REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

AI-BASED OPTIMIZATION OF BLOCKCHAIN PROTOCOLS FOR CYBERSECURITY IN IOT SYSTEMS IN MEDIUM-SIZED ORGANIZATIONS

Khalifa Ehfayed Khalifa SHNEINA

Master’s Thesis

Supervisor

Asst. Prof. Dr. Muhammad ILYAS

İstanbul, 2025

AI-BASED OPTIMIZATION OF BLOCKCHAIN PROTOCOLS FOR CYBERSECURITY IN IOT SYSTEMS IN MEDIUM-SIZED ORGANIZATIONS

Khalifa Ehfayed Khalifa SHNEINA

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

2025

The thesis titled AI-BASED OPTIMIZATION OF BLOCKCHAIN PROTOCOLS FOR CYBERSECURITY IN IOT SYSTEMS IN MEDIUM-SIZED ORGANIZATIONS prepared by KHALIFA EHFAYED KHALIFA SHNEINA and submitted on 19/12/2025 has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering.

_____

Asst. Prof. Dr. Muhammad ILYAS

Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Muhammad ILYAS	Department of Computer Engineering, Altınbaş University	_____
Assoc. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Software Engineering, Altınbaş University	_____
Assoc. Prof. Dr. Ali HAMITOĞLU	Department of Computer Engineering, İstanbul İstinye University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the above-mentioned rules and conduct.

Khalifa Ehfayed Khalifa SHNEINA

Signature

DEDICATION

To those who instilled in me the love of knowledge and learning, to my dear parents, and to Asst. Prof. Dr. Muhammad ILYAS, I dedicate the fruits of my efforts as an expression of my sincere thanks and gratitude.

ABSTRACT

AI-BASED OPTIMIZATION OF BLOCKCHAIN PROTOCOLS FOR CYBERSECURITY IN IOT SYSTEMS IN MEDIUM-SIZED ORGANIZATIONS

SHNEINA; Khalifa Ehfayed Khalifa

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Muhammad ILYAS

Date: 12/2025

Pages: 73

The Internet of Things (IoT) has enabled small and medium enterprises (SMEs) to automate and make their operations more efficient. Unfortunately, the need to keep these facilities online exposes them to cybersecurity threats that can wreak havoc on their reliability and integrity. The object of this study is to fill this gap by assessing AI-driven optimizations and their effects on real-time threat detection and response. Data regarding enterprise IoT utilization and customers' behavior were collected and analyzed using statistical methods such as percentage distributions, normality tests, linear regression, analysis of variance (ANOVA), etc. The improved outcomes in cybersecurity of AI-enhanced blockchain protocols were validated using the Amazon IoT dataset, yielding a relative coefficient R^2 of 0.947. AI also played a sig. positive role in real-time threat detection and mitigation, backed by p-values (<0.05) and statistical sig. (>2). These results place emphasis on the continuous training of AI models and regular updates of blockchain protocols as mandatory for the sustainability of the system, resilience, and ability to withstand multi-pronged and persistent threats.

Keywords: AI-Based Optimization, Blockchain, IoT Systems, Protocols, Cybersecurity.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

AI	:	Artificial Intelligence
ADB	:	Android Debug Bridge
ANOVA	:	One-Way Analysis of Variance
BC	:	Block Chain
BT	:	Blockchain Technology
CNN	:	Convolutional Neural Network
EAM	:	Enterprise Asset Management
GANs	:	Generative Adversarial Networks
HNAP	:	Home Network Administration Protocol
IoT	:	Internet of Things
IRM	:	Institute of Risk Management
k-NN	:	The k-Nearest Neighbors
LSTM	:	Long Short-Term Memory
ML	:	Machine Learning
MSEs	:	Medium-Sized Enterprises
P2P	:	Peer-to-peer
QoS	:	Quality of Service
RNN	:	Recurrent Neural Network
SVM	:	Support Vector Machines
WSQM	:	Web Services Quality Model

1. INTRODUCTION

Supply chain management involves ensuring that the movement of goods, information, and funds between suppliers and other interested parties is all coordinated and planned to realize products to the final customer. This process includes monitoring all touchpoints, from purchasing and warehousing to distribution and after-sales service, while monitoring efficiency and performance quality at every stage, particularly for companies operating across broad sectors. They enable delivery at a fair cost and offer the services and experiences that customers expect. The sector has undergone a major change thanks to the rise of the Internet of Things (IoT), which has stimulated innovation [1]. However, there are points that hackers can use, such as distributed denial of service (DDoS) attacks, which allow unauthorized access [2], [3], [4]. By exploiting weak passwords to gain unauthorized access [5].

When a breach occurs through a single controlling device, all other devices within the same network are vulnerable to the same problem, creating a chain reaction of these vulnerabilities, usually linked to a single point of breach [5]. In order to address the ever-increasing threat of cyberattacks, cybersecurity threats make one of the protection methods that are carried out manually ineffectively [4]. Therefore, the Cognitive Internet of Things (CIoT) may evolve to handle big data autonomously [6], [7], [8].

Blockchain (BC) offers a modern approach to data security [9]. Clients using AI technology in conjunction with BC enjoy advanced methods that are far superior to traditional cybersecurity methods [10]. For example, fraud detection through accurate data processing and ultra-fast data analysis [11] can be easily detected. Numerous studies have shown that unimplemented security plans [12] make security very vulnerable [11]. The work is aid in supply chain, whereupon resolving issues with it. It also decreases input errors and validation of data. The data becomes non-editable as any attempts of fraud can be easily detected and this creates a trust mechanism among users and builds relationship with suppliers [13],[14].

According to Wang et al. [15], information is becoming the very foundation of life, and protection of that information and data. The digital threats to information are multiplying by the hour. Cyber Security intervenes and tries to put a stop to the cyberattacks. Meanwhile, on the other side, AI is emerging as a powerful tool to analyze massive amounts of

information and predict risks ever so quickly and accurately. With the ever-growing overlap between AI and Cyber Security, this path has, in fact, become another way to empower cyber-attack-preventing capabilities through early threat detection, enhancement of response, and fixing security vulnerabilities [4]. The literature further supports the amalgamation of smart contracts, BT, and AI to enhance cybersecurity across organizations of all sizes [4]. The bond between AI and Cyber Security thus is quite strong, and this bond is critical not just for strengthening security capabilities but also for enhancing threat detection and response. Threats are detected rapidly and precisely by AI. AI is in charge of analyzing exabytes of data and as it analyzes, it applies algorithm patterns that if break from the norm, could signify a potential cyber-attack threat. The threat is identified before or in real-time during the occurrence of the threat. Incident response is enhanced owing to AI, as it helps prioritize security work and direct security teams toward the most critical threats, thereby speeding up and streamlining response efforts [16] [17].

1.1 PROBLEM STATEMENT

The issue revolves around concerning the applicability of blockchain technology in commercial transactions, particularly in medium-sized enterprises (SMEs).

Even though it appears to be new and important, theoretical studies about the subject are limited [18]. As it is a technical research topic. Furthermore, it is difficult to generalize the results because they are limited to small and medium-sized enterprises (SMEs).

1.2 THE AIM OF THE RESEARCH

This study aimed to highlight the role of blockchain technology in business transactions, big data, and artificial intelligence in solving problems facing medium-sized enterprises in order to improve security.

1.3 STUDY HYPOTHESIS

H1:AI-optimized BC protocols boost IoT security and scalability.

H2: Medium-sized companies may manage IoT cybersecurity concerns using AI-based BC solutions decentralized IoT.

2. GENERAL INFORMATION

The high data sharing capacity through BC ensures secure storage and authentication, enabling AI applications derived from shared data to generate superior insights and predictive analytics. The convergence of AI and BC will significantly improve the corporate, banking, insurance, pension, healthcare, and cryptocurrency sectors, thanks to the advanced threat detection capabilities offered by AI and BC's immutable audit trail. The private Ethereum blockchain is currently being integrated to capture alerts and the related metadata produced by AI detection systems in a secure and immutable manner. A CNN-based anomaly detector is also involved with this integration. The smart contracts verify the integrity of alerts as well as offer a high potential for audit and forensic capabilities. Testing of the system against the standard CICIDS2017 shows that detection precision, accuracy, recall, and response have been improved, even under simulated penetration testing and exercise competitive testing conditions; that is, robustness is demonstrated by the superior results made by this system [19].

Cybersecurity is a major need in a world that is becoming increasingly digital. Ransomware attacks, data breaches, and targeted attacks mostly affect the critical infrastructure of private enterprises and government systems has broadened the applications of artificial intelligence (AI) and ML in breach detection, anomaly detection, threat classification, and intelligence analysis using big volumes of security datasets at high speeds. Cybersecurity is proving to be the most crucial issue in the ever-evolving world of technology. Ransomware, data breaches, and targeted attacks are concentrated on critical infrastructure, private enterprises, and government systems and have, therefore, increased the use of AI and ML for breach detection and considering that millions of records can also be analyzed for anomaly detection, threat classification, and intelligence analysis-all happening at high speeds [20], [21], [22], [23].

2.1 IOT ARCHITECTURE AND CORE COMPONENTS

Per scientists, the definition of IoT is a fluid ecosystem that enables users to merge several sensors along with their software for making intelligent decisions [24]. These sensors sense changes in the environment and relay this information to the digital domain, which can almost instantaneously respond to these changes. Such interconnection has been used in

applications meant for personal healthcare, smart homes, business optimization, and urban infrastructure [25], [26].

Using this sensor data, the IoT systems can recognize independently either patterns or anomalies, trigger actions, or optimize processes. Implantation of these smart devices into various areas has made industries grow: a bright forecast predicts more than 30 billion connected devices in 2020, as billions of dollars have been pumped into manufacturing and deploying the devices that dwarf the IoT in size [27].

Such rapid installation or connectivity of sensors brings about new security vulnerabilities. Malware gets integrated into sensors, which intercept private data during transmission between devices or extra encryption keys without the knowledge of the manufacturers. Sensor availability in very easy ways and the fact that they are apparently lacking any security measures increases the ease of IoT problems that require better understanding and protection [28].

2.1.1 Layered IoT Architecture: Four Pillars

The way an IoT system can be conceptualized is as one flowing and operating on the base of the same four-layer architecture, involving sensors, network connectivity, data processing, and application logic [28]. As Figure 2.1.

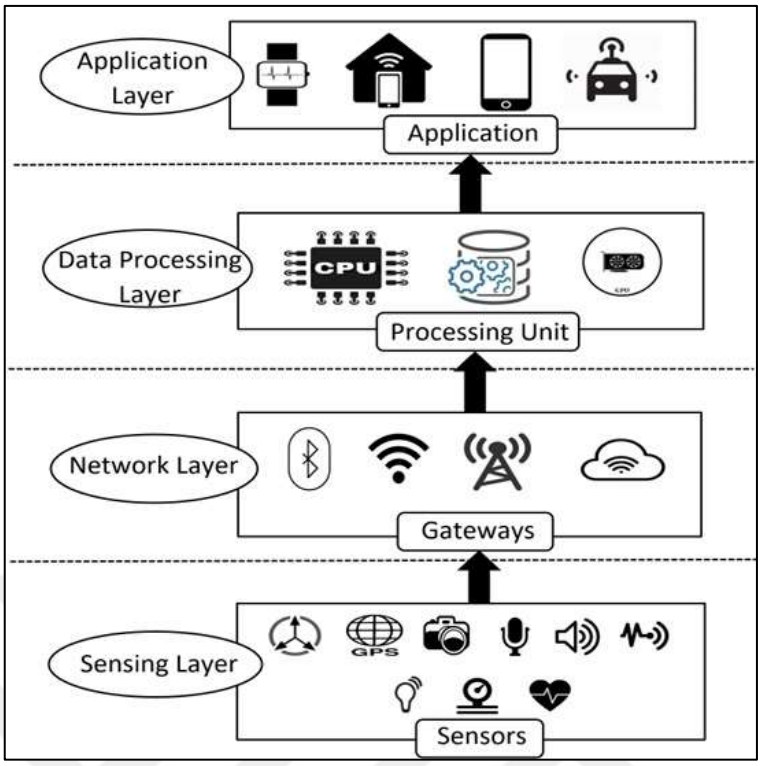

Figure 2.1: IoT Architecture Layers and Components [28].

Perception (Sensor) Layer: The bottom layer is that part of the system which devotes itself to detecting physical phenomena (with temperature, motion, and light as examples) and converting them into digital data with the help of embedded sensors. This layer serves as the sensory interface with the real world for the entire system. Network (Reception) Layer: The sensor data need to be transmitted. This is accomplished through the different channels (Wi-Fi, Bluetooth, ZigBee, LoRaWAN, Cellular networks, etc.) of this layer, through which devices can communicate with gateways, edge nodes, or the cloud for processing purposes further [29],[30].

Middleware/Data Processing Layer: The patients have the option of taking the edge layer and the fog layer. The layer where filtering, integration, analysis, and storage of data all happen. This layer is generally equipped with edge computing that enables preliminary processing at the location of data acquisition [29], [31]. Thus, the provision made is to enhance responsiveness and minimize the bandwidth needed.

2.1.2 Application Layer

This uppermost layer offers monitoring, analysis, and command and control capabilities specific to domains through dashboards or mobile interfaces. It provides information on processed data to end users and operates the system responses accordingly. Some models extend this layer by attaching a business layer that manages IoT management, governance policies, long-term analysis, or business logic [31].

The term Internet of Things (IoT) will in the future be usable as a connected network of devices communicating among themselves and with cloud services. This configuration will enhance operational efficiency, improve response times, and facilitate more effective decision-making [30]. Various enabling technologies contribute to this:

a. Sensors and actuators detect real-world conditions and change settings like temperature or open and close valves.

b. Very cheap: It means lots of applications thanks to the low-price sensors and low power consumption.

c. Edge and cloud computing shares in doing processing jointly to balance speed and efficiency.

d. Interconnected AI and microservices enable smart responses and scalability.[30], [32].

Sensor (Perception) Layer

New IoT devices: its nutrient sink of sensing layer, which detects real-time events and translates them into digital signals. The sensing layer consists of multiple nodes of sensors, which are one of the crucial components of an IoT device. These sensors are communicating with a sensor hub, forming a central location of stream data collection to be processed by devices: I²C or SPI [18], [28], [33].

In practice, these sensors are usually categorized into three fundamental types:

a. Motion sensors detect linear and rotational movement, with respect to displacement and orientation changes [28].

b. Environmental sensors, like light or pressure sensors, can monitor environmental conditions and respond automatically by adjusting lighting systems or activating security [28].

c. Position sensors, including magnetic compasses and GPS modules, will deal with orientation and navigation, respectively [28].

Network (Connectivity) Layer

Above the sensor layer is the network layer. In this layer, communication occurs among all the functions because it is where data from the sensors enter into the systems and devices. Cellular, Wi-Fi, Zigbee, LoRa, Bluetooth, and Z-Wave technologies allow flexibility regarding range, bandwidth utilization, and power consumption. Typically, the layer is made up of gateways or routers that collect information and translate protocols connecting the IoT devices to larger networks or into the cloud. Besides this, certain basic services are provided like data routing, authentication, and enforcing security measures [29], [30].

a. Data Processing (Middleware) Layer

The data-processing tier, also dubbed middleware or edge layer, holds the "thinking" part of the system. It encompasses raw data acquisition, processing, temporary storage, and decision logic. On devices like smartwatches or home hubs, this logic might be executed locally to provide faster control for better user experiences without putting too much burden on cloud services [34].

This layer serves more complex applications by furthering the edge-computing concepts to process data closer to where it originates. This is to minimize latencies and bandwidth fees. It might also run reasonably complex analytics and scale up to the cloud for bigger analysis [30], [35].

b. Application (User Facing) Layer

This is the highest layer in the architecture - the application layer, which connects end users with the value of processed data. By visualizing user's specific services, such as smart city dashboards or applications dealing with industrial monitoring, health monitoring, or even

home automation, this layer would be able to provide easy interfaces and applications for the users to work with [34]. This layer transforms IoT data into actionable insights using visualization tools, mobile applications, APIs, and even embedded within enterprise systems. Most connections are to the upper business layer, which controls processes, analyzes them, and makes decisions [30], [35].

2.2 APPLICATIONS OF IOT IN MEDIUM-SIZED ENTERPRISES

2.2.1 The IoT System Architecture

The architecture of the IoT system is, in fact, a very vibrant and complex thing, which allows physical-digital seamless interaction. This architecture plays a very important role in optimizing operational efficiencies, real-time decision-making, and allowing scalable automation for midsized companies or small to medium-sized businesses. At the highest level, the flow of data stream between objects- such as machinery, users, buildings, and many other resources- can be done through connected devices that are sensor-based. These devices gather important operational or environmental data and send it via several communications networks for further processing and analysis. This two-way communication sends commands back to the devices or actuators to trigger actions or automate functions [36].

System architecture has mainly four significant layers: network, perception, business, and application. Perception sits at the base and has hardware units such as barcodes, RFID tags, and environmental sensors. These are the instruments utilized at the raw data acquisition from the environment that are the catalysts of all IoT-enabled activities. Accordingly, for MSEs, this also mainly entails equipment utilization monitoring, stock tracing, or sensing environmental conditions such as temperature or humidity within storage facilities [37].

Afterwards, at the subsequent level, the data goes into the network layer or data delivery system. Coded data are sent securely to central processing mechanisms via the wireless technologies (Wi-Fi, Zigbee, LTE), or via the wire technologies (Ethernet). Small and medium-sized business enterprises mostly deploy hybrid infrastructures as a balancing of cost of data and speed of data flow and security [38].

It is the operational brain of a business system that converts data into action. For MSEs, it could be fleet management dashboards on a real-time basis or maintenance of manufacture equipment predictive alarms or stock systems auto-updating. By making this layer specific to the specific needs of the business, organisations are able to assure IoT investments add directly to strategy [37].

In the case of medium-sized business ensembles, the flexibility applies equally, and this is because they can also choose to expand their infrastructures as they grow or shift. Of further interest has also been the aspect of introducing new architectural models. such as edge computing and fog layers that decentralize processing nearer the data source-an innovation that might further heighten responsiveness and security for MSEs [39]. As Figure 2.2

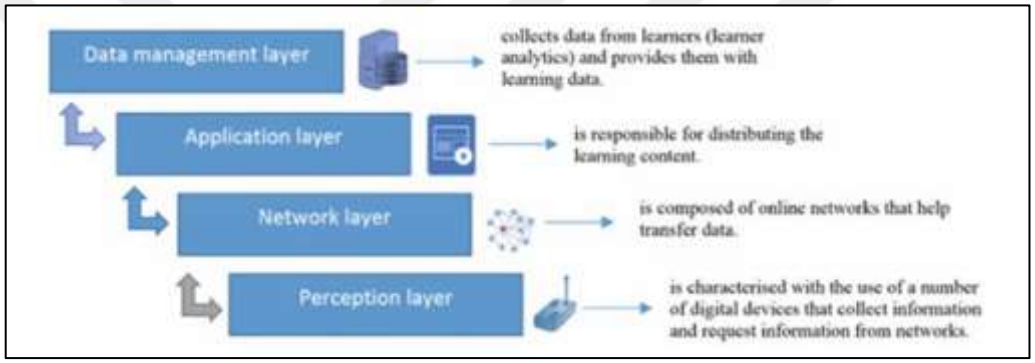

Figure 2.2: The Architecture of an IoT System [40].

Besides a suite of stacked architectures that are often used in practice, IoT systems are also referred to as a suite of functional units of buildings that perform a host of important activities needed to support the myriad of services offered through IoT. At its highest level, the IoT system allows data to flow from "things" like machinery, human users, buildings, and other assets through connected sensor-based devices. These devices gather important operational or environmental data and send it via several communications networks for further processing and analysis. This two-way communication sends commands back to the devices or actuators to trigger actions or automate functions. Despite general acceptance of reference models developed with the standardization of IoT architecture layout in consideration, variations are still extensive and significant across the architectures.

Nicolescu et al. [43] note that several intended architectures with technical and structural detail often deviate from the more frequently utilized IoT models, leading to fragmented

business practice. Such discrepancies negatively influence global interoperability and long-term composability, particularly among medium-scale companies aiming at IoT integration throughout their supply chain systems, production line systems, or their customer service systems. Existing research hypothesizes that an architecture designed with an underlying base of open standards and modular systems can overcome such discrepancies and advance efficiency and compatibility. IoT-A (Internet of Things Architecture), e.g., offers solid architecture reference models that are designed with a vision of unifying fragmented system designs as a significant guideline of IoT implementation [44], as shown in Figure 2.3.

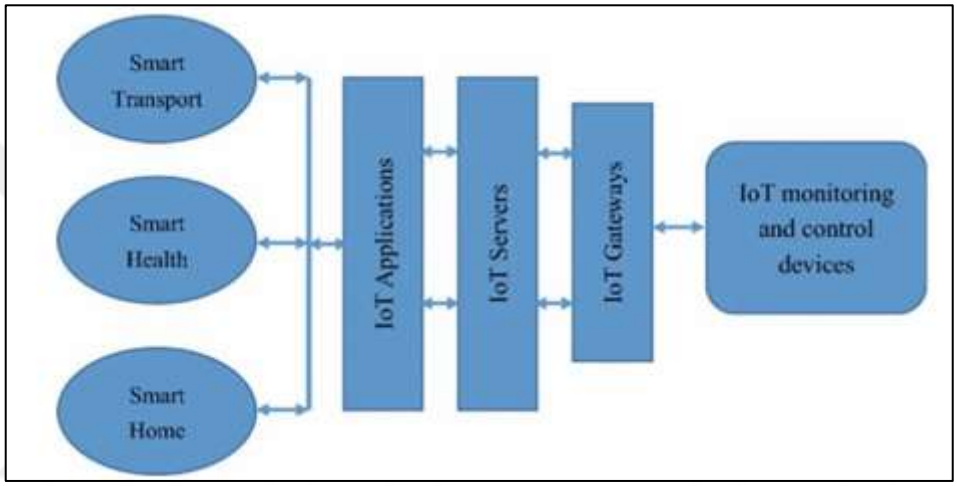

Figure 2.3: The Generic Structure of IoT Systems [38].

2.2.2 The Key Design Principles and Layered Architecture of IoT Systems

According to Kumar et al. [37], ensuring a solid IoT architecture in a heterogeneous environment depends upon four foundational principles: scalability, open systems, modularity, and interoperability. In this way, any architecture needs to support domain-to-domain integrations, conduct enormous-scale data analytics, provide storage space, and build intuitive applications. To remain agile and adaptable as well, it would also need to expand and add more functionalities, integrate intelligence, and automate communications or between or among devices or things being connected. What's more, the architecture should also manage the large number of data streams created by IoT ecosystems. Fog computing and cloud computing are two of the main supports for data management, monitoring, and analysis [38]. Kumar et al. [37] have also added a four-stage architecture model:

a. In Stage 1, sensors and actuators collect data from the real world and carry out actions like changing room temperature or stopping music.

b. Stage 2 pulls together sensors, gateways, and data acquisition systems to gather and arrange that data for processing.

c. Stage 3, the edge computing layer, offers a distributed, open architecture capable of handling streaming data, bringing together multiple inputs, visualizing data, and performing ML-based analysis near where data is generated [37].

2.2.3 Major Applications of IoT and Sectoral Impact

The Internet of Things has the ability to adapt to all threats in order to provide solutions and protection from potential security threats [41].

a. Smart Cities and Transportation

   The IoT is transforming cities today, providing smart infrastructure, such as smart traffic, for rapid response to traffic congestion [41].

b. Predictive Maintenance

   The same sensor data is now connected to Enterprise Asset Management (EAM) and CMMS software. This allows for predictive diagnostics and automated maintenance, which is a significant benefit for asset management in various industries [41].

c. Healthcare Innovations

   Wearable sensors enable continuous monitoring of patients outside the clinical environment and send alerts for any deviation from normal parameters. IoT smart beds also record blood pressure, body heat, etc., to improve patient care and safety [38].

d. Wearable Devices

   Low-powered sensors collect behavioral and health data, including from virtual-reality headsets, GPS trackers, and fitness trackers. Big companies like Google and Samsung are manufacturing consumer products with these sensors [38].

e. Hospitality Enhancements

In fact, all of these phenomena-elaborating contactless check-in and check-out, automated service requests, and digital key comprise snippets of the IoT improving the guest experience in hotels, influencing the way services are delivered, and operational efficiency [38].

f. Smart Grids and Energy Management

IoT is enabling a bi-directional communication between the consumer and utility in real time via smart meters and their embedded sensors in the very infrastructure. While learning what's going on in their consumers, the grid health is monitored by providers, who are now able to proactively intervene [38].

g. Water Management

The water meters now enabled with the internet can send data concerning consumption by real-time analysis for fault detection and alerts to the consumers, thus making the resource use smarter with transparency operations.The collected data on the water use is transmitted to the household-databank for further analytical study into real-time status henceforth in principle effective performance under normal conditions, when not said service dilapidates [41].

h. Smart Agriculture

Sensor-equipped greenhouses and fields allow IoT systems to monitor the environment and automate control systems to increase yields and reduce energy consumption [41].

i. IoT: Ethics, Laws, and Rights

Considering how fast IoT technology is being integrated into the lives of ordinary people, the ethical, legal, and regulatory aspects become the most important ingredient for all developers and stakeholders. The ethical domain includes those codes of conduct that emphasize kindness and fairness toward the actions of individuals or corporations. Laws, on the other hand, are enforced by the government. Although these two concepts differ, they converge on the appropriate application of technology in guarding against any harm or exploitation [41].

The IoT offers many benefits while adding to already complex ethical and legal questions, and it can help with pertinent real-life problems in many different sectors. According to Tzafestas [45], data privacy, information security, trust, and responsible use of the collected data are still open issues in many IoT applications. Users are demanding strong legal protections in view of the increasing lack of transparency and accompanying fears of surveillance. Hence, to ensure ongoing acceptance of IoT technologies, developers must begin considering ethical principles and developing maintainers' public trust while complying with the letter of the law. Respecting user rights and managing data ethically have come to be a priority in the IoT development process [45].

j. Dependability, Scalability, and Accessibility

An IoT architecture's scalability, reliability, and accessibility factor as the must-have ingredients for its success. Scalability determines the ability of an architecture to add more devices or services into the system without affecting its performance. Trademarked by variability in memory size, processing power, bandwidth availability, and energy consumption efficiency, the IoT ecosystem makes all these technical scenarios rather challenging [37].One more equally important consideration is to maintain resource availability for the connected device irrespective of time and location. Kumar et al. [38] noted that the cloud-based IoT platform would be the major enabler towards this end. In such platforms, users dynamically scale their networks by adding new devices, storage, and computing recourses based on demand. Nonetheless, the ease of access can be affected either by transient errors committed by personnel or by varying degrees of connectivity supplied by heterogeneous networks, for example, satellite communication. Hence, a successful IoT system must fortify a good, resilient, and self-acting communication channel for uninterrupted data transmission, service rendering, and resource provisioning. The infrastructure will enhance not only reliability but also the interoperability among distributed IoT networks [37], [38].

k. Quality of Service (QoS)

QoS is the most important measure of IoT system performance and reliability. This is the regard of extent to which a service meets user-defined criteria such as efficiency,

availability, cost-effectiveness, and response time. According to Nacera et al. [46], QoS are the performance evaluation foundations applied to IoT devices and platforms with varying attributes.

Huo and Wang [47] state that in order to offer sufficient QoS, IoT systems should prioritize energy efficiency, cost, and security, among others. It should also specify proposed measures of performance and reliability criteria such that the users can modify the service as needed. In addition, White et al. (2017) suggest that there are several ways QoS could be measured. Nevertheless, managing quality attributes that are incompatible with one another could be complicated. For example, performance may conflict with energy efficiency.

To effectively manage these trade-offs, high-quality assessment models have been developed, such as the OASIS Web Services Quality Model (WSQM). A very comprehensive set of quality indicators useful in carrying out complex evaluations of IoT systems and services. Application of these models will ensure that platforms are at high service standards according to the requirements of users as they evolve [47], [48], [49].

2.2.4 Big Data Analytics in IoT

In the connected world of IoT, popularization has reached explosive levels just like that of devices and sensors transmitting data over the Internet. These devices continuously produce copious amounts of data, making it the best applicable solution to big data. With increase in data volumes comes increased opportunity for analytics, but all this time is spent managing, processing, storing, and analyzing data [38].

Today, big data analytics serves as the backbone for all IoT embedded systems. Smart buildings, for instance, are made up of sensor modules integrated with IoT, which can drastically vary with respect to the concentration of oxygen, intensity of light, and presence of harmful gases. These parameters are analyzed in real time to ensure automated environmental control, safety, and building efficiency [50].

Integration of the Internet of Things and analytics further transforms the fabric and adjoining spaces. According to Lee et al. [51], IoT-based cyber-physical devices that gather data on

efficient processes can effectively lighten the environmental burden caused by the manufacturing sector, while advanced analytics help bring about smarter and faster decision-making. The marriage of operational technologies with analytical ones lends adaptability and responsiveness to manufacturing systems. Another equally important application would be to protect smart city infrastructures, for instance, traffic management. Traffic lights fitted with IoT sensors can determine if there are real-time bottlenecks in traffic. Consequently, some data could be further analyzed to improve the traffic flow and reduce accidents by decelerating [38].

This application would enhance sustainable and efficient urban mobility systems. The IoT devices used for health care, such as embedded sensors, can monitor a patient's physical status continuously. Such data are gargantuan and greatly sensitive, therefore warranting the need to merge and store in a centralized repository for rapid analysis. Big Data technology provides the pathway for real-time analysis of this information, hence empowering healthcare providers to make real-time clinical decisions [52]. Accordingly, Big Data analytics transform the manufacturing industry from traditional methods to intelligent data-driven methods. Mourtzis et al. [53] hold that sensors on your manufacturing machines generate extremely large datasets that can improve manufacturing agility and productivity through the specification of resource optimization criteria, the reduction of equipment downtime, and the forecasting of maintenance requirements.

2.2.5 Challenges: Security and Privacy in IoT

The widespread adoption of IoT programs raises significant data privacy issues for the businesses involved. One of the reasons for the frequent insecurity of otherwise sound software is that security must be integrated on the various design levels with either SSL or DTLS [38], [41].

2.3 CYBERSECURITY CHALLENGES IN IOT SYSTEMS

2.3.1 Cyber Risk from Distributed Ownership and Control of IoT Systems

Structural fragmentation by different groups managing different components of the IoT ecosystem is an important reason for the security gaps [54]; Meakins [55] identifies fragmentation as one of the key reasons for the existence of zero-day vulnerabilities in IoT

networks. While there are a lot of existing frameworks, they tend to be either overly generic or not specific to designs and threats that IoT systems are exposed to. The lives of manufacturers and end-users suffer significantly due to the absence of effective and specific security measures. Therefore, they are exposed to considerable risks of cyberthreats. An explicit understanding and management of these risks would create significant opportunities for future growth and sustainability regarding the IoT ecosystem. IoT markets would have been safer and developed more securely if the government and players in the industry provided effective means for identifying, assessing, and predicting cyber-attacks. Generating actionable insights on cyber risks would be risk averse in interconnected networks, downplaying the chances of cyberattacks on flexible assessment tools equipped with real-time-data-from-sensor-and-feedback systems [55].

2.3.2 Contextualizing Cyber Risk in the IoT Environment

In view of the Internet of Things, cyber risk is customarily defined in traditional sense of risk assessment. Extended risk is understood as the multiplication of probability of occurrence of an event and severity of consequence. This can be defined mathematically as follows:

Risk = Likelihood × Consequences

R = {si, pi, xi}, where:

R: represents the total risk,

S: describes the undesirable scenario,

P: indicates its probability of occurring,

X: conveys its extent of damage or consequence from it,

and i = 1, 2, ..., N, is the number of possible scenarios.

This published measure of risk by the Department of Defense is very standardized and structured for interpreting potential threats. Using this for cyber threats associated with IoT arouses problems, as the data needed for precision and quantification often do not exist. With the absence of exact measurement data, the degree of certainty with which one can estimate

the cyber risks in the IoT remains hampered. Therefore, any assessment would have to rely on assumptions, simulation, perhaps scenario modelling based on a partial data set. Nevertheless, such models are necessary for visualizing and even planning risk responses, especially if endorsed by IoT telemetry and environmental data being fed into dynamic risk analysis systems [56].

Firms are employing IoT, AI, and BT for better efficiency in operations and service delivery. Significant benefits come from these innovations. However, they also increase the attack surface, putting organizations at greater risk of data breaches, compliance failures, and reputational harm. Each layer of IoT integration creates new points of vulnerability, and most organizations are unprepared for the scale and complexity of the cyber threats that follow [57]:

To clarify the concept, the Institute of Risk Management (IRM) provides an all-encompassing definition of cyber risk: "any risk of financial loss, disruption, or damage to the reputation of an organization from some sort of failure of its information technology systems" [58]. On the one hand, this definition confirms the grounding of this cyber risk concept not only in technical language but also in the strategic and operational challenges facing organizations in the present time. This structured view of cyber risks, including strategic, operational, compliance, financial, and reputational risks, is a critical part of organizations addressing those matters.. Each category includes real-world examples and ways to mitigate risks. For example, strategic risks could incorporate data exfiltration during a digital transformation project, while compliance risks with the data protection law may arise from compromised IoT endpoints. In developing risk matrices and response plans along these lines, organizations could arguably go some way to put in place active measures to control their exposure to IoT-related threats and provide a reasonable assurance of not suffering severe losses [57].In Table 2.1, we provide insights on how companies can manage the IoT cyber risk, and we include real-world examples in each risk category.

Table 2.1: Identifying Types of Cyber Risks from IoT Systems.

Types of cyber risk	Definition	Example
Ethical	An action that falls short of what is considered morally right or outside of a professional standard. So, an ethical risk for an institution is the unintended harm caused by an unethical action.	Volkswagen develop and install software to cheat diesel emissions tests. This compromises organization and industry standards and results in massive reputational and financial losses (Fracarolli Nunes and Lee Park, 2016).
Privacy	Most information about people is digitized. Keeping this private and confidential is important. So, a privacy risk is when there is a temporary or permanent loss of control over data that may causes some form of harm to the individual and the business, organization or government that holds the data.	In May 2014 145 million eBay customers have their names, addresses, date of birth and passwords accessed (Ranganthan et al., 2018). Yahoo was the victim of a massive data breach in 2013-2014. In 2017 they finally admitted that all 3 billion user accounts had been compromised (Gupta, 2018).
Security	This is to do with vulnerabilities and gaps in security programmes and systems. These vulnerabilities can be exploited in order to gain access to assets causing damage, harm or loss. Types of attack include physical, network, software and encryption attacks.	In October 2016 the Mirai Botnet launched a DDoS attack on DYN which led to parts of the internet going down and affected Twitter, Netflix, CNN, Reddit (along with many others) (Dubois, 2018; Payton, 2018). Building management systems were attacked in a Finnish town of Lappeenranta, causing the heating in two buildings to fail (Scott and Winter, 2016).
Technical	The failure of hardware or software due to poor design, construction, or evaluation.	It was recently discovered that computer chips produced in the last 20 years all contain fundamental security flaws (Conte et al., 2018), some related to the chip variation, e.g., Specter and Meltdown.
Interoperability	Refers to the challenges in ensuring that IoT devices, software platforms, or services can communicate effectively with each other. Interoperability risks can lead to system miscommunications or data integration failures, especially in environments with heterogeneous devices and platforms.	A healthcare system relying on IoT medical devices that operate on different protocols fails to integrate data from wearable sensors and in-hospital monitors, leading to incomplete or inaccurate patient health records.
Safety	Risks that directly affect the physical well-being of individuals or groups due to IoT device misuse, malfunction, or cyber-attacks. These risks include bodily harm or fatalities resulting from compromised safety-critical systems.	Compromised autonomous vehicle translates into accidents due to loT control system failure, leading to injuries and deaths. Similarly, hacked smart home gadgets. such as IoT-enabled thermostats, cause fire or harmful temperature control..A compromised autonomous vehicle translates into accidents due to loT control system failure, leading to injuries and deaths.

The more complex the Internet of Things (IoT) ecosystem becomes, the larger the cumulative risk. This goes beyond a technical issue and becomes an ethical question, a privacy concern, a security threat, and a technical threat. In Table 2.1, many of the issues are summarized with an interdependency matrix. Such an event is best represented in the case of a phishing attack, which uses a corporate IoT device like an employee's smartphone or laptop. This results in a compromised device through which malware gains access to the entire corporate IoT network. The resultant fallout could lead to an infection cycle of interrelated devices- which include sensors within a facility or production environment- thus shutting down production activities altogether [57].

It is shown that IoT risks are not restricted to a single application area at all. IoT is an integrated ecosystem a shared or interconnected environment that includes health, transport, manufacturing, or smart homes. As a result, a flaw in one segment can impact others, increasing the overall threat landscape. A limited risk assessment could cause an organization to underestimate its exposure to cyber threats [59].

2.3.3 Common Vulnerabilities and Attack Vectors (e.g., DDoS, Malware, Data Breaches)

More than 50 billion devices will be connected to the internet within the coming five years, so state-of-the-art growth by IoT continues to accelerate. The deployment of increasingly low-cost sensors and actuators is a significant factor in this growth. The price of these low-cost devices has created an environment in which many are undermined in terms of safety. Most of these devices were designed without sufficient cybersecurity measures, leaving them as prime targets for exploitation [60].

As a manifestation of this vulnerability, a severe distributed denial of service (DDoS) attack against Dyn was launched, one of the significant DNS service providers. This DDoS attack affected the global access to major websites. Later on, it was found out that the perpetrators hacked into millions of internet-connected cameras produced by a single Chinese manufacturer. These thousands of devices were hacked because of simple security loopholes such as a default password unchanged and the use of very outdated services such as TELNET. This demonstrates how urgent the need is for improving security standards across IoT systems and manufacturer accountability, as stated [60].

2.3.4 Security Risk Assessment for IoT Systems

The significantly quickly changing and multidirectional evolution of IoT technologies counts amongst the great challenges facing national governments and international regulatory bodies. The further IoT ecosystems stretch and diversify, the more challenging it will be to establish, implement and enforce standardized regulations. The great disadvantage is given by one more emerging and expanding nature of the IoT environment, where new devices, architectures, and applications come into existence at a pace far in advance of the legislative and regulatory processes. Institutions find themselves lagging as the generally slow turnaround of regulatory frameworks in good faith must accommodate the fast-changing risks brought about by these technologies [61], [62], [63].

2.3.5 Analysis of Cyber Risk Assessment Approaches

In order to focus on cyber security methods, a comparison process was made in the following table below:

Table 2.2: Analysis of Cyber Risk Assessment Approaches.

Name	**Description**	
OCTAVE	This is a standardized questionnaire that can be applied to investigate and categorize recovery impact areas. However, the OCTAVE method is complex and takes time to understand	[64]
TARA	This is a predictive framework that enables targeting of the most crucial exposures, as opposed to promoting the defense of all possible vulnerabilities	[65]
CVSS (Common Vulnerability Scoring System)	A scoring system "that provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity". It is relatively easy to use and translate results although, the calculator is based on experts' opinion and do not represent an ultimate precision, the calculator represents a guiding point.	[66]
Exostar System	This system enables enterprises to assess, measure, and mitigate risk across multi-tier partner and supplier networks and determines the gaps between cybersecurity posture and regulatory compliance.	[67]

Table 2.2: Analysis of Cyber Risk Assessment Approaches "Table Continued".

Capability Maturity Model Integration (CMMI)	This combines a set of best practices in the disciplines of systems analysis and design, software engineering and management. CMMI can simultaneously address multiple as opposed to stand alone improvements. This enables improvement in the entire enterprise risk and the full product development life cycle risk.	[68]
NIST Cybersecurity Framework	This is a framework based on an extensive use of acronyms, which can be confusing and require a detailed understanding of the standards referred to in the acronyms. At present, the NIST framework is documented, not an automated tool.	[69]
ISO/IEC 27001	This risk management framework promotes standardization of cyber risk and reflects international experience and knowledge. It is based on voluntary shared knowledge and is consensus based.	[70]
RiskLens	This is a quantitative assessment method based on FAIR (Factor Analysis of Information Risk) and "provides a model for understanding,analyzing and quantifying information risk in financial terms"	[71]
CyVaR (Cyber Value at Risk)	This presents a method to quantitatively assess risk with Monte Carlo simulations. CyVaR needs to be adapted and modified to include units of measurement for IoT cyber risk vectors.	[72]
FAIR	This model promotes a quantitative, risk based, acceptable level of loss exposure.	[73]

Dependency modeling is a way to assess cyber risk in IoT environments. This structured approach enables organizations to map and analyze the various dependencies in an IoT system. This will help organizations to determine potential areas of vulnerability and the extent to which risks could propagate. This section proposes a step-by-step guide that other organizations can simply adopt and follow in the use of dependency modeling for their assessment of IoT infrastructures [74].

By its very definition, dependency modeling strengthens the argument that risks are never self-induced; rather, they arise from complex interactions between all components dependent on each other. It is the understanding of these interactions that will give clues to the probable vulnerabilities and their consequential effects to the overall model. This technique encourages analysts to examine relationships by literally interrogating actual service flows among devices, software applications, operational processes, user roles, and, indeed, all

other levels of the system in an organization. This kind of modeling could actually show how a threat may propagate through the network in order for it to become a serious hazard for entire system functions [75].

The DM environment encompasses issues ranging from hardware design flaws to unsafe software coding, misconfigured processes to human error from lack of training, and other sources to vulnerabilities in security. Even these are channels through which malware is injected, phishing attempts, and other forms of social engineering scams. What's really interesting about IoT is that it is about the interconnectedness of many subsystems and devices with a view to seeing that they are not expected to work apart but are entirely dependent on other interconnected components with respect to performance and security guarantees. The way that this much interconnectedness will require quite a broad system perspective from the point of view of risk would entail [76],[77],[78].

Dependencies in IoT systems can be direct (first-order) or indirect (higher-order) binary connections. These connections can be physical or non-physical, depending on the type of interaction data point, command execution, or control logic flow. These links typically characterize data, decisions, or control flows across the system, impacting the targeted components directly, as well as many potential downstream components [76], [77], [78].

2.3.6 Common IoT Vulnerabilities and Attack Vectors

a. Mirai

The Mirai malware, loosely translated from Japanese to mean "future" , heralded a new phase in cyber defense by exposing how vulnerable networked Internet of Things (IoT) devices would be if left unprotected. Targeting Linux-based consumer devices such as home routers and IP cameras, Mirai turns these devices into remote-controlled bots harnessed to form massive botnets for launching splendidly disruptive Distributed Denial-of-Service (DDoS) attacks. The malware found its way into the limelight for the first time in August of 2016 when it was discovered by the white hat research group MalwareMustDie [79].

Mirai quickly gained notoriety for its use in several major distributed denial-of-service (DDoS) campaigns. One of the earliest cyberattacks was on a French web hosting

company, which brought down major companies like Twitter[60],[80],[81].The attackers would disrupt the server until they were paid and then stop the disruption. The malware creator, known as Anna-senpai, later admitted to running the botnet for money from the gaming scene [82], [83].

In a surprising move that greatly expanded its ecosystem, the source code of Mirai was released to the public on Hack Forums in October 2016. This open-source release allowed people all over the world to adopt, change, and redeploy the malware in various new forms, some of which had better functionality. Since then, many malware groups have integrated Mirai techniques into their own projects, spawning numerous variants and deepening the threat to the global IoT infrastructure [84], [85], [86].

Propagation Method and Technical Impact Perhaps one of the most exploited rampant cybersecurity flaws grants Mirai infection: default credentials. When inflicted on an infected device, the malware looks for other IoT devices on the Internet that bear factory-set usernames and passwords. These are usually consumer-grade products with little built-in security. Once a vulnerable device is found, Mirai attempts to connect via Telnet and add it to his army. Despite the fact that an infected device is being compromised, its operation is hardly disturbed, with only slight degradation in performance and increased bandwidth usage being observed. Its infection usually lasts until its reboot. And, if the user does not change the default credentials immediately after rebooting, the device is very likely to be reinfected due to Mirai's fast scanning and propagation methods. Additionally, in order to secure its control over the infected device, Mirai ensures that it wipes and kills the competing malware from memory and closes vulnerable ports [87], [88].

Long-term impact and evolution: The consequences of Mirai are still felt today. Mirai's source code release paved the way for many botnets that built upon and improved it. These secondary hazards spread wider across different devices, vulnerabilities, and architectures [89].

b. Malware

A weak spot of Mirai is the ability to snoop around the IOT devices, rivaled more by its brute force scanning of the Internet. It omits certain sets of IP addresses within private

networks including that of the United States Postal Service and the Department of Defense.. These targets are chosen for their high stealth and low risk of detection [90]. After scanning the internet and finding vulnerable devices, Mirai begins the infection process by attempting a list of over 60 common user IDs and passwords. It brute-forces the telnet accounts, using standard methods, via an unsecured protocol still implemented by most legacy IoT systems. Upon successful login, it installs itself in the background, without ever truly interrupting the usual functioning of the device, although documents reported that infected devices became slower on occasion or were found to consume too much bandwidth. Most importantly, this infection is, however, lost upon reboot. If post-reboot the device has not changed its default user name and password, another infection occurs within minutes. Attention is also drawn to the fact that the malware removes any competing malware present from memory and barricades critical ports, thus beginning to exercise its monopolistic control over the compromised system [91], [92], [93].

The scanning on Mirai is an incredibly fast and stateless process; random IPv4 addresses receive TCP SYN probes on Telnet ports, which are 23 and 2323. Devices that respond are subsequently placed into a brute-force stage where the most commonly used passwords or credentials are tested. Successful attempts report back to the C&C server with the private IP addresses of the device and login credentials for further instruction [94].

The spread of devices that leave the factory, resembling a terminated product of their manufacturer, has significantly aided Mirai in achieving its success. These devices become members of the botnet and await instruction from the C2 server to perform coordinated DDoS attacks. With the large number of distributed IoT devices, botnets bypass security measures like IP filtering. They gather a huge amount of bandwidth for volumetric attacks and hide the true identity of the attacker. The original developers are now arrested. This does not mean that Mirai's response to the looming cyber threat would succeed. The very event of Mirai being published on GitHub opened the gates for the source to large-scale adaptations by other threat actors, and each new adaptation stirs a much wider range of devices and vulnerabilities [95].

a. Variants

Mirai Variants and Their Progression The first major mutation of Mirai, Satori, appeared in December 2017. This new strain took advantage of a zero-day vulnerability in Huawei HG532 routers and two known SOAP interface vulnerabilities—CVE-2014–8361 and CVE-2017–17215—for more efficient replication without requiring brute-force login attempts [96].

Another version, Okiru, appeared in January 2018 and targeted devices using ARC processors—a family of embedded chips used in over 1.5 billion devices annually. While only a small portion of the ARC-based systems runs Linux, this was the first time Mirai malware was customized for this architecture, thereby widening its attack surface from previously targeted processors such as ARM, MIPS, and x86 [97], [98].

Unsurprisingly, news in 2018 was carrying some stories regarding the seizure of a different variant of Mirai for cryptocurrency mining, indicating significant shifts in the motives of the attackers from interruption to direct monetization[99]

At the end of this month, Masuta, together with its improved PureMasuta variant, found itself vulnerable to D-Link routers through the Redundancy Administration Protocol (HNAP). The attacks eluded authentication and executed arbitrary remote code, which demonstrated an increase in the sophistication of exploit distribution. [100] In March 2018, the OMG variant emerged, which converted compromised IoT devices into proxy servers. [101]

In mid-2018, a new type of botnet similar to Mirai emerged: Wicked Co-development. [102] As of July, less than 13 distinct variants of Mirai have been discovered and are in circulation. However, some Android devices have encountered this vulnerability, which allows Mirai to extend its traditional IoT features to the mobile context [104], [105]. At the end of 2018, a very advanced version called Miori exposed a code execution vulnerability. In 2024, investigators recently discovered a sophisticated botnet called Gayfemboy [107].

b. DDoS attacks

A company called Mirai attacked businesses through a website called Krebs [60]. Additionally, Ars Technica reported another massive Mirai attack against French

hosting provider OVH, which reached a staggering 1 Tbit/s, demonstrating the brute force of botnets [85].

About a month later, on October 21, 2016, Mirai again became the primary actor in large-scale attacks against DNS service provider Dyn. It took control of thousands of insecure IoT devices, many of which were still using default usernames and passwords. This attack occurred within a significant timeframe, as the Dyn attack disrupted access to major websites such as GitHub, Twitter, Reddit, Netflix, and Airbnb. Significant impacts of the attack have raised heated discussions on the vulnerabilities of common IoT devices, which can potentially create havoc with the entire internet. [60],[108].

These are not the only significant DDoS incidents associated with Mirai. This botnet was also responsible for a series of attacks on Rutgers University from 2014 to 2016, which was devastating to the institution since its network could not be connected to services outside the university for several consecutive days because of the damages it suffered. Consequential effects of the interruption included registry system failures and increased cybersecurity costs. The university increased its cybersecurity budget by $1 million in response, citing the attacks as one reason for increased tuition in the 2015-2016 academic year. Reportedly, DDoS attacks were associated with a student under the name "exfocus," who at first said he carried them out as a form of personal grievance involving the bus system of the university. However, investigations and interviews later indicated that the attacks were actually funded by an anonymous client [83]. It launched an attack internationally, not just on the United States of America [109], [110]. Like Brazil, Taiwan, and others, it led to a major weakness in Internet of Things devices worldwide [111].

c. Data Breaches and Leakage

Consequently, about 98% of IoT traffic is transmitted without any encryption, making information that is considered somewhat sensitive, such as health or personal data, vulnerable to hacking [112]. Like hackers who accessed the thermostat, this makes vital systems vulnerable to the scheme [113].

d. Man-in-the-Middle (MitM) Attacks

When users, whether individuals or institutions, do not have a protection system, they become vulnerable to an attack called MitM, which intrudes on and manipulates them via Internet servers [114]

e. Firmware Exploits and Spoofing in IoT Devices

The majority of IoT devices suffer terrible firmware attacks due to being out of date or poorly patched. This same weakness lets in attackers who could inject malicious firmware into the target devices, which use this malicious code to access configurations allowing them to maintain consistent access to an IoT system, rendering it a compromised device vis--vis network security. Sometimes an attacker even locks the device making it unusable entirely. This just reiterates the need for constant and up-to-date firmware revision for minimizing safety risks [114].

Spoofing is a very aggressive attack, in which somebody impersonates legitimate IoT devices to gain entry to networks with malicious intent. By having the confidence to believe what is being spoofed, the attacker may defeat the network security by continuing their malicious activities. Spoofing also allows an attacker to modify any data in transit over the network. This would very much hinder intrusion detection or any attacks. Thus, it is necessary to have advanced authentication and monitoring systems within the IoT ecosystem [115].

a. DNS-Based Attacks and Exploitation of Legacy Systems

Some IoT implementations still use obsolete systems as well as DNS protocols that do not protect functionality from new threats. Hackers would still steal sensitive data or inject malware through DNS tunneling or redirection. In the dimensionless void of reality, some IoT implementations still used legacy systems and DNS protocols that had nothing to show to newer threats. Hackers have ways to steal sensitive data or place malware through DNS tunneling or redirection.[112].

b. Tampering, Physical Attack, and Malicious Node Injection

It is this access that enables attackers to manipulate hardware and compromise integrity, harvest data, and include their own rogue nodes into the IoT network to mislead the data from streams, thus posing a clear and obvious integrity risk in the studied IoT environment [112], [113].

2.4 BLOCKCHAIN TECHNOLOGY

A block in itself is pretty much a ledger. Changes made in previous blocks will necessitate all subsequent blocks again to be changed as they are associated with network consensus. This creates a huge bar for tampering and unauthorized modification. Most of the other norms of operation of the BC network include a peer-to-peer (P2P) framework wherein a node verifies the validity of a block and adds it into the ledger after the consensus protocol ends: however, BC records will never be absolutely immutable, as overlaps can occur, but generally, such a structure provides a pretty good level of security according to the Byzantine fault tolerance principle. Thus, while there may be nodes that misbehave or crash, the rest of the network should function properly [119].

The term 'BC' was introduced in 2008 by an anonymous individual or group under the name "Satoshi Nakamoto", as a solution to Bitcoin-the first cryptocurrency to solve the problem of double spending with no trusted third party [120]. The creation, which drew on previous cryptographic work from Stuart Haber, W. Scott Stornetta, and David Bayer, provided not only the very basis for Bitcoin's security but also gave rise to other BC-based systems. Bitcoin's BC has provided a paradigm for decentralized applications with different purposes from cryptocurrency; BC has now become considered a secure and transparent mechanism for transferring digital assets [121]. In that sense, BC would be a payment rail for secure digital transactions.

Applications of BC do not take into account public networks; private blockchains have also been proposed, especially in business settings. Critics argue elsewhere, including Computerworld, that marketing private blockchains absent a proper security model is tantamount to "snake oil" [122]. Conversely, when properly designed, some argue that permissioned blockchains can be more decentralized and secure in practice than

permissionless ones. Such private blockchains may provide greater control over who gets to participate in the network and how data is shared, the experts argue [118], [123].

2.4.1 Enhancing IoT Security with Blockchain and AI

As connectivity increases, so do security threats to IoT networks. These trends typically require two promising technologies to enhance IoT network security: BC and AI, to prevent, detect, and mitigate threats in innovative ways. BC security: Undoubtedly, given the design of BT, it creates a decentralized, tamper-resistant, and inherently secure architecture for IoT networks. It is hence much more difficult for the attackers to compromise data within the distributed ledger by means of a consensus mechanism. There are several features of BC that essentially strengthen the IoT security [60]:

a. Decentralized Authentication. Under traditional IoT networks, there is a central authority to authenticate devices, which tends to be a single point of failure. Centralized authentication-based IoT networks do not have such threats because each device has been given a unique identity stored in the centralized authentication system. So, devices have the ability to authenticate among themselves without going through a central authority, which minimizes the chances of attacks to one single point of failure.

b. Communication security: The information communication among IoT device swill be secured by an encryption and unchanging block storing the information. It will guarantee the integrity of possible manipulation. A single point of failure is further decreased with the decentralization of the central block. It will maintain all the properties of others even if one of the nodes is hacked.

c. Automating the self-executing smart contract: BT could well integrate the self-executing smart contracts into its IoT network. These contracts will have triggers that can be pre-defined for event occurrences to do such things as lock up the device or alert the administrator on a failure. This facility will help address privacy threats and ensure instant remedial response before it can lead to serious damage.

2.4.2 Cyber Risk and Anomaly Detection

Anomaly detection technique involves identifying anomalous behaviors or events associated with an external signal or the internal workings of the system that indicate possible intrusions. It is also one of the earliest forms of many defenses established in cyber safety. The presents descriptions of some methods for threat and incident detection, including statistical, remote, and machine learning. The increasing size and complexity of cybersecurity operations mandate a new and innovative approach that will automate and scale the operations with large data sets for anomaly detection [124].

a. Anomaly Detection Techniques under Cybersecurity

The anomalous patterns could indicate some strange or unaccepted behavior. In such cases, the detection mechanism can sometimes highlight new attack vectors or detect previously focused attacks. Anomaly detection also classifies patterns that deviate from normal behavior. Anomaly detection is defined as the discovery of a pattern that is abnormal from previously known normal behavior. The most prominent example of this is that the discovery of this anomaly will lead to the discovery of a new attack vector or the identification of attacks that were previously considered less significant. Cyber threats continue to evolve, accompanied by the increase in data in security systems; therefore, traditional methods no longer offer a fair attempt at classification; however, they bring with them more advanced options [124].

Statistical Methods: The method of statistical anomaly detection involves creating a model of normal system behavior. It flags deviations from this model as potential threats. One method to do this is threshold-based detection: anomalous behavior is identified when it exceeds a predefined threshold [125].

Distance-Based Methods: These techniques use the distance between data points to find those that are far from the main group. The anomaly being detected by the k-nearest neighbors (k-NN) algorithm is based on how far away an object really is from those around it [126].

ML Methods: An entire field of ML deals with anomaly detection, which may seem difficult; however, it becomes a good analytical tool for datasets that are complex and very high-

dimensional. These methods learn from the data and improve over time to deal with new plants under attack. Supervised, unsupervised, or semi-supervised, these methods are currently the most appropriate to use with this classification [127] as Table 2.3

Table 2.3: Overview of Anomaly Detection Techniques in Cybersecurity [124].

Technique	**Description**	**Example**
Statistical Methods	Use statistical models to define normal behavior. Deviations indicate anomalies.	Threshold-based detection [125].
Distance-Based Methods	Measure the distance between data points and identify anomalies as those far from others.	K-Nearest Neighbors [126]
ML	Use algorithms to model complex patterns and adapt to new data.	Support Vector Machines (SVM) [128].

2.4.3 Machine Learning Approaches

The ML techniques have assumed more and more importance in cybersecurity because they have the ability to learn from data and adapt to new threats. In relation to anomaly detection, ML provides the flexibility to deal with dynamic and ever-changing attacks. The following are some of the notable machine-learning techniques embraced in cybersecurity. Supervised Learning Methods: In these methods, the model gets trained using a labeled dataset, where both the input data and the corresponding outcome are known; in applying these methods, there is really great usefulness when a clear distinction can be made between normal and malicious activity [124]**.**

Support Vector Machines (SVM): SVMs are an excellent candidate for binary classification to describe the distinction made between normal network traffic and malicious traffic. The algorithm searches out an optimal hyperplane that maximizes separation between classes, thereby providing benefits especially in the case of high-dimensional datasets [128]. SVMs were found to work well in intrusive detection by Mukkamala [129], giving high accuracy in classifying network traffic.

Random forests: Random forest is an ensemble learning method for classification that averages multiple decision trees. The prediction value of each tree is considered for the final decision. The algorithm takes the mode of predicted classes or averages predicted values across trees for final prediction. Random forests show good resistance to overfitting, which

makes them suitable to work with noisy data [130]. Zhang [131] applied Random Forests to network intrusion detection and achieved a high detection rate with a robust resistance to overfitting.

Artificial Neural Networks (ANN): These neural networks mimic the biological neural network and are best suited for modeling data that involve complex non-linear relationships. ANNs have the capability to learn from training data and generalize to new cases that have never been presented. Cannady [132] described the use of ANNs in network anomaly detection, in which ANNs were able to detect abnormal patterns with a high degree of accuracy.

Naïve Bayes Classifier: A Naïve Bayes classifier is based on Bayes' theorem and considers that the features are conditionally independent given the class label. Although it is simple, it works quite well in such tasks as intrusion detection, most particularly whenever there is a high number of independent features. Sperotto [125] and Angiulli [126] showed Naïve Bayes was quite adept in exposing security breaches in network traffic.

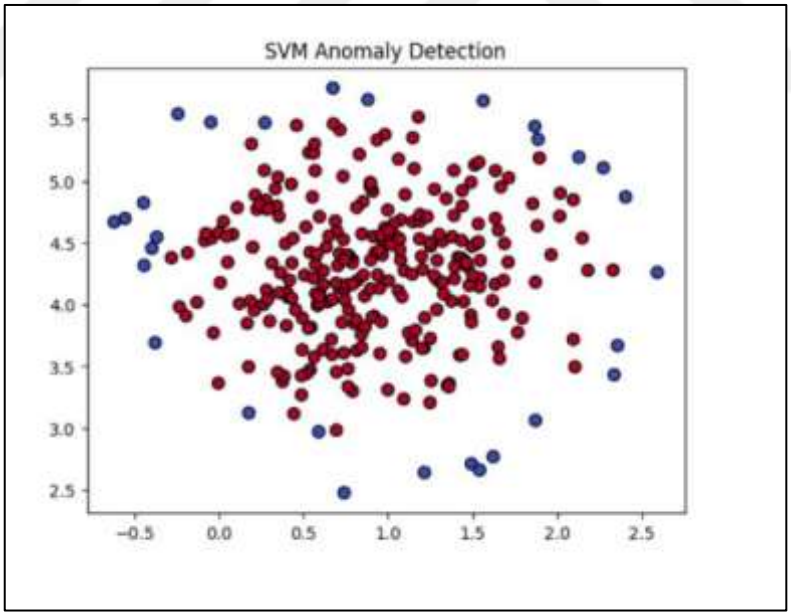

Figure 2.4: Scatter Plot with Anomalies Highlighted in a Different Color [124].

Random-forests and unsupervised learning in anomaly detection

Random Forests are an ensemble learning technique by training multiple decision trees and averaging their predictions for increased accuracy. This is particularly useful for large datasets [130]. Shyu [133] described component analysis (PCA) as an effective method for identifying anomalies in high-dimensional datasets. Liu et al. [125] introduced isolation forest, which is another powerful tool that isolates anomalies.

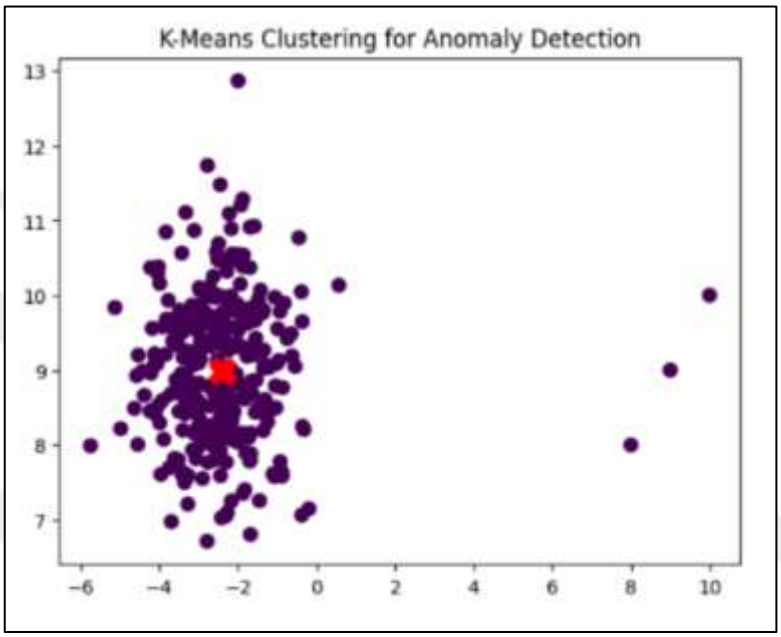

Figure 2.5: A Scatter Plot of Normal Points, Grouped in Clusters, and Outliers Marked Separately [124].

Principal component analysis (PCA) is applied to the reduction of dimensionality while maximizing variance retention. Detection of anomalies would be done based on a deviation from principal components [124].

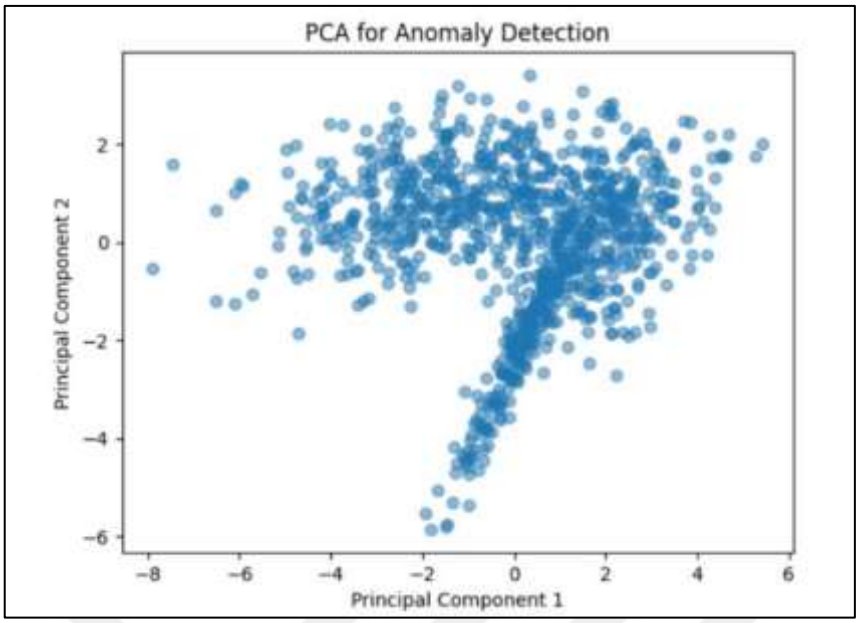

Figure 2.6: A Plot Showing the Data Points Reduced to two Dimensions, with Anomalies Potentially Appearing Away from the Dense Clusters [124].

2.4.4 Deep Learning Techniques for Cyber Security Anomaly Detection

Deep learning is an advanced branch of ML that plays an increasing role in the sphere of cybersecurity. Deep learning typically deals with multilayered neural networks (commonly termed as deep neural networks, or DNNs), which are capable of modeling data patterns that are too complex and non-linear. Anomaly detection caused by cyber threats, which has been very ineffectively dealt with in traditional methods due to their inability to handle huge, unstructured data sources, is particularly well suited to these deep learning architectures.

One of the most revolutionizing models in this domain is the Convolutional Neural Network (CNN). Even though CNNs are typically used for image processing tasks, researchers were able to adapt it into the cybersecurity world through transforming network traffic into image-like representations. In this manner, CNNs are able to leverage their natural advantage of understanding spatial hierarchies to identify network behavior anomalies. For instance, CNNs are claimed by Kim et al. [135] as able to learn how to identify network intrusions from the learned extraction of features at a spatial level that distinguishes ordinary and harmful traffic patterns.

Another equally relevant model used for this area is the Recurrent Neural Network (RNN), and particularly the Long Short-Term Memory (LSTM). True from the name itself, RNNs

are designed to possess the feature of the order of sequence of data; thus, it finds best use while handling time-related patterns such as network traffic flows. With the capability of memorizing data through longer sequences, LSTMs were discovered much better than conventional methods during the course of anomaly detection whenever the said anomalies were present in time. Yin et al. [136] explained that such features encourage better detection accuracy of time-evolving threats because LSTM networks are able to perform well at learning long-range dependencies from the incoming data at the network.

Of late, much has been discussed with regard to the utility of Generative Adversarial Networks (GANs) as per as developments of cybersecurity applications are concerned. Two networks are developed under this framework of GANs: the discriminator and the generator, both of which are trained through rivalry. The generator thus generates fake data for the discriminator to classify whether it could possibly be separated from original data or otherwise. The setting has got two significant advantages: first, the creation of fake attack data and use of such through purposes of enriching training datasets through augmentation, specially vital to assist with the problem of data scarcity; and secondly, the discriminator as an anomaly detector through reporting of any odd values inconsistent with the typical distribution. Wu et al. [137]demonstrate an example of a manner through such an adversarial process of training could enhance detection capability through an improvement of the model of resistance of patterns of unknown attacks. Another of the widely utilized models of anomaly detection is the autoencoder, an unsupervised learning model with which we can use to compress and reconstruct input

Anomaly Detection in Cloud and IoT Environments: New challenges arise, particularly with regard to anomaly detection and IoT as follows:

Table 2.4: Challenges in Cloud Security.

Challenge	**Description**	**Approach**
Scalability	Need to process vast amounts of data quickly and efficiently	Distributed ML [138].
Real-Time Detection	Anomaly detection must be performed in real-time to prevent breaches.	Online anomaly detection using stream mining [139]

2.4.5 Anomaly Detection Using Statistical Methods

Failure to identify any behavior that is considered fundamental to the network, or in other words, expected behavior based on previously provided historical data for expected behavior, thus, this model of normal behavior itself serves as a reference for detecting any anomalies, as any deviation from this fundamental behavior means that the network may exhibit abnormal behavior that may indicate a security threat [140].

Statistical methods are used to identify the underlying lines. A common method is to use probability distributions to model potential behaviors and detect anomalies [141]. Other approaches include time-series trending and regression, where patterns over time are documented and deviations from these temporal trends are considered outliers or anomalies [142]. After establishing the normal behavior model, the next task is to detect deviations that could signal a security risk [143].One of the most common methods for detecting these abnormalities is the Z-score method [140].

Integration of ML with Statistical Anomaly Detection: ML-based anomaly detection combined with statistical methods may specialize in dealing with zero-day threats: these are invisible methods used when traditional methods fail [144], [145]. Statistical methods offer the potential for early detection of threats and achieve results with low false alarms [146].

3. MATERIAL AND METHODS

Breakthroughs in networking in the near past, particularly through the one-shot rollout of 5G, are driving the rapid pace of growth in the Internet of Things. However, one role of this surge is transforming sectors through smothering and automating systems, i.e., a smart home, city, or e-health and industrial IoT applications, and precision agriculture. Include appropriate systems or infrastructure to reduce human errors and increase productivity [2], [3], [4].

However, all of them pose a number of challenges, the most important of which is security, which needs to be addressed [2], [3], [4]. This study highlights mid-sized companies through data obtained from Amazon.

3.1 RESEARCH DESIGNS

The study adopts a mixed research methodology that combines qualitative and quantitative techniques. In the investigation, quantitative techniques are utilized for the systematic gathering and interpretation of numerical data toward exploring the important research questions in a scientific manner. The trends may be examined, measures of statistics such as derivation may be determined, patterns may be identified, causal links may be validated, and the result may be generalized to wider populations (Rana et al., [147]). In parallel, using simulations of AI-managing business continuity protocols along with case studies of medium-sized enterprises is expected to infuse the research findings with real-world insights and practical considerations [147].

3.2 CASE STUDIES

The study utilized case studies that examined midsized companies to demonstrate the real-world impact of AI-integrated business intelligence protocols. Case study research is one of the scientific research methodologies through which comprehensive analyses are done on specific cases or contexts in which a defined phenomenon, such as improved cybersecurity, is actively observed. The first step in this is defining the case clearly, or its area of study, what counts as a part of a case, and what does not.

Hence, cases were delimited based on company size and industry. Such a definition being midsize has aspects which are the electronic industries; therefore, the examples will provide a consistent backdrop, and yet sufficient comparisons across implementations can be made. The value of case studies is in what it does by providing, as its title suggests, contextually specific insights into how AI and business intelligence technologies apply to real-world IoT environments. However, this information is only valid if preceded by rigorous inclusion criteria that guide the data collection process. Among the notable risks identified during analysis is the potential for data loss, which remains a critical concern in these digital ecosystems.

3.3 DATA ANALYSIS

Data were analyzed using the Statistical Package for the Social Sciences (SPSS version 26.0) at a significance level of 0.05. Descriptive statistics (frequencies, percentages, means, and standard deviations) were used for categorical variables. One-way analysis of variance (ANOVA), independent samples t-tests, and linear regression analysis were used [149].

4. RESULT AND DISCUSSION

This section presents the results obtained to evaluate the improvement of AI-based BC protocols for cybersecurity in IoT systems in medium-sized organizations in the Amazon dataset from where information is available for free, and the relationship between these variables.

Table 4.1: Distribution of Client Evaluations.

Category	Discount Price	Actual price	Discount_ percentage	Rating	Rating_ Count
A	399	1,099	64%	4.2	24,269
B	199	349	43%	4	43,994
C	199	1,899	90%	3.9	7,928
D	329	699	53%	4.2	94,363
E	154	399	61%	4.2	16,905
F	149	1,000	85%	3.9	24,871
G	176.63	499	65%	4.1	15,188
H	229	299	23%	4.3	30,411
I	499	999	50%	4.2	1,79,691
J	199	299	33%	4	43,994
K	154	339	55%	4.3	13,391
L	299	799	63%	4.2	94,363
M	219	700	69%	4.4	4,26,973
N	350	899	61%	4.2	2,262
O	159	399	60%	4.1	4,768
P	349	399	13%	4.4	18,757
Q	13,999	24,999	44%	4.2	32,840
R	249	399	38%	4	43,994
S	199	499	60%	4.1	13,045

A: USB Cables, B: HDMI Cables, C: Smart Televisions, D: Wireless USB Adapters, E: Remote Controls, F: TV Wall Mounts, G: RCA Cables, H: Standard Televisions, I: Optical Cables, J: Speaker Mounts, K: Smart Projectors, L: Bluetooth Adapters, M: Smart Home Hubs, N: IoT Surveillance Cameras, O: Smart Light Controls, P: Ethernet Cables, Q: High-End Electronics (e.g., IoT TVs), R: IoT Control Modules, S: USB Hubs / Multiplexers

In Table 4.1, the codes for many products are shown, the product name, and the discount on prices. The highest percentage was for the product name Electronics 13,999, which represents Electronics, and the actual price discount is 44 %, rating, and rating count.

Very essential information on consumer behavior as well as preferences in various IoT product categories is found in Table 4.1, which shows patterns necessary for enterprises in adopting such products. Smart home hubs M category with a discount of 69%, rated very highly at 4.4, and the largest number of reviews (426,973), show their critical importance as the central controllers in IoT systems. Indeed amazing! After the consumers have gotten so immersed in the trend of funky tech gadgets and gizmos, one lands up with a totally new object equipped with an amazing range of capabilities. In line with this, most tech innovations were developed or altered to suit the industry trend. In particular, wireless data transmission remained a significant trend on which tech markets were built.

Optical cables (I) were another key infrastructural element with an impressive 4.2 rating garnered from 179,691 reviews reflecting their reliability for high-bandwidth applications like audio/video systems and edge computing. Wireless USB adapters (D) and Bluetooth adapters (L) join the list, both rated 4.2 with massive reviews of 94,363. Their popularity attests to their role in wireless connectivity for legacy or fixed devices. All of these can be summed up as core components for scalability and mobility-in today's dynamic commercial environments, these are all indispensable.

Table 4.2: Average Scores for Medium Enterprise Dataset.

Category	Mean	SD	Max
A	5154.368	10694.79	24269
B	8909.286	19613.49	43994
C	2006.16	3404.982	7928
D	19079.15	42085.93	94363
E	3492.562	7499.534	16905
F	5204.95	11001.49	24871
G	3173.676	6719.272	15188
H	6188.706	13541.33	30411
I	375.675	476.9672	999
J	8899.266	19618.97	43994
K	2777.77	5934.592	13391
L	19093.17	42078.38	94363
M	231.0225	328.8846	700
N	703.162	945.4072	2262
O	1066.14	2075.756	4768
P	3901.906	8306.349	18757
Q	14368.53	14723.41	32840
R	8929.276	19602.51	43994
S	2749.54	5758.923	13045

A: USB Cables, B: HDMI Cables, C: Smart Televisions, D: Wireless USB Adapters, E: Remote Controls, F: TV Wall Mounts, G: RCA Cables, H: Standard Televisions, I: Optical Cables, J: Speaker Mounts, K: Smart Projectors, L: Bluetooth Adapters, M: Smart Home Hubs, N: IoT Surveillance Cameras, O: Smart Light Controls, P: Ethernet Cables, Q: High-End Electronics (e.g., IoT TVs), R: IoT Control Modules, S: USB Hubs / Multiplexers

Table 4.2 shows that the average score for mid-size companies was 19079.15 ± 42085.93 for Company D. The ± value is some measure of uncertainty under which possible measurement errors, statistical confidence, and variability may be delineated. Company I, on lower bounds, came with a score of 375.675 ± 476.96. Such scores, in turn, reflect

performances and stability along with the cost-effectiveness of IoT architectures. The relationship between customer behavior and enterprise deployment thus signals strategic purchases with smart hubs (M) and optical cables (I) being the linchpins. Wireless adapters (D) provide expansion and flexibility. Low-cost smart TVs (C) point to rapid deployment but have certain drawbacks, as seen in Figure 1.

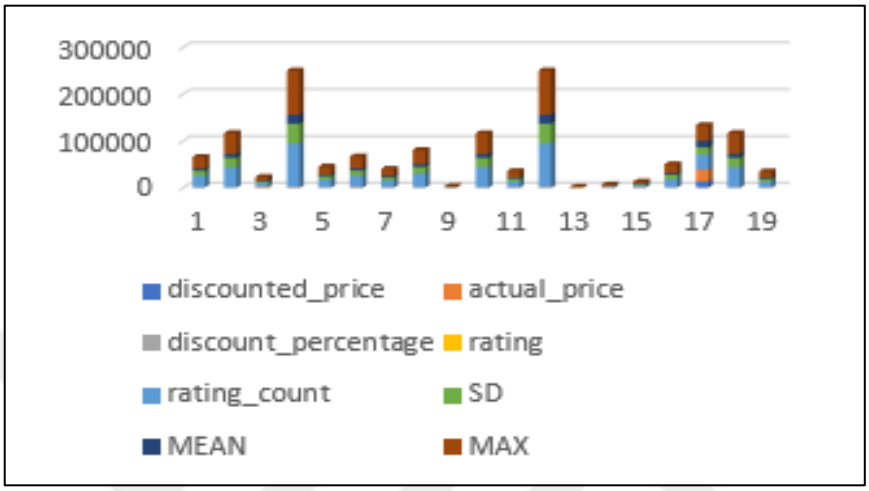

Figure 4.1: Average Scores for the Medium Enterprise Dataset.

Category I, which represents optical cables in this research, occupies the lowest average score within the presented categories. Categories M (smart home hubs) and I (optical cables) occupy critical positions because they serve as potential communication and control wires. Each of the various IoT products by a mid-sized business has an average stability score and price score, as represented in Table 3. Figure 1 shows the average stability and price scores of various IoT products employed by mid-sized businesses: Each category (A-C) represents a different IoT or electronic product (e.g., USB cables, smart TVs, smart hubs). Thus, the highest corresponding average score among all categories is category D (wireless USB adapters), which demonstrate great potential on mobility and scalability-but very discussed. The lowest average score belongs to category I (optical cables). Categories M (smart home hubs) and I (optical cables) occupy strategic positions due to their essential role in communications and control.

Table 4.3: Linear Regression Analysis of the Study Sample.

Regression Statistics	
Multiple R	0.972975
R Square	0.946681
Adjusted R2	0.872905
Standard Error	1.050388

In Table 4.3, using the Amazon dataset, this study examined the correlation between cybersecurity efficacy in IoT systems and AI-based BC protocol optimization; the results are shown in the table. The study focused on medium-sized organizations. With an R-scored value of 0.972975, the variables in the regression model are strongly positively associated with one another. The strong linear association between the independent factor (cybersecurity performance) and the dependent variable (AI-based optimization and BC protocols) is shown by an R-score of 0.973. An R-squared value of 0.947 indicates that the optimization approaches for BC-based on artificial intelligence can explain about 94.7% of the variation in cybersecurity efficacy. This proves that the model successfully describes the connection.

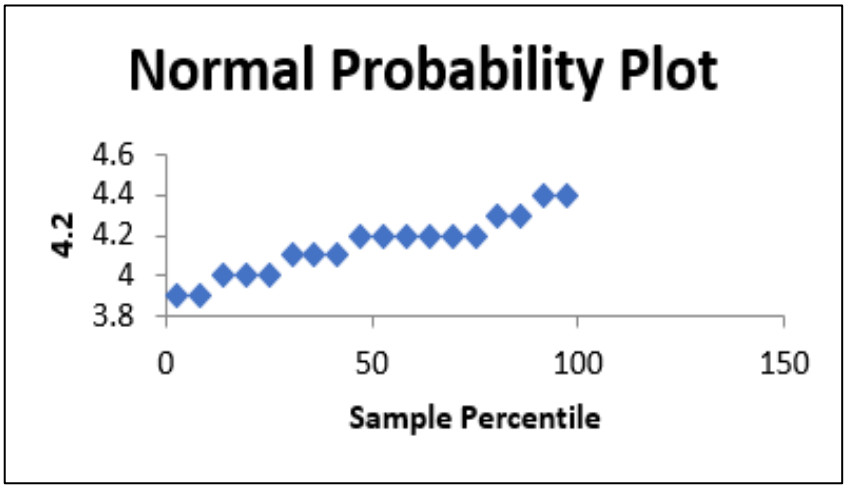

Figure 4.2: Normal Distribution of Data.

Figure 4.2 illustrates a normal probability plot that enables the evaluation of the distributions of IoT data collected from the Amazon dataset. This plot can be very useful in assessing the

stability of the assumed normal distribution of the underlying data, which is assumed by many statistical tests or ML algorithms. Thus, the x-axis indicates the sample proportions that represent the cumulative distribution of all observed data points, while the y-axis displays the actual data values related to performance metrics such as latency, throughput, and system response times.

Table 4.4: ANOVA Analysis of the Study Sample.

ANOVA					
	df	SS	MS	F	Sig
Regression	3	293.8403	97.94676	88.77499	2.3809
Residual	15	16.54972	1.103315		
Total	18	310.39002	99.050075		

Table 4.4 presents the results of the ANOVA. Regression (df = 3). Here, it is 3, indicating that the influence of three factors on cybersecurity outcomes was assessed. Residual (df = 15): represents the degrees of freedom associated with the error term (residual). Regression (SS = 293.8403): The regression sum of squares measures the variance in the dependent variable (cybersecurity outcomes) that can be explained by the independent variables (AI-based BC optimization techniques). The greater the regression SS, the model has greater explanatory power. This affirms the independent variables (BC protocols and optimization techniques) as significant in enhancing the security of IoT systems. Findings support the expectation that AI-based BC protocols increase cybersecurity for IoT systems, and the regression model makes a strong case for the correlation between these optimization methods and better security outcomes. The analysis demonstrates the effectiveness of carrying an AI and BC approach in IoT cybersecurity strategies among medium companies.

Table 4.5: Blockchain Optimization Model Coefficients for Study Sample.

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95.0%
Intercept	0	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
399	0.005897	0.001399	4.21551	0.000749	0.002915	0.008878	0.002915
1099	-0.00328	0.00079	-4.14786	0.000859	-0.00496	-0.00159	-0.00496
0.64	8.452318	0.617032	13.69835	6.9423451528	7.137147	9.76749	7.137147

Table 4.5 demonstrates that a coefficient signifies for each unit increase in the corresponding independent variable; the cybersecurity performance measure increases by 0.005 units, keeping all other factors constant. 0.001 for the other variable: Because of its comparatively small size, the coefficient indicates that this independent variable has relatively minor impacts on the cybersecurity outcomes. Statistically significant in its own right as well, as its t-statistics and p-value indicate. Above 2 for t-statistics, well below 0.05 for p-values, and some very narrow confidence intervals mean that these results talk of applied AI-based optimization techniques as highly critical for cybersecurity improvement in IoT systems within mid-sized enterprises, as demonstrated through analysis of the Amazon dataset: The coefficient estimates for an analytical model of enterprise-level cybersecurity performance relying on BT include estimates about how certain technological factors and operational functions impact enterprise-level security outcomes. Some digital tokens appear corrupted or disorganized, but regression results can still be informative enough to help understand how BT can improve IoT systems. The coefficients indicate the direction and intensity of each predictor's impact with respect to cybersecurity performance.

The present research investigates the applications of BC, even in-depth, toward extending coverage under the concept of combating cyber threats, especially within the IoT environment. Previous findings and literature notes have shown time and again that

decentralization of control, data integrity, and secure communication among devices were enhanced through the activity of BC. For instance, Rai et al. [150] used the example of the BC-can-opienten-the-doors to Simulates-Without-Pollution Act (BCT) models within IoT-based nuclear energy applications to demonstrate that the BC significantly enhances performance in terms of data management through the safety-netting of the available data exchanges against misuse and malicious threats. Zafer and Pomeroy [151] also attested to the efficacy of today's BC technology which helps to ascertain establishment of the so-called trust in IoT networks by way of offering a solid understanding of all the necessary breakout points achieved through transparent and immutable records that reduce vulnerability to attacks or interference with unauthorized access.

These results, therefore, accord with previous studies. Changes as small as a 0.005 increase in cybersecurity performance per unit change in certain variables can have significant effects when multiplied by the numbers at which they apply-as the case with the IoT networks associated with such an observation. This was noted by Anwar et al. [152] when they indicated that each of the components that make up BC may appear minor when examined individually. However, the collection of these impacts may serve to considerably alter large systems. Although BC is not a panacea for security, its strategic implementation provides part of the solution to improving the resilience of IoT systems.

Statistically significant wings improvement in cybersecurity can enter small coefficients of 0.001, having t-statistics quite high enough for its entry. According to Alfahaid et al.[153], although AI-based models have low coefficient values, their effects on risk reductions in vast IoT infrastructures could be considerable given their capacity to provide real-time optimizations and threat mitigations.

Scalability is one major aspect that has been emphasized in previous researches regarding improvements in cybersecurity. Incremental device-level upgrades accumulate to massive advancements in security at the level of entire massive IoT networks, as noted by Sadhu et al.[154]. What are also observed by Gholami et al.[155] is that while the effect of BC applies to IoT security, this effect becomes amplified through scale. Little risk diversions per device can yield significant improvements across system resilience.

5. CONCLUSIONS

5.1 STUDY LIMITATION

As technology advances and AI is maturing, small and medium enterprises worldwide are coping with several minimal cyber threats. The major one shall even continue to enlarge and cloud understanding of increasing cyberattack paths used by more sophisticated attackers who amplify weaknesses in the system. Such attacks even stretch to small and medium enterprises, thus making the defensive works harder. With the advancements in the Internet of Things and increasing adoption of cloud technologies, the need for more integration in the work of risk management strategies has attained urgency. The other dimension with AI advancement lies in that having advanced cyber defense is parallel processing with allowing the attackers to mask by using the same mechanism to build even more powerful techniques to be more successful in attacking the targets. AI in itself can be seen as a compare and contrast process between the traditional countermeasures and the countermeasures augmented with AI that can study and adapt to a target system more quickly than the traditional methods. These imply that the defensive methods applied should be instant and flexible to the assumption of machine-learning-based systems reinforced with big data analytics for more precise identification of suspicious behavioral patterns with that of a user as well as the network. Accordingly, it becomes the responsibility to promote cybersecurity awareness to every member of staff operating at any level of the organization. Only this way can firms create a proactive defense measure against growing threats, like that of an active and sound security culture that raises awareness of cybersecurity risks.. Such actions minimized the likelihood of breaches and would also contain the damage from weakened attacks. Collaboration among various stakeholders, including governments and private companies, results in the development of shared databases and effective defense strategies that expect future challenges to grow further in intensity.

On the other hand, this study has a limitation in that it restricts its scope to SMEs; hence, generalizability is not possible. In addition, its reliance on longitudinal data rather than on cross-sectional data makes a more complete view of these technologies impossible.

5.2 CONCLUSION

Against the threats posed by growing and emerging orientations in this field, a good deal of effort will need to be able to successfully aggregate actions across diverse entities and modes. Because AI increases the impact of other business continuity systems for cybersecurity applications, we use a number of methods, including partnerships, and this study emphasizes the major significance of AI and business continuity with respect to the safeguarding of IoT environments. Such a partnership is for example described where a bank collaborates with IT companies to develop a new system to detect suspicious activity by sharing common trainings for building awareness on security with employees, as well as their analytical and response skills against threats. Sharing of information is critical for increasing defense. A channel should be opened for organizations to share information about perceived attacks and what the attackers did in each case. Data regarding individual behaviors, or trends in behavior that may indicate a threat, could also be shared. This includes the opening of a channel for cyber actors to discuss research output and the development of the cybersecurity framework. Going through this channel contributes significantly to establishing a cohesive community aimed at countering cyber threats, which in turn enhances the resilience of these organizations against the ever-rising risks.

Results from regression and ANOVA strongly support AI-based optimization positively correlating to the improvement of cybersecurity performance, with a stunning R-square of 0.947. Evidence from the Amazons dataset indicated the AI Business Continuity protocols as mitigating the threat levels for authorized data access, data breach incidences, and cyberattacks. These findings were supplemented by real-world case studies showcasing applications within medium-sized electronics firms.

5.3 RECOMMENDATIONS

In addition, any future developments should also draw from data from sectors apart from electronics.

Fast change is what future cybersecurity practices will be based upon. The most significant trend of tomorrow is the increasing dependence on the technologies of AI and ML, enhancing the analysis and prediction of cyber threats. Organizations are pouring in resources towards the development of self-learning systems that will analyze anomalous

behavior and will help identify abnormal patterns in data traffic, which would allow swift responses to potential breaches a step ahead of their occurrence.

Cloud security- the increasing mainstay of information protection strategy; in terms of better and better encryption and data inspection techniques to protect sensitive information from ever-raising threats.

A consideration of these trends brings up future challenges regarding the realization of cybersecurity strategies. Chief among them is the increasingly sophisticated nature of attack capabilities and modes, as a greater number of attackers employ highly advanced tactics, such as cyber warfare and ransomware attacks against critical infrastructure.

But this would not be possible without awareness elevation concerning the importance of cybersecurity both at individual and organizational levels, besides upgrading international cooperation regarding sharing information about cyber threats and attack modelling. Among these, the major hindrances to establishing systems have been a generally low supply of specialized skills in this field, hence the move by universities and research centres to localize the teaching of essential competencies that would result in creating a strong base of cybersecurity experts.

Adaptable and evolving systems, capable of addressing new threats, are assumed as essential ingredients towards creating a secure and sustainable digital environment. So, indeed, the immediate future of cybersecurity is expected to depend on the integration of technology with smart protection strategies, aided by innovations like blockchain and the IoT.

REFERENCES

[1] M. M. Abdelhamid, L. Sliman, and R. B. Djemaa, "AI-enhanced blockchain for scalable IoT-based supply chain," Logistics, vol. 8, no. 4, p. 109, 2024. doi: 10.3390/logistics8040109.

[2] A. Y. Afonkin and N. A. Nozdrina, "Prospects for the development of blockchain technology in the near future," in Scientific Trends: Issues of Exact and Technical Sciences, vol. 16, 2018, pp. 20–21.

[3] Y. Y. Goncharenko and F. N. Pavo, "Development of a decentralized application for the implementation of digital identity using blockchain technology," Bulletin of the Ural Federal District, vol. 29, no. 3, pp. 23–28, 2018.

[4] L. Alevizos, "Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts," International Journal of Information Technology, 2024, Advance online publication. doi: 10.1007/s41870-024-02324-9.

[5] S. Gorshkova, "New technologies in the service of intellectual property rights: Blockchain, artificial intelligence, virtual reality," presented at the IX International Legal Forum (IP Forum), Moscow, Russia, 2021.

[6] L. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, "Resource optimized federated learning-enabled cognitive internet of things for smart industries," IEEE Access, vol. 8, pp. 168854–168864, 2020. doi: 10.1109/ACCESS.2020.3023940.

[7] M. Khan, "A formal method for privacy-preservation in cognitive smart cities," Expert Systems, vol. 39, no. 4, 2021, Art. no. e12855. doi: 10.1111/exsy.12855.

[8] J. Park, M. M. Salim, and J. Kim, "CIoT-Net: A scalable cognitive IoT-based smart city network architecture," Human-Centric Computing and Information Sciences, vol. 9, no. 1, p. 29, 2019. doi: 10.1186/s13673-019-0190-9.

[9] H. Han, R. K. Shiwakoti, R. Jarvis, and C. Mordi, "Accounting and auditing with blockchain technology and artificial intelligence: A literature review," International Journal of Accounting Information Systems, vol. 48, 2023, Art. no. 100598. doi: 10.1016/j.accinf.2022.100598.

[10] N. Shengelia, N. Chitadze, and T. Chitadze, "The impact of financial technologies on digital transformation of accounting, audit and financial reporting," Economics, vol. 105, no. 1, pp. 385–399, 2022. doi: 10.36962/ecs105/3-2022-385.

[11] A. Arora and R. Gupta, "SNRLM: A cyber-physical-based stepwise noise removal and learning model for automated quality assurance," International Journal of Information Technology, vol. 16, pp. 1917–1929, 2024. doi: 10.1007/s41870-024-01835-9.

[12] I. Atoum, A. Otoom, and A. Abu Ali, "A holistic cybersecurity implementation framework," Information Management & Computer Security, vol. 22, no. 3, pp. 251–264, 2014. doi: 10.1108/IMCS-07-2013-0053.

[13] S. Quamara and A. K. Singh, "SChain: Towards the quest for redesigning supply-chain by augmenting blockchain for end-to-end management," International Journal of Information Technology, vol. 14, pp. 2343–2354, 2022. doi: 10.1007/s41870-022-00999-6.

[14] G. A. Al-Kafi, M. Al-Amin, M. A. Ullah, M. S. Hossain, and M. M. Hasan, "SHBF: A secure and scalable hybrid blockchain framework for resolving trilemma challenges," International Journal of Information Technology, vol. 16, pp. 3879–3890, 2024. doi: 10.1007/s41870-024-01880-4.

[15] K. Wang, J. Dong, Y. Wang, and H. Yin, "Securing data with blockchain and AI," IEEE Access, vol. 7, pp. 77981–77989, 2019.

[16] L. Alevizos and M. Dekker, "AI-powered threat intelligence for next-gen cybersecurity," arXiv preprint, 2024. [Online]. Available: https://arxiv.org/pdf/2403.03265

[17] P. Ohri, M. Kumar, and U. Singh, "Blockchain-based security framework for mitigating network attacks in multi-SDN controller environment," International Journal of Information Technology, 2024, Advance online publication. doi: 10.1007/s41870-024-01933-8.

[18] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in Proc. 10th Int. Conf. Frontiers Inf. Technol. (FIT), 2012, pp. 257–260. doi: 10.1109/FIT.2012.53.

[19] S. Goundar, "Blockchain-AI integration for resilient real-time cyber security," in Proc. Global Congr. Emerg. Technol. (GCET), 2024, pp. 342–349.

[20] K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, "Real-time cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach," Computer Science & IT Research Journal, vol. 4, no. 12, pp. 478–501, 2023.

[21] M. Ozkan-Okay et al., "A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," IEEE Access, vol. 12, pp. 12229–12256, 2024.

[22] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms," Knowledge and Information Systems, vol. 67, pp. 6969–7055, 2025.

[23] N. Bari, G. Mani, and S. Berkovich, "Internet of things as a methodological concept," in Proc. 4th Int. Conf. Comput. Geospatial Res. Application (COM. Geo), 2013, pp. 48–55.

[24] N. D. Lane et al., "A survey of mobile phone sensing," IEEE Commun. Mag., vol. 48, no. 9, 2010.

[25] Y. Yu, J. Wang, and G. Zhou, "The exploration in the education of professionals in applied internet of things engineering," in Proc. 4th Int. Conf. Distance Learn. Educ. (ICDLE), 2010, pp. 74–77.

[26] J. Greenough, "How the 'internet of things' will impact consumers, businesses, and governments in 2016 and beyond," Apr. 2015. [Online]. Available: http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10

[27] A. K. Sikder, H. Aksu, and A. S. Uluagac, "6thsense: A context aware sensor-based attack detector for smart devices," in Proc. 26th USENIX Security Symp. (USENIX Security 17), Vancouver, BC, 2017, pp. 397–414.

[28] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," International Journal of Computer Applications, vol. 111, no. 7, pp. 1–6, 2015.

[29] A. S. Gillis and K. Yasar, "What is IoT (internet of things)?," 2025. [Online]. Available: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

[30] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surv. Tutor., vol. 17, no. 4, pp. 2347–2376, 2015.

[31] S. T. Kaniganti and V. N. S. K. Challa, "Leveraging microservices architecture with AI and ML for intelligent applications," International Journal of Advanced Research in Engineering & Technology, vol. 11, no. 12, pp. 11-20, 2020. doi: 10.34218/IJARET.11.12.2020.353.

[32] C. Perera, P. P. Jayaraman, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Dynamic configuration of sensors using mobile sensor hub in internet of things paradigm," in Proc. 2013 IEEE 8th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process., 2013, pp. 473–478.

[33] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[34] I. I. Umeh and K. C. Umeh, "Redefining the future of data processing with edge computing," World Journal of Advanced Research and Reviews, vol. 24, no. 2, pp. 2865-2877, 2024. doi: 10.30574/wjarr.2024.24.2.3463.

[35] A. Jahnke, "The 4 stages of IoT architecture," 2020. [Online]. Available: https://www.zibtek.com/blog/iot-architecture/

[36] C. Pereira and A. Aguiar, "Towards efficient mobile M2M communications: Survey and open challenges," Sensors, vol. 14, no. 10, pp. 19582–19608, 2014. doi: 10.3390/s141019582.

[37] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: A review," Journal of Big Data, vol. 6, no. 1, 2019, Art. no. 1. doi: 10.1186/s40537-019-0268-2.

[38] B. Dorsemaine et al., "Internet of Things: A definition and taxonomy," Procedia Comput. Sci., vol. 56, pp. 300–307, 2015.

[39] S. Causevic, A. Colakovic, and A. Haskovic, "The model of transport monitoring application based on the internet of things," in Proc. 2018 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH), 2018.

[40] R. Nicolescu, M. Huth, P. Radanliev, and D. De Roure, "Mapping the values of IoT," Journal of Information Technology, vol. 33, no. 4, pp. 345–360, 2018. doi: 10.1057/s41265-018-0054-1.

[41] M. R. Palattella et al., "Standardized protocol stack for the Internet of (Important) Things," IEEE Access, vol. 8, pp. 148015–148029, 2020.

[42] S. G. Tzafestas, "Ethics and law in the internet of things world," Smart Cities, vol. 1, no. 1, pp. 98–120, 2018.

[43] T. Nacera, C. Abdelghani, D. Karim, and M. Ahmed-Nacer, "A distributed agent-based approach for optimal QoS selection in web of object choreography," Journal Title, vol. X, no. Y, pp. ZZ–ZZ, 2018.

[44] L. Huo and Z. Wang, "Service composition instantiation based on cross-modified artificial Bee Colony algorithm," China Commun., vol. 13, no. 10, pp. 233–244, 2016. doi: 10.1109/CC.2016.7733047.

[45] G. White, V. Nallur, and S. Clarke, "Quality of service approaches in IoT: a systematic mapping," J. Syst. Softw., vol. 132, pp. 186–203, 2017. doi: 10.1016/j.jss.2017.05.125.

[46] Web Services Quality Factors Version 1.0, OASIS Standard, 2012.

[47] M. K. Saggi and S. Jain, "A survey towards an integration of big data analytics to big insights for value-creation," Inf. Process. Manage., vol. 54, no. 5, pp. 758–790, 2018. doi: 10.1016/j.ipm.2018.01.010.

[48] C. K. M. Lee, C. L. Yeung, and M. Cheng, "Research on IoT based cyber-physical system for industrial big data analytics," in Proc. 2015 IEEE Int. Conf. Ind. Eng. Eng. Manag. (IEEM), 2015. doi: 10.1109/IEEM.2015.7385969.

[49] C. Vuppalapati, A. Ilapakurti, and S. Kedari, "The role of big data in creating sense EHR, an integrated approach to create next-generation mobile sensor and wearable data-driven electronic health record (EHR)," in Proc. 2016 IEEE 2nd Int. Conf. Big Data Comput. Service Appl. (BigDataService), 2016. doi: 10.1109/BigDataService.2016.18.

[50] D. Mourtzis, E. Vlachou, and N. Milas, "Industrial big data as a result of IoT adoption in manufacturing," Proc. CIRP, vol. 55, pp. 290–295, 2016.

[51] H. Zeng, M. Yunis, A. Khalil, and N. Mirza, "Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity," Journal of Innovation & Knowledge, vol. 9, 2024, Art. no. 100601. doi: 10.1016/j.jik.2024.100601.

[52] J. Meakins, "A zero-sum game: the zero-day market in 2018," J. Cyber Policy, vol. 4, pp. 60–71, 2019. doi: 10.1080/23738871.2018.1546883.

[53] Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, U.S. Department of Defense, 2017. [Online]. Available: https://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf

[54] P. Radanliev and O. Santos, "Adversarial attacks can deceive AI systems, leading to misclassification or incorrect decisions," ACM Comput. Surv., 2023, Advance online publication.

[55] Cyber Risk, Institute of Risk Management, 2019. [Online]. Available: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

[56] L. M. Tanczer, I. Steenmans, M. Elsden, J. Blackstock, and M. Carr, "Emerging risks in the IoT ecosystem: who's afraid of the big bad smart fridge?," in Living in the Internet of Things: Cybersecurity of the IoT, London: Institution of Engineering and Technology, 2018.

[57] "KrebsOnSecurity Hit with Record DDoS," Krebs on Security, Sep. 2016. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[58] I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock, "Standardising a moving target: the development and evolution of IoT security standards," in Living in the Internet of Things: Cybersecurity of the IoT, London: Institution of Engineering and Technology, 2018.

[59] H. R. Schindler et al., Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of Things, RAND, 2013. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/18e2ee38-75a8-4b61-aad5-97b1728d11ee

[60] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Hansom AFB, MA: CERT, 2007.

[61] J. Wynn et al., Threat Assessment and Remediation Analysis (TARA), MITRE Corporation, 2011. [Online]. Available: https://apps.dtic.mil/sti/tr/pdf/ADA576473.pdf

[62] NVD-CVSSv3 Calculator, NIST, 2022. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

[63] R. Shaw, V. Takanti, and T. Zullo, Best Practices in Cyber Supply Chain Risk Management, NIST, 2017. [Online]. Available: https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf

[64] What Is Capability Maturity Model Integration (CMMI)?, CMMI Institute, 2017. [Online]. Available: http://cmmiinstitute.com/capability-maturity-model-integration

[65] Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2014.

[66] ISO - International Organization for Standardization, 2017. [Online]. Available: https://www.iso.org/home.html

[67] FAIR-U Model, FAIR Institute, 2020. [Online]. Available: https://www.fairinstitute.org/fair-u

[68] A. Erola et al., "A system to calculate cyber value-at-risk," Comput. Secur., vol. 113, 2022, Art. no. 102545.

[69] Quantitative Information Risk Management, FAIR Institute, 2017. [Online]. Available: http://www.fairinstitute.org/

[70] Y. Cherdantseva et al., "A configurable dependency model of a SCADA system for goal-oriented risk assessment," Appl. Sci., vol. 12, no. 10, 2022, Art. no. 4880. doi: 10.3390/app12104880.

[71] T. Alpcan and N. Bambos, "Modeling dependencies in security risk management," in Proc. 4th Int. Conf. Risks Security Internet Syst. (CRiSIS), 2009, pp. 113–116.

[72] T. B. Callo Arias, P. Van Der Spek, and P. Avgeriou, "A practice-driven systematic review of dependency analysis solutions," Empir. Softw. Eng., vol. 16, pp. 544–586, 2011. doi: 10.1007/s10664-011-9158-8.

[73] A. Laugé, J. Hernantes, and J. M. Sarriegi, "Critical infrastructure dependencies: a holistic, dynamic and quantitative approach," Int. J. Crit. Infrastruct. Prot., vol. 8, pp. 16–23, 2015. doi: 10.1016/j.ijcip.2014.12.004.

[74] P. O'Neill, "Protecting critical infrastructure by identifying pathways of exposure to risk," Technol. Innov. Manage. Rev., pp. 34–40, 2013. doi: 10.22215/timreview/714.

[75] unixfreaxjp, "MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled," MalwareMustDie, Aug. 2016. [Online]. Available:

https://web.archive.org/web/20160905131212/http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html

[76] D. Bonderud, "Leaked Mirai malware boosts IoT insecurity threat level," Security Intelligence, Oct. 2016. [Online]. Available: https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/

[77] L. H. Newman, "What we know about Friday's massive East Coast internet outage," Wired, Oct. 2016. [Online]. Available: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

[78] "Who is Anna-Senpai, the Mirai worm author?," Krebs on Security, Jan. 2017. [Online]. Available: https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

[79] J. Biggs, "Hackers release source code for a powerful DDoS app called Mirai," TechCrunch, Oct. 2016. [Online]. Available: https://techcrunch.com/2016/10/19/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/

[80] R. Hackett, "Why a hacker dumped code behind colossal website-trampling botnet," Fortune, Oct. 2016. [Online]. Available: https://fortune.com/2016/10/03/botnet-code-ddos-hacker/

[81] S. K. Datta and C. Bonnet, "An edge computing architecture integrating virtual IoT devices," in Proc. 2017 IEEE 6th Global Conf. Consum. Electron. (GCCE), 2017, pp. 1–3.

[82] F. Chen and Y. Luo, "An inside look at IoT malware," in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering: Industrial IoT Technologies and Applications, vol. 202, 2017, pp. 176–186. doi: 10.1007/978-3-319-60753-5_19.

[83] N. Statt, "How an army of vulnerable gadgets took down the web today," The Verge, Oct. 2016. [Online]. Available:

https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained

[84] "IoTroop Botnet: The Full Investigation," Check Point Research, Oct. 2017. [Online]. Available: https://research.checkpoint.com/2017/iotroop-botnet-full-investigation/

[85] I. Zeifman, D. Bekerman, and B. Herzberg, "Breaking Down Mirai: An IoT DDoS Botnet Analysis," Incapsula, Oct. 2016. [Online]. Available: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/

[86] T. Moffitt, "Source Code for Mirai IoT Malware Released," Webroot, Oct. 2016. [Online]. Available: https://www.webroot.com/blog/2016/10/10/source-code-mirai-iot-malware-released/

[87] C. Osborne, "Mirai DDoS botnet powers up, infects Sierra Wireless gateways," ZDNet, Oct. 2016. [Online]. Available: https://www.zdnet.com/article/mirai-ddos-botnet-powers-up-infects-sierra-wireless-gateways/

[88] Xander, "DDoS on Dyn The Complete Story," ServerComparator, Oct. 2016. [Online]. Available: https://web.archive.org/web/20161121175123/https://servercomparator.com/vpn/blog/dyn-mirai-ddos-complete-story

[89] M. Antonakakis et al., "Understanding the Mirai botnet," in Proc. 26th USENIX Security Symp. (USENIX Security 17), 2017.

[90] D. Goodin, "100,000-strong botnet built on router 0-day could strike at any time," Ars Technica, Dec. 2017. [Online]. Available: https://arstechnica.com/information-technology/2017/12/100000-strong-botnet-built-on-router-0-day-could-strike-at-any-time/

[91] "IoT Botnet: More Targets in Okiru's Cross-hairs," Fortinet, Jan. 2018. [Online]. Available: https://www.fortinet.com/blog/threat-research/iot-botnet-more-targets-in-okirus-cross-hairs

[92] J. Leyden, "New Mirai botnet species 'Okiru' hunts for ARC-based kit," The Register, Jan. 2018. [Online]. Available: https://www.theregister.com/2018/01/16/arc_iot_botnet_malware/

[93] W. Ashford, "Next-gen Mirai botnet targets cryptocurrency mining operations," Computer Weekly, Jan. 2018. [Online]. Available: https://www.computerweekly.com/news/450433414/Next-gen-Mirai-botnet-targets-cryptocurrency-mining-operations

[94] C. Cimpanu, "New Mirai Variant Focuses on Turning IoT Devices into Proxy Servers," Bleeping Computer, Feb. 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-mirai-variant-focuses-on-turning-iot-devices-into-proxy-servers/

[95] R. Joven and K. Yang, "A Wicked Family of Bots," Fortinet, May 2018. [Online]. Available: https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots

[96] T. Seals, "Wicked Botnet Uses Passel of Exploits to Target IoT," Threat Post, May 2018. [Online]. Available: https://threatpost.com/wicked-botnet-uses-passel-of-exploits-to-target-iot/132125/

[97] Malwaremustdie/Unixfreaxjp, "Mirai mirai on the wall.. how many are you now?," Imgur, Jul. 2018. [Online]. Available: https://imgur.com/a/mirai-mirai-on-wall-how-many-are-you-now-july-2018s-status-post-by-malwaremustdie-org-53f29O9

[98] J. B. Ullrich, "Worm (Mirai?) Exploiting Android Debug Bridge (Port 5555/tcp)," SANS ISC InfoSec Forums, Jul. 2018. [Online]. Available: https://isc.sans.edu/diary/Worm+Mirai+Exploiting+Android+Debug+Bridge+Port+5555tcp/23856

[99] S. Narang, "ThinkPHP Remote Code Execution Vulnerability Used To Deploy Variety of Malware (CVE-2018-20062)," Tenable, Feb. 2019. [Online]. Available: https://www.tenable.com/blog/thinkphp-remote-code-execution-vulnerability-used-to-deploy-variety-of-malware-cve-2018-20062

[100] SC Staff, "Gayfemboy botnet evolution: Fortinet researchers unveil advanced cyber threat," SC Media, Aug. 2025. [Online]. Available: https://www.scworld.com/brief/gayfemboy-botnet-evolution-fortinet-researchers-unveil-advanced-cyber-threat

[101] C. McGoogan, "Unprecedented cyber-attack takes Liberia's entire internet down," The Telegraph, Nov. 2016. [Online]. Available: https://www.telegraph.co.uk/technology/2016/11/04/unprecedented-cyber-attack-takes-liberias-entire-internet-down/

[102] M. Kan, "DDoS attack from Mirai malware 'killing business' in Liberia," PCWorld, Nov. 2016. [Online]. Available: https://www.pcworld.com/article/410934/ddos-attack-from-mirai-malware-killing-business-in-liberia.html

[103] M. J. Schwartz, "Mirai Malware Is Still Launching DDoS Attacks," bankinfosecurity.com, 2016. [Online]. Available: https://www.bankinfosecurity.com/blogs/mirai-malware-still-launching-ddos-attacks-p-2303

[104] M. K. Pratt, "Top 15 IoT security threats and risks to prioritize," TechTarget, 2025. [Online]. Available: https://www.techtarget.com/iotagenda/tip/5-IoT-security-threats-to-prioritize

[105] IoT security issues in 2022: A business perspective, Thales Group, 2022. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats

[106] B. Farrukh, "Top IoT vulnerabilities: How to secure smart devices in 2025," Astrill, 2025. [Online]. Available: https://www.astrill.com/blog/iot-device-vulnerabilities/

[107] V. Vajratiya, G. J. Saxena, A. Pundir, and S. Singh, "Identifying spoofing attacks in Internet of Things (IoT) environments using machine learning algorithms," Journal of High Speed Networks, vol. 31, no. 1, pp. 1-15, 2024. doi: 10.1177/09266801241295886.

[108] D. Z. Morris, "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting," Fortune, May 2016. [Online]. Available: https://fortune.com/2016/05/15/leaderless-blockchain-vc-fund/

[109] N. Popper, "A Venture Fund With Plenty of Virtual Capital, but No Capitalist," The New York Times, May 2016. [Online]. Available: https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html

[110] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton, NJ, USA: Princeton University Press, 2016.

[111] M. Iansiti and K. R. Lakhani, "The truth about blockchain," Harvard Business Review, vol. 95, no. 1, pp. 118-127, 2017.

[112] V. Villanueva Collao, "DeFi-A framework of the automated financial open system," Tulane Journal of Technology & Intellectual Property, vol. 26, p. 75, 2023.

[113] A. Whitaker, "Art and blockchain: A primer, history, and taxonomy of blockchain use cases in the arts," Artivate: A Journal of Entrepreneurship in the Arts, vol. 8, no. 2, pp. 21-47, 2019. doi: 10.34053/artivate.8.2.2.

[114] H. Mayer, "ECDSA security in bitcoin and ethereum: A research survey," CoinFaabrik, pp. 1–10, Jun. 2016. [Online]. Available: https://www.semanticscholar.org/paper/ECDSA-Security-in-Bitcoin-and-Ethereum-%3A-a-Research-Mayer/434a117a2717cdbf78035365d8bab2b0a3410be9?p2df

[115] P. De Filippi, M. Mannan, and W. Reijers, "Blockchain as a confidence machine: The problem of trust & challenges of governance," Technology in Society, vol. 62, 2020, Art. no. 101284. doi: 10.1016/j.techsoc.2020.101284.

[116] M. Almansoori, "AI-Driven Anomaly Detection in Cybersecurity," M.S. thesis, Rochester Inst. Technol. RIT Dubai, Dubai, UAE, 2024.

[117] A. S. Sperotto, "An Overview of IP Flow-Based Intrusion Detection," IEEE Commun. Surv. Tutor., vol. 12, no. 3, pp. 343-356, 2010. doi: 10.1109/SURV.2010.033010.00054.

[118] F. Angiulli and P. Pizzuti, "Fast Outlier Detection in High Dimensional Spaces," in Proc. 6th Eur. Conf. Princ. Data Min. Knowl. Discovery (PKDD), 2002, pp. 15-27. doi: 10.1007/3-540-45681-3_2.

[119] B. Park and J. K. Bae, "Using machine learning algorithms for housing price prediction: The case of Fairfax County, Virginia housing data," Expert Syst. Appl., vol. 42, no. 6, pp. 2928-2934, 2015. doi: 10.1016/j.eswa.2014.11.040.

[120] C. Cortes and V. Vapnik, "Support-Vector Networks," Mach. Learn., vol. 20, no. 3, pp. 273-297, 1995. doi: 10.1007/BF00994018.

[121] S. Mukkamala, G. Janoski, and A. Sung, "Intrusion Detection Using Neural Networks and Support Vector Machines," in Proc. Int. Joint Conf. Neural Netw. (IJCNN), vol. 2, 2002, pp. 1702-1707. doi: 10.1109/IJCNN.2002.1007774.

[122] L. Breiman, "Random Forests," Mach. Learn., vol. 45, no. 1, pp. 5-32, 2001. doi: 10.1023/A:1010933404324.

[123] J. Cannady, "Artificial neural networks for misuse detection," in Proc. Nat. Inf. Syst. Security Conf., vol. 26, Oct. 1998.

[124] M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn, and L. Chang, "A Novel Anomaly Detection Scheme Based on Principal Component Classifier," in Proc. IEEE Found. New Directions Data Min. Workshop, 2003, pp. 172-179. doi: 10.1109/ICDMW.2003.1253329.

[125] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in Proc. 2008 8th IEEE Int. Conf. Data Min. (ICDM), 2008, pp. 413-422. doi: 10.1109/ICDM.2008.17.

[126] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "CNN-Based Network Intrusion Detection Against Denial-of-Service Attacks," Electron. Lett., vol. 53, no. 10, pp. 679-681, 2017. doi: 10.1049/el.2017.1581.

[127] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954-21961, 2017. doi: 10.1109/ACCESS.2017.2762418.

[128] W. Wu and B. Chien, "Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics," in Proc. 2016 Int. Conf. Inf. Syst. (ICIS), 2016.

[129] K. Hsieh, A. Phanishayee, O. Mutlu, and P. B. Gibbons, "Gaia: Geo-Distributed Machine Learning Approaching LAN Speeds," in Proc. 14th USENIX Symp. Netw. Syst. Des. Implement. (NSDI), 2017, pp. 629-647.

[130] R. A. R. Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, "Fuzziness Based Semi-Supervised Learning Approach for Intrusion Detection System," Inf. Sci., vol. 378, pp. 484–497, 2017. doi: 10.1016/j.ins.2016.08.060.

[131] J. B. Awotunde and S. Misra, "Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks," in Illumination of Artificial Intelligence in Cybersecurity and Forensics. Cham: Springer, 2022, pp. 21–44. doi: 10.1007/978-3-030-93453-8_2.

[132] H. J. Shiu, C. T. Yang, Y. R. Tsai, W. C. Lin, and C. M. Lai, "Maintaining secure level on symmetric encryption under quantum attack," Appl. Sci., vol. 13, no. 11, 2023, Art. no. 6734. doi: 10.3390/app13116734.

[133] F. Gatica-Neira, P. Galdames-Sepulveda, and M. Ramos Maldonado, "Adoption of cybersecurity in the Chilean manufacturing sector: A first analytical proposal," IEEE Access, vol. 11, pp. 133475–133489, 2023. doi: 10.1109/ACCESS.2023.3336818.

[134] M. A. Ali and A. Alqaraghuli, "A survey on the significance of artificial intelligence (AI) in network cybersecurity," Babylonian Journal of Networking, vol. 2023, pp. 21–29, 2023. doi: 10.58496/bjn/2023/004.

[135] M. Amin et al., "Cyber security and beyond: Detecting malware and concept drift in AI-based sensor data streams using statistical techniques," Comput. Electr. Eng., vol. 108, 2023, Art. no. 108702. doi: 10.1016/j.compeleceng.2023.108702.

[136] A. Kathirvel and C. P. Maheswaran, "Enhanced AI-based intrusion detection and response system for WSN," in Artificial Intelligence for Intrusion Detection Systems. Boca Raton, FL, USA: CRC Press, 2023, pp. 155–177.

[137] M. Tubishat, F. Al-Obeidat, A. S. Sadiq, and S. Mirjalili, "An improved dandelion optimizer algorithm for spam detection: Next-generation email filtering system," Computers, vol. 12, no. 10, 2023, Art. no. 196. doi: 10.3390/computers12100196.

[138] J. Rana, P. L. Luna Gutierrez, and J. Oldroyd, "Quantitative methods," in Global Encyclopedia of Public Administration, Public Policy, and Governance. Cham: Springer, 2021, pp. 1-6. doi: 10.1007/978-3-319-31816-5_460-1.

[139] H. Mammadov, Á. Ruiz-Gandara, L. Gonzalez-Abril, and I. Romero, "Adoption of artificial intelligence in small and medium-sized enterprises in Spain: The role of competences and skills," Amfiteatru Economic, vol. 26, no. 67, p. 848, 2024. doi: 10.24818/EA/2024/67/848.

[140] J. Karkavelraja, "Amazon Sales Dataset," Kaggle, 2023. [Online]. Available: https://www.kaggle.com/datasets/karkavelrajaj/amazon-sales-dataset

[141] H. M. Rai, K. K. Shukla, L. Tightiz, and S. Padmanaban, "Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies," Heliyon, vol. 10, no. 19, p. e38917, 2024. doi: 10.1016/j.heliyon.2024.e38917.

[142] U. Zafer and J. Pomeroy, "Blockchain-powered IoT security: Ensuring data integrity and device trustworthiness," ResearchGate, 2025. doi: 10.13140/RG.2.2.15756.22404.

[143] F. Anwar, B. U. I. Khan, L. B. Mat Kiah, and N. A. Abdullah, "A comprehensive insight into blockchain technology: Past development, present impact, and future considerations," International Journal of Advanced Computer Science and Applications, vol. 13, no. 11, 2022. doi: 10.14569/IJACSA.2022.01311101.

[144] A. Alfahaid et al., "Machine learning-based security solutions for IoT networks: A comprehensive survey," Sensors, vol. 25, no. 11, p. 3341, 2025. doi: 10.3390/s25113341.

[145] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of things: Security and solutions survey," Sensors, vol. 22, no. 19, p. 7433, 2022. doi: 10.3390/s22197433.

[146] M. Gholami et al., "Blockchain integration in IoT: Applications, opportunities, and challenges," Computers, Materials and Continua, vol. 83, no. 2, pp. 1561–1605, 2025. doi: 10.32604/cmc.2025.063304.

[147] J. Rana, P. L. Luna Gutierrez, and J. Oldroyd, "Quantitative methods," in Global Encyclopedia of Public Administration, Public Policy, and Governance. Springer, 2021, pp. 1–6. doi: 10.1007/978-3-319-31816-5_460-1.

[148] H. Mammadov, Á. Ruiz-Gandara, L. Gonzalez-Abril, and I. Romero, "Adoption of artificial intelligence in small and medium-sized enterprises in Spain: The role of competences and skills," Amfiteatru Economic, vol. 26, no. 67, p. 848, 2024. doi: 10.24818/EA/2024/67/848.

[149] J. Karkavelraja, "Amazon Sales Dataset," Kaggle, 2023. [Online]. Available: https://www.kaggle.com/datasets/karkavelrajaj/amazon-sales-dataset

[150] H. M. Rai, K. K. Shukla, L. Tightiz, and S. Padmanaban, "Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies," Heliyon, vol. 10, no. 19, p. e38917, 2024. doi: 10.1016/j.heliyon.2024.e38917.

[151] U. Zafer and J. Pomeroy, "Blockchain-powered IoT security: Ensuring data integrity and device trustworthiness," ResearchGate, 2025. doi: 10.13140/RG.2.2.15756.22404.

[152] F. Anwar, B. U. I. Khan, L. B. Mat Kiah, and N. A. Abdullah, "A comprehensive insight into blockchain technology: Past development, present impact, and future considerations," International Journal of Advanced Computer Science and Applications, vol. 13, no. 11, 2022. doi: 10.14569/IJACSA.2022.01311101.

[153] A. Alfahaid et al., "Machine learning-based security solutions for IoT networks: A comprehensive survey," Sensors, vol. 25, no. 11, p. 3341, 2025. doi: 10.3390/s25113341.

[154] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of things: Security and solutions survey," Sensors, vol. 22, no. 19, p. 7433, 2022. doi: 10.3390/s22197433.

[155] M. Gholami et al., "Blockchain integration in IoT: Applications, opportunities, and challenges," Computers, Materials and Continua, vol. 83, no. 2, pp. 1561–1605, 2025. doi: 10.32604/cmc.2025.063304.