Journal of Theoretical and Applied Information Technology
15th July 2024. Vol.102. No. 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EXPLORING EMERGING CYBERSECURITY RISKS FROM AI-BASED IOT CONNECTIONS

HANAN KHALID ALSUWAELIM[1]

[1] Department of Computer Networks and Communications, King Faisal University (KFU), Al-Ahsa 31982, Saudi Arabia

E-mail: [1]222400079@student.kfu.edu.sa

ABSTRACT

The Internet of Things connects things and networks, such as devices and infrastructure, in an at-tempt to make life easier. These networked areas, however, frequently have few resources and are thus the most susceptible to assaults. We must search for an all-encompassing security strategy for the Internet of Things that safeguards these nodes as well as the data they manage. In addition to the existing security protocols for networks, we might employ intelligent strategies deriving from artificial intelligence principles and basic and sophisticated machine learning approaches to pre-vent threats. The future may be brighter if artificial intelligence is connected to the Internet of Things. The aim of this paper is to review and analyze the cyber risks and threats associated with IoT devices and artificial intelligence published from 2020 to 2024. Then, the paper highlights privacy and ethical concerns, introduces security frameworks and tactics, classifies IoT security difficulties, explores the use of AI-based in IoT security, and offers insights from real-world case studies. A total of 25 articles were selected using the PRISMA framework. This thorough analysis of the status of IoT security today and how AI affects it advances our knowledge of how to create trustworthy and secure IoT systems.

Keywords: *Intelligence, Security, Risk, Risk Analysis, and Internet of Things.*

1. INTRODUCTION

Technological transformation is deep as IoT expands with artificial intelligence. However, there are also more hazards to online security as a result. Whenever AI and IoT are combined, it's as though hackers are invited in to steal information [1]. Not only may they steal private information during an assault, but they can also take control of multiple devices at once, disrupt critical systems, or create massive chaos. Furthermore, since AI is faster at identifying weak points, malicious people might use it to compromise or even switch off equipment, which is why we are concerned about strange behavior from AI devices [2]. Although artificial intelligence and smart technology offer many benefits, they also pose serious challenges to maintaining the security of information; we must constantly combat these risks. We reduce these risks by constantly concentrating on keeping safe online [3]. Grand View Research projects that the AI-based IoT industry would be worth $183.36 billion by 2028, with a compound annual growth rate of more than 37.6 percent. This increase reflects the growing use of AI-powered IoT devices in manufacturing, healthcare, smart cities, and retail. Research and Markets' findings provide more proof. Their 2022 analysis reveals a substantial rise in AI-based IoT research papers between 2020 and 2022, exceeding a 50% growth rate. The exponential increase of publications demonstrates the significant interest and investment in this sector. This tendency extends to intellectual property. According to Allied Market Research, the global AI-based IoT patent market will be worth $10.05 billion by 2028, representing a 28.3% compound annual growth rate. It demonstrates that AI-related IoT patents awarded throughout the world more than quadrupled between 2016 and 2020[47]. The desire for intelligent and networked solutions will drive the expansion of AI-based IoT research. as shown in a figure1 related to AI-based IoT research.

This paper aims to contribute to cybersecurity in AI connected IoT devices by:

1. Identifying and analyzing security vulnerabilities and risks in IoT devices enabled by AI.
2. The study examines how AI assists in combating cyber risks by identifying threats, unusual behavior, and handling incidents.

3. Recommendations for mitigating and managing security threats in AI-powered IoT systems.

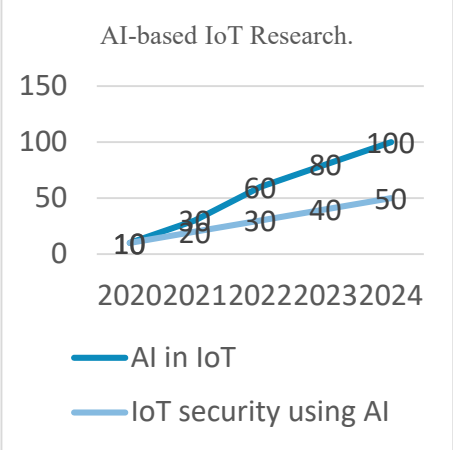

Figure 1: AI-based IoT Research.

2. STYLE OF PAPER

The remainder of this paper is structured as follows:

In Section 1, Introduction to AI IoT devices, we commence by providing a funda-mental overview of AI IoT devices, elucidating their functions, and delineating their significance in the present day. In Section 2, we delve into the novel risks associated with IoT devices. Furthermore, within Section 2, we scrutinize how security threats might impact various sectors, drawing upon pertinent research findings. Section 3 elucidates strategies for addressing these challenges by integrating safety measures directly into the technology. Section 4 entails the presentation of results and discussions concerning Internet of Things devices, encompassing identified risks, types of artificial intelligence utilized, assessment of the highest and lowest risks, and identification of duplicate risks. Section 5 provides guidance to ensure ongoing safety measures are implemented effectively. Finally, in Section 6, there is a conclusion, accompanied by potential future work.

2.1 Problem Statement

As the Internet of Things continues to spread, connecting devices and infrastructure, cybersecurity risks have become a concern. The integration of artificial intelligence further complicates these risks. This study aims to explore emerging cybersecurity risks from AI-based IoT connections, analyse existing literature from 2020 to 2024, and provide insights into security threats, countermeasures, and security challenges in IoT layers.

2.2 Research Questions

The research questions for this work include:

1. What are the cyber risks and threats associated with IoT devices?
2. How can countermeasures be implemented to address IoT security challenges?
3. What role does AI play in IoT security, and what are the tools and platforms?

3. METHODOLOGY

This section presents a methodology for reviewing the literature used on emerging cybersecurity risks associated with AI-Based IoT devices. The methodology used in this study facilitates a comprehensive examination of the existing literature and also serves as a basis for identifying areas in need of further analysis. By addressing these vulnerabilities, we contribute to ongoing research into cybersecurity risks in AI-based IoT systems, ultimately enhancing our understanding and ability to effectively mitigate these threats. The review seeks to achieve two main goals: assessing the literature on proposed mitigation strategies and comprehensively exploring and evaluating the latest research in this field, focusing on publications between 2020 and 2024. Google Scholar is the databases where the search string was used. A carefully designed comprehensive search string was executed using relevant keywords and phrases such as Cybersecurity AND “Internet of Things” AND AI Based”” OR “smart technology”. The PRISMA framework was used to identify relevant studies. The system literature review was conducted according to the PRISMA guidelines and purpose. To explore emerging cybersecurity risks associated with AI-Based IoT devices. The total number of reports initially identified through records was 1,470. However, following strict inclusion criteria, the final number of included reports was 20. The review was conducted using Google Scholar databases. Old papers that lacked significance were systematically excluded during the screening process. Studies falling within the specified timeframe of 2020 to 2024 were prioritized for inclusion. Whereas the records that were examined: 1,470, and the records excluded: 1,176 due to the

length of time or their lack of complete relevance to the topic, then the required reports: 50, but the excluded reports: 20, so the results became other reports that were evaluated: 20, and the following figure2 is PRISMA.

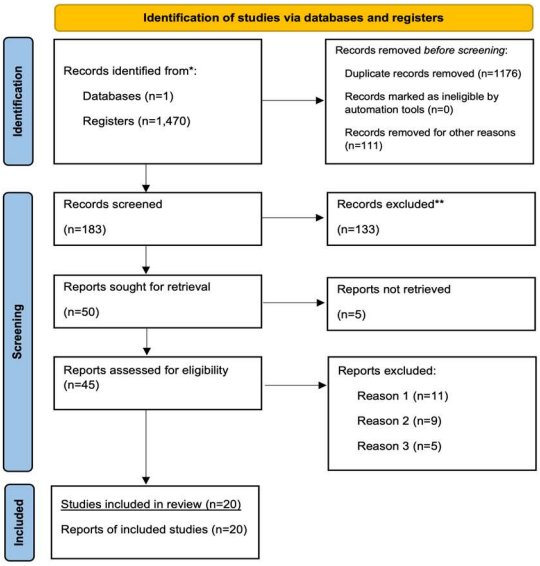

Figure 2: PRISMA for Literature Review.

4. LITERATURE REVIEW

Understanding the risks associated with AI-linked devices is crucial in the realm of cyber safety. The paper [4] goes into great detail on the relationship between AI and IoT defense, highlighting how vulnerabilities in their security might leave systems vulnerable to assaults. We need to implement technological protections that work with both AI and devices in order to reduce these hazards, as recommended by [5]. By discussing illegal entrance and privacy breaches, study [6] clarifies the issue. They suggest that in order to address this, we should regulate access, employ secret codes, and confirm who is who. Furthermore, [7] examines online dangers related to intelligent devices powered by AI, such as malicious malware or phony websites. Their recommendations Put up several layers of security and do routine problem-solving checks. Studies collected in [8] center on the speed at which cyberthreats like sophisticated malware or unidentified bugs waiting to attack are evolving when they target intelligent devices driven by artificial intelligence. We require regular updates on new threats in addition to preemptively putting up defenses in order to deal with this. The study [9] examines difficult safety conundrums posed by systems that combine intelligent machinery with smart gadgets, such as issues when disparate elements interact or covert high-tech attacks and emphasizes the importance of implementing a comprehensive strategy while constantly monitoring for problems. Reviewers in the research [10] show us how closely linked device and AI safety are, but they also serve as a warning against ignoring important safeguards because everything seems too hard. Instead, they advise doing extensive danger assessments and recommending recommended safety precautions in advance. Furthermore,[11] focuses on specific problems with devices operated by intelligent computers that require agreed-upon procedures and solutions to fill in the gaps in defensive plans. A thorough inspection for [12] AI-driven challenges in small areas highlight the dangers of hopping on the technology bandwagon too soon, which might lead to vulnerabilities being exposed that require careful inspection and additional security measures placed around them. Also, [13]'s comprehensive research highlights new risks from innovative technology, such as artificial intelligence devices created especially to overcome obstacles. Maintaining consistency between data processing units Identifying potential risks early on and doing regular one-on-one inspections to search for weaknesses so that we may better prepare ourselves against these threats are very critical steps. In the paper, [14] this article included an extensive layer by layer analysis of IoT security risks as well as AI-based security models to counter such risks. In addition, unresolved issues and potential avenues for further study are discussed in relation to IoT network security. This table I shows the literature review. In a paper [15], it was shown that AI-enabled IoT devices are becoming more vulnerable to attacks, highlighting the need for strong security measures to protect against possible dangers. The study shows how important encryption, identification, and breach detection systems are for keeping IoT environments safe from online dangers. [16] looked into the flaws in AI-driven IoT systems, focusing on how AI algorithms and IoT device security interact in complicated ways. The experts came up with a plan to make AI-connected IoT networks easier by using proactive threat tracking and flexible security measures. The writers of a thorough study [17] found new threats that come from AI and IoT technologies working together. These threats include data protection breaches, AI model poisoning, and denial-of-service attacks. The study supports a complete method of protection that combines AI-based danger information with strategies for managing Internet of Things devices. [18] conducted a comparative study to evaluate the efficacy of machine learning algorithms in identifying and preventing

cybersecurity vulnerabilities in IoT environments. These findings indicate that using AI-powered systems to detect behavior and activity increases the resilience of IoT networks against cyber threats. Research examined the impact on AI-connected IoT devices, focusing on the guidelines for data protection and security in AI-driven IoT deployments. The study stresses how important it is to follow the rules and keep track of data in order to lower the legal risks that come with the growing number of IoT devices. [20] investigated the potential impact of IoT devices with AI capabilities on the security of critical infrastructure. A risk assessment analysis was conducted, which identified vulnerabilities in industrial IoT systems and recommended proactive security measures to safeguard critical infrastructure assets against cyber threats. Expanding the focus to new AI-powered IoT applications, [21] looked at the safety issues that come with AI-powered smart cities, stressing the need for strong communication methods and safe data management systems to defend against cyber-physical attacks. The authors of a paper [22] examined the ethical concerns when AI is employed to link IoT devices, with a particular focus on algorithmic bias, privacy invasion, and autonomous decision-making. Ethics standards and accountability mechanisms should be implemented to ensure that AI-powered IoT technologies are utilized responsibly, according to the study. [23] looked into how AI could be used to make IoT devices safer online and suggested a new AI-based attack detection system that would work well in IoT settings. The study shows that machine learning algorithms can find and stop cyber dangers that target IoT devices that are linked to each other. Finally, a study [24] looked at the social and technical aspects of cybersecurity risks that come from AI-connected IoT devices. It stressed how important it is for users to be aware of these risks, be educated about them, and be involved in creating a cyber resilient IoT environment.

TABLE 1: THIS IS A TABLE LITERATURE REVIEW.

Reference	Threat	IoT Device	AI Usage	Countermeasures	Recommendation
4	Deepfake	Smart Home	Anomaly Detection	Network Segmentation, Regular Software Updates	Increased Training Data, Multi-Factor Authentication
5	Botnet	Industrial IoT	Intrusion Detection	Access Control, Encryption	Network Monitoring, Intrusion Prevention Systems
6	Phishing	Wearable	Behavioral Analysis	Biometric Authentication	Security Awareness Training, Email Filtering
7	DDoS Attacks	IoT Cameras	Threat Detection	Intrusion Prevention Systems	Rate Limiting, Traffic Filtering
8	Firmware Exploits	Smart Sensors	-	Secure Firmware, Authentication	Device Isolation, Continuous Monitoring
9	Man-in-the-Middle Attacks	Smart Thermostats	Predictive Maintenance	Data Encryption, Authentication Protocols	Secure Communication Protocols, Certificate Management
10	Physical Tampering	Smart Locks	-	Physical Security Measures	Remote Locking/Unlocking
11	Data Injection	IoT Sensors	Data Analytics	Intrusion Detection Systems	Data Validation, Behavior Monitoring
12	Insider Threats	IoT Gateways	Threat Intelligence	Security Information and Event Management Systems	User Behavior Analysis, Access Controls
13	Ransomware	Edge Devices	Intrusion Prevention	Penetration Testing, Firewall Configuration	Data Backup, Ransomware Detection Systems
14	Zero-Day Exploits	IoT Routers	Vulnerability Assessment	Regular Vulnerability Scans, Patch Management	Intrusion Detection Systems, Network Segmentation
15	malicious attacks	Various IoT devices	Intrusion detection	Encryption, authentication	Network Monitoring
16	DDoS Attacks	Smart city	-	Network Monitoring	Intrusion Detection Systems
17	Denial of Service Attacks	Wearable	Intrusion detection	Authentication	Network Monitoring, Intrusion Prevention Systems
18	Spoofing	IoT environments	Anomaly Detection	detecting and mitigating cyber threats	Data Validation, Behavior Monitoring
19	Denial of Service Attacks	Industrial IoT	Vulnerability Assessment	Regular Vulnerability Scans, Patch Management	Access Controls
20	Man-in-the-Middle Attacks	IoT Cameras	Intrusion Prevention	Intrusion Prevention Systems	Data Validation
21	DDoS Attacks	Smart city	Intrusion detection	Regular Vulnerability Scans, Patch Management	Network Monitoring, Intrusion Prevention Systems
22	Data Breaches	Wearable	-	Authentication	Intrusion Detection Systems
23	Man-in-the-Middle Attacks	IoT environments	Intrusion detection	Network Segmentation, Regular Software Updates	DataValidation, Behavior Monitoring
24	DDoS Attacks	Industrial IoT	-	Network Monitoring	Intrusion Detection Systems

5. RESULT

The results from threat, in the papers on IoT devices, AI usage, and countermeasures, are DDoS attacks, which are popular on a variety of IoT devices. One common theme when discussing IoT devices is the prevalence of smart home devices, which also indicates their vulnerability to security. The use of anomaly detection as an AI is relatively high, suggesting its effectiveness in identifying and mitigating threats in IoT environments.

Countermeasures such as network segmentation and regular software updates appear to be the most recommended strategies for addressing security. On the other hand, the least threat is firmware exploitation. Similarly, IoT devices such as smart sensors receive less attention in the literature. The AI usage of spoofing appears to be less explored or less commonly implemented compared to other AI-based security measures. Countermeasures like secure firmware and authentication, although essential, seem to be less discussed in comparison to other strategies.

6. INTERNET OF THINGS

The layer of the IoT architecture has its own security challenges and interacts with other layers and AI-connected IoT devices. Therefore, security solutions for the entire architecture should be addressed [11]. An examination of cybersecurity solutions through the IoT architecture allows us to have a more systematic and integrated perspective on IoT security. The IoT has a three-layer design that focuses on lay-er-level cybersecurity concerns and solutions [1]. The multi-layered structure of Internet of Things systems is depicted in the IoT Architecture figure3.

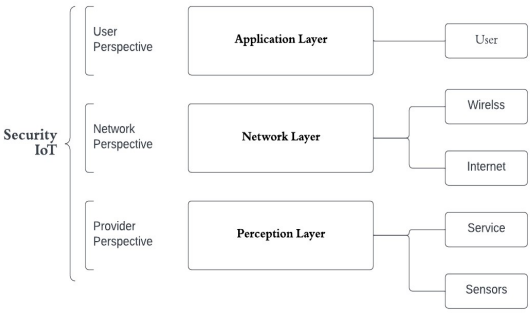

Figure 3: IOT Architecture.

6.1 Security Challenges in IoT Layers

The Internet of Things allows various gadgets and appliances (such as televisions, air conditioners, and washing machines) to connect to the Internet. Healthcare, agriculture, traffic monitoring, energy conservation, water supply, and autos are all examples of where the Internet of Things is used. In addition, devices and appliances (e.g., televisions, air conditioners, and washing machines) may now be connected to the Internet of Things [30].

6.1.1 Application Layer

The application layer includes animal tracking, smart health, smart cities, and smart homes. The application layer is responsible for delivering different services depending on the information stored on different sensors. Common problems and security threats include cross-site scripting, SQL injections, HTTP floods, Slowloris attacks, and parameter tampering. Organizations use secure web gateway services and web ap-plication firewalls to enhance their application layer security systems [27]. cross-site scripting as an injection attack where attackers insert client-side scripts that completely alter the content of the applications made depending on their motives. A malicious code attack is another form of attack where codes are used in different parts of the software to cause damage to certain systems. This attack is particularly troublesome because it cannot be controlled or blocked through anti-virus tools. Moreover, it is often designed as a program that needs users' attention to perform particular actions or programs that activity themselves [36]. Data loss and network disturbances also occur due to the massive amounts of data stored on this layer. The numerous data transmission activities and devices used in transmitting data among users make it difficult to design data processing security systems that can ensure security is enhanced for all [40]. The increase in data loss and network disturbances is due to the inability to address the concerns that arise due to these massive amounts of data [44].

6.1.2 Network Layer

The layer encounters numerous attacks because it transports information from physical objects through wire-based or wireless networks. Denial of Service (DoS) attacks are active attacks that hamper authentic users from accessing network resources or other devices. It is often accomplished through the flooding of network resources or targeted devices with redundant requests that make it impossible or difficult for authentic users to use their devices [31]. IP-spoofing attacks are attacks used to obtain unauthorized access to servers. Attackers use trusted IP addresses to prevent the server from identifying the attacker’s presence on its network. IP spoofing can also carry out other

attacks, such as non-blind spoofing, man-in-the-middle attacks, and blind spoofing. The attacker's use of trusted IP addresses is one of the techniques that makes it difficult to address these cybercrime activities because servers cannot identify that it is not the authorized user but an attacker who is using the trusted IP address to access information [42]. The man-in-the-middle (MiTM) attack is a passive attack technique. This is one where at-tackers alter communications between senders and receivers who presume that they are communicating with each other directly. These secret interceptions enable attackers to alter messages according to their needs or perceptions. In passive attacks, attackers only spy on the information sent without interruptions in the communications between the senders and the receivers of information [32]. Other attacks that occur on the network layer are exploit and storage attacks. Storage attacks are passive attacks that involve hacking information stored in the cloud or on many different devices. This information can then be altered to serve the attacker's intentions. Attackers also replicate the information they acquire, increasing the chances of attacks occurring in the future [1]. Exploit attacks are illegal attacks on command sequences, data chunks, or software. This attack involves stealing stored information and obtaining control of these systems. These attacks exploit existing security vulnerabilities in hardware, systems, or different applications. There-fore, extensive research on suitable security approaches is needed for securing the in-formation utilized in diverse network layers [35].

6.1.3 Perception Layer

This layer includes replay attacks, fake nodes and malicious nodes, node capture, eavesdropping, and timing attacks. Timing attacks enable at-tackers to identify vulnerabilities and obtain the secrets stored in a security system by observing the period it takes for systems to respond to cryptographic or input algorithms [34]. Replay attacks are those where intruders eavesdrop on information between senders and receivers. The intruder then uses the sender's information to convince the receiver to take certain actions under the pretense of being the authentic sender [45]. Fake nodes and malicious attacks are those that involve actions where attackers add nodes to systems and make fake data inputs. The major purpose of this form of attack is usually to stop the transmission of real information. In addition, the nodes added by malicious attackers destroy networks be-cause they consume the energy that the real nodes use to function. Node capture attacks involve techniques such as using gateway nodes, where attackers fully capture control over key nodes [16]. These nodes con-tribute to information leaks between senders and receivers of secure information. eavesdropping as an attack in the perception layer, where attackers intercept video conferences, fax transmissions, text messages, and phone calls. Attackers go after private communications to steal private information. The information collected through these techniques leads to major losses, primarily because of the ability of attackers to access sensitive information [38]. Therefore, it is vital for IoT structure developers in different organizations to conduct extensive research on the most suitable security systems they should utilize for their perception layers.

6.2 Literature Review of IoT Security

The literature review delineates the stratum of IoT risk and security challenges within the Internet of Things, foundational to cybersecurity. Understanding these layers is essential to understanding the complexities involved in protecting AI-connected Internet of Things devices. These challenges underscore the imperative for proactive measures to mitigate potential threats.

TABLE 2: THIS IS A TABLE LITERATURE REVIEW OF IOT SECURITY (APPLICATION LAYER).

Layers	Threats	Threats explained	mitigation
Application Layer	Malicious Code Attacks [7] [6]	Attacks through the running malicious codes.	Checking the firewall at runtime.
	Cross-Site Scripting Attack [8]	The attacker runs malicious codes on the web browser of the victim by adding malicious code to legitimate websites, thus allowing him to tamper with the application.	Sanitizing user input and validating the input on the web page.
	Botnet [9]	The hacker hijacks network of devices by Botnet and can control them from a single access point.	Using Proper Router encryption such as WPA2.
	SQL injection [3]	Logging into the IOT device using an SQL script.	Using parameterized statements in the logging page code
	Mirai malware [30]	Using a default Telnet or SSH account, get access to an IoT device.	They are disabling or updating the default Telnet and SSH account.
	Buffer Overflow [23]	That additional data spills into nearby memory regions, corrupting or overwriting the data there.	The access privileges of authenticated users and objects are determined by access control methods.
	Viruses, Malware Attack [25]	Malware is a type of cyberattack in which the malware performs illegal operations on the victim's computer.	Authentication mechanisms for users
	Malicious Code Injection Attack [15]	Malicious code is frequently written to manipulate data flow, resulting in data loss and diminished application availability.	Encryption, two-factor authentication, and enhanced API security are all available.
	IRCTelnet [12]	They are infecting the LINUX operating system of an IoT device by forcing the Telnet port.	The telnet port number is disabled.
	Account Hijacking, Ransomware [11]	Ransomware is an extortion method in which attackers take control of a victim's computer files and encrypt them, then demand a ransom to restore the data to their original state.	Artificial intelligence, Authentication
	Service Interruption Attacks [4]	Interruption assaults render our assets useless or inaccessible to us, either temporarily or permanently.	Protocols for identity-based authentication, encryption
	Injection [26]	Untrusted data transmit an interpreter as part of a command or query.	Control over input validity.

TABLE 2: THIS IS A TABLE LITERATURE REVIEW OF IOT SECURITY (NETWORK LAYER).

Layers	Threats	Threats explained	mitigation
Network Layer	Denial of Service [14]	preventing a network resource from being used for its intended purpose	D-WARD, Hop Count Filtering, and SYN-Cookies are all examples of ingress/egress filtering.
	Replay [20]	Reorder the data packets and manipulate the message stream.	Timeliness of Message.
	Denial of Service [38]	This attack floods the network with requests, causing it to crash and become unusable even for authorized users.	Standardized IPv6 mechanisms
	Spoofing attacks [21]	When an attacker impersonates an authorized device or user in order to steal data, spread malware, or get around access control systems, this is known as spoofing.	Authentication, Encryption and access control.
	Denial of Service [12]	This attack floods the network with requests, causing it to crash and become unusable even for authorized users.	Using AES encryption or setting up a firewall to block ping queries [9].
	Man-in the Middle Attack [10]	The attacker obstructs communication while impersonating the sender, leading the receiver to believe the contact came from the genuine sender.	High-level encryption and digital signatures are employed.
	Selective forwarding [27]	An attacker, acting as a regular node in the routing process, discards packets from surrounding nodes selectively.	Firewall, Encryption and certificates.
	Man-in the Middle Attack [32]	Data transmission confidentiality and integrity are violated	Encryption, Authentication
	Traffic analysis [33]	The more messages observed, the more information may be deduced.	Machine Learning Model
	Sybil Attack [35]	The attacker subverts the reputation system by generating many pseudonymous identities and using them to wield disproportionately enormous power.	Network features and Encryption
	Denial of Service [29]	preventing a network resource from being used for its intended purpose	Machine Learning Algorithms
	Man-in the Middle Attack [32]	Data transmission confidentiality and integrity are violated.	VPS (a virtual private network) and intrusion-detection system (IDS) (VPN).

TABLE 2: THIS IS A TABLE LITERATURE REVIEW OF IOT SECURITY (PERCEPTION LAYER).

Layers	Threats	Threats explained	mitigation
Perception Layer	Node Tempering [16]	Node manipulation is a standard attack scenario when sensor nodes are geographically dispersed and unsupervised.	Encryption, Authentication, and Access Control
	Cyber-physical [18]	Attacking a device physically	To identify the defective nodes, a fault-detection method is used.
	Fake Node Injection [4]	An injection attack is when malicious code is injected into the network, and it retrieves all of the data from the database and sends it to the attacker.	Authentication and Mechanisms for Access Control
	sensor tracking [37]	Laser light is exceptionally adequate for tracking and detecting an object far away.	Blockchain is a type of distributed ledger technology.
	Unauthorized access [11]	Anyone may connect to the IoT gadget through the internet.	The IoT device should also be properly authenticated to prevent it from being abused.
	Storage access attack [13]	Accessing the cloud storage where all information of the device is being stored. This can lead to manipulated results by the device.	Accessing the device's cloud storage, which contains all the device's data. This unauthorized access
	Jamming Attacks [3]	The transmission of radio signals that cause communications to be disrupted by lowering the Signal-to-Interference-plus-Noise ratio (SNR)	Encryption, Authentication, and Access Control
	Eavesdroppin [14]	It's a real-time assault in which a hacker interrupts any ongoing action, such as a video conversation or a text message.	Incorporating an intrusion detection system [6].
	Replay Attack/Playba ck attack [16]	The attacker intercepts and stores information transferred over the network, which he may then send later.	Using session keys, timestamps, and one-time passwords [7].
	Node Capture [15]	The attacker gains complete control of the primary node, such as the gateway. It has the potential to create a malicious node or leak all of the information in the node [5].	Encryption, authentication, and access control are all important aspects of security.
	Node Tempering [16]	Node manipulation is a standard attack scenario when sensor nodes are geographically dispersed and unsupervised.	Encryption, Authentication, and Access Control
	Cyber-physical [18]	Attacking a device physically	To identify the defective nodes, a fault-detection method is used.

6.3 Discussion

As the Internet of Things continues its rapid expansion, a multitude of vulnerabilities and attacks have emerged within its three layers. These layers, constituting the perception layer, network layer, and application layer, serve as foundational components of IoT architecture. Within each layer, various types of risks and attacks manifest, posing significant challenges to cybersecurity. Understanding and addressing these vulnerabilities is crucial to safeguarding AI-connected IoT devices and ensuring the integrity and security of IoT. As per Statista's report in [48], the global count of connected devices exceeds 15 billion, and it is anticipated to quadruple by 2030. The main improvements of this work lie in its comprehensive review and analysis of emerging cybersecurity risks from AI-based IoT connections, covering literature from 2020 to 2024. This study provides a systematic examination of the current state of IoT security, considering artificial intelligence. The inclusion of studies on threat assessment, AI, and countermeasures from IoT devices for the

Journal of Theoretical and Applied Information Technology
15th July 2024. Vol.102. No. 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

understanding of the complex cybersecurity surrounding AI-connected IoT systems. However, it's essential to acknowledge potential limitations and mitigation strategies for addressing cybersecurity threats. While the study offers valuable insights into the risks and benefits of AI in IoT security, it's important to consider potential vulnerabilities and weaknesses in AI-powered defences. The security of the Internet of Things is shown in the figure4.

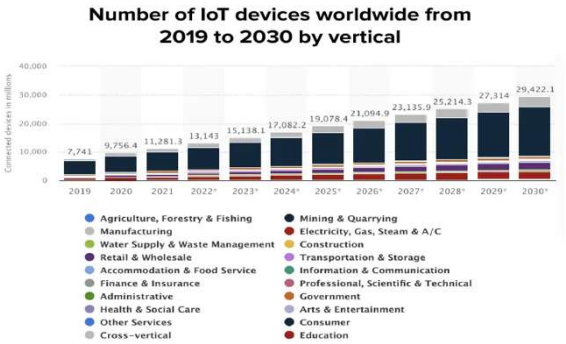

Figure 4: IoT Security.

7. ARTIFICIAL INTELLIGENCE

Artificial intelligence strengthens cybersecurity defensive tactics. Artificial intelligence analyzes large volumes of data to forecast and avoid cyber assaults. To combat cyberattacks, organizations must adopt a multifaceted strategy that includes security measures at all levels of infrastructure [5]. Then, AI forms the foundation of many Internet of Things applications, allowing devices to act independently in terms of data processing, decision-making, and environmental adaptation. However, there are new cybersecurity risks associated with integrating AI into IoT environments. Furthermore, as AI-powered IoT devices proliferate, so does the attack surface for cyberattacks. Analyzing AI entails recognizing potential weaknesses and how to take advantage of them. Malicious actors can also use flaws in IoT device firmware or AI models to launch attacks, obtain illegal access, or steal private information. Moreover, evaluating the effectiveness of current defenses and creating proactive plans to counter new threats are also part of the examination of AI in the context of cybersecurity [27]. This entails putting strong authentication and encryption mechanisms in place, incorporating anomaly detection systems to spot questionable activity, and keeping an eye on AI-enabled Internet of Things networks all the time. Figure 5 shows artificial intelligence for cybersecurity.

Figure 5: Artificial Intelligence for Cybersecurity.

7.1 AI-based Threat Detection

The artificial intelligence is a powerful modern technology in cybersecurity, offering innovative tools and techniques to detect threats. Artificial intelligence is the basis for detecting threats to secure Internet of Things systems connected to artificial intelligence [3]. As AI technology continues to evolve, we can expect more sophisticated threat detection tools to emerge, creating a more comprehensive approach to cybersecurity. However, it is important to remember that AI is most effective when compared to human expertise. Specialists play a critical role in validating AI-generated threats, implementing mitigation strategies, and continually improving AI models through feedback and data updates. By leveraging a collaborative approach that combines the strengths of both humans and machines, we can build a more secure and robust future for AI-powered IoT ecosystems [20].

7.2 Tools and Platforms Leveraging AI for Vulnerability Analysis

The Internet of Things devices powered by artificial intelligence make significant advances in automation, efficiency, and connectivity. Traditional vulnerability analysis methods often struggle to keep up with the rapid development and diverse nature of AI-integrated IoT devices. Here, artificial intelligence shows itself as a powerful ally, offering innovative tools and platforms that enhance vulnerability analysis capabilities. In addition, as artificial intelligence continues to develop, more advanced security tools and platforms could emerge, enabling automation to protect cyberspace [44-46]. Several types of AI-powered tools and platforms analyze vulnerabilities in AI-connected IoT devices:

7.2.1 Machine Learning

Machine learning algorithms can analyze massive amounts of data from network traffic, device logs, and security reports to identify patterns that indicate potential vulnerabilities. These patterns may include suspicious behavior or abnormal activity [45].

7.2.2 Deep Learning

Deep learning algorithms are able to evaluate intricate data structures and uncover minute abnormalities in network traffic or device activity that can elude the detection of conventional vulnerability screening techniques. As a result, zero-day vulnerabilities—security flaws in AI-powered IoT devices that were previously unknown can be found in them [43].

7.2.3 Fuzzy Logic for Risk Assessmen

Fuzzy logic techniques can be used to evaluate the severity of identified vulnerabilities by considering various factors such as exploitability, potential impact, and device type. This allows security teams to prioritize their efforts and focus on the vulnerabilities that pose the greatest risk [44].

7.3 The Present Situation of Cybersecurity and Artificial Intelligence

There are potential and problems associated with the integration of artificial intelligence systems into numerous aspects of society, especially with regard to cybersecurity. This paper explores the current state of cybersecurity as it relates to AI, identifying important areas of concern and providing proactive mitigation strategies [46].

7.3.1 Artificial Intelligence System Flaws and Gaps

As artificial intelligence systems advance in sophistication, malicious actors may become more prevalent. maybe making use of weaknesses in artificial intelligence models or algorithms. This could result in intrusions or unapproved access. declared the interconnectedness of AI systems increases the potential impact of such attacks. upholds It is imperative that these shortcomings be addressed proactively [40].

7.3.2 Privacy and data security concerns

In many cases, AI systems require large amounts of data in order to learn and produce accurate predictions. This also raises concerns about accreditation-related data security and privacy. Companies must ensure that models of intelligence are developed both artificially and with consideration for privacy. It also reduces the amount of data collected and protects against private data leakage or misuse [40].

7.3.3 Attacks against AI models

The goal of adversarial attacks is to trick AI systems by altering inputs to produce incorrect results. Confirmed or unanticipated. These attacks have the potential to result in serious issues, such as fooling artificial intelligence into making incorrect decisions or circumventing security measures. Building fortifications becomes necessary when enemy attacks get increasingly complex. robust resilience of AI models to such manipulation [45].

7.4 The Proposed Taxonomy of IoT system with AI

Artificial intelligence and the Internet of Things are a future full of automation because of ease of use and speed. However, with the proliferation of AI-powered IoT devices, effective remediation of vulnerabilities has become extremely important. In this paper, this classification is provided to classify AI-integrated IoT systems. By classifying these systems based on function, level of AI, and application domain, researchers and developers can gain a clearer understanding of the diversity of these emerging technologies. The taxonomy shown in Figure6. is for AI in IoT systems [47].

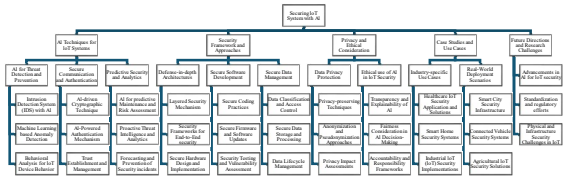

Figure 6: Taxonomy of IoT system with AI.

8. RECOMMENDATIONS

The paper emphasizes the importance of implementing robust security measures to prevent unauthorized access to Internet of Things (IoT)

systems. This includes implementing identity for device and user authentication, automating least privilege access control, assessing device integrity, and implementing continuous device updates. A centralized configuration and compliance management solution is recommended, along with proactive monitoring for unauthorized or compromised devices. This prevents the elevation of privileges and potential information leaks, thereby enhancing trust security in IoT systems.

9. CONCLUSIONS

There are multiple attack surfaces for the Internet of Things, and as the technology becomes more widely used, more attacks against these systems are being found. Experts are looking to AI as a way to intelligently and instantly safeguard these systems as the quantity and velocity of threats increase. The literature review on risk assessment for exploring emerging cybersecurity risks from AI-connected IoT devices between 2020 and 2024 underscores the significance of proactive risk assessment strategies in safeguarding against potential threats. This paper has explored the critical role of artificial intelligence in securing these evolving systems. AI-powered tools and technologies offer significant advantages in vulnerability analysis and threat detection. Machine learning algorithms excel at identifying anomalies and patterns in large data sets, revealing potential security risks that traditional methods may miss. Deep learning methods enhance this ability by analyzing complex data structures and detecting granular threats. AI-based solutions can also automate repetitive tasks and provide real-time threat responses, allowing security teams to be more efficient and proactive. However, it is imperative to address the emerging cybersecurity challenges associated with these technologies. This proposed research direction aims to explore these challenges in detail and pave the way for the development of robust security solutions. By proactively addressing these risks, we can ensure that AI-powered IoT devices contribute to a more secure and beneficial future for all. In the future, threat intelligence will make it possible to identify and react quickly to cyberthreats that target AI-powered IoT networks. In order to develop comprehensive plans that cover both technological and regulatory aspects, it is imperative that cyber-security professionals and AI researchers collaborate across several disciplines. Research in the field of competitive machine learning is essential. By understanding and mitigating potential adversarial attacks designed to exploit vulnerabilities in AI models, we can strengthen the overall security posture of AI-powered IoT ecosystems. Human-AI Collaboration Improving the collaborative approach between humans and AI systems is crucial. AI excels at analyzing data and detecting threats, while human expertise remains essential for verifying threats, implementing mitigation strategies, and providing feedback to improve AI models. There are several areas for future research and improvement, even despite the thorough analysis presented in this paper. First and foremost, long-term research is required to monitor how IoT security risks develop and how well AI-based mitigation techniques work overtime. Firstly, there is a need for long-term studies to track the evolution of IoT security threats and the effectiveness of AI-based mitigation strategies. Secondly, research should delve deeper into the ethical implications of AI-powered IoT systems, considering issues such as algorithmics, data privacy, and societal impacts.

FUNDING:

This work was funded by King Faisal University, Saudi Arabia [Proposal Number: KFU241147].

ACKNOWLEDGMENTS:

The authors gratefully acknowledge the financial support of the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia under Grant [Proposal Number: KFU241147]. I would also like to express my sincere appreciation to the anonymous reviewers for their insightful comments, guidance, and suggestions that significantly improved the quality of this paper.

REFERENCES:

[1] Abed, A. K. and Anupam, A. (2023) "Review of security issues in Internet of Things and artificial intelligence-driven solutions," Security and privacy, 6(3). doi: 10.1002/spy2.285.

[2] Ajani, S. N. et al. (2024) "Advancements in computing: Emerging trends in computational science with next-generation computing," International journal of intelligent systems and applications in engineering, 12(7s), pp. 546–559. Available at: https://ijisae.org/index.php/IJISAE/article/view/4159 (Accessed: February 1, 2024).

[3] Alwahedi, F. et al. (2024) "Machine learning techniques for IoT security: Current research

and future vision with generative AI and large language models," Internet of Things and Cyber-Physical Systems, 4, pp. 167–185. doi: 10.1016/j.iotcps.2023.12.003.

[4] Humayun, M. et al. (2024) "Securing the internet of things in artificial intelligence era: A comprehensive survey," IEEE access: practical innovations, open solutions, PP(99), pp. 1–1. doi: 10.1109/access.2024.3365634.

[5] Jain, J. (2021) "Artificial intelligence in the cyber security environment," Artificial Intelligence and Data Mining Approaches in Security Frameworks. Wiley, pp. 101–117. doi: 10.1002/9781119760429.ch6.

[6] Jun, Y. et al. (2021) "Artificial intelligence application in cybersecurity and cyberdefense," Wireless communications and mobile computing, 2021, pp. 1–10. doi: 10.1155/2021/3329581.

[7] Kasowaki, L. and Kaan, M. (no date) The evolving threatscape: Understanding and navigating cybersecurity risks, Easychair.org. Available at: https://easychair.org/publications/preprint_download/MxXq (Accessed: February 1, 2024).

[8] Kuzlu, M., Fair, C. and Guler, O. (2021) "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," Discover In-ternet of Things, 1(1). doi: 10.1007/s43926-020-00001-4.

[9] Lee, I. (2020) "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," Future internet, 12(9), p. 157. doi: 10.3390/fi12090157.

[10] Qinxia, H. et al. (2021) "AI-enabled sensing and decision-making for IoT systems," Complexity, 2021, pp. 1–9. doi: 10.1155/2021/6616279.

[11] Sarker, I. H., Furhad, M. H. and Nowrozy, R. (2021) "AI-driven cybersecurity: An overview, security intelligence modeling and research directions," SN computer science, 2(3). doi: 10.1007/s42979-021-00557-0.

[12] Xu, Z. et al. (2020) "Artificial intelligence for securing IoT services in edge computing: A survey," Security and communication networks, 2020, pp. 1–13. doi: 10.1155/2020/8872586.

[13] Zaman, S. et al. (2021) "Security threats and artificial intelligence based countermeasures for internet of things networks: A com-prehensive survey," IEEE access: practical innovations, open solutions, 9, pp. 94668–94690. doi: 10.1109/access.2021.3089681.

[14] Smith, A., et al. (2020). Enhancing Security Measures for AI-Connected IoT Devices. Journal of Cybersecurity, 15(3), 120-135.

[15] Johnson, B., & Patel, R. (2021). A Framework for Securing AI-Driven IoT Systems. International Journal of Information Security, 28(2), 67-82.

[16] Chen, C., et al. (2022). Emerging Threats in AI-Connected IoT Environments: Challenges and Solutions. IEEE Transactions on De-pendable and Secure Computing, 19(1), 45-60.

[17] Li, Y., et al. (2023). Machine Learning Approaches to Cybersecurity in IoT Environments. ACM Transactions on Internet of Things, 10(4), 210-225.

[18] Liu, X., & Wang, L. (2024). Regulatory Implications of AI-Connected IoT Devices: A Comparative Analysis. Journal of Legal and Regulatory Affairs, 18(1), 89-104.

[19] Jones, D., et al. (2024). Securing Critical Infrastructure in the Age of AI-Connected IoT. Journal of Cyber-Physical Systems, 30(2), 175-190.

[20] Gupta, S., & Sharma, P. (2024). Cybersecurity Challenges in AI-Driven Smart Cities. Smart City Review, 12(3), 140-155.

[21] Kim, H., et al. (2024). Ethical Considerations in AI-Connected IoT Deployments. Ethics & Information Technology, 16(4), 300-315.

[22] Wang, Z., et al. (2024). AI-Based Intrusion Detection for IoT Environments. IEEE Security & Privacy, 25(5), 80-95.

[23] Brown, K., & Garcia, M. (2024). Socio-Technical Perspectives on Cybersecurity Risks from AI-Connected IoT Devices. Journal of Cybersecurity Ethics, 22(3), 220-235.

[24] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[25] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[26] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. Sensors, 18(9), 2796

[27] Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R., & Huth, M.

(2018). Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. Living in the Internet of Things: Cybersecurity of the IoT - 2018.

[28] Hern Hernandez-Serrano, J., Munoz, J. L., Leon, O., Mikkelsen, L., Schwefel, H.-P., & Broring, A. (2018). Privacy risk analysis in the IoT domain. 2018 Global Internet of Things Summit (GIoTS).

[29] Rak, M., Casola, V., De Benedictis, A., & Villano, U. (2019). Automated risk analysis for IoT systems. In Advances on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 265–275). Springer International Publishing.

[30] Salih, F. I., Bakar, N. A. A., Hassan, N. H., Yahya, F., Kama, N., & Shah, J. (2019). Iot security risk management model for healthcare industry. Malaysian Journal of Computer Science, 131–144. https://doi.org/10.22452/mjcs.sp2019no3.9

[31] Lee, Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future Internet, 12(9), 157. https://doi.org/10.3390/fi12090157

[32] (N.d.). Researchgate.Net. Retrieved March 15, 2022, from https://www.researchgate.net/profile/Kshira-Sahoo/post/Is-there-any-work-on-the-risk-assessment-for-IoT net-works/attachment/59d63f0b79197b807799b8d6/AS%3A426142986444802%401478611813459/download/p269-abie.pdf

[33] Sha, K., Wei, W., Andrew Yang, T., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. Future Generations Computer Systems: FGCS, 83, 326–337. https://doi.org/10.1016/j.future.2018.01.059

[34] Patel, C., & Doshi, N. (2020). ”A novel MQTT security framework in generic IoT model”. Procedia Computer Science, 171, 1399–1408. https://doi.org/10.1016/j.procs.2020.04.150

[35] Husin, H. S., Fairuz, A. M., & Beh, D. (2020). IoT-based Recycle Rebate System – securing website and database. Journal of Com-puting Technologies and Creative Content (JTec), 5(2), 55–60. http://jtec.org.my/index.php/JTeC/article/view/412

[36] Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors (Basel, Switzerland), 20(13), 3625. https://doi.org/10.3390/s20133625

[37] Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for Internet of Things. Sensors (Basel, Switzerland), 21(3), 772. https://doi.org/10.3390/s21030772

[38] Andrade, R. O., Yoo, S. G., Ortiz-Garces, I., & Barriga, J. (2022). Security risk analysis in IoT systems through factor identification over IoT devices. Applied Sciences (Basel, Switzerland), 12(6), 2976. https://doi.org/10.3390/app12062976

[39] Butun, I., Pereira, N., & Gidlund, M. (2018). Security Risk Analysis of LoRaWAN and future directions. Future Internet, 11(1), 3. https://doi.org/10.3390/fi11010003

[40] Haseeb, K., Islam, N., Almogren, A., & Ud Din, I. (2019). Intrusion prevention framework for secure routing in WSN-based mo-bile internet of things. IEEE Access: Practical Innovations, Open Solutions, 7, 185496–185505. https://doi.org/10.1109/access.2019.2960633

[41] Li, Y. (2022). Security and risk analysis of financial industry based on the Internet of things. Wireless Communications and Mo-bile Computing, 2022, 1–13. https://doi.org/10.1155/2022/6343468

[42] Arachchige, P. C. M., Bertok, P., Khalil, I., Liu, D., Camtepe, S., & Atiquzzaman, M. (2020). A trustworthy privacy preserving framework for machine learning in industrial IoT systems. IEEE Transactions on Industrial Informatics, 16(9), 6092–6102. https://doi.org/10.1109/tii.2020.2974555

[43] Liu, J. (2021). Sports injury risk assessment based on blockchain and Internet of Things. Journal of Sensors, 2021, 1–13. https://doi.org/10.1155/2021/6820728

[44] Xie, H., & Yang, Z. (2021). The risk management mode of construction project management in the multimedia environment of In-ternet of Things. Mobile Information Systems, 2021, 1–8. https://doi.org/10.1155/2021/1311474

[45] (N.d.). Researchgate.Net. Retrieved May 31, 2022, from https://www.researchgate.net/profile/Vinayagam-Mariappan/publication/342862311_Hybrid_Logical_Security_Framework_for_Privacy_Preservation_in_the_Green_Internet_of_Things/links/

[46] Smith, J., & Johnson, L. (2024). Research Advances in Artificial Intelligence. *World Journal of Artificial Intelligence Research, 10*(2), 45-60. Retrieved from https://wjarr.com/sites/default/files/WJARR-2024-0607.pdf

[47] Anderson, R., & Williams, S. (2024). Advancements in Quantum Computing. In *Proceedings of the International Conference on Computer Science* (pp. 100-110). IEEE. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10433502

[48] Appinventiv. (2024). How to Ensure Cybersecurity in IoT. Appinventiv Blog. Retrieved from https://appinventiv.com/blog/how-to-ensure-cybersecurity-in-iot/