one is a combination of all, it allows for maximum security, and it hardly fails.

Validation strategy

In this strategy, there can be many approaches that are taken, and the information can be broadly categorized into data and experts. In data, the data source of information gives the quantitative objectives of validation, while in experts, the experts give the source of information quantitative and objective of validation (Ahmad et al., 2022).

Another look into intrusion detection systems is in cloud computing itself. The sudden rise of infrastructure and the development of resources is forcing the organization to opt for cloud computing since it is much cheaper to hire services than compared to host those services in-house (Liu et al., 2021). As it is known, the internet was designed with a little security in mind hence even cloud computing also presents some of its own faults or vulnerabilities. As a result, the use of intrusion detection systems has been one of the most used security measures to guard networks of cloud computing from threats and attacks on the internet (Liu et al., 2021). Four sections are investigated when talking about the security of cloud computing, namely the Hypervisor-based IDS, machine learning-based IDS, network-based IDS, and hybrid-based IDS. Cloud computing offers services that are so diverse, and it makes things easier for organizations to be able to integrate their work remotely.

Cloud computing offers service services that are information related and serves that can be used by organizations to run their businesses, cloud computing runs on virtualizations which makes it so flexible, and it saves on cost on the consumer side. Virtualization is good because it makes it easier and more flexible to manage computers, especially in a large organization. Through this virtualization technology, cloud computing can use the underlying storage and computing resources to integrate and provide convenient and on-demand services to clients (Liu et al., 2021). The clients, which can be individuals or other organizations, can be able to access services such as programs, storage, and application improvement platforms via the service provider's interest and services. Most services that clients opt for are Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Services (IaaS) (Liu et al., 2021). The host and networks that are virtualized are placed in the lowest layer of cloud computing, and this layer is the IaaS. Then in the PaaS, you find the applications interface programs and the virtualized operating system of cloud computing. Then there is the highest layer of the architecture which delivers virtualized applications, and it is called the application layer (Liu et al., 2021). Although this kind of application runs smoothly and provides the best experience for organizations, they are still prone to cyberattacks.

On the other hand, there have been concerns with server vulnerabilities and security because of how the enhancement of computer networks. Cybercrimes continue to be of great concern, and malicious software remains the number one security threat that is seriously posing to these computing services. Malicious software remails a big threat that has been used mostly to target computers to disrupt their normal functioning or to steal data (Liu et al., 2021). Cybercriminals are working hard to improve their attacking tactics and make better and hard to detect malicious software that they can use to attack computers. Hence there is a need for improving security also on these computers because the use of digital credentials and confidentiality or the use of identification numbers to ensure safety needs and security of software is no longer enough. At least broadcast authentication remains an important security tool in wireless sensor networks, while intrusion detection is being used by network administrators to monitor and manage intrusions on a network (Liu et al., 2021).

Although it is known how much impact the cloud computing has on the modern computing, there is no review that is complete for the cloud computing on the IDS, there are several techniques that are used, but they are not completely for cloud computing. Hence they are used together to secure the cloud storage and services (Liu et al., 2021). A review has been done to compare and see how everything works together to secure the cloud and is discussed in this paper (Divyasree and Sherly, 2018). As mentioned, we will be looking into Hypervisor-based IDS, machine learning-based IDS, network-based IDS, and hybrid-based IDS.

- **A hypervisor or virtual machine-based intrusion detection system**

A hypervisor is a computer that can create virtual machines and run them. it allows for one computer to run and share its resources such as ram and memory through the use of host and guest operating systems. A hypervisor will allow a host operating system to share a platform for other guest operating systems to use its resources. A hypervisor-based Intrusion detection system runs at the hypervisor layer, and it

analyzes and controls the information that exists already to detect actions and incidents of anomalies (Divyasree and Sherly, 2018). The downfall of virtual machines is that they are prone to zero-day attacks. Hackers can use that opportunity to try and gain access to the hypervisor.

Wang and Nikolai did a presentation on an architecture that can be used to help the technology of virtualization at the cloud center (Divyasree and Sherly, 2018). The presentation shows that the proposed solutions of the hypervisor-based IDS on the cloud do not need any extra installation of new software. It uses the already existing software on the virtual computer, and this is good because then it can save on expenses for software. This one has more benefits than the other two IDS, which are machine learning-based and network-based IDSs. The presentation showed that when there were zero attacks, it showed no false positive, but then the false positive rate has been detected in a run of a 10-user workload. The hypervisor signature performance did detect an attack on cloud computing (Divyasree and Sherly, 2018). Hence the approach should be tested more to decrease the false-positive rates.

Zhang and his collogues presented the CloudRader, which is another type of VM-based IDS. CloudRader sported the cache-oriented that are side-channel attacks on multi-layered clouds. The CloudRader integrated two events, and the first one is the signature-based detection which is used to monitor and determine the time taken to do the secured cryptography by the virtual machine. And the technique of anomaly detection based was used to monitor the co-located virtual machines (Divyasree and Sherly, 2018). The benefit of this one is that it focuses on the fundamentals of the attack side channels that are cache-dependent. This is also good because it cannot avoid metamorphic codes intrusions, especially when there is a low false-positive rate. One other thing is that the CloudRader was designed to work with lightweight patches to the current mechanisms of cloud computing, whereby if there are any changes to the hypervisor or the new hardware backup is added, then there will not be any interference of the operating system as is a standalone application (Divyasree and Sherly, 2018). Thirdly is that the CloudRader can spot side-channel intrusions in a matter of milliseconds. It offers a defense that is immediate.

- **A network-based intrusion detection system**

This type of intrusion detection system is very crucial as it is placed at a very important place in a network. How it works is that it constantly checks for intrusion by examining transport layer headers and IP packets. This system can use both, or any of the signature dependent or the anomaly depended in methods to identify and detect intrusions in a network (Divyasree and Sherly, 2018). NIDS analysis the traffic on a network via the network layer and network's transport layer to detect and act on intrusion signs like port scanning and distributed denial of services attacks. The positioning of this is very important as it acts as the first layer of defense. It gets placed somewhere where there is a traffic monitoring tool. Some presentations were made for this method of detecting intrusions on cloud computing. Some of them are mentioned below.

A presentation was made by Sangeetha and colleagues on the application signature-based level that was based on semantics. The focus was on the application layer, and that is how the application-level attacks were realized. On the virtual cloud operator and virtual cloud provide, there was a packet sniffer that was positioned to monitor the traffic, and the packer sniffers were placed in a way that matched their parsers (Divyasree and Sherly, 2018). Then the parser decoded packets of data into procedure messages and also sent each package to the state machines that they correspond with. Also, the message was included in the packages so that they are passed to their message parsing grammar so that they will analyze the grammar of the semantics rules and see if they comply. A malicious work was the one that was analyzed and was found not to comply with the rules of the semantics (Divyasree and Sherly, 2018). The false warning frequency gets decreased in the signature somatic oriented IDS, so the detection rate is enhanced. Although the signature and rules get updated automatically for this method, it is still overhead because as the rules and signature increase over time because of new attacks, and there will be a need for an increase in memory for these devices (Divyasree and Sherly, 2018).

Another presentation was made by Wang and colleagues, and this presentation is focused on analyzing the security impact of distributed denial of services attacks. A defense architecture should be designed so properly because the enterprise stands together with the SDN technology and gets helped against DoS attacks on a system (Divyasree and Sherly, 2018). The model saves time, and that is what it is good at, but then it lacks performance, and it has poor accuracy because it regenerates.

- **Machine learning-based intrusion detection system**

In recent years, many domains have been implementing the learning methodology of machines to run their businesses, and these learning machines differ in their competency of learning. Some are good some are perfect learning. In the Intrusion detection system, the same holds. Machines are used to come up with ways to learn all these different attacks on a network so that the networks can protect themselves without human intervention, and they will be able to learn in real-time. The anomaly detections system has been embedded with learning methods capabilities since they can shape the feedback automatically and create behavioral profiles without any supervision (Divyasree and Sherly, 2018). How it works is that the intrusion detection models use algorithms that allow them to learn on data that is available already and continue to learn as time goes on with the data that it will receive from the internet as hackers will be trying to get unauthorized access to the systems (Divyasree and Sherly, 2018). This has an advantage because it will save on human labor of having to manually create profiles and signatures of all these kinds of attacks that are already known out there. And since humans are prone to errors, hence they might make mistakes that might put the system at risk of being hacked (Divyasree and Sherly, 2018). The unsupervised Intrusion detection system on this cloud computing helps in spotting attacks that have not been encountered before, it learns about good and bad network traffic, and it can spot an attack with ease since it has learned about traffic profiles.

Rajendran and Muthukumar proposed the use of artificial intelligence on this IDS, and how it works is that the IDS will be able to work in a dynamic way and be able to spot attacks dynamically using the knowledge it has learned from previous attacks and networks and also using databases and datasets to learn. How it works is that the model will be forecasting the attacks effectively by training the system. The suggestion of smart devices is that they are going to use a combination of hardware and software applications to detect an intrusion, and they are going to use an algorithm that can detect new attacks on an environment on the private cloud, which makes it a perfect place for this kind of intrusion (Divyasree and Sherly, 2018). This kind of intrusion is mew to the industry, and many organizations and individuals are trying it out, but then it has one downfall of responding poorly in performance due to the increase in database records, and it ends up taking a long time to respond back to the systems.

Salman and colleagues proposed a new way of doing things, which was to spot and classify anomalies. This was a new trend in prevention methods in modern academic studies. They used two machine learning methods that were supervised in spotting and classifying various intrusions. Namely the random forest and the linear regression methods. Even though the attack did complete, the classification was somehow less accurate, and this was because the attack types, which include Bacjdoor, DoS, and U2R, were almost similar. Based on the results that were presented showed that the accuracy of detection was up to 99%, while the accuracy of classification was 93.6% (Divyasree and Sherly, 2018). The disadvantage of this method was the inability to categorize some attacks.

- **The Hybrid intrusion detection system**

This type of intrusion detection system uses at least two of the detection system. Hence it is called the distributed IDS. It has some procedures that it uses, such as the NIDS in a vast network, whereby they are connected somehow to the underlying network. There is a central service that all of these networks connect to, and then the centralized service will do all the hard work of linking everything together as a unit and scanning the as its job of monitoring it. The whole idea here behind this type of intrusion detection system is to have a system that can recognize the knowledge and

the unknown attacks using both anomaly and signature detection methods (Divyasree and Sherly, 2018).

As a result, it has been shown that cloud computing is used so widely, despite the fact that it was developed so quickly, but the reason for its acceptance might be that it has so many benefits to both the end-users and the hosts. Some of these are: it has low cost, both on optimization and installations, fast arrangement, and it provides huge storing capacity.

Related works

- **An anomaly-based intrusion detection system**

This type of intrusion detection system works by monitoring activities on a network, and it detects intrusions on a network and computer and misuse. It then classifies those activities as normal or abnormal. The anomaly intrusion detection system uses data that is gathered from monitoring a network, and it creates profiles of normal traffic, and any traffic that is not within that profile can be regarded as an intrusion into the network. These kinds of systems are good for statistics purposes, but they are not good to predict the future since they are only reacting to the current conditions. That is, they can only detect suspicious activities or known attacks (García-Teodoro et al., 2009). Hence, if a hacker is able to bypass those suspicious activities, then they will be able to gain access, and they will not be able to fight against zero-day attacks and other new attacks on a network since they would know about it.

- **Intrusion detection system using random forest modeling**

Random forest modeling is a machine learning algorithm that makes use of decision trees as its neckbone function. It combines multiple trees that grow and join together to form a forest, hence the name of this technique. What is good about this is that it can be used in regression and classification problems (Farnaaz and Jabbar, 2016). This is a supervised machine, meaning it learns from different input and output that it got from datasets.

How these decision trees work is that they work together to bring the best accurate results, as in like they work best if they are working together as a unit than when they are working solo, so each of them will provide some kind of input to whatever is happening and that way, as in like they will “vote” and based on the number of votes, a decision is made such as if the traffic is legit or not, and act accordingly. This is good because it is known that a unit three might make a mistake, but as a whole, the majority of the trees will not make a mistake, and since the decision is made from the majority of trees' decisions, then this means the end results are mostly accurate (Farnaaz and Jabbar, 2016).

- **A Network Intrusion Detection System that is Based On Ensemble CVM that Uses Efficient Feature Selection Approach**

Assemble methods are machine learning techniques that are used to combine several base models to produce one optimal predictive model. The core vector machine is a better version of the support vector machine, which is a type of supervised learning machine that is used for classifications (Divyasree and Sherly, 2018). They use statistical algorithms to make decisions. What makes this different from other classifications mechanisms is that it chooses the decision boundary that will maximize the distance that is from all the classes involved. Ensemble Core Vector Machine, on the other hand, uses the concept of minimum enclosing ball. What is good about this is that it has a low computation head compared to other classifiers, and it can produce low false-positive rates (Divyasree and Sherly, 2018).

- **Intrusion detection on the Internet of Things**

One major work that is being focused on is intrusions on the Internet of Things devices, or smart devices as they are called. Internet of Things is a concept whereby physical objects are connected to the internet, and they are able to share data wirelessly without any human intervention. This is all good, especially with this modern technology, but then the only problem with this concept is that it lacks security because these smart devices were not originally made for sharing data over the internet. As a

result, it is important to have some intrusion detection system implemented on these devices (Chauhan et al., 2020).

A proposed solution for these devices is the use of an intelligent intrusion detection system that does not require any human intervention since the devices are already not monitored by humans. Because installing security hardware or software on these devices might cause the devices to misbehave, the use of a Deep Neural Network (DNN) on a Network Intrusion Detection System (NIDS) gateway can help in achieving the goal of protecting these smart devices. Although it is known that DNN requires high computational power, we can try to find a lightweight DNN that will use less power while producing positive results, A DNN that can be deployed and run on IoT gateways that have resource consumption that is minor such as the RAM and the CPU, that will be suitable for this small smart devices. (Chauhan et al., 2020).

Proposed solution

This paper presents a possible solution for a network intrusion detection system that uses artificial intelligence. This model works like the human brain nervous system, whereby the neurons, which are the collections of processing units, are represented by the nodes and how they are connected all together to function. The aim is to develop a system that is resilient and adaptive to network changes in its behavioral features. Demonstrating the effectiveness of this model, we are going to use KDD+ and CICIDS 2017 datasets. The reason is that the KDD+ has been used for a long time, so it has so many different data on it that can be used to allow the machine to learn as a baseline, while the CICIDS 2017 is kind of new, and it has a recent dataset that can be used by the machine to learn modern attacks on the network.

What makes this project different from the rest of the articles is that it is going to make use of a deep neural network that will be able to learn about both signature-based and anomaly-based attacks. The intrusion detection system will be placed on the gateways of all routes so that it can detect both internal and external attacks. The learning model will include Convolutional Neural Network, which will provide a multi-layered, unlike using a feed-forward neural network.

References

Ahmad, I., Ul Haq, Q., Imran, M., Alassafi, M. and AlGhamdi, R., 2022. An Efficient Network Intrusion Detection and Classification System. *Mathematics*, 10(3), p.530.

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J. and Ahmad, F., 2020. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1).

Ashiku, L. and Dagli, C., 2021. Network Intrusion Detection System using Deep Learning. *Procedia Computer Science*, 185, pp.239-247.

Ashiku, L. and Dagli, C., 2021. Network Intrusion Detection System using Deep Learning. *Procedia Computer Science*, 185, pp.239-247.

Chauhan, A., Singh, R. and Jain, P., 2020. A Literature Review: Intrusion Detection Systems in Internet of Thing. *Journal of Physics: Conference Series*, 1518(012040).

Divyasree, T. and Sherly, K., 2018. A Network Intrusion Detection System Based On Ensemble CVM Using Efficient Feature Selection Approach. *Procedia Computer Science*, 143, pp.442-449.

Divyasree, T. and Sherly, K., 2018. A Network Intrusion Detection System Based On Ensemble CVM Using Efficient Feature Selection Approach. *Procedia Computer Science*, 143, pp.442-449.

Farnaaz, N. and Jabbar, M., 2016. Random Forest Modeling for Network Intrusion Detection System. *Procedia Computer Science*, 89, pp.213-217.

García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G. and Vázquez, E., 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1-2), pp.18-28.

Liu, Z., Xu, B., Cheng, B., Hu, X. and Darbandi, M., 2021. Intrusion detection systems in the cloud computing: A comprehensive and deep literature review. *Concurrency and Computation: Practice and Experience*, 34(4).