Research Article

Liqaa Nawaf* and Vibhushinie Bentotahewa

Optimization of cyber security through the implementation of AI technologies

https://doi.org/10.1515/jisys-2024-0226
received April 19, 2024; accepted August 29, 2024

Abstract: Identification of cyber threats is crucial and significant for determining substantial security techniques and approaches. This research illustrates a brief discussion of cyberspace challenges and threats in a disruptive era alongside comprehensive approaches in mitigating the risk of cyber threats. Additionally, the aim of this research is to provide beneficial approaches on how to handle cyber threats in detail. For example, threats and attacks may be caused in the absence of legislation, ethical standardization, support system, and lack of access control. The governance system, therefore, will put a lot of effort into communicating, identifying, and enforcing the principles of security to moderate risk. The Metaheuristic algorithms are stimulated by the human brain, so implementing Artificial Intelligence (AI) that assists the Neural Network to mimic the behaviour of the human brain is important to predict significant outcomes. In this study, the author investigates and analyses the rapid growth of cyber threats to outline the solutions. The aim of this study is to contribute to cyber security optimization through implementing AI methodologies.

Keywords: optimization, cyberspace, cyber threat, AI, IoT, security, privacy, GDPR, COVID-19

1 Introduction

Cyber Threats are significantly growing globally with the rapid increase in digitalized technology [1]. Currently, reports on global cyber threats continue to grow aggressively demonstrating a lack of awareness and assessment to ascertain the level of vulnerability. As these significant cyber threats continue, the National Cyber Security Centre (NCSC) plays a vital role in mitigating these threats, while making UK the safest place to live and work online [1]. Ultimately, human error is identified as the main cause of cyberattacks, e.g. business executives and IT managers face high risk to include deception, and the intrinsic security of business continuity is recognized as a crucial matter. Various reports provide comprehensive approaches and strategies on how to avoid or mitigate the growth of cyber threats.

The Internet of Things (IoT) industry has shown rapid development emerging in modern life that plays a role that is an essential concern of cyber security [2]. IoT technologies are also used in the medical setting and emphasizes interconnected medical technologies. The evolution of such technologies has generated novel risks and caused an enormous impact on businesses and individuals. Therefore, it is important to consider the security of evolving technologies during this disruptive era.

For example, the number of potential targets for cyber threats has increased during the COVID-19 pandemic, and in turn, has significantly influenced the worldwide cyberspace threat scene. However, the

*** Corresponding author: Liqaa Nawaf**, Cybersecurity, Information Networks Centre (CINC), Cardiff School of Technologies, Llandaff Campus, Cardiff Metropolitan University, Western Avenue, Cardiff, CF5 2YB, United Kingdom, e-mail: LLLNawaf@Cardiffmet.ac.uk
Vibhushinie Bentotahewa: Cybersecurity, Information Networks Centre (CINC), Cardiff School of Technologies, Llandaff Campus, Cardiff Metropolitan University, Western Avenue, Cardiff, CF5 2YB, United Kingdom, e-mail: Vibentotahewa@cardiffmet.ac.uk

COVID-19 pandemic has prompted this explosion of cyber threats thereby presenting opportunities for cybercriminals and malicious actors to exploit these vulnerabilities and threats.

Improving and supporting security challenges to mitigate risk is essential for a resilient society. Collecting and analysing huge data have increased in recent years, and even more data will be collected and stored alongside the evolution of technology, which brings us to the necessary precision and solutions to be developed and implemented for the sake of robust security.

Therefore, due to the ever-changing landscape of cyber security, the demand for updated knowledge and skills training is significant factor in increasing awareness among users and the general population. From gov UK reports of cyber security breaches, the survey 2020 [3] initial results show the lack of awareness, essential knowledge, and skills training courses based learning potential opportunities. Hence, cyber threats are a massive problem and must be considered immediately to explore different aspects of cyber security solutions within the fast-paced technology and IT infrastructure.

This article explores and investigates the crucial steps of implementing Artificial Intelligence (AI) to mitigate cyber threats. AI plays an important role in realizing the next generation of research in cyber security. This research contribution tackles cyber threats that went beyond national boundaries through implementing AI and aims to contribute to cyber security optimization through employing AI methodologies and identifying the AI application benefits to cyber security.

This article is organized as follows: Section 2 gives the literature review, methodology is described in Section 3, Section 4 discusses the related work on security challenges in evolving IoT, AI evolution, security challenges in Wireless Mesh Networks (WMN), and security and privacy challenges associated with the use of wireless technologies during COVID-19. Section 5 presents the analysis of the research question. Section 6 presents the cyber security and AI, and investigates how AI technology linked to cyber security. The algorithms, techniques, and approaches used to ensure security are discussed in Section 7. Section 8 concludes the study. Section 9 presents the recommendations.

2 Literature review

AI refers to developing computer systems that can perform tasks that typically require human intelligence These duties encompass natural language understanding, finding patterns, problem-solving solutions, and making decisions. Machine learning, frequently referred to as learning from expertise, represents one of these duties. AI aims to create machines or software that mimic cognitive functions such as reasoning, problem-solving, perception, and language understanding. Cyber security refers to the practice of protecting computer systems, networks, devices, and data from theft, damage, unauthorized access, and other cyber threats. The primary goal of cyber security is therefore to ensure the confidentiality, integrity, and availability of information in the digital realm [4].

The future sees a growing prominence of AI in cyber security, leveraging automation to enhance tasks, elevate threat detection, and efficiently responding to security incidents. Due to their flexibility, AI systems are crucial for improving cyber security measures [4]. Here are some ways AI is likely to be utilized in cyber security in the future:

Threat detection and prevention: It is of two types (a) behavioural analysis, and b) pattern recognition.

(a) Behavioural analysis: AI analyses user and system behaviour pinpoint anomalies that may signal potential security threats, and enhancing the ability to detect and respond to irregularities in a proactive manner.
(b) Pattern recognition: AI algorithms excel at discerning patterns within extensive datasets, facilitating the identification of both familiar and novel threats. This capability enhances the effectiveness of threat detection in diverse cyber security scenarios.

Endpoint security: It is of two types (a) AI-powered antivirus and (b) endpoint deduction and responses (EDR).

(a) AI-powered antivirus: By integrating AI, conventional antivirus software can be strengthened, enhancing its ability to identify and counter emerging malware threats with improved detection capabilities against new and evolving forms of malicious software.
(b) EDR: AI aids in real-time identification and response to suspicious activities occurring on endpoints, enhancing overall cyber security measures and threat mitigation.

Incident response: It is of two types (a) automated incident response and (b) threat intelligence analysis.
(a) Automated incident response: Leveraging AI allows for the automation of specific incident response elements, resulting in swift and efficient reactions to security incidents. This capability enhances the overall effectiveness of incident response protocols.
(b) Threat intelligence analysis: Leveraging its processing power, AI can analyse extensive threat intelligence data efficiently, delivering actionable insights. This level of capability enhances the method for generating tactical choices for effectively dealing with and minimizing risks associated with cyber security.

User authentication: It is of two types (a) behavioural biometrics and (b) multifactor authentication (MFA).
(a) Behavioural biometrics: Utilizing AI, user behaviour analysis – including typing patterns and mouse movements – strengthens authentication processes, enhancing security measures through advanced and personalized identification methods.
(b) MFA: Enhancing the security of MFA systems, AI proves valuable by dynamically adapting to emerging threats. Its adaptive nature contributes to the continual strengthening of MFA defences.

The security challenges in cyberspace encompass cyber-attacks, insufficient knowledge, awareness, and technical support, issues with confidentiality and trust meaning that the arrival of emerging technologies, advanced threats, presents a shortage of qualified specialists. Addressing these challenges necessitates the use of sophisticated algorithms and metaheuristic algorithms to optimize security, which are discussed further in Section 4.

The study by Jawaid [5] presents AI technologies, such as machine learning, which can enhance cyber security defences, provide more effective threat detection and response capabilities, and improve compliance and governance. The AI and machine learning aspects in cyber security allow systems to recover rapidly and efficiently after a cyber-attack, evaluate damage, and respond to incidents [6].

Adil et al. [7] specified that AI-enabled emerging edge computing technology can efficiently and securely utilize available resources in healthcare – (i.e., IoT applications), but future research should focus on unresolved security challenges. Thippeswamy et al. [8] presented an integrated framework using deep learning algorithms for network management and security concerns in 5G IoT networks, focusing on both optimizing network resources and detecting attacks.

Syed et al. [9] proposed an ML-based cyber security mechanism to optimize intrusion detection for IoT. The ML-based cyber security mechanism achieves 93.66% classification quality rate and 0.882 consistency rate for IoT intrusion detection.

The study by Elhoseny et al. [10] showed that AI risk management model effectively enhances cryptocurrency security by using social media indicators, achieving a mean accuracy of 77% for risk analysis, identification, and assessment.

The study by Tabassum et al. [11] indicated that improving the security performance and offering superior defence against a wide variety of sophisticated cyber threats can be done through AI-powered security [11]. Therefore, incorporating AI with cyber security in Smart Industry 4.0 applications can enhance the security posture of industrial environments and condense the risk of cyber-attacks and data breaches [12].

Therefore, the current and latest research reviews integrate the findings of implementing AI technology to enhance and optimize cyber security. We established from the recent research that AI enhances cyber security by improving support, and reducing cyber attacks.

Creating an intelligent cyber security system with AI necessitates the incorporation of advanced technologies and a multi-source transfer learning approach. This method involves integrating various data sources to fortify the protection of sensitive information, ensuring robust safeguards against evolving cyborg threats [13]. Here is a conceptual overview of the process:

- Understanding transfer learning:

  Transfer learning involves training a model for one task and leveraging its knowledge to enhance performance in related tasks, adapting pertained models for challenges in cyber security.
- Data gathering:

  Collect diverse datasets, encompassing electronic records. Train the model with this varied data to identify cyber security threats.
- Pre-processing and feature extraction:

  Refine data by removing noise, extraneous details, and extracting essential features. Use techniques such as data normalization, dimensionality reduction, and feature engineering for effective model training.
- Model selection:

  Selecting the right pre-trained model is vital; for cyber security, passive aggressive algorithm suit image threats, while recurrent neural networks fit sequence threats. Verify the model's efficiency with multi-source data.
- Multi-source transfer learning:

  Train the chosen model with diverse datasets from various sources, using domain adaptation techniques to align data distributions and ensure effective generalization to new environments.
- Fine-tuning:

  Refine the model for a cyber security task by incorporating specific data from the organization, enabling adaptation to its unique cyber security landscape.
- Continuous monitoring and updates:

  Establish a continuous monitoring system for the cyber security model, ensuring regular updates with new threat data and periodic retraining to adapt to evolving cyber threats.
- Compliance and ethical considerations:

  Prioritize privacy and data security by ensuring the developed system adheres to the organization's regulations and ethical guidelines throughout development and deployment.
- User training and support:

  Train organization and IT personnel in cyber security system usage. Implement a support system to address operational questions or issues promptly.

In the evolving landscape of cyber security, AI stands as a linchpin, particularly in the context of security. A forward-thinking strategy involves incorporating intelligent AI systems through multi-source transfer learning. This innovative approach enhances adaptability and robustness by integrating diverse data sources.

The integration of multi-source transfer learning represents a pivotal step forward. By leveraging pre-trained models from varied cyber security domains, this method addresses unique challenges posed by cyber security effectiveness. Hence, these intelligent systems, rooted in AI, exhibit a dynamic and responsive nature, by adapting to the intricate demands of safeguarding sensitive data [13].

Additionally, the implementation of Explainable AI (XAI) within cyber security protocols adds a layer of transparency and interpretability. Understanding the decisions made by AI models is essential, where clear insights into threat assessments can facilitate more informed responses from cyber security teams and practitioners.

In essence, the integration of intelligent AI, specifically tailored through multi-source transfer learning, marks a paradigm shift in cyber security. This comprehensive strategy, coupled with advancements like XAI and industry collaboration, is pivotal in creating a secure, adaptive, and interconnected ecosystem for the future.

In summary, the intersection of AI and multi-source transfer learning emerges as a revolutionary influence in cyber security [13] As infrastructures increasingly incorporate the IoT and interconnected technologies, the indispensable adaptive capabilities of intelligent AI systems provide comprehensive protection across various endpoints. These systems, with their proactive learning mechanisms and integration of XAI, not only offer a robust defence against evolving threats but also ensures transparency in the decision-making processes.

3 Methodology

In order to optimize cyber security using AI, a literature review was conducted using publicly available secondary data sources to explore, discuss, and analyse security and privacy challenges associated with evolving IoTs, AI evolution, and WMN. Based on the analysis, the authors identified and presented techniques and approaches that can be used to ensure robust security. The authors relied mainly on IEEE, Springer, Frontier, Google Scholar, and General Data Protection Regulations (GDPR) legal documents to gather information. Keyword searches were also used to find related work and reviewed them to develop the literature review and to answer the research questions set out in this study.

Data collection: A dataset is essential, with a variety of data collected and analysed in this study, we used an open publicly available dataset from GitHub – social media such as (Facebook, Twitter, Instagram). The analysis for the collected datasets used Colab Notebooks and Python packages.

The dataset link: https://github.com/JustAnotherArchivist/snscrape

4 Related work on security challenges

Cyber security in the organizations is a subject of persistent concern as they are subject to growing threats in a progressively digitalized world. Just as there is an attention rising on threats and risks associated with AI in the present, the early 2000s saw an emphasis on investigative concrete challenges related to ensuring the development of security and safety. These included potential social and ethical issues, health and environmental impacts, rule and governance, and a growing requirement for community and stakeholder association. A number of businesses are experiencing negative impacts from cyber threats as improvements are not guaranteed because improvement has been maintained but not enhanced. So, there is scope for improvement in this area. Sections 4.1–4.4 discuss the security challenges in evolving technologies.

Figure 1 demonstrates the cyber security breaches from 2007 to 2014. In 2007, breaches were minimal, contrasting sharply with the peak in 2013, exceeding 175 incidents. From 2007 to 2008, breaches ranged

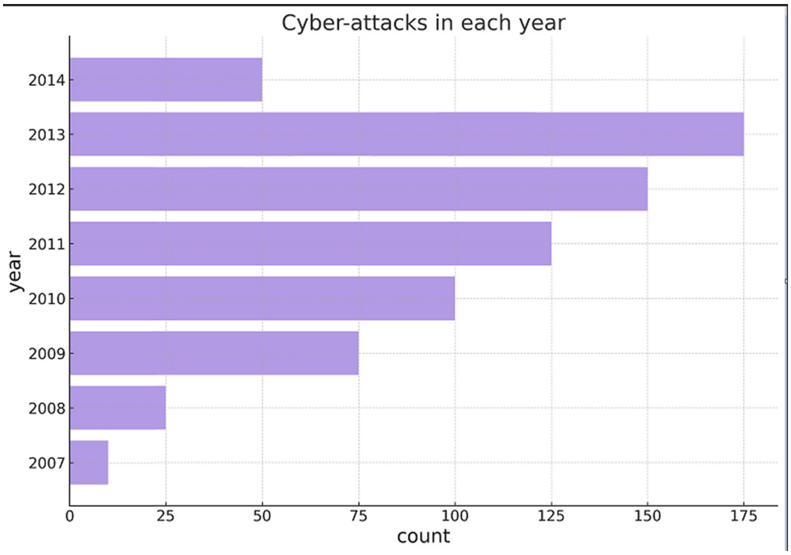

Figure 1: Cyber security breaches 2007–2014. Source: This figure has been created by the authors.

between 0 and 25, while 2014 and 2009 saw counts between 25 and 50. In 2010, breaches escalated to 125–150, and from 2011 to 2012, they fluctuated between 150 and 175. Notably, 2013 marked the zenith with over 175 breaches, gradually declining in 2014. This trend indicates a significant reduction compared to the preceding years, emphasizing a positive shift in cyber security measures over time.

Figure 2 illustrates a comprehensive analysis of breach types, encompassing hacking/IT incident, unauthorized access/disclosure, loss, theft, improper disposal, and other. Notably, improper disposal has the lowest count, ranging from 0 to 50, while theft exhibits the highest count, falling between 350 and 400. Hacking/IT incident, loss, and other fall within the 50–100 range, with loss extending to 100–150. The data underscore a significant prevalence of cyber security breaches in the form of theft, emphasizing the imperative for robust security measures in countering this particular threat.

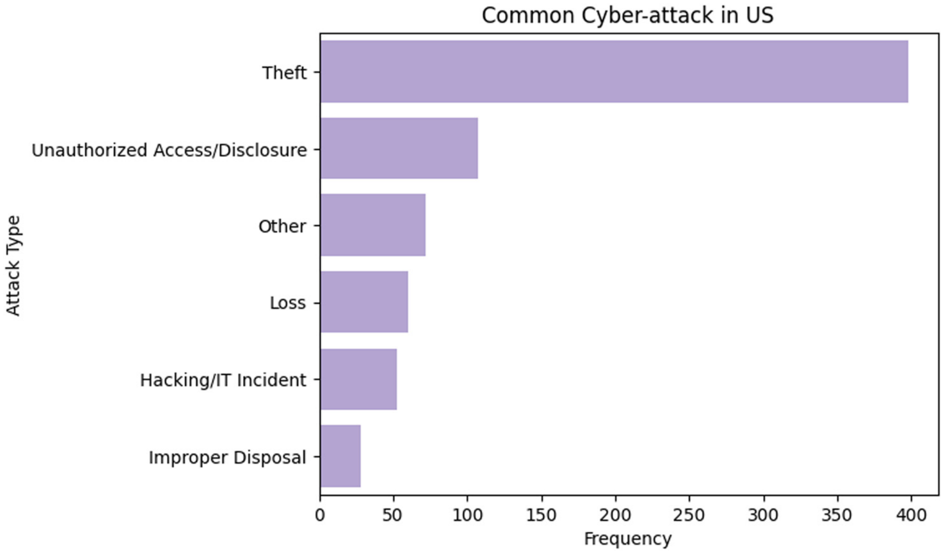

Figure 2: A comprehensive analysis of breach types. Source: This figure has been created by the authors.

4.1 Evolving security challenges of IoT

The IoT is an evolving area of technology that has rapidly grown in recent days [14]. In the context of IoT devices, it is important to mention that the storage capacity of these devices is very small, therefore it is difficult to install security applications and antivirus in IoT devices to secure them. Considering reducing the usage of IoT edge devices will be effective and beneficial in reducing and eliminating cyber threats but this is not possible with the modern technology of IoT development.

In the context of cognitive IoT, Wireless sensor network (WSN) is the most essential candidate that can be subject to the environment. The networks are dynamically adaptable to various network conditions and can make intelligent decisions. The WSN with cognitive nodes can assist and cooperate with each other in making intelligent decisions using previous experience, based on current knowledge, and the more knowledge placed, the better decision can be made. IoT is used in many different domains and demonstrates a rapid development in the IoT industry relating to both WSN to allow the communication between devices, and Radio Frequency Identification (RFID), which enables device labelling [2].

A WSN consists of nodes that have sensing, computation, monitoring, and wireless communication that are started as the main components of IoT. There are many protocols for routing, power management, and data distribution that have been developed precisely for WSN where energy awareness is an essential design consideration [15]. A sophisticated technique such as metaheuristic algorithms can be applied to optimize the security problem to implement a solution that enables network sensor nodes to act as an intelligent system [16].

There are some security concerns such as signal jamming, distributed denial of service, battery exhaustion attacks, wormhole attacks, black hole attacks, location disclosure attacks, spoofing of wireless infrastructure, traffic flooding attacks, etc. These security concerns would be considered to reduce cyber threats.

4.2 Security challenges in WMN

Designing a WMN is a fundamental issue in improving network efficiency and maximizing coverage and throughput capacity. In terms of technical innovation, a WMN is created through the installation and connection of a wireless mesh router at each network user's premises. Each mesh router not only acts as a stand access point to provide WIFI coverage to local devices but also acts as part of the network infrastructure, aggregating and forwarding traffic to other nodes towards an Internet Gateway. In this sense, each network user generates traffic, but also acts as a relay, forwarding data from other nearby nodes to the next node towards the gateway.

The routing operation of the data traffic in WMN architecture creates a vulnerable security system caused by the multi-hop traffic transmission and loose node-to-node data exchange during the inter-node authentication mechanism. The reliability and authentication of data traffic in WMN during neighbourhood node exchanges through link-state and in routing operations are wobbly and insecure. The WMN is a dynamic multi-hop network and these frequent changes in the topology require security authentication for notification updates.

Security attacks can occur in the routing layers, (client node update and notification message poisoning). In addition, there are communication security gaps in routing operation and packet transmission, thus the IEEE 802.11 s security is not yet fully standardized. The evidence to date indicates that the design of the solution holds the potential to achieve a significant result, particularly around the formulation of an optimal WMN infrastructure using metaheuristic algorithms that will provide a significant model to be used successfully for a secure network [17–19]. Other researchers [20] have also used an optimization approach and have successfully demonstrated a generated synthetic instance of WMN by changing several network parameters. In light of this research study, another way to achieve better secure network performance is to optimize the placement and characteristics of the access points before network deployment.

4.3 Security challenges of AI evolution

The evolution of AI has eliminated some human jobs and enhanced technologies in many aspects. Thus, higher attention from AI experts and researchers is to be given to integrating the impact of cybercriminal threats. Scientists and researchers have used computational tools and software to make suitable predictions related to genetic data. AI algorithms will compare the dataset and make predictions such as facial expressions predictions and human behaviour predictions.

The research by Nawaf et al. [17,18] aimed to provide a solution in the field of wireless networks by applying metaheuristic algorithm to detect foreign nodes by designing and implementing algorithms for improving the performance and efficiency of wireless networks by exploring different machine learning algorithms to determine the best placement of physical nodes within a network to prevent common security attacks. They also recommend a method for the ideal physical distance between each node in the grid area to help lower the risk of common threats while still maintaining a stable network signal and good connection for packet transmission. The main contribution of the research study by Nawaf et al. [17,18] is to minimize the risk of foreign nodes interfering with the network and optimize the best placement of physical nodes allocation within the network for better performance.

The ethical standards which are the principles to communicate its fundamental moral values can provide a framework that can be used as a reference for the decision-making process. Decision-making enables an agent to achieve its goal by determining what action to perform; hence, creating AI with ethical standards will support security in terms of responsibility, honesty, and transparency. This AI technique will allow the network to perceive user needs and provide data-based distributed intelligence in the network and help to eliminate cyber threats. AI and Ethical Standards will enable an approach to forming a secure network in the system.

4.4 Security and privacy challenges associated with the use of wireless technologies during COVID-19

Advances in wireless technology made a remarkable difference to the COVID-19 pandemic response. Innovative wireless technologies such as contact tracing applications, bracelets, drones, robots, digital thermometers, and other consumer wireless devices were used by the countries to maintain social distancing, detect individuals having COVID symptoms, isolate those diagnosed with symptoms, and conduct online consultations to return to a level of semblance of normality [21]. The integration of wireless technology fulfilled the government's aim to minimize and mitigate the risk of spreading the pandemic.

The bar graph in Figure 3 represents the true and false count of data breaches in the COVID-19 era. The *X*-axis shows the years whereas the *Y*-axis shows the count of breaches. Every year, true is higher than false. Most of the data breaches were in the year 2020, followed by 2019 and 2021. Least number of data breaches occurred in the year 2021.

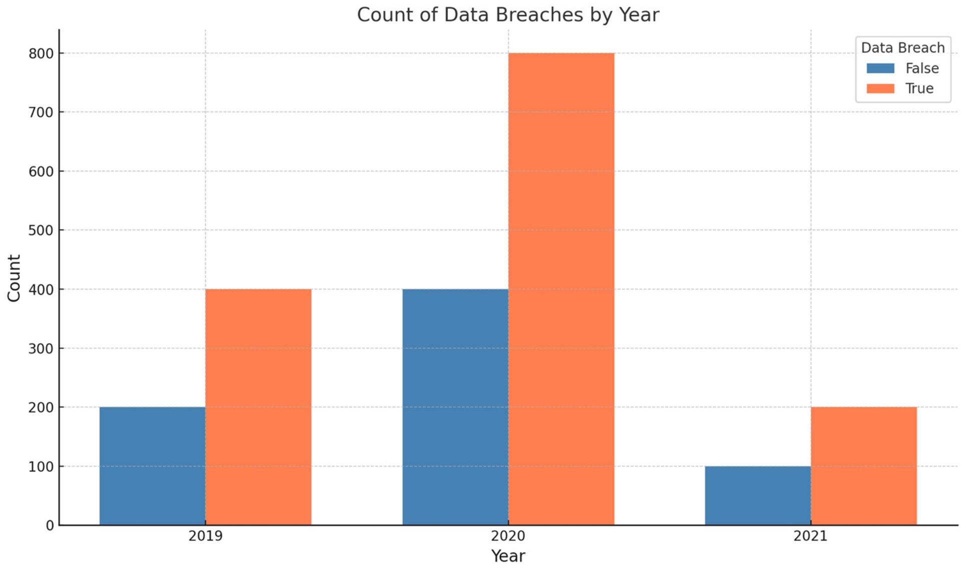

Figure 3: Data breaches in the COVID-19 era. Source: This figure has been created by the authors.

Figure 4 represents the cyber breach count in the COVID-19 period. The highest number of breaches was experienced in the year 2020 with the count near 1,200. The 2019 year has above 600 cyber breaches. Cyber breaches have gradually decreased by the year 2021 with the count close to 400. Surprisingly there had been an obvious drop in cyber breach in 2021. The upward change indicates a dynamic environment in cyber security throughout the research.

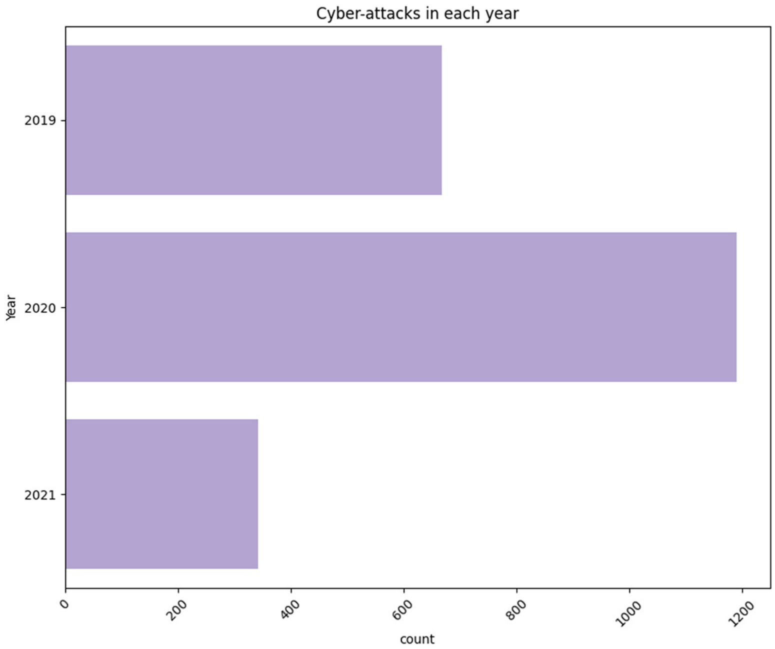

Figure 4: Cyber breach count in COVID-19 era. Source: This figure has been created by the authors.

The application of wireless technologies depends on the resource capacity of the countries. The healthcare sector benefited from the robots that assisted medical doctors and nurses in minimizing the need for hospital room visits, safeguarding healthcare personnel [22], and disinfecting hospital wards and other facilities [23]. Also, in some instances, drones and robots have enabled countries to deliver essential medical supplies to remote areas to lessen the impact of human-to-human contact and protect the medical staff [22]. A different approach used by Kinas Health in the US was to distribute smart thermometers to remotely collect temperature and geospatial information from individual households to predict the spread of the virus [22].

The governments had also used wireless technologies such as cellular positioning systems and Global Positioning Systems (GPS) to monitor the transmission of the virus, and to track the spread of the pandemic, in some cases, using mobile Apps to observe adherence to lockdown measures [24]. For example, the South Korean government placed all foreign passengers in self-quarantine as a precautionary measure. They were compelled to use a self-diagnosis app and provide regular updates on their health condition during the quarantine period so that the government could track and trace any symptomatic individuals, and those who may have come in direct contact with the travellers were also subjected to self-quarantine under surveillance procedures [25]. The reports suggested that the data acquired for these measures had been arbitrarily shared with multiple entities, such as the police department and health insurance companies, central government agencies, health care professionals, health care associations, and others in violation of data privacy regulations [25].

The normal life of the countries was severely affected by the pandemic causing immense disruptions to the sustainability of normal services provided by the state institutions, academia, business, and auxiliary services, and to overcome these effects, steps were taken to maintain a level of normalcy. The use of novel ideas such as video conferencing technologies like Zoom, Skype, and others became the norm and reliance on them became customary amongst the general population during the lockdown and movement restrictions. In addition, technologies such as Bluetooth, Ultra-wideband (UWB), Global navigation satellite systems (GNSS), and thermal sensors also became widely used in various countries [25]. These ideas for instance allowed for the tracking and movement of infected individuals. Also, to augment these efforts during the pandemic, drones were used to enforce the regulations on social distancing with the capacity to monitor temperature, sneezing, and coughing in public places. In the retail and supply chain industries, GPS and RFID technologies were also used to track and regulate the timely delivery of goods to prevent panic buying and disruptions [23]. Table 1 demonstrates the use of wireless technologies in the industry.

Table 1: Wireless technologies used in different industries

Industry	Wireless technologies
Hospital	Robots, drones, smart thermometers, zoom, skype
Healthcare	Contact tracing, cellular positioning system, GPS, Bluetooth, UWB, GNSS, thermal sensors, pandemic drones
Education	Zoom, skype
Retail	GPS and RFID technology

Wireless technologies were one of the common approaches implemented in the countries to control the spread of the virus and to strengthen public safety, and these technologies generated a mass amount of personal data. The Cable News Network report suggested that the Health Code app users were asked about their symptoms, travel history, the possibility of exposure to COVID-19-positive individuals, their workplaces, private addresses, mobile phone numbers, passport information, and the national identity number [25]. Contact tracing apps, on the other hand, also collected data such as names, contact numbers, locations, and the movement of the people, and the hospitals also collected a mass amount of data on the patients ranging from their names to their medical history [21]. The app developers provided justification for the necessity to collect personal information about the users, emphasizing the importance of collecting sufficient information to deliver accurate results [25]. The downside to that is a higher quantity of information leads to potential violations of privacy, which has become a serious concern to society. Therefore, it is vitally important to understand the type of data collected through wireless technologies for the purpose of recognizing the privacy risks associated with them.

During the pandemic, wireless technologies were used widely, and that added to privacy concerns. It is of paramount importance that companies/governments should not unnecessarily and excessively use the available technologies to track and monitor the movements and behaviour of the citizens. It is a key requirement of the GDPR to collect data with consent, use and retain those data for the collection purpose, and to destroy the data when no longer necessary for the purpose intended [26].

Wireless technologies have facilitated governments to respond to the pandemic effectively. However, a large amount of data collected have put personal privacy at risk. To give an example, contact tracing technologies had been helpful in restraining the spread of the virus, but at the same time, this technology has intruded on people's privacy during tracking their movements and tracing their contacts. In addition, drones were used to monitor social distancing or track debilitated people located in public places, but they had raised privacy concerns about infringement on individuals' rights to privacy and freedom of movement. The state institutions could collect and retain user location information for an unspecified period for surveillance purposes in the national interest. Additionally, people's willingness to use wireless technologies should not be taken for granted and disregard the need to respect their personal privacy.

The generating and processing of a massive volume of data using wireless technologies could also be seen as contravening the data minimization principle of the GDPR. The data minimization principle clearly states that only a limited amount of data should be collected with consent, and it should be for a pre-defined purpose [27]. It is also a condition in the GDPR that data should not be kept for longer than necessary [27], and the failure to comply may lead to security threats such as data breaches. However, most wireless technologies fail to provide clear indications as to how they process data and the retention period.

The GDPR also makes it a requirement that the data subject should be provided with information about the processing of the collected data [28]. However, given the number of devices in use and the amount of data processed, the likelihood of failures to inform the subject could not be ruled out. The volume of data could also affect data rectification. Furthermore, an excessive amount of data processing without human intervention could also give rise to privacy concerns.

Human rights activists have warned that the use of wireless technologies during the pandemic has the potential to become standard surveillance protocols in the future [22]. Therefore, in the design stage (before the implementation of these applications), it is incumbent on the governments and the companies to carefully consider what information is collected, how the data would be processed, how data would be stored, the data retention period, how to invoke the right to erasure, who would have access to these data, and whom they would share the data with. In addition, explicit consent is deemed necessary to minimize wireless devices (such as smartwatches and apps) collecting and processing personal data, advertently or inadvertently.

From the literature review, we observe that the security challenges are obvious and indicate a high number of cyber threats and at the same time high demand for security solutions.

5 Analysis of security challenges

AI's impact on cyber security has been thoroughly analysed. This assessment involves the integration of AI into cyber security measures and its contribution to improving cyber security. These findings shed light on AI's pivotal role in fortifying both sectors against evolving threats and vulnerabilities.

The violin graph in Figure 5 illustrates the types of breaches throughout the years from 2006 to 2014. The *X*-axis represents the year, and the *Y*-axis represents the types of breach such as theft, unauthorized access/disclosure, loss, etc. Theft has the lowest probability between 2006 and 2008, and the highest probability between 2010 and 2014, and decreased again after 2014. Unauthorized access/disclosure has the highest probability between 2012 and 2014 and the lowest probability between 2006 and 2008. It has decreased after 2014. Loss has the highest probability in the year 2010 and between 2012 and 2014. Loss has the lowest probability in the year 2008. Hacking/IT incident has the lowest probability from 2006 but has the highest probability between 2010 and 2014. Improper disposal has the highest probability in the years between 2010 and 2014 and has the lowest probability in 2008. Others have the highest probability in 2010 followed by 2012–2014 years. The median for theft is between 2010 and 2012, and for unauthorized access/disclosure, loss, hacking/IT incident, improper disposal, and other is in the year 2012.

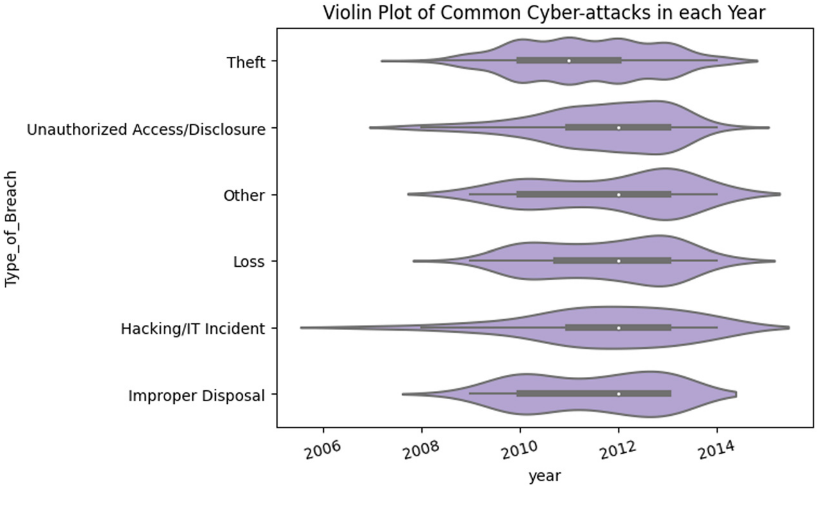

Figure 5: Types of breaches throughout 2006–2014. Source: This figure has been created by the authors.

These data underscores the varying degrees of cyber-attacks challenges faced by different types of breaches in each year.

Figure 6 represents the uncertainty of breaches that occurred during the period 2007–2013. In the bar graph, it is certain that in 2007 and 2008, there were less breaches. Eventually, there is a growth in breach from the year 2009. Theft is a most uncertain breach that has attacked the individual in the years 2009 and 2013. When compared to the years 2010 and 2011, the highest-ranked breach is the loss and the lowest is the hacking/IT incident. The loss having most uncertain attack on the individual was in the year 2011. Overall, attributes of theft and loss played a major role in causing trouble to each individual. Whereas all the other attributes have made less impact. Hence, the theft attribute plays a crucial role in determining the years in the data frame. This score of breaches indicates that the evolving of technologies over these years has impacted the cyber security significantly.

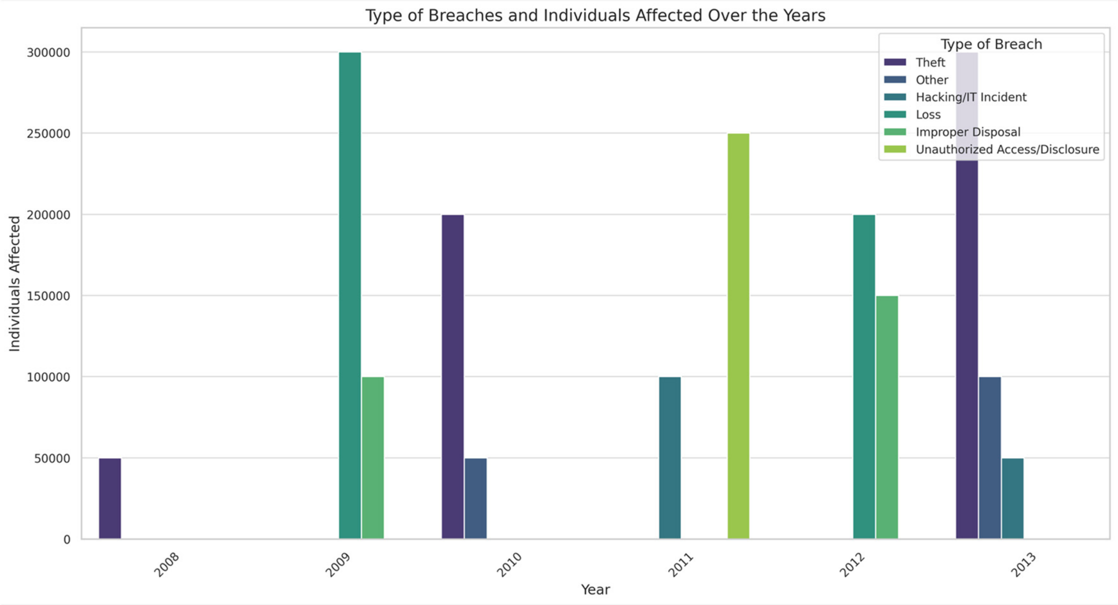

Figure 6: Breaches that occurred during the period 2007–2013. Source: This figure has been created by the authors.

In Figure 7, the highest individual affect was recorded in the year 2013 and the lowest was recorded in the year 2007. Over the years, the number of individuals affected by cyber-attacks has also increased. There was an extreme increase in cyber-attacks comparing the years 2007 and 2013. There was a strong decent in cyber-attacks after 2013.

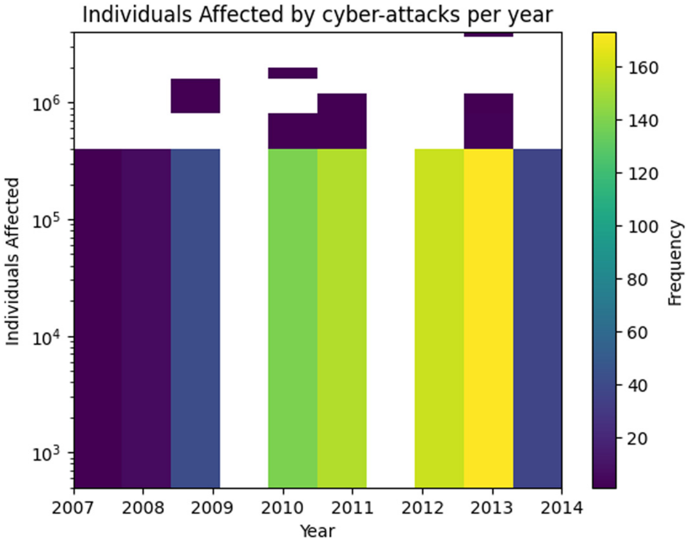

Figure 7: Individuals affected by cyberattack. Source: This figure has been created by the authors.

The correlation heatmap showing the percentage of cyber-attacks per year is shown in Figure 8. The heat map represents the types of breaches from the year 2007 to 2014. The *X*-axis represents the years, and the *Y*-axis represents the types of breaches. The light-yellow colour represents the highest value, and the brown colour represents the lowest value. As stated in the scatter plot, theft had a major impact in the years 2010–2012. All the other breaches show comparatively less impact, which can be determined by the percentage values in the heatmap. In the year 2007, the only attack was the hacking/IT incident. The hacking/IT incident has the lowest value in the years 2007 and 2008 and the highest value in the year 2011. The inadequate disposal has the lowest value in the year 2009 and the highest value in the years 2010 and 2013. The loss has the lowest value in the year 2009 and the highest value in the year 2013. The other type has the lowest value in the year 2009 and the highest value in the year 2013. Theft has the lowest value in the year 2008 and the highest value in the year 2011. The unauthorized access/disclosure has the lowest value in the year 2008 and the highest value in the year 2013.

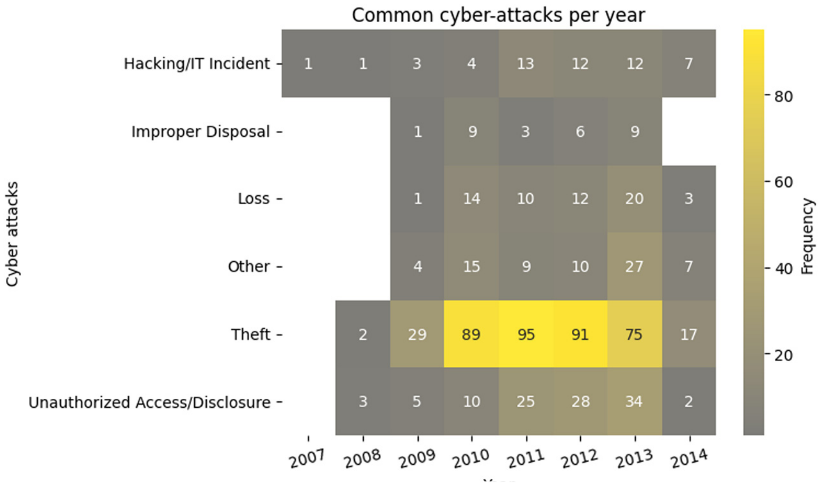

Figure 8: The correlation heatmap of cyberattacks. Source: This figure has been created by the authors.

The cyberattacks during Covid-19 period illustrated in Figure 9 represents the count of breach occurrences by country. The cyberattack investigation involves the following countries: the USA, UK, India, and Canada. The highest occurrence of breaches is in the USA, followed by UK, India, and Canada. USA is the highest with a count of above 800 and the rest of other countries have counts with less than 200 as shown in Figure 9.

The bar plot in Figure 10 represents the data breaches throughout COVID-19 for nine different countries. The countries compared in the bar plot are the USA, UK, Singapore, Russia, Japan, India, China, Canada, and Australia. The country with the highest data breaches is the USA throughout the COVID-19 era. The UK was the second highest country in 2020 followed by 2019 and 2021 subsequently. The lowest data breach of the countries in 2019 and 2021 was Japan, while Russia and Singapore in year 2020.

6 Cyber security and AI

The implementation of AI in the cyber security discipline has significantly improved threat detection, fraud prevention, and identification of phishing attempts. This advancement has the potential to enhance the accuracy and speed of identifying and responding to threats in a business environment [29]. Given the increasing complexity and diversity of cyber threats, AI can effectively pinpoint vulnerabilities and analyse the behaviour of malicious actors. In addition, AI has the ability to efficiently analyse substantial data volumes in real-time, identifying patterns, anomalies, and potential threats that may not be recognized by human

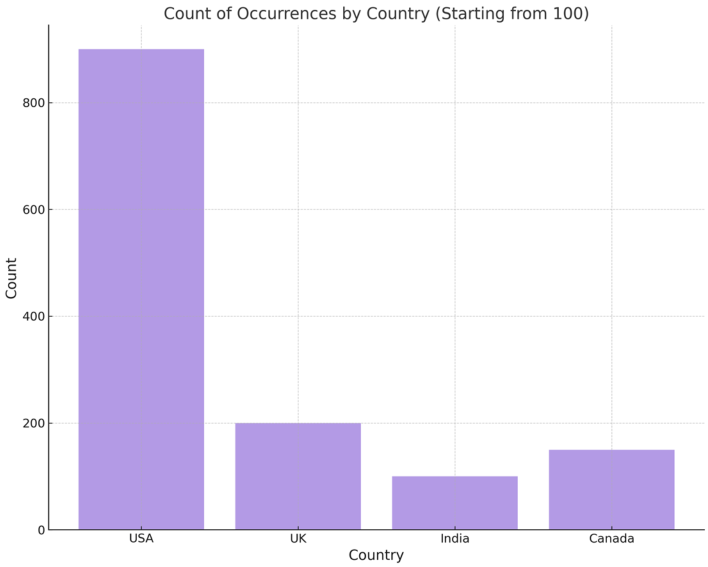

Figure 9: Cyber-attacks during Covid-19 period in UK, USA, India, and Canada. Source: This figure has been created by the authors.

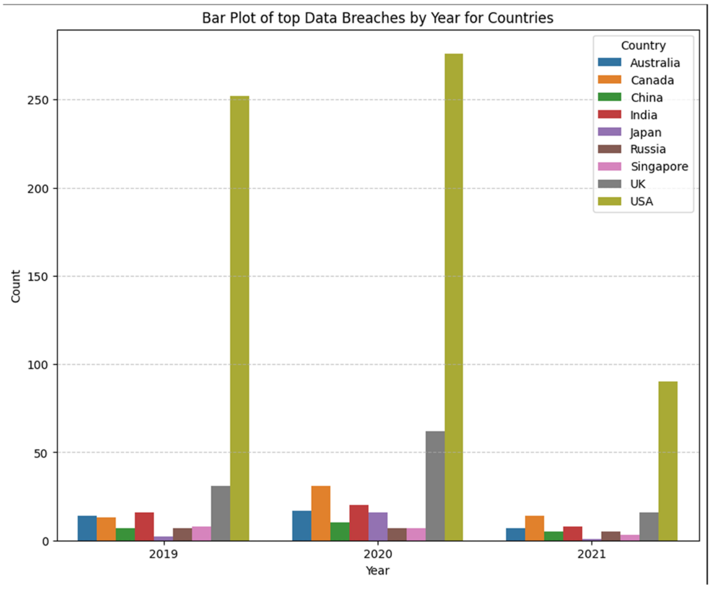

Figure 10: Data breaches during COVID-19 for nine countries. Source: This figure has been created by the authors.

analysts [30]. Furthermore, AI technology can alert users to imminent attacks and vulnerabilities that could be overlooked by human personnel. This has shown to be quite effective in bolstering defense measures against cyber threats. By continuously monitoring operations and detecting deviations, AI can flag any suspicious activities for further investigations, and this can assist law enforcement agencies in identifying the perpetrators and holding them accountable through legal means.

In addition, trough the analysis of historical data and patterns from past cyber security incidents, AI can forecast future attack vectors and vulnerabilities [31]. This proactive approach enables organizations to enhance their security measures proactively, mitigating risks before they escalate to critical levels. In addition, AI enabled predictive analysis can evaluate risk levels for various assets and activities within an organization

[32], assisting in prioritizing security efforts by pinpointing vulnerable area, and it also allows organizations to address vulnerabilities before they are exploited, helping in strategic planning and resource allocation to ensure robust defenses are in place to address the possible upcoming threats. AI technologies can also help enhance the efficiency of incident response teams. Automated response systems that utilize AI can swiftly address threats in real-time, reducing the window for attackers to exploit vulnerabilities. These technologies are capable of identifying the threats and isolating the infected endpoints, block malicious traffic, and initiate remediation procedures automatically [33]. These prompt responses are essential for reducing risks and threats and decreasing operational disruptions for the organizations.

As organizations navigate through this complex environment, the strategic integration of AI in cyber security will be essential for establishing robust and resilient defense mechanisms to protect organizations from potential cyber threats in the digital era. While the incorporation of AI in the cyber security field offers numerous opportunities, it also brings challenges such as over-reliance on data automation, biases, ethical issues, and necessitates immediate attention to address potential consequences. Therefore, it is crucial to regularly monitor and update AI models to maintain the accuracy of AI systems in detecting and addressing emerging threats. Moreover, the integration of AI technology with human expertise can serve as a pivotal factor in effectively addressing the existing and upcoming challenges. Furthermore, while AI is used for analysing data and recognizing patterns, cyber security experts can also play a crucial role in reviewing the documents generated by AI technologies to ensure accuracy and impartiality. In addition, in order to maximize the benefits of use of AI in the field of cyber security and effectively address current and future cyber-related challenges, a comprehensive regulatory framework is necessary.

Table 2 outlines the fundamental ways AI can be utilized in cyber security and the benefits it provides in improving security measures. Table 2 demonstrate and summarize the AI technologies links with cyber security.

Table 2: AI technologies links with cyber security

AI application	Utilization description	Benefits to cyber security
Threat detection and prevention	Conducting detailed analysis of large datasets to detect potential security risks	Enhanced capabilities to identify and mitigate cyber security threats
Fraud detection and prevention	Recognizing and analysing irregularities in transactions	Improving the efficiency of identifying fraudulent activities
Incident response	Implementing automated responses to specific types of cyber security attacks	Improved efficiency in incident containment
Vulnerability management	Determining the severity of vulnerabilities based on their potential impact	Allocating resources for most critical issues
Predictive analysis	Predicting potential security breaches by analysing past incidents	Enhancing defensive security
Phishing detection and prevention	Reviewing emails to detect and prevent phishing attacks	Safeguarding users against social engineering attacks
Behavioural analysis	Analysing behaviour patterns of threat actors	Identifying external and/or insider threats

7 Algorithms, techniques, and approaches used to optimize security

The previous sections explore the incidents of threats and cyber-attacks associated with different technologies to present consolidated sophisticated technical and legal solutions to protect and mitigate the risks.

- This section presents that algorithms, techniques, and approaches used to optimize security include machine learning and evolutionary swarm intelligence, genetic algorithms, combinatorial optimization techniques, and hybrid metaheuristic algorithms.

- Optimization algorithms with machine learning and evolutionary swarm intelligence based techniques are used to minimize threats and ensure data security in IoT networks [34]. Optimization algorithms like particle swarm optimization, ant colony optimizations, artificial bee colony, genetic algorithm, and AdaBoost algorithm are able to enhance cyber security in IoT [35].
- Optimizing adversarial behaviour of agents using deep reinforcement learning (DRL) and evolutionary strategies (ES) can efficiently improve cyber security by choosing complex exploits that defeating defences in cyber security simulations when both attackers and protector are trained [36]. Oh et al. [37] present from their experiments on synthetic network security that the DRL framework surpass existing methods in learning optimal attack actions, enhancing cyber security against adversarial simulation. Thus, a complex, dynamic, and high-dimensional cyber defence problems can be resolved by DRL algorithms through integrating deep learning into traditional reinforcement learning [38]. Mathematical model and optimization algorithms are used to optimize losses that organization may suffer from risk and costs necessary to prevent them. The recent research demonstrates that AI algorithms, and integrated optimization and classification methods are used to optimize security.

Implementation of different processes and techniques is essential in AI (machine learning) algorithms to improve the efficiency of these algorithms. Passive aggressive algorithm works by responding as passive for correct classifications and responding as aggressive for any miscalculation in the prediction. Online Passive-Aggressive Algorithm (PA) represents a major breakthrough in online learning algorithms, controlling classification and regression tasks Working as the virtual equivalent of support vector machine classification compared to other methods such as online perceptron and margin-infused relaxed algorithm approach has shown excellent performance [39].

At its core, the PA classifier works by actively searching for hyperplanes that correctly classify instances in real-time, adapting to a simple streaming input. This dynamic learning process enables the algorithm to continuously refine its understanding of evolving data streams, making it a strong choice for various online education environments The effectiveness of the PA algorithm depends on its ability to accommodate flows of information and the speed of light. PA, an online classifier, works by training a model to accurately recognize current communication activity. Using a stored and labelled knowledge register, this algorithm learns the pattern. Subsequently, exposing this model to online testing enhances its learning capabilities and adaptability to the dynamic web environment [39].

In online binary classification, algorithms work in successive rounds. In each round, the algorithm encounters an instance and issues a prediction, labelling it as +1 or −1. The true score is then displayed, revealing the accuracy of the algorithm's prediction through an immediate loss analysis. Post-prediction, the algorithm uses the two newly discovered instance labels to improve its prediction model for subsequent rounds [40]. However, unclassy prediction is particularly notable for classification and regression methods. Here the predictions are made without prior involvement in external factors such as Xt. Instead, the algorithm holds a vector (Wt $\in R^n$) in its memory and predicts that the next element in the sequence is Wt. This prediction is extended, resulting in a temporary loss when the next item in the sequence is displayed [40].

Nawaf et al. [17] indicates that the aggressive move operators of increasing or decreasing the bandwidth allocation in the WMN placement have demonstrated a significant effect. There is a substantial amount of research work [41–43] on network optimization and infrastructure placement that has established significant results by implementing aggressive algorithms. Implementation of sophisticated hybrid AI algorithms will help connect the nodes securely.

Many of the data processing activities come under the GDPR, given the large amount of personal data collected and processed. Consequently, one of the GDPR principles, privacy by design, should be considered in the design stage and throughout the life cycle of device/technology development. Impact Assessment also should be undertaken before making devices available to the consumer, with documented evidence as a requirement of the GDPR.

In summary these studies suggest that optimization algorithms are effective in enhancing cyber security by improving attack simulations, decision-making, sensor placement, classification accuracy, and network monitoring. The goal of the research is to create and apply cyber-attack detection algorithms to safeguard digital assets and infrastructure from emerging cyber threats by combining deep learning and detailed hardware inspection. Effective and efficient risk mitigation has long been a goal in the field of information security networks. Potential avenues for further exploration and improvement in the field of deep learning algorithms for cyber-attacks detection could be explored additionally in future study. These potential avenues offer fascinating opportunities to strengthen cyber-attacks detection systems and cyber security.

8 Conclusion

The evolution of technologies has provoked new challenges in securing cyberspace. Scientists are in search of information and guidance on cyber security, identifying cyber security risks, and managing these risks through significant AI approaches, and technical and legal regulations.

This study explores the requirement of applying security techniques to reduce cyber threats by implementing AI and ethical standards. The implementation of metaheuristic algorithms in WMN infrastructure will ensure the security of the networks. The key area of implementing the solution is to understand the network environment and how to design algorithms to enhance network access and provide improved secure communications. Thus, for an extremely effective way of finding the solution, metaheuristic algorithms may be considered for resolving IoT security issues. In addition, GDPR principles of privacy by design and privacy by default can be integrated into the devices/technologies to assure the personal privacy of the data subject.

This research study outlines the essential applications of AI in cyber security and the advantages it offers in enhancing security measures. It also summarizes the connection between AI technologies and cyber security.

For threat perception, the recent research reviews of algorithms and techniques consolidate findings on the implementation of AI technology to enhance and optimize cyber security. The latest studies demonstrate that AI improves cyber security by enhancing support and reducing cyber-attacks.

This study contributes to optimize cyber security through employing AI methodologies, and detecting the AI application benefits to cyber security. The novelty lies in combining network design, algorithm design, and human-computer interaction design to solve this real-world network security problem with the evolution of cyber threats effectively.

9 Recommendations

The advancement of and the extensive use of wireless technologies opens exciting new opportunities to communities worldwide. Therefore, it is necessary to investigate further the role of the digital technologies that would lead to future resilience and sustainability of smart communities, as set out in the UN Sustainable Development Goal 11 (Make cities and human settlements inclusive, safe, resilient, and sustainable).

WSNs are a foundational technology gaining importance within the IoT. This market was valued at $46.76 billion in 2020 and is expected to reach $126.93 billion by 2026, growing at a compound annual growth rate of 17.64% from 2021 to 2026. Consequentially, the utilization of WSNs is steadily increasing. Researchers [39,40] find applications across different domains such as monitoring systems, transportation tracking, health monitoring, home automation, security and surveillance, object tracking, and agricultural methods.

WSNs are classified into five groups based on the deployment of sensor nodes: terrestrial, underground, multimedia, underwater, and mobile. Their versatility makes WSNs crucial across numerous industries, furthering their expanding role in the IoT landscape [39]. The IoT refers to connected devices embedded with sensors, software, and other technologies that enable the collection and exchange of data These devices can range from everyday objects such as home appliances. And, from wearables and automobiles to industrial devices and accessories. In recent years, the IoT has received a lot of attention, representing a complex network of software and hardware that connects the physical realm with the digital world [43]. The rise in popularity of this model has spurred significant improvements in the complex number of IoT devices.

By 2025, it is estimated that more than 75 billion such devices will be seamlessly connected to the Internet, significantly impacting the global market. IoT devices, characterized by their powerful computing power and compact memory, have the ability to generate large amounts of data. This flood of data presents opportunities and challenges, drives economic impact, and shapes industries around the world [43]. AI is transforming the future landscape. AI-driven IoT capabilities in vehicles enable self-sustaining features like parking, braking, lane shifting, and reconstructing driving experiences [44].

In the domain of big data, healthcare has great benefits from AI, aiding doctors to match human intelligence. With AI advancements, health care ensures specific treatments and diagnoses, improving the overall quality of life. Within computer systems emulating human judgment, AI learns, reasons, and gains insights from experiences. The AI field encompasses machine learning and deep learning, unleashing system evolution. Primary AI learning styles include supervised, unsupervised, and reinforcement learning methods [44]. Edge AI involves deploying AI on local devices and performing computations near users instead of relying on centralized cloud data centres. This approach, situated at the network's edge, takes advantage of AI's efficiency gains, the surge in IoT devices, and the growth of edge computing [45]. This convergence has unlocked the potential of edge AI. Now, robots and devices possess human-like cognition regardless of their location. AI-driven IoT applications adapt to new scenarios and perform tasks effectively.

The exponential increase in IoT-connected devices drives unplanned data growth. The mobile edges computing transitioned to multiaccess edge computing and acknowledged IoT's prominence to harmonize edge computing systems in diverse wireless networks. This evolution, driven by AI advances, IoT expansion, and the ascension of edge computing, has fully unleashed the potential of edge AI [45]. To that end, AI Algorithms could be embedded in the IoT/wireless devices by default to protect personal privacy. The key area of implementing the solution is to understand the network environment and how to design algorithms to enhance network access and provide improved secure communications.

Acknowledgement: This work is supported by the Cybersecurity, Information Networks Centre (CINC), Cardiff School of Technologies; Cardiff Metropolitan University.

Funding information: Authors state no funding involved.

Author contributions: Study Conception: LN; Design: LN and VB; Data Collection: LN; Analysis: LN and VB; Interpretation of Results: LN and VB.

Conflict of interest: The authors declare that there is no conflict of interest. Both authors have contributed toward writing this article. This journal article is funded by the School of Technologies, Cardiff Metropolitan University. The authors give their consent to the journal owner to make the data public.

Data availability statement: The dataset available via the following link: https://github.com/JustAnotherArchivist/snscrape.

References

[1] NCSC, 2022. "NCSC Annual Review 2022." [Accessed: 12 June 2023]. [Online]. Available at: https://www.ncsc.gov.uk/collection/annual-review-2022.

[2] Yousif M, Hewage C, Nawaf L. IoT technologies during and beyond COVID-19, a comprehensive review. Future Internet. 2021;105:13. doi: 10.3390/fi13050105.

[3] Government of UK. Government of UK, Department for digital, culture, media and sport. Cyber security breaches survey 2020; 2020. [Accessed 1 June 2020]. [Online]. www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020.

[4] Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Inf Fusion. 2023;97:101804. doi: 10.1016/j.inffus.2023.101804.

[5] Jawaid SA. Artificial intelligence with respect to cyber security. J Adv Artif Intell. 2023;1(2):96–102. doi: 10.18178/jaai.2023.1.2.96-102.

[6] Bago P. Cyber security and artificial intelligence. Economy Finance. 2023;10(2):189–212. doi: 10.33908/ef.2023.2.5.

[7] Adil M, Khan MK, Farouk A, Jan MA, Anwar A, Jin Z. AI-driven EEC for healthcare IoT: Security challenges and future research directions. IEEE Consum Electron Mag. 2022;13(1):39–47. doi: 10.1109/MCE.2022.3226585.

[8] Thippeswamy SNP, Raghavan AP, Rajgopal M, Sujith A. Efficient network management and security in 5G enabled internet of things using deep learning algorithms. Int J Electr Comput Eng (IJECE). 2024;14(1). doi: 10.11591/ijece.v14i1.pp1058-1070.

[9] Seyed C, Kebe M, El Arby MEM, Mahmoud EBM, Mahmoud Seyidi CM. Cybersecurity mechanism for automatic detection of IoT intrusions using machine learning. J Comput Sci. 2024;20(1):44–51. doi: 10.3844/jcssp.2024.44.51.

[10] Elhoseny M, Darwiesh A, El-Baz AH, Rodrigues JJ. Enhancing cryptocurrency security using AI risk management model. IEEE Consum Electron Mag. 2023;13(1):48–53. doi: 10.1109/MCE.2023.3238848.

[11] Tabassum I, Bazai SU, Zaland Z, Marjan S, Khan MZ, Ghafoor MI. Cyber security's silver bullet-a systematic literature review of AI-powered security. In 2022 3rd International Informatics and Software Engineering Conference (IISEC). IEEE; 2022, Dec. p. 1–7. doi: 10.1109/IISEC56263.2022.9998305.

[12] Goyal SB, Rajawat AS, Solanki RK, Zaaba MAM, Long ZA. Integrating AI with cyber security for smart industry 4.0 application. 2023 International Conference on Inventive Computation Technologies (ICICT). IEEE; 2023, April. p. 1223–32. doi: 10.1109/ICICT57646.2023.10134374.

[13] Chakraborty C, Nagarajan SM, Devarajan GG, Ramana TV, Mohanty R. Intelligent AI-based healthcare cyber security system using multi-source transfer learning method. ACM Transactions on Sensor Networks; 2023.

[14] Menter Z, Tee WZ, Dave R. Application of machine learning-based pattern recognition in IoT devices. Proceedings of International Conference on Communication and Computational Technologies: ICCCT 2021. Singapore: Springer; 2021. p. 669–89.

[15] Indu S. Wireless sensor networks: Issues & challenges. Int J Comput Sci Mobile Comput (IJCSMC). 2014;3:681–85. doi: 10.47760/ijcsmc.2021.v10i09.003.

[16] Osamy W, Khedr AM, Salim A, AlAli AI, El-Sawy AA. Recent studies utilizing artificial intelligence techniques for solving data collection, aggregation and dissemination challenges in wireless sensor networks: A review. Electronics. 2022;11(3):313. doi: 10.3390/electronics11030313.

[17] Nawaf LF, Allen SM, Rana O. Optimizing infrastructure placement in wireless mesh networks using NSGA-II. *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City*; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE; 2018. p. 1669–76.

[18] Nawaf L. Optimizing IoT security by implementing Artificial Intelligence – Infosecurity Magazine; June 2022, [Online]. https://www.infosecurity-magazine.com/next-gen-infosec/optimizing-iot-ai/. [Accessed 15 June 2022].

[19] Nawaf L, Allen SM, Rana O. Internet transit access point placement and bandwidth allocation in wireless mesh networks. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC). IEEE; 2017. p. 1–8.

[20] Amaldi E, Capone A, Cesana M, Filippini I, Malucelli F. Optimization models and methods for planning wireless mesh networks. Comput Networks. 2008;52(11):2159–71. doi: 10.1016/j.comnet.2008.02.020.

[21] Bentotahewa V, Hewage C, Williams J. Solutions to Big Data privacy and security challenges associated with COVID-19 surveillance systems. Front Big Data. 2021;4:645204. doi: 10.3389/fdata.2021.645204.

[22] Saeed N, Bader A, Al-Naffouri TY, Alouini M-S. When wireless communication responds to COVID-19: combating the pandemic and saving the economy. Front J. 2020;1:566853. doi: 10.3389/frcmn.2020.566853.

[23] Ahmadi H. Wireless Communication and the Pandemic: The Story So Far. IEEE Communications Society; 2020. https://www.comsoc.org/publications/ctn/wireless-communication-and-pandemic-story-so-far [Online]. [Accessed 21 June 2022].

[24] Nguyen CT, Saputra YM, Van Huynh N, Nguyen NT, Khoa TV, Tuan BM, et al. A comprehensive survey of enabling and emerging technologies for social distancing – part I, fundamentals and enabling technologies. IEEE Access. 2020;8:153479–507. doi: 10.1109/ACCESS.2020.3018140.

[25] Murad SS, Yussof S, Badeel R. Wireless technologies for social distancing in the time of COVID-19: literature review, open issues, and limitations. Sensors. 2022;22(6):2313. doi: 10.3390/s22062313.

[26] Intersoft consulting, "GDPR Chapter 2 Principles." Accessed 27 June 2022. [Online]. Available at: https://gdpr-info.eu/chapter-2/.

[27] Intersoft consulting, "Art. 5 GDPR Principles relating to processing of personal data." Accessed 27 June 2022. [Online]. Available at: https://gdpr-info.eu/art-5-gdpr/#:~:text=5%20GDPR%20Principles%20relating%20to,lawfulness%2C%20fairness%20and%20transparency%27)%3B.

[28] Intersoft consulting, "Art. 7 GDPR Conditions for consent." Accessed 27 June 2022. [Online]. Available at: https://gdpr-info.eu/art-7-gdpr/.

[29] Jada I, Mayayise TO. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data Inf Manag. 2023;100063. doi: 10.1016/j.dim.2023.100063.

[30] Sindiramutty SR. Autonomous threat hunting: A future paradigm for AI-Driven Threat Intelligence, arXiv.org; 2023. https://arxiv.org/abs/2401.00286 (Accessed: 10 July 2024).

[31] Urs D (2024) Cybersecurity enhancement: harnessing the power of AI to strengthen cyber defenses. [online]. Available at: https://www.linkedin.com/pulse/cybersecurity-enhancement-harnessing-power-ai-strengthen-desh-urs-vqpmc [Accessed 11 July 2024].

[32] Kalogiannidis S, Kalfas D, Papaevangelou O, Giannarakis G, Chatzitheodoridis F. The role of artificial intelligence technology in predictive risk assessment for business continuity: a case study of greece. Risks. 2024;12(2):19. doi: 10.3390/risks12020019.

[33] Medium (2024) AI in endpoint security: Protecting devices from advanced threats, Medium. Accessed 10 July 2024. Available at: https://megasisnetwork.medium.com/ai-in-endpoint-security-protecting-devices-from-advanced-threats-d1a6a6738ba3.

[34] Jose J, Judith JE. A review on optimization and feature selection techniques for data security in IoT. 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN). Salem, India: 2023. p. 1290–4. doi: 10.1109/ICPCSN58827.2023.00217.

[35] Bhatnagar KV, Kushwah R. Cyber security in internet of things using optimization algorithms: a systematic mapping of literature. Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing; 2023. doi: 10.1145/3607947.3608068.

[36] Shashkov A, Hemberg E, Tulla M, O'Reilly U. Adversarial agent-learning for cybersecurity: a comparison of algorithms. Knowl Eng Rev. 2023;38:e3. doi: 10.1017/S0269888923000012.

[37] Oh SH, Jeong MK, Kim HC, Park J. Applying reinforcement learning for enhanced cybersecurity against adversarial simulation. Sensors. 2023;23(6):3000. doi: 10.3390/s23063000.

[38] Nguyen T, Reddi V. Deep reinforcement learning for cyber security. IEEE Trans Neural Network Learn Syst. 2019;34:3779–95. doi: 10.1109/TNNLS.2021.3121870.

[39] Faris M, Mahmud MN, Salleh MFM, Alnoor A. Wireless sensor network security: A recent review based on state-of-the-art works. Int J Eng Bus Manag. 2023;15:18479790231157220. doi: 10.1177/18479790231157220.

[40] Crammer K, Dekel O, Keshet J, Shalev-Shwartz S, Singer Y, Warmuth MK. Online passive-aggressive algorithms. J Mach Learn Res. 2006;7:551–85. http://jmlr.org/papers/v7/crammer06a.html.

[41] Sakamoto S, Ozera K, Ikeda M, Barolli L. Implementation of intelligent hybrid systems for node placement problem in WMNs considering particle swarm optimization, hill climbing and simulated annealing. Mobile Network Appl. 2018;23:27–33. doi: 10.1007/s11036-017-0897-7.

[42] Sayad L, Bouallouche-Medjkoune L, Aissani D. A chemical reaction algorithm to solve the router node placement in wireless mesh networks. Mobile Network Appl. 2020;25:1915–28. doi: 10.1007/s11036-017-0941-7.

[43] Merenda M, Porcaro C, Iero D. Edge machine learning for AI-enabled IoT devices: A Review. *MDPI*. 2020 Apr;20(9):2533. doi: 10.3390/s20092533.

[44] Abed AK, Anupam A. Review of security issues in Internet of Things and artificial intelligence-driven solutions. Secur Priv. 2023;6(3):e285. doi: 10.1002/spy2.285.

[45] Singh R, Gill SS. Edge AI: a survey. Internet Things Cyber Phys Syst. 2023;3:71–92. doi: 10.1016/j.iotcps.2023.02.004.