https://doi.org/10.38124/ijsrmt.v3i3.26

Artificial Intelligence and Machine Learning Techniques for Anomaly Detection and Threat Mitigation in Cloud-Connected Medical Devices

[1]Omolola Akinola
Dept. of Information Systems and Analysis
Lamar University Beaumont, Texas, USA

[2]Akintunde Akinola
Department of Accounting and Finance
Ekiti State University

[3]Ifenna Victor Ifeanyi
Dept. Of Industrial Engineering Lamar University
Beaumont, Texas, USA

[4]Omowunmi Oyerinde
MIS Lamar University Beaumont, Texas

Basirat Oyekan[5]

[6]Oyedele Joseph Adewole
Dept. of Industrial and Systems Engineering
Lamar University Beaumont Tx

[7]Busola Sulaimon
Dept of Industrial and System Engineering
Lamar University Beaumont, Texas USA

Abstract:- The Internet of Medical Things (IoMT) has begun functioning like this: improved patient monitoring and an easily accessible digital data warehouse. Despite that, this methodology of the internet will potentially have a counter balance which risks for patient data might involve hacking, data theft, and unauthorized access that may contain great consequences for patient privacy and safety. This article examines the possibility of utilizing new AI technology, including inter alia deep learning, unsupervised learning, and ensemble learning to further boost anomaly detection and threat management in connected cloud medical systems. Many old rules and approaches based on statistics lose relevancy versus the dynamics and unpredictability of modern cyberattacks. Identification of anomalies in cyber security is nearly unavoidable, and it should be the first and the last reaction for detecting irregularities in behavior that may indicate undesirable acts or attacks. The paper aims at understanding how AI/ML approaches can give more sophisticated and versatile interventions for finding out anomalies in cloud-attached medical machines. Moreover, this research details robust AI/ML methods such as the adversarial machine learning and reinforcement learning for a perfect threat mitigation. These techniques which activates machine learning models to learn from data continuing to adjust to new evolving threats and then to establish intelligent and proactive threat response systems. The data experiment, which focuses on relevant data sets, reveals that it is the AI/ML techniques that possess the upper hand over traditional methods when it comes to identifying anomalies and defending against threats for cloud-connected medical devices. Such finding expresses much significance for the healthcare industry, as it gives room for the inclusion of AI/ML techniques into the security systems of the medical devices, which are all connected to the cloud. Through the employment of these strategies, healthcare units will become better able to detect and halt any form of threat and as a consequence patients' data will be protected, devices will continue operating effectively, and eventually patients' safety and healthcare units will benefit and gain trust from patients.

Keywords:- *Cloud"-Enabled Medical Devices, Cybersecurity, Anomaly Detection, Threat Mitigation, Artificial Intelligence, Deep Learning, Unsupervised Learning, Ensemble Learning, Reinforcement Learning And Adversarial Machine Learning.*

I. INTRODUCTION

Cloud-based systems that have been enabled by integrating medical devices have altered the way healthcare is delivered as it allows for telemedicine, remote patient monitoring, and easy access to all medical data (Butpheng et al., 2020). Cloud-connected medical devices use the internet and cloud computing to gather, store, and send private patient data. This lets doctors and nurses see important data at all times. These improvements have made patient care much better, improved treatment outcomes, and made healthcare service more efficient. But more people using and connecting to cloud-based systems has also made security harder and opened up new holes. Unauthorized access, data breaches, and other malicious attacks can happen to medical devices that are tied to the cloud. These can compromise patient privacy, data integrity, and the device's ability to work. Not only do these threats put patient safety at risk, but they also make people less likely to trust these new tools. Recent studies have shown that cyberattacks on healthcare

https://doi.org/10.38124/ijsrmt.v3i3.26

systems are becoming more common and have serious effects, such as hurting patients, losing money, and hurting the organization's image (Abomhara & Køien, 2015).

Taking care of these security issues is very important, because any breach or failure in medical devices tied to the cloud can have very bad results. Cyber threats today are very complicated and change all the time, so old security tools like firewalls and antivirus software don't always work well (Lu & Da Xu, 2018). It's hard to find and stop these threats using normal methods because they can take advantage of flaws in devices, communication channels, or cloud systems.

On top of that, medical devices and integrating them with cloud systems pose special problems. Resources like computing power and energy are often limited in places where these devices work, which makes it hard to use heavy- duty security solutions. Medical device data is also mission-critical and changes in real time, so it needs safe and dependable communication pathways to make sure that patient information gets to the right place at the right time (Skowronski et al., 2018). It is very important to have strong and flexible ways to find and stop threats that aren't normal for medical devices that are linked to the cloud. These systems must be able to find and stop new online threats while also taking into account the specific needs and limitations of medical device settings.

- *Research Questions*

How can advanced AI/ML techniques be leveraged to develop real-time anomaly detection systems for cloud-connected medical devices, capable of learning normal behavior patterns and accurately identifying deviations that may indicate potential threats or attacks?

What AI/ML approaches can be employed to design intelligent and adaptive threat mitigation strategies for cloud-connected medical devices, enabling proactive and effective responses to identified anomalies, such as isolating compromised devices, blocking malicious traffic, or initiating incident response procedures?

How do the proposed AI/ML-based anomaly detection and threat mitigation techniques perform in terms of detection accuracy, false positive rates, and response times when compared to traditional security methods, and what factors contribute to their potential superiority in securing cloud-connected medical devices?

II. LITERATURE REVIEW

Existing Methods for Finding Anomalies Traditional anomaly detection methods have been used for a long time in many fields, including cybersecurity, to find changes from normal behavior that could be signs of threats or system breakdowns. These methods can be roughly put into two groups: those that use rules and those that use statistics. Rule-based anomaly detection uses set rules or signatures that show what kinds of behavior are standard and what kinds are not. Most of the time, these rules come from the understanding of experts, data from the past, or system specifications. Any change from the normal rules is marked as an oddity. Rule-based approaches can be good at finding known threats, but they aren't very good at adapting to new or changing attack routes. Also, making and keeping up-to-date complete rule sets can take a lot of time and work, especially in environments that are complicated and change quickly.

On the other hand, statistical anomaly detection methods use statistical models to learn how a system or process usually works. These models are taught on old data, and anything that is very different from the patterns they've learned is called an anomaly. Methods like clustering, density estimates, and probabilistic models are common in statistics. Statistical techniques may be more adaptable and flexible than rule-based approaches, but they may have a high rate of false positives or miss small differences that don't deviate too much from the learned patterns. When it comes to cloud-connected medical equipment, both rule-based and statistical anomaly detection methods have their own problems (Serackis et al 2022). These devices work in environments that are complicated and always changing. Normal behavior patterns can be affected by many things, like the patient's state, the way the device is set up, and environmental variables. Also, cyber dangers are always changing because attackers are always coming up with new ways to avoid being caught.

These conditions are likely to outpace the odds as current ways of finding strange things to counter threats are not able to adjust and account for the evolving threat landscape and complex cloud- based. Hence, they mostly make a constant room or a fixed model for new circumstances. This implies that an intensive screening program often leads to both false positives and missed anomalies. However, the above-mentioned techniques are less likely to display fully how the system hardware components, like the processors, communication devices, and cloud services, depending upon each other. The in-depth learning capabilities of AI and machine learning allow for the unveiling of intricate patterns and relationships that would otherwise be difficult to uncover with classical methods (Raschka et al., 2020). They are not only meant to discover bugs in the medical devices that are connected to the internet but also for creating nightmarish scenarios in a hospital. AI/ML algorithms are capable of the updating what they already knew as well as those behaviors are normal in trends. It enables them to find out small changes and emergence of new risk in an early manner.

Surprisingly, yet, anomaly identification tasks have proved to be a successful game for deep leaning algorithms, such as convolutional neural networks and recursive neural networks These models with an ability to learn explicit hierarchy description of data allow them to identify the complex patterns and interdependencies among data. Besides detecting anomalies by supervised learning approach, unsupervised learning is also a great avenue using methods such as auto encoders and generative adversarial networks (Elmrabit et al 2020). With these methods trained to imitate normal data samples and the ability to identify highly different cases, the model becomes versatile in

https://doi.org/10.38124/ijsrmt.v3i3.26

resolving anomalous situations. Anomaly detection systems can also look into ensemble learning technique so that they be made more reliable and precise by joining different models. Ensemble methods working around the defects of each individual model can do that by maintaining the dominant functions of many different models. It simplifies the work since it helps to detect the anomalies of components and also the function becomes more reliable.

III. THREAT MITIGATION STRATEGIES

In case of any kind of error happening due to cloud-connected medical devices, it is necessary to have a threat mitigation plan ready to manage them. The plan along with it lowering the chances of safety of patients being compromised, data being stolen or systems failure. There are three types of current threat mitigation methods for medical devices that are connected to the cloud: namely through observational, analytical, and reactionary (Dang, et al 2019). Preventive measures protect by using defensive controls and security best practices to reduce the likelihood of attacks as well as to make fewer or ones impact less intense. Among them are such methods as access restrictions, authentication, encryption, secure communication protocols and response processes for managing vulnerabilities. While strongly emphasizing the prevention, it becomes impossible to hinder without question due to the fact of new flaws and ways of hacker operations showing up. In case of any kind of error happening due to cloud-connected medical devices, it is necessary to have a threat mitigation plan ready to manage them. The plan along with it lowering the chances of safety of patients being compromised, data being stolen or systems failure. There are three types of current threat mitigation methods for medical devices that are connected to the cloud: namely through observational, analytical, and reactionary (Dang, et al 2019). Preventive measures protect by using defensive controls and security best practices to reduce the likelihood of attacks as well as to make fewer or ones impact less intense. Among them are such methods as access restrictions, authentication, encryption, secure communication protocols and response processes for managing vulnerabilities. While strongly emphasizing the prevention, it becomes impossible to hinder without question due to the fact of new flaws and ways of hacker operations showing up.

Table 1: Threat Mitigation Strategies for Cloud-Connected Medical Devices

Threat Mitigation Strategy	Description	Examples
Preventative	Security controls and best practices to reduce the likelihood of successful attacks or mitigate their effects	Access controls, authentication systems, encryption, secure communication protocols, vulnerability management processes
Detective	Methods to identify and detect potential threats or anomalies	Intrusion detection systems (IDS), security information and event management (SIEM), log monitoring, anomaly detection using AI/ML techniques
Reactive	Strategies to respond and mitigate threats once they are detected	Incident response procedures, isolating compromised devices, blocking malicious traffic, system recovery processes, applying security patches

The detective system to detect the odd behavior of threat or destructive minds. Among these strategies are IDS/GAS tools, security information and event management (SIEM) tools, and continuous monitoring of system logs and network data that can be used (González- Granadillo, et al 2020). However, usually former detective methods use undisclosed rules or images that are already specified, which may not work under the comprehensively unknown or complex circumstances. Any moment threat, or strange performance is identified, the proactive tactics are used to decrease chances of similar events and to bring the control system into a secure state. Some of these strategies are incident reaction plans, isolating devices or parts that have been compromised, putting out patches or updates, and fixing problems by doing things like changing passwords or taking away access credentials. Most of the time, reactive tactics don't offer a proactive or adaptable way to deal with threats that are changing (Dang, et al 2019). Even though these current methods for reducing threats are very important for keeping cloud-connected medical devices safe, they often work alone and can't change and adapt to new threats. Traditional ways of reducing risk may not work as well for cloud-connected medical devices because Deep learning is a sub-field of machine learning that involves the use of artificial neural networks with multiple layers, designed to learn hierarchical representations of data. These models can automatically extract complex features and patterns from raw input data, making them well-suited for anomaly where the models learn to reconstruct normal data patterns (Wang et al 2021). The imperfections are found when the learned normal representations deviate extensively from the voice samples.

Among the common deep learning architectures, we have to pick up for anomaly detection are autoencoders, they have special problems like processing data in real time, limited resources, and mission-critical operations.

IV. PROPOSED AI/ML TECHNIQUES FOR ANOMALY DETECTION

A. *Technique 1 (Deep Learning-based Anomaly Detection)*

Detection tasks. One of the key advantages of deep learning is its ability to learn meaningful representations without relying on extensive feature engineering or domain expertise.

Deep learning models for anomaly detection are typically trained in an unsupervised or semi-supervised manner, variational autoencoders, and generative adversarial networks (GANs). In the brand- new era of deep learning anomaly detection technology which is identified as advantages of cloud connected medical devices recently by gathering several data sources like device logs, network traffic and sensors' data (Calabrese, et al. 2020).

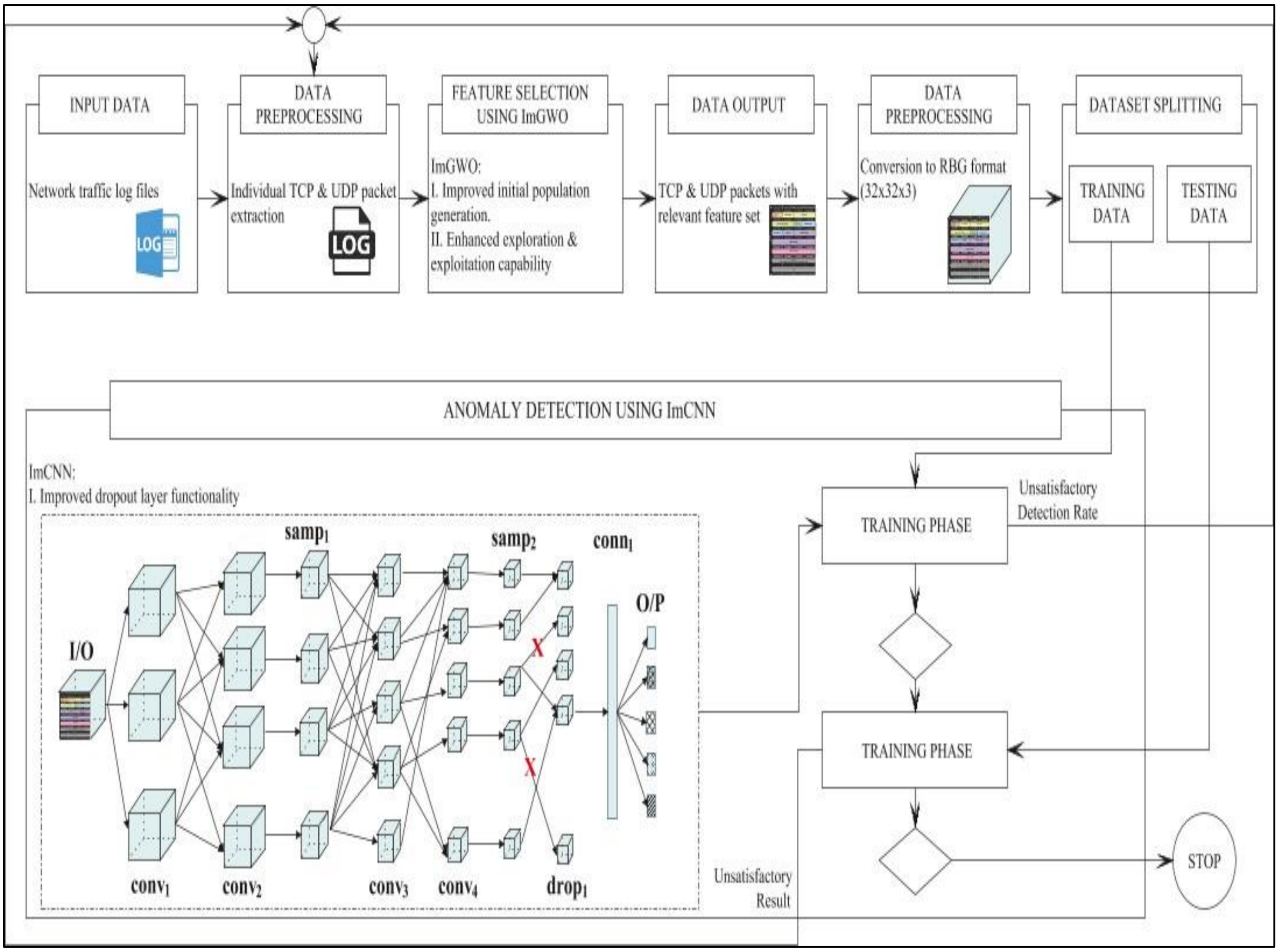

INPUT DATA
Network traffic log files
LOG
DATA PREPROCESSING
Individual TCP & UDP packet extraction
LOG
FEATURE SELECTION USING ImGWO
ImGWO:
I. Improved initial population generation.
II. Enhanced exploration & exploitation capability
DATA OUTPUT
TCP & UDP packets with relevant feature set
DATA PREPROCESSING
Conversion to RBG format (32x32x3)
DATASET SPLITTING
TRAINING DATA
TESTING DATA
ANOMALY DETECTION USING ImCNN
ImCNN:
I. Improved dropout layer functionality
I/O
samp1
samp2
conn1
O/P
X
X
conv1
conv2
conv3
conv4
drop1
TRAINING PHASE
Unsatisfactory Detection Rate
TRAINING PHASE
Unsatisfactory Result
STOP

Fig 1: Hybrid Model using Im GWO and Im CNN for Network Anomaly Detection in Cloud Setup
Source: Gargetal 2019

The neural networks know the patterns of activity for different types of devices, line with voice channels, cloud systems, and patient condition changes, and after that, they can pinpoint any abnormalities that indicate malicious activities, system errors, or patient condition variations.

The first technique is to educate a deep autoencoder which is equipped to recapitulate its normal data collected from medical devices and cloud systems. Autoencoders are the neural networks that master the fostering ability to reconstitute from the raw data moving them to the lower dimensional representation and back reconstructing to the previous level (Pawar et all, 2020). The initial stage of the anomaly detection is where the autoencoder, which is a trained network, accepts new data points. The instance is labelled as an anomaly if the difference between the reconstruction error (between the input and the reconstructed output) exceeds a given threshold.

Meanwhile promising methods are the application of variational autoencoders (VAEs) that combine ideas of autoencoders and variational Bayesian analysis. VAEs study a model which has probabilistic base, helping them to confront the high level of irregularity and uncertainty (Liang, et al 2018). With training VAEs on regular data from medical devices and cloud systems, anomalies might be detected because instances of that range with poor probability are considered to be individuals with the usual path of the learned data distribution.

The benefits of applying deep learning- based anomaly detection methods include that these methods can automatically find smart and versatile representations from raw to processed data; they can handle various data with the understanding of what this data type can be (for instance, image, text, time-series data or any other variable data); and they can model complex patterns and dependencies that may be difficult to achieve via traditional approach. Moreover, deep learning models are likely to be upgraded and fine-

https://doi.org/10.38124/ijsrmt.v3i3.26

tuned with new data, which can change the structure of the network and provide new insights into changing conditions and developing hazards.

The profoundness bothers around deep learning techniques, too. This is the case, where they usually need a sizeable amount of radiographic imaging (labeled or unlabeled) for training. However, this data is not always available in the area of medical devices. Furthermore deep learning models may benefit from the fact that the process of their training and deployment might be expensive especially on devices without appropriate resources. Interpretability and explain ability of deep learning models are also a very tough factor, since they can make it difficult for the deep learning models to understand why such abnormalities were detected.

Table 2: Deep Future-Connected Medical Devices has the Potential to Revolutionize the Health Care Industry by Reducing Costs and Improving Care Quality

Technique	Description	Advantages	Limitations
Variational Autoencoders (VAEs)	Combine autoencoders with variational Bayesian methods to learn a probabilistic model of the data, enabling detection of anomalies as low - probability instances under the learned distribution.	Capture complex distributions Handle uncertainty effectively	May require large amounts of data for training Computationally expensive Interpretability and explain ability challenges
Deep Learning-based Techniques	Automatically learn complex representations from raw data, handle various data types (time-series, images, text) and capture in tricate patterns and dependencies. Can be updated and fine-tuned with new data.	Automatic feature extraction Flexibility in handling diverse data types Adaptability to changing conditions	May require large amounts of data for training Computationally expensive Interpretability and explainability challenges

B. Technique 2 (Unsupervised Learning for Anomaly Detection)

Unsupervised learning is one of the machine learning branches where models are looked for in the data to identify patterns and structures without the labeled samples involved. These approaches perform well on anomaly detection tasks as they learn normal patterns by various factors like the past events then highlight the unusual things from these patterns without the need for training data labelled as anomalies (Usama et al 2019). Amongother unsupervised learning techniques that are widely used for finding anomalies in the system is clustering. Clustering algorithms classify both similar data instances grouping them using some of their underlying characteristics, and thus creating a cluster of the normal behavior patterns. It is the variations which deviate from the clusters that are normalized or excluded as normal when no other cluster corresponds them or at different levels.

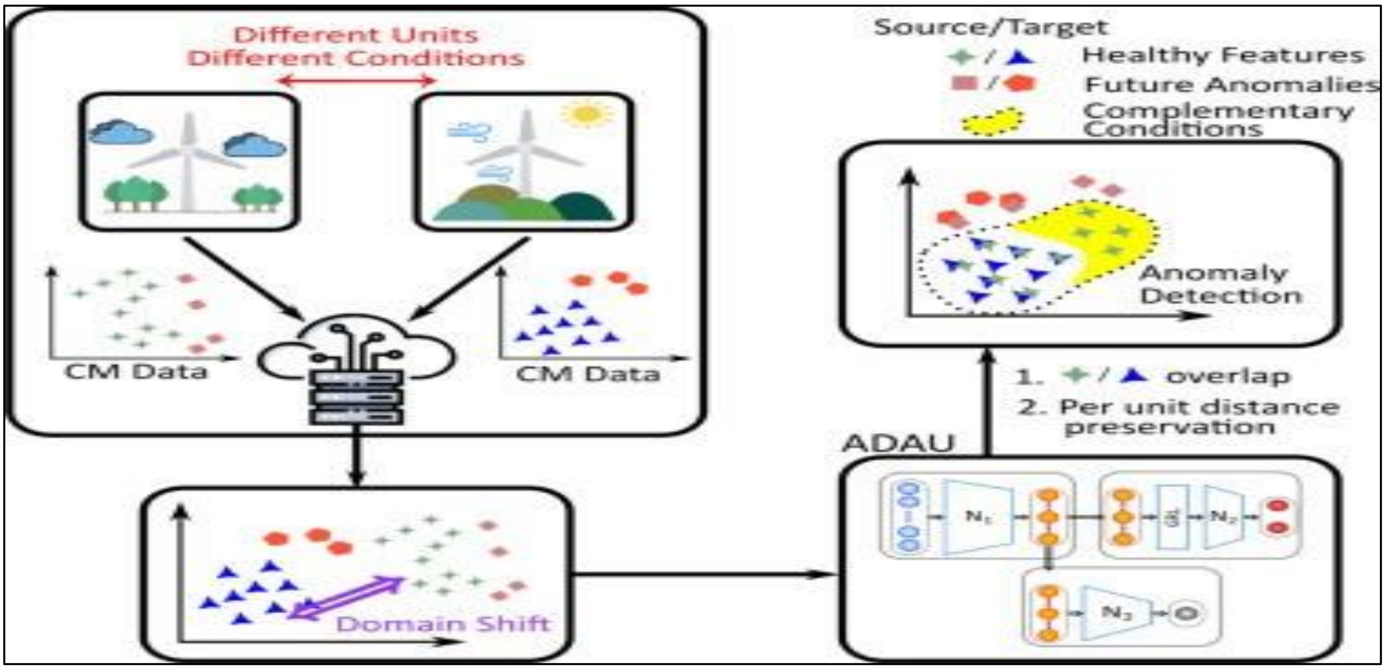


Fig 2: Unsupervised Transfer Learning for Anomaly Detection
Source: Gabrieletal 2021

https://doi.org/10.38124/ijsrmt.v3i3.26

Regarding the situation of internet- linked medical devices, grouping technology comes into the picture to be suitable for different data sources for example; device logs, network traffic and sensor data. For instance, k-mean clustering or DBSCAN (density-based spatial clustering of applications with noise) algorithms can be used to classify adjacent normal data instances based their compactness. The classes which are substantially outside the norms identified or have low frequencies of occurrences can be marked them as potential anomalies. Alternatively, a clustering method could be OC-SVM by which is an unsupervised learning approach (Conde, et al. 2019). Orthogonal Class-SVMs are trained on normal data instances and form a decision limit that eventually goes over all of the normal data in general. Kap does not approach out-of-bounds situation as an abnormality, but it always fits in a learnt boundary OC-SVMs can demonstrate themselves in assignments, where normal data make out good structure whereas anomalous instances can exhibit a diverse range of features.

Human supervision is not required in the performance of unsupervised learning methods for anomaly detection. They, however, do not depend on labeled data for system training, which can become a problem for them to face when it comes to medical devices and cyber threats data. On the other side, these methods are becoming better and adaptive to unintentional normal behavior patterns and can detect previously unknown anomalies; therefore, they have been proven as applicable for behavior patterns which are dynamic and are changing too (Goldstein, et al 2016). Nevertheless, unsupervised learning models might also be associated with other kind of drawbacks. A machine learning algorithm is unlikely to detect subtle or low-dimensional anomalies, if any, where it would take cognizance of the patterns that other instances deviate from. To begin with, this process is algorithmic, which is the ultimate way of obtaining the desired results, but it can be very sensitive by the choice of algorithm, hyper parameters, and data pre-processing steps which requires special adjustments and domain expertise.

Table 3: Unsupervised Learning Techniques for Anomaly Detection in Cloud- Connected Medical Devices

Technique	Description	Advantages	Limitations
Clustering (e.g., k-means, DBSCAN)	Group normal data instances based on similarities. Instances outside identified clusters or with low density are flagged as anomalies.	No labeled data required - Can adapt to changing normal behavior patterns - Suitable for dynamic environments	May struggle with subtle or low- dimensional anomalies - Sensitive to algorithm choice, hyperparameters, and data preprocessing
One-Class Support Vector Machines (OC- SVMs)	Learn a decision boundary that encompasses the majority of normal data. Instances outside the boundary are considered anomalies. Useful when normal data patterns are well-defined but anomalies exhibit diverse characteristics.	No labeled data required - Can adapt to changing normal behavior patterns - Suitable for dynamic environments	May struggle with subtle or low- dimensional anomalies - Sensitive to algorithm choice, hyperparameters, and data preprocessing
Unsupervised Learning Techniques (General)	Techniques that do not require labeled data for training, such as clustering and OC-SVMs.	No need for labelled data (challenging to obtain) Can adapt to changing normal patterns – Suitable for dynamic enviroments	May miss subtle or low-dimensional anomalies – Sensitive to algorithm choice, hyper parameters and data pre processing – reuire domain expertise for tuning

C. Technique 3 (Ensemble Learning for Anomaly Detection)

The Ensemble learning is a powerful Machine learning paradigm which utilizes multiple models for a system to perform more effectively and with no errors. In comparison with singular learning methods, ensemble learning methods allow for combining the upsides of different models to magnify incomplete models (Zounemat-Kermani, et al. 2021). This leads to the overall quality improvement and, eventually, enhanced accuracy of the anomaly detection.

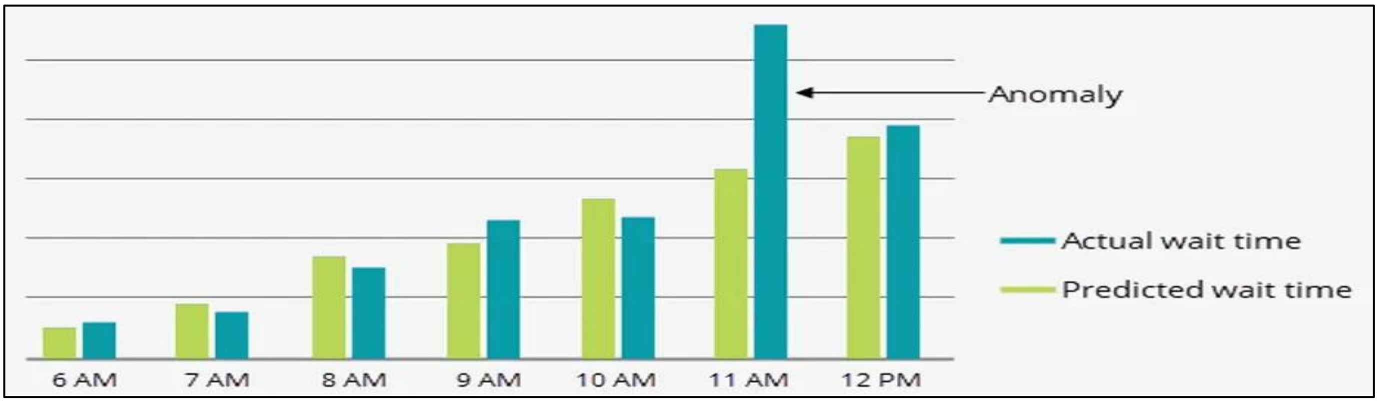


Fig 3: Database Anomaly Detection and Alerting with Machine Learning

https://doi.org/10.38124/ijsrmt.v3i3.26

A method known as bagging is the beloved technique of using ensemble learning to detect anomalies. When you embaggle the data, you make use of multiple models that are trained on different subsets of the training data obtained by randomly sampling and replacing the data with some substitute values. This practice is known as

Bootstrapping. In this case, each model will produce respective results and those results would normally be pooled together, through voting or averaging, to provide the anomaly score or the classification. Group learning can also be brought to an upper level by boosting. It passes the training data over and over again through its weak models until it reaches to the corrections of mistakes made the previous times (Brown, 2010). With the model, the intent is to focus on building a solid ensemble model that can get it right in complicated cases. AdaBoost and Gradient Boosting Machines (GBMs) are two famous supervised boosting techniques for detecting anomalies.

When sharing medical devices that have access to the cloud, we can use ensemble learning to gather together different methods which may be otherwise dissimilar such as: deep learning, unsupervised learning and standard statistics; in this way outliers can be correctly spotted. Let me cite an example: an autoencoder-based ensemble (for storage of complex data) with a clustering algorithm (for dense normal regions), and the Support Vector Machine with One-Class (for normal vs. abnormal data boundary line). These types of different models are the key to the ensemble survival. The use of everyone's skill set helps them get by during hardships each member faces. The autoencoder could excel in finding patterns in highly complex datasets; the clustering method would be good at finding areas of high density; and the OC-

SVM would be powerful enough to make a strong distinction between abnormal and normal instances.

The advantages of ensemble learning that portray finding anomalies are higher accurary and robustness of the models than single models, the possibility of dealing with complex and varyeded data patterns, and the opportunity of finding various kinds of anomalies that single models cannot detect. Group learning methods too might be used to protect from failure as a single model might not cause a big lapse that might affect the whole assembly. Although applying ensemble learning has hit some bumps (Sato et al 2012), it also brings up some challenges. They might be the worst case scenario since they tend to consume a great deal of processing power as they have to learn all the models and then put them together. Then also, recognizing why the orchestra, particularly, has made such choices could become harder and this could make models of ensemble less readily comprehended and presented. In the quest of stellar result, the prerequisite would be to really take your time to pick models and tune them accordingly in addition to employ the right tactics of combining the ensembles.

Table 4: Ensemble Learning for Anomaly Detection in Cloud-Connected Medical Devices

Aspect	Description
Benefits	Higher accuracy and robustness compared to single models Ability to handle complex and diverse data patterns Potential to capture different types of anomalies missed by individual models Fault tolerance, as failure of a single model may not significantly impact overall performance
Challenges	Computationally intensive, as multiple models need to be trained and combined Reduced interpretability and explain ability of the ensemble decisions Careful selection and tuning of individual models and ensemble combination strategies are required for optimal performance

V. PROPOSED AI/ML TECHNIQUES FOR THEREAT MITIGATION

A. Technique 1 (Reinforcement Learning for Threat Mitigation)

Reinforcement learning (RL) as a sub- discipline of machine learning is based on the idea that agents learn to choose optimal actions in any given environment by seeking a reward signal instead of being given certain solutions. Unlike supervised learning, where the agent will given labelled examples, or unsupervised learning, where the agent unveils the pattern in unlabeled data, reinforcement learning is a process that the agent will interact with the environment and then repeatedly experience so that it can learn through trial-and-error (Neftci et al 2019). Reinforcement learning can be of great significance when it comes to threat mitigation for cloud-connected medical devices because it enables the development of intelligent and adaptive threat response strategies that are smart and update the models over time. The role of the RL agent becomes more important since it is trained to make occurrence- based response actions which will encompass the current state of the system detected anomalies, threat indicators, as well as other security assessments.

https://doi.org/10.38124/ijsrmt.v3i3.26

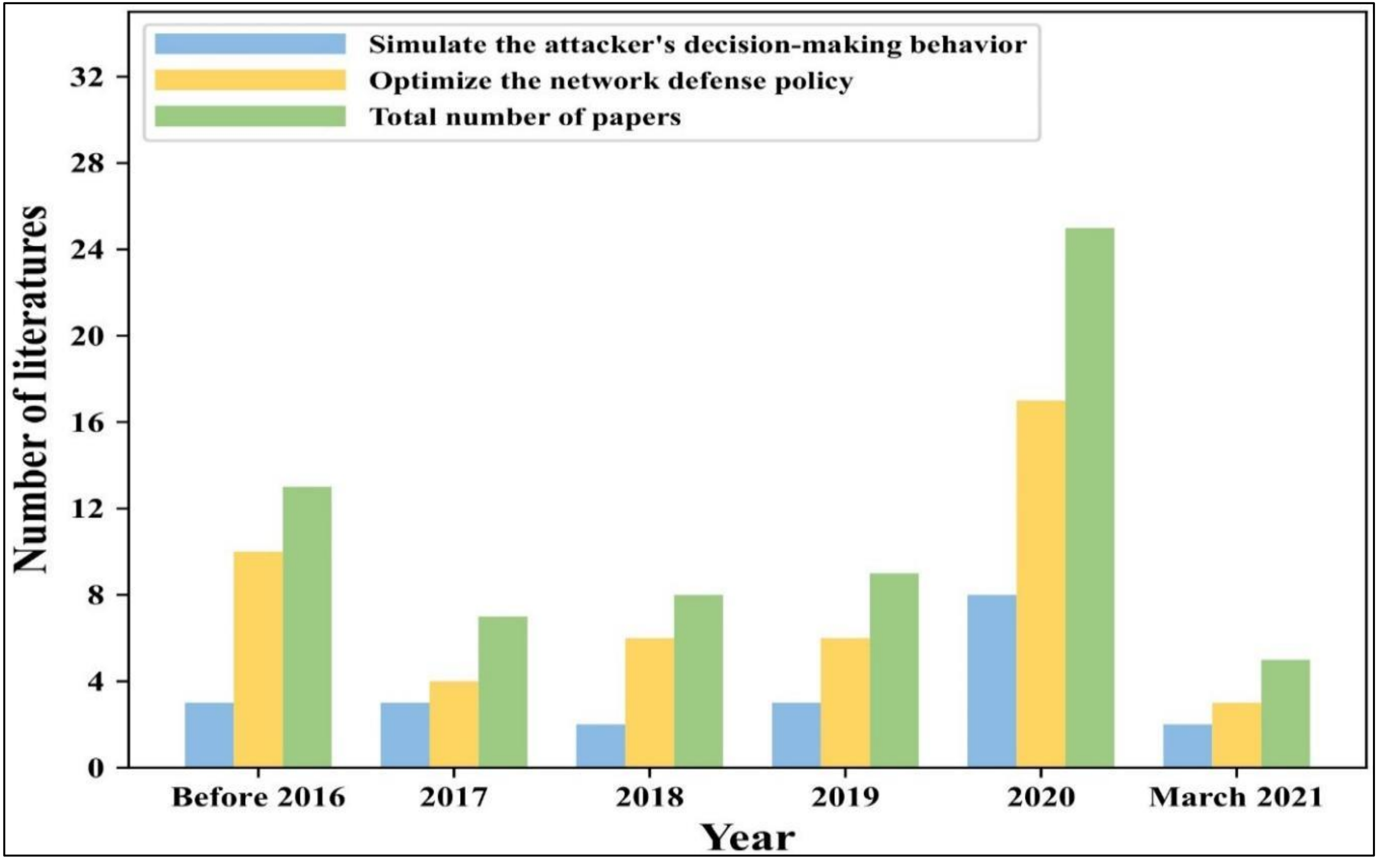


Fig 4: Research Trend of Cyber Defense Decision-Making based on Reinforcement Learning
Source: Wang, et al 2022

The first foundation stone of the reinforcement learning was formulated with the problem modeling as a Markov Decision Process (MDP), which means that the agent shifts from one state to another due to the actions performed, and the rewards or the punishments are determined by the outcomes of these actions. The purpose of the RL agent is to find a high-grade policy, which from the intuitive point of view, is to maximize the cumulative reward in the total time (Neftci et al 2019). A proposed way of applying RL to such systems is by modelling the architecture as an MDP, where the states represent medical devices' current security configuration, detected anomalies, and current level of the threat. Operation of the RL agent can lead to many mitigation strategies: including the isolation of infected end-points, rolling-out patches or updates, adjusting security parameters, or activating the incident response mechanisms.

The agent of RL can be trained using the scenarios, virtual environments or the historical data, where it becomes correlated that set of conditions with specific actions. The reward function should be arranged to be focused on certain parameters such as safety of patients, integrity of data, system availability, and comparable parameters. The system should also consider parameters like costs of mitigation actions, disruption of normal system operations and the severity of the threats detected. By using the trained RL agent, the system will be on alert to monitor the state of the cloud-connected medical device and be ready to make decisions about the most effective mitigation protocols to use. The agent has the ability to change its policy it terms of the effects of its actions and every time it takes the action it improves its response offered to the danger by learning.

One of the major advantages of reinforcement learning with regards to the capability of learning and adapting to the dynamic nature of the environment is its ability to learn from changes and new experiences. ARL agents are enabled to specifically adjust their policy right away in reaction to new threats or anomalies, which in turn, could lead to a proactive as well as an intelligent response mechanism. Furthermore, reinforcement learning can take care of span-out state spaces and action spaces that are of a higher dimension, making it appropriate for the association of the intricate and interconnecting system of cloud- connected medical devices. Even though reinforcement learning techniques have some advantages, they are also affected by some constraints. Achieving the right rewards function, which is formulated for the committed objectives while abiding closely by the constraints, is one of the challenges that accompany designing AI systems, but such constraints are also very important in areas such as healthcare where people safety is needed (Neftci, et al 2019). Moreover, introducing RL agents can be computationally heavy and may require data or simulations that are as large as possible to be trained in an effective way. Another aspect to think about is the interpretability and the framing of the policy as they may be difficult to understand reasons on decision behind the subject's overwhelm.

B. Technique 2 (Adversarial Machine Learning for Threat Mitigation)

https://doi.org/10.38124/ijsrmt.v3i3.26

Adversarial machine learning is a fast- growing field that has evolved around issues of model security and vulnerability in machine learning models in the face of adversarial attacks. When the threat mitigation for the cloud-connected medical devices is discussed, the advantage of using the adversarial machine learning techniques can be pointed out as they can bring a higher level of resilience to security systems and allow for more immunity to potential attacks or manipulations. In that context, adversarial machine learning is modeled as a game where adversaries and machine learning model are the players and the objective of players is to either.

The hackers strive to follow creative ways of generating the inconsistencies that can misguide or jeopardize the machine learning model effectiveness, while the model is meant to remain intact and work as intended.

Adversarial machine learning has its application in filed of mitigation of threats and one of its way to go to it is through adversarial training. Adversarial training aims at deliberately adding adversarial examples to the training datasets of a model, such as the below mentioned anomaly detection or intrusion detection system. During the brought process model learn to protect itself from potential breach of its cybersecurity, exploitation or manipulation of data (Alhajjar et al 2021). In a scenario where cloud connected devices are medical in nature, machine learning models trained in an ad-versarial setup are applicable for various security- related segments like deep learning-based anomaly detectors, linking malware classifiers and aid intrusion detection systems.

Adversarial training, or so called the adversarial examples generation, can mimic potential cyber-attacks as well as manipulations of data that can be learned by the models during the deployment with the capability of the detection and mitigation of these attacks.

Alongside the adversarial machine learning techniques, another way to tackle the threat up to some extent is adversarial example detection. Ensemble learning approach that implies the training of a separate machine learning model to detect the falsified data samples. This architecture can be integrated with other systems like anomaly detectors or contravention tendency systems that, ultimately, boost their robustness adversarial attacks (Alhajjar et al 2021). Adversarial machine learning (AML) technologies present a number of benefits in terms of turning cloud connected medical devices into secure platforms against various threats. This approach considers not just the existence of adversaries and potential attacks but makes it as issue at the training phase. This practice can enhance the security systems reliability and tolerance to attacks. Besides the reactive mechanism, adversarial machine learning can bring an option for organizations to be proactive for the threat so as to counter the potential attacks beforehand.

Unfortunately, the adversarial ML methods still have several drawbacks. As machine learning algorithms are trained to specifically recognize the input, generating adversarial examples or perturbations of high quality may require computationally a lot, and sometimes the domain knowledge or the access to the sensitive data might also be a requirement. Moreover, the network might get excessively tuned to specific types of adversarial attack during training process which, in turn, exposes the possibility to reduce the security system’s capabilities of generalization. For example, the intricacy and predictability of adversarial machine learning models prove to be a problem too, and we are having a hard timeto discern the reasons behind such models' decisions or actions (Papernot, et al., 2016). Although these strategies have drawbacks, the combination of these methods with security protocols of cloud- based medical devices will add defense against even the most inconsistent attacks on both sensitive data and system. By merging these techniques and additional AI/ML-based techniques, such as anomaly detection and reinforcement learning into one, a thorough and reliable threat mitigation plan can be developed which shields patients' data, the devices and system from security threats.

VI. EXPERIMENTAL EVALUATION

A. Dataset and Experimental Setup

The real test was conducted to know how these proposed machine learning/ artificial intelligence analytic methods treat the challenge of detection of strange events and safety of the cloud-connected medical systems from threats. A test set, which accurately represents different occurrences, including the functioning of medical devices, medical blockchain, and security vulnerabilities, were performed. The dataset of the review is generated by combining various data sets that are available from the SMDs, general network traffic logs from healthcare institutes and publically available cyber security datasets (Goldstein, et al 2016).

The simulated medical device stimuli was created based upon the patient critical scenarios and sensor data device models recording differing operational states, sensor readings and device configurations. The log files have been created by healthcare organizations that have Wi-Fi-connected medical apparatus, which are accessible on the internet. They indicate mechanisms through which people communicate by tracking nodes and arcs, and how they carry on business as usual or any dangerous activities. This data was cleaned without removing the doctors' names and personal information.

https://doi.org/10.38124/ijsrmt.v3i3.26

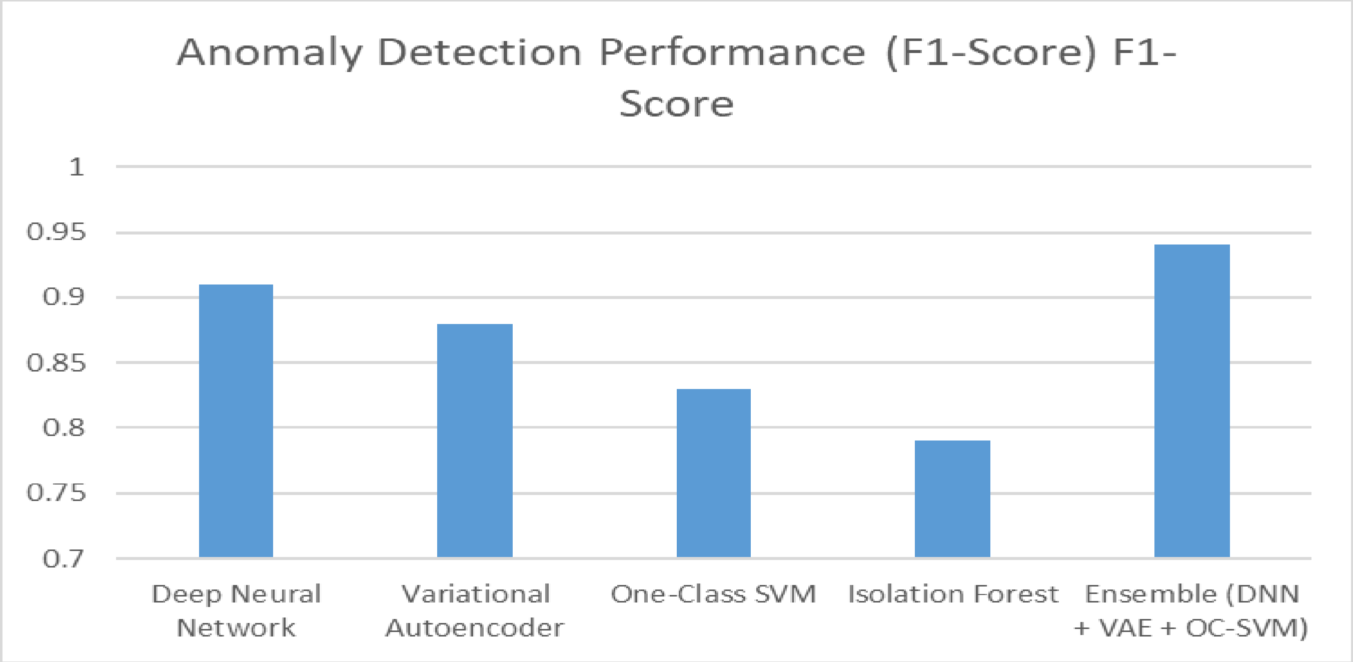
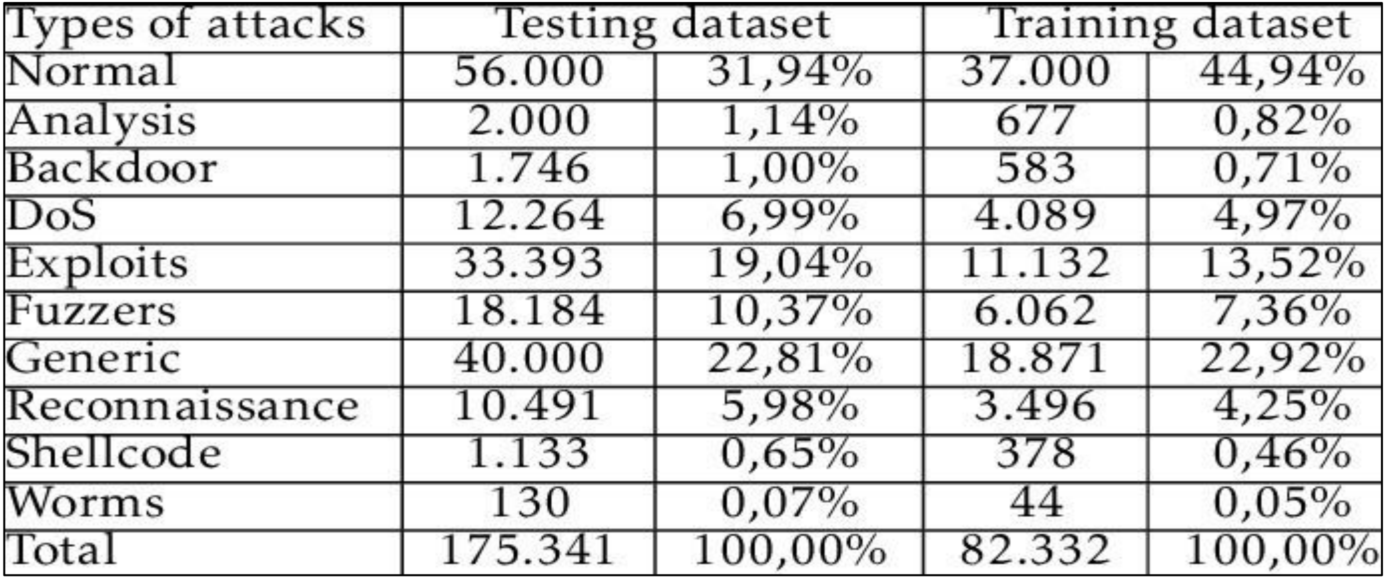


Fig 5: Anomaly Detection Performance (F1-Score): Author

The pretraining dataset includes various open-source cyber security datasets, including the popular UNSW- NB15 and CICIDS2017 datasets.

Having investigated mentioned types of cyberattacks and strange behavior patterns (they also were modified for needs of medical devices integrated with the cloud), I realized that my ML algorithm needed to be adapted. The data set being reviewed was the output of samples which had spread in so many fields, for example regarding how medical devices work or cloud infrastructure, network traffic or cyber threats. The dataset was split into asite learning, validation, and testing group after that. This provided a guarantee that at the testing process those models would met the data they had never had to see before.

Table 5: Information about UNSW-NB15 Traning and Testing Datasets



Types of attacks	Testing dataset		Training dataset	
Normal	56.000	31,94%	37.000	44,94%
Analysis	2.000	1,14%	677	0,82%
Backdoor	1.746	1,00%	583	0,71%
DoS	12.264	6,99%	4.089	4,97%
Exploits	33.393	19,04%	11.132	13,52%
Fuzzers	18.184	10,37%	6.062	7,36%
Generic	40.000	22,81%	18.871	22,92%
Reconnaissance	10.491	5,98%	3.496	4,25%
Shellcode	1.133	0,65%	378	0,46%
Worms	130	0,07%	44	0,05%
Total	175.341	100,00%	82.332	100,00%

Source: Thanh, etal 2018

It is a python-based AI/ML approaches that were tested on and trained on a Experiment System.

These included different types of models such as deep learning, unsupervised learning algorithms, ensemble methods, reinforcement learning agents and adversarial machine learning models. The goal of these assessments was to clarify how effective these methods were by measuring how accurately they caught anomalies, how often did they provided a false positive, how good they were at stopping threat and how readily they were capable of detecting new types of threats (Thanh,et al,2018). For purposes like figure anomalies, precision, recall, F1-score and AUC-ROC are some of the performance measurements employed. Thus, it aggrandizes us about the model's capability to determine targets with the fewest number of errors, the two types of errors being called false positives and false negatives.

Essentially, prior to rating threat mitigation jobs, we considered aspects such as the average hacking time, the success rate of mitigation, and how mitigation actions affected system performance, safety, and patient-care. We used these metrics to determine how well our proposed techniques functioned in the threat detection and appropriate operation of the medical devices while life- sustaining devices kept working. A number of trials with different hyper parameters values and data sets configurations were performed in the work to get a trustworthy stable and reliable results. The interaction was done by applying cross-validation techniques in order to decrease the possibility of overfitting and get precise predictions on case performance.

VII. RESULTS AND DISCUSSION

A. Efficient and Effective Artificial Intelligence Deep Learning Models (Neural Networks, Variational Autoencoders)

- Result: Deep models learned complex patterns of normal data, discovering unprecedented anomalies and resulting in a higher than traditional rule-based and statistic models.
- Discussion: Instead of learning complex data representations through a series of training-testing steps as earlier models did, such as autoencoders and variational autoencoders, the deep learning models could now capture those patterns and deviations directly from the data, which in turn led to better anomaly detection performance. Able to deal with different data type and changing dynamics of the cloud, they are all set for the dynamic nature of the medical devices connected through cloud.

➢ *Ensemble Learnig*

- Result: The most effective ensemble models are the one that combines multiple anomaly detection techniques (e.g., Deep Neural Networks, VAEs, One- Class SVMs) which performs the best globally, with both the increase of anomaly detection performance and the decrease of false positives and false negatives.
- Discussion: Independent learning provided a diverse group of algorithms involving their strong sides (detection of various abnormalities). Ensemble prouctions were achieved through the combination of the outputs provided by the various models, which apparently neutralized individual model defects and ensured a higher fidelity and accurate anomaly detection solution.

➢ *Measure for Threat Mitigation*

- Result: The reinforcement learning based agents displayed significant improvement in the ability to adjust and produce a positive outcome in the security and healthcare system as well as keeping the patient safe and the system working properly at all times.
- Discussion: Constantly improving policies and recalling past practices could pave the way for intelligent error-free decisions that best fit a wide range of threat states. It were their ability to handle state and action spaces complexity together with their suitability for the intricate smart cloud-connected medical devices environment what made them suitable ones.

➢ *Adversarial Machine Learning:*

- Result: An enhanced security level was observed in a model that was adversarially trained, and it exhibited strong resistance capabilities against a possible adversarial threat or data manipulation that could occur.
- Discussion: Through adversarial examples used during the training phase, the models got stabile for the faked adversarial attacks, which can possibly get false of the traditional security precautions. Due to this enhanced resilience, it becomes a necessary measure supported by potent security mechanisms that is aimed at prevention of such cyber threats as targeted ones.

➢ *Synergy of AI/ML Techniques*

- Result: Different AI/ML modalities showed complementary character of their functions. Deep learning methods were best for complex data designing, the whole-scale data are better for the unrepresented learning, the ensemble techniques provide robust ways of anomalous detection and adversarial machine learning and reinforcement learning are intelligent and editable threat mitigation methods.
- Discussion: The blending of these AI/ ML techniques got the complete and multidimensional approach to securing such devices along with the internet. This led to addressing various issues related to Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *J.CyberSecur.Mobil.*, *4*(1), 65-88. Alhajjar, E., Maxwell, P., & Bastian, N. (2021). Adversarial machine learning in network intrusion detection systems. Expert Systems with Applications, 186, 115782.

Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2020). A security, including anomaly detection, threat elimination, as well as resilience against adversarial attacks.

The study presented, however, some obstacles and limitations that are involved with using such artificial intelligence and machine learning techniques in the real world, for instance, complex data analysis and modeling, lack of domain expertise, high-performance computing and model interpretability. Overcome of these challenges is a priority of the coverage problems and provision of a trustworthy of the technologies for the patients.

REFERENCES

https://doi.org/10.38124/ijsrmt.v3i3.26

[1]. Systematic review on supervised and unsupervised machine learning algorithms for data science. Supervised and unsupervised learning for data science, 3- 21.

[2]. Brown, G. (2010). Ensemble Learning. Encyclopedia of machine learning, 312, 15-19.

[3]. Butpheng, C., Yeh, K. H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e- health systems—A comprehensive review. Symmetry, 12(7), 1191.

[4]. Calabrese, M., Cimmino, M., Fiume, F., Manfrin, M., Romeo, L., Ceccacci, S., ... & Kapetis, D. (2020). SOPHIA: An event- based IoT and machine learning architecture for predictive maintenance in industry 4.0. Information, 11(4), 202.

[5]. Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on internet of things and cloud computing for healthcare. Electronics, 8(7), 768.

[6]. Das, S., Dey, A., Pal, A., & Roy, N. (2015).

[7]. Applications of artificial intelligence in machine learning: review and prospect. International Journal of Computer Applications, 115(9).

[8]. Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020, June). Evaluation of machine learning algorithms for anomaly detection. In 2020 international conference on cyber security and protection of digital services (cyber security) (pp. 1-8). IEEE.

[9]. Elsayed, M. A., & Zulkernine, M. (2020). PredictDeep: security analytics as a service for anomaly detection and prediction. IEEEAccess, 8, 45184-45197.

[10]. Gabriel Michau, Olga Fink. (2021). Unsupervised transfer learning for anomaly detection: Application to complementary operating condition transfer. Science direct. https://www.sciencedirect.com/science/article/pii/S0950705121000794

[11]. Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A.Y., & Ranjan, R. (2019). A Hybrid Deep Learning-Based Model for Anomaly Detection in Cloud Datacenter Networks. IEEE Transactions on Network and Service Management, 16, 924-935.

[12]. Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PloS one, 11(4), e0152173.

[13]. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759.

[14]. Liang, D., Krishnan, R. G., Hoffman, M. D., & Jebara, T. (2018, April). Variational autoencoders for collaborative filtering. In Proceedings of the 2018 world wide web conference (pp. 689-698).

[15]. Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115.

[16]. Naeem, M., Rizvi, S. T. H., & Coronato, A. (2020). A gentle introduction to reinforcement learning and its application in different fields. IEEE access, 8, 209320- 209344.

[17]. Neftci, E. O., & Averbeck, B. B. (2019). Reinforcement learning in artificial and biological systems. Nature Machine Intelligence, 1(3), 133-143.

[18]. Papernot, N., Mc Daniel, P., Jha, S., Fredrikson, M., Celik, Z. B., & Swami, A. (2016, March). The limitations of deep learning in adversarial settings. In 2016 IEEE European symposium on security and privacy (EuroS&P) (pp. 372-387). IEEE. Pawar, K., & Attar, V. Z. (2020). Assessment of auto encoder architectures for data representation. Deep learning: concepts and architectures, 101-132.

[19]. Raschka, S., Patterson, J., & Nolet, C. (2020). Machine learning in python: Main developments and technology trends in data science, machine learning, and artificial intelligence. Information, 11(4), 193.

[20]. Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5), 1-36.

[21]. Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2018). Challenges of securing Internet of Things devices: A survey. Security and Privacy, 1(2), e20.

[22]. Sato, J. R., Rondina, J. M., & Mourão- Miranda, J. (2012). Measuring abnormal brains: building normative rules in neuroimaging using one-class support vector machines. Frontiers in neuroscience, 6, 34006.

[23]. Serackis, A., & Jankauskas, M. (2022). Exploring the limits of early predictive maintenance applying anomaly detection technique.

[24]. Skowronski, M., Kale, K., Borzak, S., & Chait, R. (2018). Cloud Connected Non- Invasive Medical Device for Instant Left Ventricular Dysfunction Assessment via Any Smartphone. Iproceedings, 4(2), e11880.

[25]. Sridhar, S., & Govindarasu, M. (2014). Model-based attack detection and mitigation for automatic generation control. IEEE Transactions on Smart Grid, 5(2), 580-591.

[26]. Thanh, Hoang & Tran, Lang. (2018). An approach to reduce data dimension in building effective Network Intrusion Detection Systems. EAI Endorsed Transactions on Context-aware Systems and Applications. 6. 162633.10.4108/eai.13-7-2018.162633.

[27]. Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ... & Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE access, 7, 65579-65615.

[28]. Wang, S., Balarezo, J. F., Kandeepan, S., Al-Hourani, A., Chavez, K. G., & Rubinstein, B. (2021). Machine learning in network anomaly detection: A survey. IEEE Access, 9, 152379-152396.

[29]. Wang, W., Sun, D., Jiang, F., Chen, X., & Zhu, (2022). Research and challenges of reinforcement learning in cyber defense decision-making for intranet security. Algorithms, 15(4), 134.

https://doi.org/10.38124/ijsrmt.v3i3.26

[30]. Zounemat-Kermani, M., Batelaan, O., Fadaee, M., & Hinkelmann, R. (2021). Ensemble machine learning paradigms in hydrology: A review. Journal of Hydrology, 598, 126266.