AI-based Cybersecurity Attacks and Countermeasures in IoT Environment: A Survey .

Fatimah Alakeel[1*], Rehab Alfallaj[2], Hanan Alshehri[3], Ali Almousa[4].

1. Department of Computer Science and Engineering, King Saud University, Kingdom of Saudi Arabia; Fyalakeel@ksu.edu.sa

2. Department of Computer Science and Engineering, King Saud University, Kingdom of Saudi Arabia; ralfallaj@ksu.edu.sa

3. Researcher, Kingdom of Saudi Arabia, hanan_alshehri@outlook.com

4. Computer Engineering, Department King Fahd University of Petroleum and Minerals, Kingdom of Saudi Arabia, 2160004188@iau.edu.sa

Abstract

The Internet of Things (IoT) has been considered an innovative integrated solution that opened opportunities for intelligent appliances to communicate over the Internet. However, IoT suffers from various cybersecurity threats because of its openness and the constraints of the used devices that share substantial amounts of classified information. Artificial intelligence (AI) is an effective key technology in solving cybersecurity issues. Cybercriminals are adopting AI techniques to conduct sophisticated attacks on IoT environments. Precise and elusive attacks across various applications have exemplified the deliberate employment of artificial intelligence for malicious intentions. Threat actors are constantly changing and improving their attack strategies with particular emphasis on applying AI-driven techniques in the attack process, called AI-based cybersecurity attacks, which can be used with conventional attack techniques to cause considerable damage. Moreover, AI techniques can be utilized in cyber-attack countermeasures and have proven effective. Unfortunately, these types of attacks and countermeasures have not been investigated enough in the existing literature. This paper surveys the current studies of AI-based cybersecurity attacks and countermeasures in the IoT environment. The aspects captured by this paper highlight future research in this field and will assist in recognizing the power and impact of using AI in cybersecurity, especially in the IoT environment.

Keywords:

Artificial Intelligence-based attacks, Internet of things (IoT), IoT security, cybersecurity and AI, AI-based cyber-attack, Attacks.

1. Introduction

IoT devices have become our all-time companions as technologies emerge and play a crucial role in our day-to-day lives. Millions of IoT devices, embedded systems, and applications have enhanced our lives, making them more accessible, faster, productive, convenient, and, most importantly, automated. It is expected that from 2023 to 2025, the number of IoT devices will rise from approximately 14.4 billion to 27 billion active devices[1]. However, the booming demand for the technologies poses many major security issues in our day-to-day activities and critical infrastructures. Cybercriminals are adopting

AI techniques to conduct sophisticated attacks on IoT networks [1].

Thus, this paper's main objective is to survey the studies found in the literature investigating AI-based cybersecurity attacks and countermeasures in IoT environments where AI techniques, such as machine learning and deep learning, are used. The survey targets the efforts from 2018 until 2023. Almost 80+ papers were investigated and analyzed. The range of years was chosen to encapsulate the emergence and development of IoT as a distinct field and its intersection with AI for cybersecurity purposes. The keywords used are AI attacks, AI countermeasures, IoT cyber-attacks, IoT security challenges, and AI and Cybersecurity.

This paper aims to assist network and cybersecurity experts and researchers in focusing more on throttling the harmful usage of AI techniques in IoT and other network systems. In addition, it encourages the positive use of AI techniques to defend and protect against IoT network attacks.

The remainder of this paper is structured as follows: Section 2 presents a background on IoT and its main components. Section 3 explains how artificial intelligence techniques are used in cybersecurity attacks. Section 4 discusses the AI-based cyber-attack countermeasure in IoT networks. Section 5 discusses using AI approaches in cybersecurity. Section 6 concludes the paper with future research directions and recommendations.

2. Internet of Things (IoT) Background

This section provides an overview of the infrastructure and components of IoT networks and describes the main applications of IoT networks.

2.1 IoT Components

The Internet of Things (IoT) pertains to the interconnection of physical objects, such as devices, vehicles, buildings, and various items equipped with sensors, software, and network connectivity. This enables these objects to gather and exchange data. Although the idea of IoT has existed for many years, it has recently gained significant recognition and acceptance [2].

The history of IoT can be traced back to the 1980s, when the first IoT-like devices, such as barcode readers and automated teller machines (ATMs), were introduced[3]. However, it was not until the late 1990s and early 2000s that the term "Internet of Things" was coined, and technology began to gain traction.

The phrase "Internet of Things" was initially used in a presentation about the potential for RFID technology to connect everyday objects to the Internet in 1999 by Kevin Ashton, a researcher at the Auto-ID Center at MIT. In the following years, the creation of inexpensive microcontrollers and wireless communication standards like Wi-Fi and Bluetooth prepared the path for the widespread use of IoT devices [4]. Since then, IoT has seen tremendous growth and development. According to a report from the International Data Corporation (IDC), the worldwide IoT market is expected to grow from $157 billion in 2019 to $1.1 tril-

lion in 2027 at a compound annual growth rate of 21.5% during the forecast period [5].

IoT is being adopted across a wide range of industries. For example, IoT devices are used in the manufacturing industry to monitor and optimize production processes. In contrast, they track patients' vital signs in the healthcare industry and improve medical treatments. Additionally, cities worldwide use IoT to manage public services like lighting and waste management [6]. The following explains IoT components and how they interact, according to [2]:

1. **Sensors and actuators:** IoT devices have several sensors and actuators used to collect data and perform actions. Sensors can measure temperature, humidity, motion, or sound, while actuators can control things like lights, motors, or valves.
2. **Data collection:** The sensors in IoT devices collect data and send it to the device's processor for processing. This data can be sent to the cloud for storage and analysis or processed locally on the device.
3. **Communication:** IoT devices use wireless communication technologies to send and receive data. Some standard technologies include Wi-Fi, Bluetooth, Zigbee, and cellular networks. IoT devices can also communicate with other devices and systems using the internet protocol (IP).
4. **Data processing and analysis:** The data collected by IoT devices is processed and analyzed to extract meaningful insights. This can be done locally on the device or sent to the cloud for further processing and analysis.
5. **Actuation:** Based on the data and insights gained, IoT devices can actuate and perform various tasks. For example, an IoT-enabled thermostat might adjust the temperature in a room based on the data it receives from temperature sensors.
6. **Remote access and control:** Many IoT devices provide remote access and control through a smartphone application or a web portal. This allows users to monitor and control their devices from anywhere, anytime.

IoT systems can be simple or complex, depending on the application. Some devices may only need to send a small amount of data to a single endpoint, while others may involve multiple devices and systems communicating [7].

IoT has the potential to bring many benefits, such as increased efficiency, reduced costs, improved decision-making, and better lives for people. However, it also has raised concerns about data privacy, security, and lack of standardization [8].

2.2 IoT Network Applications

The Internet of Things (IoT) is a network of objects with sensors, software, and connectivity that can collect and share data. These objects include smartphones, laptops, home appliances, vehicles, and industrial equipment. Some examples of IoT uses are explained below.

2.2.1. Smart Cities

A smart city is an urban area that lever-

ages technology and data to enhance the well-being of its residents. The primary aim of a smart city is to tackle the issues associated with urbanization, such as traffic congestion, environmental pollution, and limited resources. These cities employ various technologies, including the Internet of Things (IoT), advanced data analysis, and cloud computing, to accomplish this objective. These technologies help to collect and analyze data from multiple sources like sensors, cameras, and other devices. The sources are then used to inform decision-making and improve the delivery of public services, transportation, energy, healthcare, and education. Specifically, IoT is used to optimize transportation networks, manage energy, improve public safety, monitor environmental conditions, and optimize building operations. Implementing these technologies in smart cities can improve the quality of life for citizens, reduce costs, reduce resource usage, and increase the overall efficiency of urban systems [9]–[11].

2.2.2. Smart Grids

A modernized electrical grid, known as a smart grid, uses advanced technology to monitor and control the flow of electricity from power plants to consumers. The smart grid aims to improve efficiency, reliability, and sustainability while providing a more flexible and responsive electricity system that can adapt to changing energy needs and demands. The smart grid is designed to be more efficient, dependable, and secure than traditional grids, enabling the integration of renewable energy sources such as wind and solar power. Smart grid features include two-way communication between devices and the power grid, advanced sensors and control systems, more effective use of renewable energy, advanced metering infrastructure, and increased security with advanced cybersecurity measures. The IoT technology can be employed in smart grids to enhance efficiency, reliability, and sustainability while empowering customers with more control over their energy consumption [12]–[14].

2.2.3. Smart Homes

Smart homes leverage IoT technology to connect various devices and appliances, such as lights, thermostats, security systems, and appliances, providing a more convenient and energy-efficient living environment. Homeowners can remotely control and monitor their smart home using a smartphone application, or voice commands through a smart speaker, such as Amazon Echo or Google Home. Smart home technologies can automate various tasks, such as adjusting the thermostat, turning off lights, or setting security alarms. Additionally, smart home systems enable homeowners to monitor their homes remotely using video cameras or other sensors. The objective of using IoT in a smart home is to make it more convenient for homeowners to manage their living environment while enhancing energy efficiency and security [15]–[17].

2.2.4. Smart Cyber-physical Systems (CPS)

Cyber-physical Systems (CPS) combine computation and physical processes to enable real-time control of physical

processes. Smart cyber-physical systems (SCPS), a subcategory of CPS, can make decisions based on data and knowledge, and they often integrate sensors, actuators, and computing elements. SCPS can be used in various applications, such as transportation and manufacturing systems, and are designed to be self-adaptive, using machine learning algorithms or following predetermined plans to improve efficiency, reliability, and safety. IoT devices can be used to collect and transmit data from sensors and actuators to a central system for analysis and control, enabling remote monitoring and control of CPS. Integrating IoT technologies into CPS can enhance their performance, reliability, and efficiency, allowing them to adapt and respond to changes in their environment or operating conditions [18]–[20].

2.2.5. Smart Transportations

Smart transportation aims to enhance transportation systems' efficiency, safety, and sustainability using technology [21]–[23]. It can include various technologies such as intelligent transportation systems (ITS), Connected and Autonomous Vehicles (CAVs), public transport, and active transportation. ITS uses sensors, cameras, and other technologies to collect data, optimize traffic flow, reduce congestion, and improve safety. CAVs have sensors to communicate with other vehicles and infrastructure and operate independently. Smart transportation also involves improving public transportation systems and promoting active transportation through technology such as real-time data, smart ticketing systems, bike-sharing systems, and pedestrian-friendly streets. IoT technologies can enhance transportation systems' efficiency, safety, and sustainability in traffic management, public transportation, and infrastructure maintenance. Smart transportation aims to create more efficient, safe, and sustainable transportation systems that cater to the needs of communities and individuals.

2.2.6. Wireless Sensing Network (WSN)

Wireless sensing networks (WSNs) are networks of wireless sensors that are deployed to monitor and collect data from physical or environmental conditions [24],[25]. These sensors are typically small, low-power devices with various sensors such as temperature, humidity, pressure, or motion. They can communicate wirelessly with each other and with a central device or server. WSNs are used in various applications, such as monitoring the environment, collecting data from remote or hard-to-reach locations, and providing real-time data for control and decision-making. They are often deployed in agriculture, industrial automation, healthcare, and military and defense. WSNs can monitor and collect data from various physical and environmental conditions, including temperature, humidity, pressure, motion, sound, light, and more [26]. They can be used to detect and track the movement of objects, monitor the health of plants and animals, and collect data on environmental conditions such as air quality, water quality, and soil moisture.

3. AI-Based Cybersecurity Attacks on IoT Networks

Artificial intelligence is a discipline that focuses on addressing problems and simulating cognitive abilities. It is a multidisciplinary field incorporating various machine learning and deep learning methods to develop intelligent machines capable of performing diverse tasks.

Since IoT devices are typically introduced to accomplish simple tasks, they do not have security mechanisms against cyber threats [27]. Therefore, IoT networks are vulnerable to several attacks and security threats. Several studies have been conducted to analyze IoT attacks and categorize them. For instance, attacks on IoT devices can be classified by network layer affected as in [28], on which critical infrastructure it occurs as in [29], or by attack vector as in [30].

As technologies advance, merging AI and IoT allows IoT devices to operate smartly and help them make decisions based on their data and experience [31]. Cybersecurity attacks also take advantage of these advancements and utilize capabilities to launch complicated and sophisticated attacks on IoT devices and networks [32]. These attacks aim to control AI systems and maliciously change their behavior. Attacking an AI system can be through data poisoning, tempering of categorization models, backdoors, etc. [33]. The sections below list common and most recent AI-based attacks targeting IoT devices and networks.

3.1. Data Poisoning/False Data Injecting

Data poisoning involves injecting false and polluted data over a prolonged period into the AI training dataset to produce a flawed model and alter the behavior of an AI system maliciously or at least as the attacker (injector) wants the system to behave [34] [35]. The flawed model frequently resembles a good model, yet it gives the opponent certain evil leverages [36].

AI data poisoning attacks usually target AI systems in a continuous learning phase during their operational life, accepting and analyzing data to make predictions and adjusting them based on the constant acceptance of datasets [34].

Data poisoning can be categorized as poisoning datasets, models, and algorithms. In dataset poisoning, mislabeled raw data are injected into the AI dataset to classify data and process it later for a specific action or decision. This misleading and mislabeled data allows AI to alter the machine learning models' accuracy [34].

The second type of poisoning affects AI models. As some AI models are publicly available for organizations, some AI models can be potentially dangerous and have poisoned data affecting the organizations' supply chain [37]. BadNet is an example of an AI model that some users or organizations could outsource and use as a trained AI model. BadNet poisoned a deep learning neural network to classify US street sign classifiers and injected a backdoor that identified stop signs as speed limit signs instead. This caused autonomous vehicles and passengers to face severe safety

situations [38].

The third type of poisoning occurs in AI algorithms, especially in the federated learning type. In federated learning and for data protection and user privacy, the learning process is conducted on small models of users' data on their own devices. Then, the resulting models are combined to form the final model rather than collecting users' sensitive data into a single dataset for further processing [34]. However, if the algorithm uses an attacker's data, the attacker will have the opportunity to poison the data and further poison the model [34]. Polluted models injected into AI systems, especially in the training phases, are one of the most dangerous attacks that would target AI systems [39].

Shen et al. [39] proved that it is possible to inject a Trojan virus into the real Go AI that changes the AI's predefined actions and manipulates it intentionally and maintained undetected. They prove that 3.2% of poisoned data is enough to poison the AI effectively and change its behavior to the intended ones.

In [40], Nguyen et al. proved that IoT intrusion-detecting systems (IDS) based on federated learning types of AI are susceptible to poisoning attacks. The author slowly injected a backdoor to the aggregated detection model to mislead the model to classify the injected poisoned data as normal data to avoid being detected by the IDS.

3.2. Phishing Attacks

Phishing attacks include sending several copies of the same message or robo-phone calls to target victims to either deceive them to gain sensitive information or persuade them to do harmful actions [41]. These attacks can be automated through AI services, such as Google's assistant, which can make calls on someone's behalf. Imagine an AI bot is instructed to target a specific victim, then calls their colleague, which is previously located using social media data, then clones the colleague's voice through deepfake "Speech synthesis" techniques, later calling the victim using their colleague's voice to degrade their trust [41].

In IoT networks, eavesdropping is one of the common cyber-attacks that occurs. Eavesdropping is a passive attack. It breaks down the confidentiality and privacy of the data transferred through the network by illegally listening to opened ports of unsecured devices [42]. An attacker can intercept real-time personal communication, such as emails, instant messages, video calls, or any confidential data, without the authorization of the communication parties. Detecting eavesdropping attacks is particularly challenging because the network transmissions will appear to operate normally. With the rise of IoT, this attack became more difficult and can result in failures on the personal and financial fronts [9], [42].

3.3. AI-based Malware Obfuscation Tools

Numerous programs can get assistance from AI to complete a specified goal in the attacker's interests. For example, AI can assist in intelligently obfuscating malware code that can be quickly injected into IoT networks. Machine learning models can

be used to hide the malicious intentions of malware and extend the offensive time [41]. Advanced metamorphic malware with the obfuscation feature can change its infrastructure with every attack. If an IoT device gets infected with such malware, even if detected, the malware can change its internal structure and infect other devices on the IoT network. ADVERSARIALuscator is an innovative method of using deep reinforcement learning to adversarial obfuscate malware at the opcode level [43].

3.4. Attack Vectors Identification

AI can assist adversaries in detecting and choosing the preferable entry point to exploit a system, i.e., attack vectors. Statistical models of an organization's attributes are used to predict the number of intrusions it receives. Then, AI trains a model on similar information to select the weakest organization and the most potent attack vector [41].

Since IoT devices have limited resources and, therefore, limited security mechanisms, detecting attack vectors suitable for a specific IoT device increases the attack's success. For example, a successful attack on the base node/device of an RFID-powered inventory control system could lead to the shutdown of the entire network [30].

3.5. AI Attack Automation

Attack automation on systems and devices makes things easier, gives adversaries more flexibility, and allows them to run more extensive campaigns that rely less on C2 signals. Attackers use AI to intelligently adapt their malware and other attacking methods to unfamiliar or new environments and search for potential targets[41]. IBM researchers were able in Black Hat'18 to demonstrate how malware may trigger itself using Deep Learning (DL). By recognizing a target's machine and analyzing the victim's face, voice, and other characteristics, DL was used onsite to extract critical information [41].

Falco et al. [44] proposed an AI planning tool that automatically identifies attack trees that compromise several IoT and smart cities' critical systems and infrastructure. In addition, Recurrent Neural Network RNN-based models have been applied to automate the password-cracking process of IoT devices [45].

3.6. Speech Synthesis Attacks on IoT Devices

Advancements in the malicious utilization of deep learning have enabled attacks to develop synthesis tools to create fake audio or videos of known politicians, CEOs, celebrities, etc. These tools learn to intelligently imitate individuals' voices or videos [46].

Statistical parametric speech synthesis is an emerging data-driven machine-learning approach that develops speech synthesis. This method uses a time-series stochastic generative model, typically HMM, to simulate several acoustic characteristic[s] [47]. By modifying background models acquired from other speakers based on the standard model adaptation approaches from speech recognition, HMM-based speech synthesizers can also learn speech models from modest quantities of speaker-specific data[47].

One of the well-known speech synthesis attack incidents happened to a UK-based energy company when the managing director was defrauded by a phone call and believed his boss ordered him to transfer an amount of money to a Hungarian supplier account. Although the director found it a strange demand due to the accuracy of the voice, he could not but commit the order and found later that the amount of money had been transferred to a German account instead [48].

Smart speakers, e.g., Amazon Alexa and Google Home, and many IoT devices are considered Voice-Controlled Systems and hence suspected of voice spoofing/cloning and speech synthesis, especially after the COVID-19 crisis. Attacks on those Voice-Controlled Systems increased to gain unauthorized access to devices and bypass the authentication mechanisms of many businesses and organizations. Deep learning algorithms facilitate the synthetic formation of voice commands [49].

Wenger et al. [50] proved in their study that deep neural network DNN-based speech synthesis tools, such as Microsoft Azure, Amazon Alexa, etc., can be used to fool smart speakers.

These attacks could be linked to voice-cloning attacks or voice replay attacks. A replay attack occurs when an attacker eavesdrops on a secure network communication, intercepts the acknowledgments, and then fraudulently delays or misdirects the receiver into doing what the adversary wants through the message replay [51]. This attack interferes with how devices in the network typically operate, forcing them to conduct operations that they should not, or it directs the outcomes in a direction the attacker desires. Because the entire message may be replayed to acquire access to the server, replay attacks are more straightforward to implement after packet seizing because subsequent stages do not require sophisticated abilities for message decryption [52]. Replay attacks are harmful as they challenge the confidentiality and integrity of the communicated data and could increase network congestion and interference, causing route disturbance and bandwidth reduction [51].

4.The Use of AI to Countermeasure Cyber-Attacks on IoT Networks

AI has the potential to revolutionize existing security techniques. By leveraging the power of machine learning, deep learning, and automation, AI can improve the overall cybersecurity posture of an IoT network and help protect its infrastructure and data. This section discusses how AI is being used to countermeasure IoT network attacks.

4.1. Preventing Poisoning Attacks

As discussed earlier, data, AI models, or algorithm poisoning attacks are common AI-based attacks. AI approaches can also be utilized to countermeasure this category of attacks. Sagduyu et al. [53] employed a Feedforward Neural Network (FFN) to defend against poisoning attacks in IoT networks. They also introduced a Stackelberg game approach to optimize the performance of the defense mechanism over

the FFN algorithm. These results offer new perspectives on effectively attacking and defending IoT networks with a high success rate.

The work in [54] introduced the 'DeepRing' architecture that merges CNN architecture with some aspects of blockchain technology to detect and prevent attacks. Within each block of DeepRing, essential information aids in authenticating the block to prevent tampering. The DeepRing architecture can detect and thwart attacks, whether at each block's parameter or input levels, referred to as network-level attacks. It has been observed that CNN models lacking blockchain integration are susceptible to tampering. However, incorporating blockchain technology into CNN, as seen in DeepRing, effectively eliminates network-level attacks on CNN. MNIST and CIFAR-10 datasets were used to train and obtained a 99.07% and 83.89% accuracy rate, respectively.

Authors in [55] proposed a defense strategy for identifying poisonous data to train an arbitrary supervised learning model by using contextual information about the origin and transformation of the data points. This approach can be used with or without a trusted test dataset and effectively detects and mitigates poisoning attacks in IoT environments with reliable provenance information.

4.2. Spoofing and Tampering Detection

Supervised learning methods, such as Frank-Wolfe (dFW) and incremental aggregated gradient (IAG), could enhance the resistance against spoofing in IoT systems. In the authentication system discussed in [56], dFW and IAG were employed, leveraging the Received Signal Strength Indicators (RSSIs) from multiple reference points to reduce overall communication overhead and enhance spoofing detection accuracy. Specifically, the dFW-based authentication reduces communication overhead by 37.4%, while IAG lowers computation overhead by 71.3% compared to the FW-based approach.

Deep learning techniques such as DNN can further enhance authentication accuracy for IoT devices with sufficient computational and memory resources. The DNN-based user authentication method outlined in [57] extracts Channel State Information (CSI) features from Wi-Fi signals and utilizes DNNs to detect spoofing attackers. This scheme achieves a spoofing detection accuracy of approximately 95% and a user identification accuracy of 92.34%.

4.3. AI in Intrusion Detection and Prevention Systems

One primary application of AI in cybersecurity attack countermeasures is intrusion detection and prevention. Intrusion detection systems (IDS) are used to identify unauthorized access or activities on a computer system, while intrusion prevention systems (IPS) are designed to block such access or activities [58]. Traditional IDS and IPS systems rely on predefined rules or patterns to identify and prevent intrusions, which can be ineffective against new or unknown threats.

AI-based IDS and IPS systems can analyze substantial amounts of data in re-

al-time and identify patterns and anomalies that may indicate an intrusion.

a) Anomaly Detection

Machine Learning (ML) algorithms can be trained to identify unusual behavior in the data collected from IoT devices. For example, if an IoT device begins sending a large amount of data at unique times or to unexpected destinations, this could be a sign of a security threat. Stoian [59] explored the use of ML algorithms for detecting anomalies in data from IoT networks, focusing on security. The study compared several ML algorithms, including Random Forest, Naive Bayes, Multi-Layer Perceptron, Support Vector Machine, and AdaBoost, regarding various parameters and methods. The results showed that the Random Forest algorithm performed the best, with an accuracy of 99.5%.

In [60], a new centralized scheme based on ML was proposed for securing IoT devices. This scheme allowed authorized users to communicate with the system and securely store their information. The proposed peer-to-peer security protocol requires clients to be registered with the cloud server before sharing in the IoT system.

Alam et al. [61] proposed a model to secure IoT devices using a neural network and the ElGamal algorithm. This model used private and public keys to control its cryptosystem and segments manipulated data into groups, comparing them with training data to detect attacks.

Doshi et al. [62] designed an ML pipeline identifying and classifying IoT traffic related to DDoS attacks. The pipeline includes data collection, feature extraction, and binary classification using several algorithms, including random forests, K-nearest neighbors, support vector machines, decision trees, and neural networks. The authors tested these algorithms on a dataset of ordinary and DDoS attack traffic from an IoT device network and found that all had a test set accuracy greater than 0.99. The results suggested that home gateway routers or other network middle-boxes could effectively detect local IoT devices that are causing DDoS attacks by using low-cost ML algorithms and traffic data that is flow-based and protocol-agnostic.

Ahmad et al. [63] present an anomaly detection method based on a deep neural network for IoT networks. The proposed approach used the IoT-Botnet 2020 dataset to learn complex patterns from IoT network traffic and classify them as benign or anomalous. The experimental results showed that the proposed model outperforms other deep neural network methods, with a detection accuracy of 99.01% and a false positive rate of 3.9%. The authors also indicated that using the top 16-32 numerical features selected using mutual information reduced model complexity with minimal impact on performance. Including the top five categorical features can further improve detection accuracy.

The work in [64] presents a Deep Learning (DL) model designed to detect anomalies in IoT networks. The model utilizes various Recurrent Neural Network (RNN) techniques, including Long Short-Term

Memory (LSTM), Bidirectional LSTM (BiLSTM), and Gated Recurrent Unit (GRU). Additionally, convolutional neural networks are incorporated into the model to enhance its performance, resulting in a hybrid approach. The researchers also propose another DL model specifically for binary classification, employing LSTM, BiLSTM, and GRU methods. Multiple datasets, such as NSLKDD, BoT-IoT, IoT-NI, IoT-23, MQTT, MQTTset, and IoT-DS2, are utilized to evaluate the effectiveness of the proposed models. The results indicate that both the multiclass and binary classification models achieve high accuracy, precision, recall, and F1 scores, surpassing existing DL approaches in performance.

b) Intrusion Detection

ML algorithms can detect network intrusions by analyzing patterns in the data collected from IoT devices. For example, if an IoT device starts sending data to a malicious server or a sudden increase in traffic from an IoT device, this could indicate an intrusion.

ML algorithms were used in [65] to develop an AI-based IDS system that could detect intrusions accurately and with a high degree of accuracy. More specifically, the actual positive rate achieved was 97.67%, and the false positive rate was 1.20%.

In [66], Zahra et al. suggested a framework for detecting rank and wormhole attacks in IoT networks that rely on the RPL standard for information broadcast. RPL is a networking standard designed explicitly for IoT devices' resource-constrained and lightweight nature. Their proposed framework used ML techniques to develop practical solutions for routing attacks in RPL-based IoT networks.

Farzaneh et al. [67] introduced a Fuzzy-based technique for detecting local repair attacks on the RPL routing protocol. When a local repair attack occurs, the affected node deliberately contaminates itself by resetting its rank to an infinitely high value and disseminating poison messages to all neighboring nodes. The effectiveness of the proposed approach was demonstrated by evaluating distance, residual energy, and expected transmission count metrics. The simulations conducted using the Cooja simulator on the Contiki OS revealed that the proposed method exhibits a notably high true positive rate and an exceptionally low false positive rate when detecting local repair attacks.

The researchers in [68] developed an IoT platform for studying and executing IoT attacks within a network. One attack, the Man in the Middle attack, was performed using ARP Poisoning. The data collected during these attacks was labeled as attack data, and several machine learning classifiers, including Naïve Bayes, SVM, decision tree, and Adaboost, were employed to classify the data into two categories: normal and attack. The classifiers exhibited accurate classification of the data. The study highlighted the significance of having a high-quality training dataset to enhance the performance of machine learning algorithms.

4.4. Predictive Maintenance

ML algorithms can predict when an IoT

device will fail or be compromised. This can help organizations proactively replace or repair devices before they become a security risk.

The work by [69] developed a predictive maintenance system for manufacturing production lines using data from real-time IoT sensors. The system used ML methods to detect signs of potential failures before they occur. Comparison evaluations of various machine learning algorithms found that the Random Forest and XGBoost models outperformed the others. These top-performing models were then integrated into the production system at the factory. The evaluation results showed that the predictive maintenance system successfully identified potential failure indicators and can help prevent production stoppages.

In [70], the Genetic Algorithm (GA) was proposed as a technique for resource management in an assets management application for Industry 4.0. The GA was compared to other scheduling techniques, including MinMin, MaxMin, FCFS, and RoundRobin, using FogWorkflowsim as the simulation tool. The performance metrics used in the evaluation were execution time, cost, and energy. The results of the simulation experiments showed that the GA outperformed the other techniques in terms of having the lowest execution time, cost, and energy. Additionally, an ML model based on two-class logistic regression was deployed for equipment predictive maintenance and could predict equipment failure and provide early warning alerts for the production line. The training and testing accuracies for the model were 95.1% and 94.5%, respectively.

In [71], a method for detecting faults in data-driven predictive maintenance using low-data-rate IoT sensors and the OC-SVM ML algorithm was demonstrated in rural areas. The OC-SVM algorithm was trained using normal data from a test setup and achieved an accuracy of 87.56% on normal data and 82.09% on abnormal data. By remotely monitoring infrastructure in remote locations, maintenance teams can stay informed about the status of installed systems.

4.5. AI in Malware Detection and Prevention

AI is also used in the scope of malware detection and prevention. Malware is software specifically designed to damage or disrupt computer systems, and it can take many forms, including viruses, worms, and Trojans [72]. Traditional malware detection systems rely on predefined rules or patterns to identify known types of malware, but they are often ineffective against new or unknown types.

AI-based malware detection systems can analyze software behavior and identify patterns that may indicate malicious intent. For example, machine learning algorithms were used in [72] to develop an AI-based malware detection system that could detect malware with more than 90% accuracy.

AI can also be applied on the network level to detect malware. Network security systems that rely on AI can analyze network traffic in real-time and identify patterns and anomalies of malware that may

indicate an attack. For example, in a recent study [73], researchers used ML algorithms to develop an AI-based network security system that could accurately detect and prevent cyber-attacks with a high degree of accuracy, reaching upwards of 97%.

DL algorithms can be trained to recognize patterns and features in malware that may not be detectable by traditional security measures. By analyzing substantial amounts of data, these algorithms can accurately identify and classify several types of malware, allowing organizations to take appropriate action to prevent attacks.

The work in [74] proposed a solution for detecting IoT botnet anomalies using a deep autoencoder model. The approach was evaluated through experiments and was found to have an accuracy of 99.7%, a precision of 0.99, and a recall of 0.99. The false positive rate of the model was also analyzed, and it was found that the threshold could be increased to improve the model's performance further.

Gu et al. [75] developed a consortium blockchain framework for detecting and gathering evidence on malicious code in mobile devices, particularly in Android-based systems. The proposed framework combined statistical feature modeling to identify malware families with a multi-feature detection method. Using blockchain, authors created a distributed fact repository for Android malicious code. Experiments showed that the proposed approach achieved higher accuracy with lower false positives and false negatives compared to previous algorithms.

Authors in [76] utilized Convolutional Neural Networks (CNNs) for malware detection in the Industrial Internet of Things (IIoT). The study assessed the resilience of a CNN-based malware detector against polymorphic attacks, revealing that the effectiveness of neural network-based detectors relies on specific assumptions about malware design. When these assumptions are violated, as with polymorphic attacks, CNNs can be misled, resulting in misclassification and significant performance degradation. This approach focused on a specific category of malware, namely those that disguise themselves within Windows PE or Linux ELF binary files.

In [77], researchers explored using machine learning techniques to identify unfamiliar malware by analyzing the frequency of opcodes. The authors utilized the Kaggle Microsoft malware classification challenge dataset to conduct their investigation. They applied several feature selection techniques, such as Fisher score, information gain, gain ratio, Chi-square, and symmetric uncertainty, to derive the top 20 features. Furthermore, they evaluated multiple classifiers accessible through the WEKA GUI-based machine learning tool. Interestingly, they found that five classifiers, namely Random Forest, LMT, NBT, J48 Graft, and REPTree, achieved near-perfect accuracy in detecting malware, with accuracy levels reaching close to 100%.

Ahmed et al. [78] proposed a DL model to detect real-time zero-day botnet attacks. The authors used a reliable dataset called

CTU-13 from the Botnet Capture Facility, containing 10,000 randomly selected flows and nine input features. After normalizing the data and applying Adam's optimizer, their model achieved over 99.6% accuracy after 300 training epochs. It outperformed other algorithms like Naive Bayes, SVM, and backpropagation.

The work in [79] introduced a novel model known as the transferred deep-convolutional generative adversarial network (tDCGAN) to identify zero-day malware efficiently. This model is built upon the foundation of Deep AutoEncoder (DAE) and generative adversarial network (GAN) principles [36]. It acquires knowledge from genuine and model-generated modified data. Subsequently, it leverages this knowledge to produce synthetic malware samples and trains itself to differentiate between these fabricated malware instances and genuine ones.

4.6. Expert Systems

Expert systems are AI systems that use knowledge and reasoning to solve problems. They can be used in an IoT environment to identify security threats by analyzing data and making recommendations based on their knowledge and expertise.

The work in [80] introduced the Boost-Defence framework, which aims to safeguard IoT networks against different cyber-attacks occurring at various layers of the IoT system. Boost-Defence utilizes the AdaBoost machine learning method in conjunction with Decision Trees and various data engineering techniques. This combination allows for developing a robust classifier to detect and identify multiple cyber-attacks within IoT networks. To assess the performance of Boost-Defence, the researchers conducted evaluations on the TON_IoT_2020 datasets. These datasets were designed for 3-layered IoT systems, encompassing the physical, network, and application layers. The experimental outcomes demonstrated that Boost-Defence exhibits outstanding classification accuracy, effectively enhancing the resilience of IoT infrastructures.

In [81], the researchers presented ESSecA (Expert System for Security Assessment), a tool designed to aid penetration testers in evaluating the security of IoT systems. ESSecA utilizes knowledge bases, including those curated by MITRE, to analyze the system model. It then generates a threat model and a collection of attack plans for each identified threat. Penetration testers can leverage these attack plans to systematically conduct a thorough security assessment of the targeted IoT infrastructure. The effectiveness of ESSecA was demonstrated by applying it to a specific home automation system known as the Open Energy Monitor. The researchers also provided several attack patterns for security evaluation.

4.7. Machine Learning for Threat Detection

Machine learning algorithms can be trained to recognize patterns of behavior that may indicate a cyber-attack, such as unusual login attempts or network traffic. By continuously learning and adapting, these algorithms can detect and defend against potential threats more effectively

[58]. For example, an ML algorithm might be trained to analyze log files and identify patterns indicative of a cyber-attack. If the algorithm detects such a pattern, it can alert cybersecurity professionals and provide them with the necessary information to act.

4.8. Real-Time Incident Response

AI can also be used to improve the effectiveness of cyber incident response [82]. When a cyber-attack occurs, it is crucial for organizations to quickly identify the nature and scope of the attack, assess the damage, and respond appropriately to mitigate the impact. Traditional incident response processes are manual and can be slow, which leads to delays in identifying and responding to attacks. This is incredibly challenging in an IoT context due to the network and processing constraints.

AI-based incident response systems can automate many tasks in responding to cyber-attacks, including collecting and analyzing data from multiple sources, identifying patterns and anomalies that may indicate an attack, and generating recommendations for responding. For example, in [82], ML algorithms were used to develop an AI-based incident response system that could identify and classify cyberattacks accurately in real-time.

4.9. Enhancing Cyber Risk Assessments

AI can also improve the accuracy and efficiency of cyber risk assessments [83]. Cyber risk assessments involve identifying and evaluating potential vulnerabilities and threats to an organization's information systems and infrastructure. Traditional risk assessment processes can be time-consuming and resource-intensive and may only sometimes provide a complete or accurate picture of an organization's cyber risk profile. This issue is even more prevalent in an IoT context, where the network parameters are not easily defined.

AI-based risk assessment systems can automate many tasks involved in risk assessments, including collecting and analyzing data from multiple sources, identifying vulnerabilities and threats, and generating recommendations for mitigating those risks. For example, in a recent study [83], ML algorithms were used to develop an AI-based risk assessment system to identify and accurately assess cyber risks. This can benefit IoT risk assessment as many parts of the assessment can be entirely automated, which can overcome a challenge as IoTs tend to have vast amounts of data.

4.10. Fake Speech Detection on IoT Devices

As discussed earlier, IoT devices that rely on speech commands may suffer from AI-based attacks. AI approaches can be utilized to detect such attacks. Malik et al. [84] introduced a CNN model for detecting cloned speech. They initially converted audio samples to spectrograms and used a CNN framework to extract deep features and classify real and fake speech. This approach exhibits higher accuracy in counterfeit audio detection but experiences performance degradation with noisy samples.

Monteiro et al. [85] proposed an ensemble-based model to detect synthetic speech, utilizing deep learning models LCNNs and ResNets to extract deep fea-

tures that distinguish natural and spoofed speech. While effective in fake speech detection, this model requires the evaluation of standard datasets.

Chen et al. [86] presented a deep learning-based framework for detecting audio deepfakes. They extracted 60-dimensional linear filter banks (LFB) from speech samples, using them to train a modified ResNet model. While improving fake audio detection, this method comes with a significant computational cost.

Zhang et al. [87] introduced a DL approach utilizing ResNet-18 and one-class softmax. They trained the model to acquire knowledge of a feature space capable of distinguishing actual speech from manipulated samples with a specific margin. While this method enhances the model's ability to generalize against unforeseen attacks, its performance diminishes when faced with voice conversion attacks generated through waveform filtering.

Jiang et al. [88] introduced a self-supervised learning approach that utilizes eight convolutional layers to extract deep features and distinguish between genuine and fake speech. While this method is computationally efficient, there is room for improvement in detection accuracy.

4.11. Automating Cybersecurity Analysis Tasks

AI can also be used to automate tasks related to cybersecurity analysis, such as the analysis of log files or the creation of reports. This can free up time and resources for cybersecurity professionals, allowing them to focus on more complex tasks and respond more effectively to potential threats [89]. For example, an AI system might be able to analyze log files and create a report summarizing the key findings, saving cybersecurity professionals the time and effort of manually reviewing these logs [89]. This is a key feature given the amount of data IoT devices generate.

Overall, suitable AI-based cybersecurity countermeasures depend on the specific security threats, attacks, and vulnerabilities present in the IoT environment and the resources and capabilities available to the organization.

5. Discussion

IoT networks are challenging environments that are evolving continuously. New devices are added to these networks daily. The multiple vendors, different architectures, the use of cloud services, the vast amount of traffic data, and the different security approaches needed with each IoT component pose significant security challenges. Hence, this paper sheds light on the importance of utilizing AI approaches to protect these networks. Unfortunately, attackers also use AI approaches to conduct tailored attacks on such networks, so it was important to understand their adversary approaches.

To achieve this goal, this paper surveyed the studies utilizing AI approaches to provide more sophisticated attacks and countermeasures in the evolving IoT environment. The approaches found in the literature can be categorized according to their type, i.e., machine learning, deep learning, or both. Some approaches can be

combined or layered depending on the required goal, such as in ensemble learning. In addition, these approaches can be distinguished by the impact and implications of AI approaches on the context in which they are utilized. The approaches vary in accuracy and rates of false positives, indicating their robustness in detecting or initiating attacks.

Table 1 summarizes the approaches used to initiate attacks in IoT networks. In Addition, Table 2 summarizes the approaches used to countermeasure and detect attacks on IoT networks.

Table 1: A Synthesis of Surveyed AI-based Approaches Used in Attacks on IoT Networks

Study	Attack Scope	ML	DL	Approach	Accuracy	Implication
[34]	Dataset poisoning	X		Introduce new incorrect patterns to alter ML.	-	Alter accuracy.
[38]	AI model poisoning	X		BadNet	25%	Severe safety situations.
[39]	AI algorithm poisoning	X		Poisoning data used in AlphaGo Zero	3.2% of poisoned data	The opportunity to poison the data and further poison the model.
[40]	Injection of backdoor	X		Mirai malware on FL	35% Poisoning data rate 20 % Poisoning model rate	Classify the injected poisoned data as normal to avoid being detected by the IDS.
[41]	Phishing Attacks Robo-calls	X		Deepfake	High rate of accuracy of deceiving	Deceive victims to gain sensitive information or persuade them to do harmful actions.
[43]	Malware Obfuscation Tools		X	deep reinforcement learning ADVERSARIALuscator	33%	Malware can change its internal structure and infect other devices.
[41]	Attack automation		X	MESSAGETAP decision trees xRAT-malware	-	Extract victims' critical information.
[44]	Attack automation	X	X		-	Identifies attack trees that compromise several IoT and smart cities' critical systems and infrastructure
[45]	Attack automation Password cracking		X	RNN-based model	-	Break the victims' confidentiality.
[46]	Speech Synthesis on IoT Devices		X	Deepfake	-	Deception by creating fake audio or videos of known people.
[47]	Speech Synthesis on IoT Devices	X		Statistical parametric speech synthesis	-	Learn speech models for deception purposes.
[50]	Speech Synthesis on IoT Devices		X	DNN	50 − 100%	Deceit smart speakers.

Table 2: A Synthesis of the Surveyed AI-based Approaches Used for Countermeasure of Attacks in IoT Networks

Study	Countermeasure Scope	ML	DL	Approach	Accuracy	Impact
[53]	Poisoning attack	X	X	Feedforward Neural Network (FFN) with Stackelberg game approach	High success rate.	Defending IoT networks against poisoning attacks.
[54]	Poisoning attack		X	DeepRing combining CNN with blockchain	99.07% for the MNIST dataset and 83.89% for the CIFAR-10 dataset.	Eliminates network-level attacks.
[55]	Data Poisoning attack	X		Supervised learning model	-	Mitigates poisoning attacks with reliable provenance information.
[56]	Spoofing and Tampering Detection	X		Supervised learning methods: dFW, IAG	Enhance spoofing detection accuracy.	
[57]	Spoofing and Tampering Detection in Wi-Fi		X	DNN	Accuracy of ~ 95% and a user identification accuracy of 92.34%.	Spoofing detection
[60]	Anomaly Detection	X		P2P protocol	-	Only authorized users can access the IoT devices and protect them from unauthorized access.
[61]	Anomaly Detection	X		ElGamal algorithm	-	Manipulate data into groups, comparing them with training data to detect attacks.
[62]	Anomaly Detection	X		An ML pipeline identifying and classifying IoT traffic related to DDoS attacks	Test set accuracy greater than 0.99.	Home gateway routers or others could detect local IoT devices that are causing DDoS attacks by using low-cost ML algorithms and traffic data that is flow-based and protocol-agnostic
[63]	Anomaly Detection		X	DNN-based NIDS model	Detection accuracy of 99.01% and a false positive rate of 3.9%	This method learns complex patterns from IoT network traffic and classifies them as benign or anomalous.
[64]	Anomaly Detection		X	Recurrent Neural Network (RNN) techniques	Both the multiclass and binary classification models achieve high accuracy and precision.	Enhance the performance of detecting abnormal traffic on IoT networks.
[65]	Intrusion Detection	X		AI-based IDS system	The actual positive rate achieved was 97.67%, and the false positive rate was 1.20%.	This method detects intrusions accurately and with a high degree of accuracy.
[66]	Intrusion Detection	X		Used ML techniques to develop practical solutions for routing attacks in RPL-based IoT networks.	-	Detecting rank and wormhole attacks in IoT networks that rely on the RPL standard
[67]	Intrusion Detection	X		A Fuzzy-based technique for detecting local repair attacks on the RPL routing protocol	High true positive rate and an exceptionally low false positive rate.	It detects local repair attacks on the RPL routing protocol.
[68]	Intrusion Detection	X		IoT platform including Naïve Bayes, SVM, decision tree, and Adaboost.	The classifiers exhibited accurate classification of the data.	Focus on the man-in-the-middle attack.
[69]	Predictive maintenance for real-time IoT sensors	X		Random Forest and XGBoost models	-	The system detects signs of potential failures before they occur, and it successfully identifies potential failure indicators and can help prevent production stoppages.

Study	Countermeasure Scope	ML	DL	Approach	Accuracy	Impact
Study	Countermeasure Scope	ML	DL	Approach	Accuracy	Impact
[70]	Resource Management	X		Genetic Algorithm (GA) and ML model based on two-class logistic regression	95.1% for training and 94.5% for testing.	Successful resource management in an assets management application for Industry 4.0.
[71]	Predictive maintenance	X		The OC-SVM used.	87.56% on normal data and 82.09% on abnormal data.	By remotely monitoring infrastructure in remote locations, maintenance teams can stay informed about the status of installed systems.
[72], [73]	Malware detection and prevention	X		-	[72] Detect malware with more than 90% accuracy. [73] high degree of accuracy, reaching upwards of 97%.	AI-based malware detection systems can analyze software behavior and identify patterns that may indicate malicious intent.
[74]	Malware detection and prevention		X	Deep autoencoder model.	An accuracy of 99.7%, a precision of 0.99, and a recall of 0.99.	Detecting IoT botnet anomalies using a deep autoencoder model.
[76]	AI-based Malware Obfuscation – Polymorphic attacks	X		Convolutional Neural Networks (CNNs)	-	The effectiveness of neural network-based detectors relies on specific assumptions about malware design.
[77]	AI-based Malware Obfuscation	X		Random Forest, LMT, NBT, J48 Graft, and REPTree.	Achieved nearly perfect malware detection accuracy, nearing 100%.	Identify unfamiliar malware by analyzing the frequency of opcodes.
[78]	Identifying Attack Vectors		X	-	99.6% accuracy after 300 training epochs.	Real-time zero-day botnet attack detection
[79]	Identifying Attack Vectors		X	tDCGAN is built on AutoEncoder (DAE) and generative adversarial network (GAN) principles.	-	It identifies zero-day malware efficiently.
[84]	Speech Synthesis		X	A CNN framework for detecting cloned speech	High for clean audio samples	Detecting counterfeit audio; performance degradation noted with noisy samples.
[85]	Speech Synthesis		X	LCNNs and ResNets methods, Ensemble-based model		It extracts deep features that distinguish between real and spoofed speech.
[86]	Speech Synthesis		X	A deep learning-based framework for detecting audio deep fakes	-	It is improving fake audio detection.
[87]	Speech Synthesis		X	ResNet-18 and one-class (OC)	-	Distinguish real speech from manipulated samples with a specific margin.
[88]	Speech Synthesis	X		A self-supervised learning approach	-	Distinguish between genuine and fake speech.
[54]	Network-level attack detection		X	DeepRing architecture (CNN with blockchain integration)	-	Effectively eliminates network-level attacks on CNN models.
[55]	Poisonous data identification	X		Contextual information-based supervised learning model	99% accuracy rate	Detects and mitigates poisoning attacks in IoT environments
[56]	Spoofing and tampering detection	X		Frank-Wolfe (dFW) and Incremental Aggregated Gradient (IAG)		Enhances resistance against spoofing in IoT systems

Study	Countermeasure Scope	ML	DL	Approach	Accuracy	Impact
[57]	Spoofing detection in IoT		X	DNN-based user authentication	Spoofing detection ~95%, user identification ~92.34%	Enhances authentication accuracy for IoT devices
[83]	Cyber risk assessment	X		Security risk modeling in smart grid	-	Automates and accurately assesses cyber risks for IoT.

As a result of the analysis of the previous tables, it is challenging to create a general theme around the approaches used in initiating or preventing the attacks. However, this opens a new direction for future research focusing on the algorithm type and the frameworks created to achieve high accuracy goals. It is important for the scope of this paper and to assist researchers in this field to conduct this comparison to collect and categorize the literature.

The analysis conducted in this paper reveals the power of AI in making attacks more sophisticated and sometimes undetectable. The ability of the attackers, using AI approaches, to dynamically change their attack behaviors depending on the context is quite alarming. In addition, using AI in the countermeasures and mitigation side illustrates its impact in making the defense more systematic and robust.

It is important to highlight that while AI can offer significant benefits in cybersecurity, it is essential to recognize that this technology has potential challenges and limitations. One concern is that AI systems may be vulnerable to attacks by manipulating their algorithms or exploiting vulnerabilities in the hardware or software they run on [90]. Additionally, there is the potential for AI systems to make mistakes or produce false positives, which could result in unnecessary alerts or the disruption of legitimate activities [91]. It is essential for organizations to consider these potential challenges carefully and to respond appropriately to mitigate them.

6. Conclusion

The growing usage of artificial intelligence in technologies has expanded the horizon of advancing technologies, devices, applications, and services that serve and affect our lives. These developments in AI have no limit on what they are capable of and need to be entirely under our eyes and control as the impact of using the advanced methods of AI negatively attacks IoT devices attached to our bodies, homes, and vehicles. In general, our cities' infrastructure could be fatal. This paper discussed some of the leading IoT applications, such as smart cities, smart homes, and smart grids, and how we benefit from these technologies.

Moreover, this paper surveyed and investigated the recent AI-based cybersecurity attacks and countermeasures on IoT networks. The AI techniques frequently used within IoT environments can be categorized as machine learning and deep learning. The paper discussed that AI could be used adversely to generate malicious codes used as malware, for instance, which can change its behavior frequently to evade IDS detection or poison AI data-

sets, modules, and algorithms to form different behavior from what it was intended to do. Also, AI techniques can serve as remedies and corrective countermeasures to IoT attacks. AI techniques enhance IoT threat mitigation through self-organizing routines, elevating system performance for human users and IoT devices.

The analysis conducted in this paper reveals the power of AI in making attacks more sophisticated and sometimes undetectable. In addition, using AI in the countermeasures and mitigation side illustrates its impact in making the defense more systematic and robust.

However, the need for more usable datasets impedes assessing the practical efficiency of ML and DL protection systems. Due to ongoing theoretical development, optimizing AI and ML/DL model efficiency requires further explanation. Emerging learning methods and innovative techniques are pivotal for precise data comprehension. As this paper focuses on the adversary utilization of AI in the IoT community in addition to attack mitigation, it is essential to encourage researchers to conduct more research on the AI models themselves. This includes the focus on how AI technologies may be able to detect any slight deviation from the behavior that AI models and algorithms do on the original behavior. In addition, it is important to examine the potential benefits and risks associated with using AI in cybersecurity, including privacy, bias, explainability, and accountability.

References

[1] Hologram, "What's Ahead for IoT in 2023?" IoT For All, Dec. 30, 2022. https://www.iotforall.com/whats-ahead-for-iot-in-2023 (accessed Nov. 15, 2023).

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of things-IoT: definition, characteristics, architecture, enabling technologies, application & future challenges," International Journal of Engineering Science and Computing, vol. 6, no. 5, 2016.

[4] "Worldwide Internet of Things Spending Guide," IDC: The premier global market intelligence company. https://www.idc.com/getdoc.jsp?containerId=IDC_P29475, 2023.

[5] K. Ashton and others, "That 'internet of things' thing," RFID Journal, vol. 22, no. 7, pp. 97–114, 2009.

[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and Applications," IEEE Communications Surveys & tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[7] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Computer networks, vol.

144, pp. 17–39, 2018.

[8] F. A. Alhaidari and E. J. Alqahtani, "Securing Communication between Fog Computing and IoT Using Constrained Application Protocol (CoAP): A Survey.," J. Commun., vol. 15, no. 1, pp. 14–30, 2020.

[9] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, Mar. 2022.

[10] S. S. Haghshenas, G. Guido, A. Vitale, and S. J. Ghoushchi, "Quantitative and Qualitative Analysis of Internet of Things (IoT) in Smart Cities and its Applications," in 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2022, pp. 1–6.

[11] T. M. Ghazal et al., "IoT for smart cities: Machine learning approaches in smart healthcare—A review," Future Internet, vol. 13, no. 8, p. 218, 2021.

[12] L. Tightiz and H. Yang, "A comprehensive review on IoT protocols' features in smart grid communication," Energies (Basel), vol. 13, no. 11, p. 2762, 2020.

[13] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," International Journal of Critical Infrastructure Protection, vol. 25, pp. 36–49, 2019.

[14] H. Shahinzadeh, J. Moradi, G. B. Gharehpetian, H. Nafisi, and M. Abedi, "IoT architecture for smart grids," in 2019 International Conference on Protection and Automation of Power System (IPAPS), 2019, pp. 22–30.

[15] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: challenges, issues, and solutions at different IoT layers," J Supercomput, vol. 77, no. 12, pp. 14053–14089, 2021.

[16] C. B. Liang, M. Tabassum, S. B. A. Kashem, Z. Zama, P. Suresh, and U. Saravanakumar, "Smart home security system based on Zigbee," in Advances in Smart System Technologies, Springer, 2021, pp. 827–836.

[17] C. Sisavath and L. Yu, "Design and implementation of security system for smart home based on IOT technology," Procedia Comput Sci, vol. 183, pp. 4–13, 2021.

[18] D. G. S. Pivoto, L. F. F. de Almeida, R. da Rosa Righi, J. J. P. C. Rodrigues, A. B. Lugli, and A. M. Alberti, "Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review," J Manuf Syst, vol. 58, pp. 176–192, 2021.

[19] A. N. Jahromi, H. Karimipour, A. Dehghantanha, and K.-K. R. Choo, "Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber-Physical Systems," IEEE Internet Things J, vol. 8, no. 17, pp. 13712–13722, 2021.

[20] S. A. Latif et al., "AI-empowered,

blockchain and SDN integrated security architecture for IoT network of cyber-physical systems," Comput Commun, vol. 181, pp. 274–283, 2022.

[21] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," Future Internet, vol. 11, no. 4, p. 94, 2019.

[22] D. H. Mrityunjaya, N. Kumar, S. Ali, H. M. Kelagadi, and others, "Smart transportation," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)(I-SMAC), 2017, pp. 1–5.

[23] B. Jan, H. Farman, M. Khan, M. Talha, and I. U. Din, "Designing a smart transportation system: An internet of things and big data approach," IEEE Wirel Commun, vol. 26, no. 4, pp. 73–79, 2019.

[24] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," Applied System Innovation, vol. 3, no. 1, p. 14, 2020.

[25] K. Gulati, R. S. K. Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," Mater Today Proc, vol. 51, pp. 161–165, 2022.

[26] R. E. Mohamed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Survey on wireless sensor network applications and energy efficient routing protocols," Wirel Pers Commun, vol. 101, no. 2, pp. 1019–1055, 2018.

[27] I. H. Sarker, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," 2021.

[28] A. N. Ozalp, Z. Albayrak, M. Cakmak, and E. Ozdogan, "Layer-based examination of cyber-attacks in IoT," in HORA 2022 - 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022.

[29] R. Da and M. Zekeriya Gündüz, "Analysis of Cyber-Attacks in IoT-based Critical Infrastructures." International Journal of Information Security, 2020.

[30] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber Security Threats to IoT Applications and Service Domains," Wirel Pers Commun, vol. 95, no. 1, pp. 169–185, Jul. 2017.

[31] Vinugayathri, "AI and IoT Blended - What It Is and Why It Matters?," www.clariontech.com. https://www.clariontech.com/blog/ai-and-iot-blended-what-it-is-and-why-it-matters.

[32] A. Pandse, "Transforming cybersecurity with AI and ML: View - ET CISO," ETCISO.in, Feb. 11, 2019. https://ciso.economictimes.indiatimes.com/news/transforming-cybersecurity-with-ai-and-ml/67899197 (accessed Dec. 04, 2023).

[33] M. Taddeo, T. McCutcheon, and L. Floridi, "Trusting artificial intelligence in cybersecurity is a double-edged sword," Nat Mach Intell, vol. 1, no. 12, pp. 557–

560, Nov. 2019.

[34] M. Kuzlu, C. Fair, and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," Discover the Internet of Things, vol. 1, no. 1, Dec. 2021.

[35] P. Kiourti, K. Wardega, S. Jha, and W. Li, "TrojDRL: Trojan Attacks on Deep Reinforcement Learning Agents," Feb. 2019, [Online]. Available: http://arxiv.org/abs/1903.06638

[36] Y. Ma, K.-S. Jun, L. Li, and X. Zhu, "Data Poisoning Attacks in Contextual Bandits," Aug. 2018, [Online]. Available: http://arxiv.org/abs/1808.05760

[37] E. Montalbano, "Machine Learning Models: A Dangerous New Attack Vector." 2022.

[38] T. Gu, B. Dolan-Gavitt, and S. Garg, "BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain," Aug. 2017, [Online]. Available: http://arxiv.org/abs/1708.06733

[39] J. Shen and M. Xia, "AI Data poisoning attack: Manipulating game AI of Go," arXiv preprint arXiv:2007.11820, 2020.

[40] T. D. Nguyen, P. Rieger, M. Miettinen, and A.-R. Sadeghi, "Poisoning Attacks on Federated Learning-based IoT Intrusion Detection System," Internet Society, Aug. 2021.

[41] Y. Mirsky et al., "The Threat of Offensive AI to Organizations," Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.15764

[42] Y. Shah and S. Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices," in 2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 0406–0413.

[43] M. Sewak, S. K. Sahay, and H. Rathore, "ADVERSARIALuscator: An Adversarial-DRL Based Obfuscator and Metamorphic Malware SwarmGenerator," Sep. 2021.

[44] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe, "A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities," IEEE Access, vol. 6, pp. 48360–48373, Aug. 2018.

[45] S. Nam, S. Jeon, H. Kim, and J. Moon, "Recurrent gans password cracker for IoT password security enhancement," Sensors (Switzerland), vol. 20, no. 11, Jun. 2020.

[46] E. A. AlBadawy, S. Lyu, and H. Farid, "Detecting AI-Synthesized Speech Using Bispectral Analysis," Jun. 2019.

[47] M. Sahidullah et al., "Introduction to Voice Presentation Attack Detection and Recent Advances," Jan. 2019, [Online]. Available: http://arxiv.org/abs/1901.01085

[48] D. Harwell, "An artificial intelligence first: Voice-mimicking software reportedly used in a major theft," Washington Post, Sep. 04, 2019. Available: https://www.washingtonpost.com/tech-

nology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/.

[49] A. Javed, K. M. Malik, A. Irtaza, and H. Malik, “Towards protecting cyber-physical and IoT systems from single- and multi-order voice spoofing attacks,” Applied Acoustics, vol. 183, Dec. 2021.

[50] E. Wenger et al., “‘Hello, It’s Me’: Deep Learning-based Speech Synthesis Attacks in the Real World,” in Proceedings of the ACM Conference on Computer and Communications Security, Association for Computing Machinery, Nov. 2021, pp. 235–251.

[51] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, “A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues,” Electronics (Switzerland), vol. 10, no. 19. MDPI, Oct. 01, 2021.

[52] Rachit, S. Bhatt, and P. R. Ragiri, “Security trends in Internet of Things: a survey,” SN Applied Sciences, vol. 3, no. 1. Springer Nature, Jan. 01, 2021.

[53] Y. E. Sagduyu, Y. Shi, and T. Erpek, “IoT Network Security from the Perspective of Adversarial Deep Learning,” in Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks workshops, 2019.

[54] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, “DeepRing: Protecting deep neural network with blockchain,” in IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2019.

[55] N. Baracaldo, B. Chen, H. Ludwig, A. Safavi, and R. Zhang, "Detecting Poisoning Attacks on Machine Learning in IoT Environments," 2018 IEEE International Congress on Internet of Things (ICIOT), San Francisco, CA, USA, 2018, pp. 57-64.

[56] L. Xiao, X. Wan, and Z. Han, “PHY-Layer Authentication with Multiple Landmarks with Reduced Overhead,” IEEE Trans Wirel Commun, vol. 17, no. 3, 2018.

[57] C. Shi, J. Liu, H. Liu, and Y. Chen, “Smart User authentication through actuation of daily activities leveraging Wi-Fi-enabled IoT,” in Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2017.

[58] D. Dasgupta, Z. Akhtar, and S. Sen, “Machine learning in cybersecurity: a comprehensive survey,” The Journal of Defense Modeling and Simulation, vol. 19, no. 1, pp. 57–106, 2022.

[59] N. A. Stoian, Machine Learning for anomaly detection in IoT networks : Malware analysis on the IoT-23 data set. 2020. [Online]. Available: http://essay.utwente.nl/81979/

[60] B. N. Kiran, R. S. G, and S. A. Balthar, “7993 www.ijariie.com 2707 SECURITY FOR IoT SYSTEMS USING MACHINE LEARNING,” 2018. [Online]. Available: www.ijariie.com

[61] Alam, M. S., Husain, D., Naqvi,

S., & Kumar, P. "IOT security through Machine Learning and homographic encryption technique." In International Conference on New Trends in Engineering & Technology (ICNTET), Chennai, 2018.

[62] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of things devices," in Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018, Institute of Electrical and Electronics Engineers Inc., Aug. 2018.

[63] Z. Ahmad et al., "Anomaly detection using deep neural network for IoT architecture," Applied Sciences (Switzerland), vol. 11, no. 15, Aug. 2021.

[64] I. Ullah and Q. H. Mahmoud, "Design and Development of RNN Anomaly Detection Model for IoT Networks," IEEE Access, vol. 10, pp. 62722–62750, 2022.

[65] D. Tian et al., "An intrusion detection system based on machine learning for CAN-bus," in International Conference on Industrial Networks and Intelligent Systems, 2017, pp. 285–294.

[66] Fatima-tuz-Zahra, N. Jhanjhi, S. N. Brohi, and N. A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning," in 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2019, pp. 1–9.

[67] B. Farzaneh, M. Koosha, E. Boochanpour, and E. Alizadeh, A New Method for Intrusion Detection on RPL Routing Protocol Using Fuzzy Logic. 2020.

[68] K. V. V. N. L. Sai Kiran, R. N. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, "Building an Intrusion Detection System for IoT Environment using Machine Learning Techniques," in Procedia Computer Science, Elsevier BV, 2020, pp. 2372–2379.

[69] A. Kanawaday and A. Sane, "Machine learning for predictive maintenance of industrial machines using IoT sensor data," in Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, IEEE Computer Society, Apr. 2018, pp. 87–90.

[70] Y. K. Teoh, S. S. Gill, and A. K. Parlikad, "IoT and Fog Computing based Predictive Maintenance Model for Effective Asset Management in Industry 4.0 using Machine Learning," IEEE Internet Things J, p. 1, 2021.

[71] W. B. Richardson, J. Meyer, and S. Von Solms, "Towards Machine Learning and Low Data Rate IoT for Fault Detection in Data-Driven Predictive Maintenance," in 2021 IEEE World AI IoT Congress, AIIoT 2021, Institute of Electrical and Electronics Engineers Inc., May 2021, pp. 202–208.

[72] K. Liu, S. Xu, G. Xu, M. Zhang, D. Sun, and H. Liu, "A review of Android malware detection approaches based on machine learning," IEEE Access, vol. 8, pp. 124579–124607, 2020.

[73] T. T. Khoei, H. O. Slimane, and N. Kaabouch, "A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure

Techniques, and Future Directions," arXiv preprint arXiv:2207.07738, 2022.

[74] I. Apostol, M. Preda, C. Nila, and I. Bica, "IoT botnet anomaly detection using unsupervised deep learning," Electronics (Switzerland), vol. 10, no. 16, Aug. 2021.

[75] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," IEEE Access, vol. 6, 2018.

[76] C. Catalano, A. Chezzi, M. Angelelli, and F. Tommasi, "Deceiving AI-based malware detection through polymorphic attacks," Comput Ind, vol. 143, 2022.

[77] S. Sharma, C. Rama Krishna, and S. K. Sahay, "Detection of advanced malware by machine learning techniques," in Advances in Intelligent Systems and Computing, 2019.

[78] A. A. Ahmed, W. A. Jabbar, A. S. Sadiq, and H. Patel, "Deep learning-based classification model for botnet attack detection," J Ambient Intell Humaniz Comput, vol. 13, no. 7, 2022.

[79] J. Ashraf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in the internet of things: Challenges, solutions, and future directions," Electronics (Switzerland), vol. 9, no. 7. 2020.

[80] Q. Abu Al-Haija, A. Al-Badawi, and G. Bojja, "Boost-Defence for resilient IoT networks: A head-to-toe approach," Expert Syst, vol. 39, Jan. 2022

[81] M. Rak, G. Salzillo, and D. Granata, "ESSecA: An automated expert system for threat modeling and penetration testing for IoT ecosystems," Computers and Electrical Engineering, vol. 99, p. 107721, Apr. 2022.

[82] S. Yadav, K. D. Kalaskar, and P. Dhumane, "A Comprehensive Survey of IoT-Based Cloud Computing Cyber Security," Oriental Journal of Computer Science and Technology, vol. 15, no. 1, 2, 2022.

[83] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," Sustainability, vol. 13, no. 6, p. 3196, 2021.

[84] H. Malik and R. Changalvala, "Fighting AI with AI: Fake speech detection using deep learning," in Proceedings of the AES International Conference, 2019.

[85] J. Monteiro, J. Alam, and T. H. Falk, "Generalized end-to-end detection of spoofing attacks to automatic speaker recognizers," Comput Speech Lang, vol. 63, 2020.

[86] T. Chen, A. Kumar, P. Nagarsheth, G. Sivaraman, and E. Khoury, "Generalization of Audio Deepfake Detection," 2020.

[87] Y. Zhang, F. Jiang, and Z. Duan, "One-Class Learning towards Synthetic Voice Spoofing Detection," IEEE Signal Process Lett, vol. 28, 2021.

[88] Z. Jiang, H. Zhu, L. Peng, W. Ding, and Y. Ren, "Self-supervised spoofing audio detection scheme," in Proceedings of the Annual Conference of the International Speech Communication Association, INTERSPEECH, 2020.

[89] M. AbuOdeh, C. Adkins, O. Se-

tayeshfar, P. Doshi, and K. H. Lee, "A novel AI-based methodology for identifying cyber-attacks in honey pots," in Proceedings of the AAAI Conference on Artificial Intelligence, 2021, pp. 15224–15231.

[90] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," IEEE Internet Things J, vol. 6, no. 4, pp. 6822–6834, 2019.

[91] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," Applied Sciences, vol. 9, no. 20, p. 4396, 2019.