SCIENTIFIC Publishing Limited

Journal of Intelligent Communication
http://ojs.ukscip.com/index.php/jic

Review

An Intelligence-Based Cybersecurity Approach: A Review

Mahmood Saidu Badara, Yakubu Bala Mohammed* and Hussaini Dan'azumi

Department of Computer Science, Abubakar Tatari Ali Polytechnic, Bauchi-State 740211, Nigeria
* E-mail: mohammedbala0079@gmail.com

Received: 11 March 2024; **Revised**: 5 April 2024; **Accepted**: 31 May 2024; **Published**: 31 May 2024

Abstract: Nowadays, cybersecurity stands out as a prominent topic frequently discussed by companies aiming to safeguard their sensitive information from hacking attempts. The rise of internet has fuelled the expansion of online systems, creating a virtual digital realm that links portable devices and computers within the Internet of Things framework. Thus, the paper aims to presenting the progress made thus far in utilizing AI-based intrusion detection systems (IDSs) to address cybercrimes, demonstrating their efficacy in detecting and preventing cyberattacks. The review utilized 4 scholarly databases; ScienceDirect, IEEE-Explore, Web of Science, and Springer. 437 studies were extracted from the 4 chosen databases out of which only 54 studies were found to be relevant, thus included. The review found AI-based intrusion detection systems (IDSs) to be more robust and flexible compared to other conventional IDSs. Interestingly, the study results highlight how AI-based intrusion detection systems such as; ANN-based intrusion detection systems, agent-based intrusion detection systems, and Genetic-fuzzy intrusion detection systems, and other machine learning detection systems can be used to assist security experts in analysing, designing, and developing security frameworks for combating cybercrimes. Lastly, the study proposed some areas for future studies.

Keywords: cybersecurity; cybercrimes; AI-based applications; intrusion detection systems

1. Introduction

With the advancements in information technology (IT) and emergence of different artificial intelligence (AI) tools, criminals are exploiting cyberspace to commit various cybercrimes. The rising trends of intricate internet and distributed computing raise crucial concerns regarding information protection and confidentiality. Consequently, cyber infrastructures are highly susceptible to different attacks and other threats. For instance, Dilek [1] in their study argued that "Physical devices like detectors and sensors are inadequate for monitoring and protecting these infrastructures". Thus, the need for more sophisticated security gadgets to detect abnormal behaviours and model the normal ones. The authors stressed that these systems should be flexible, adaptable, robust, and capable of identifying a wide array of threats and making intelligent real-time decisions. Also, given the rapid pace and volume of cyberattacks, human intervention alone is insufficient for prompt attack analysis and suitable response. Notably, the majority of network-centric cyberattacks are orchestrated by intelligent agents such as computer worms and viruses [2]. Consequently, combating them necessitates intelligent semi-autonomous agents capable of detecting, evaluating, and responding to cyberattacks. These computer-generated forces must handle the entire attack response process promptly, determining the type of attack, identifying targets, formulating an appropriate response, and prioritizing and preventing secondary attacks.

Cyber intrusions transcend geographical boundaries, posing a global threat to online computer systems worldwide at an escalating rate. While cybercrimes were previously limited to educated specialists, the proliferation of the Internet and different AI tools has provided individuals and organizations access to various

tools and knowledge for committing these crimes. Traditional fixed algorithms have become ineffective against dynamically evolving cyberattacks. Hence, innovative approaches like applying Artificial Intelligence (AI) methods are essential, providing flexibility and learning capabilities to software to aid humans in combating cybercrimes. Natural language processing (AI) tools present numerous possibilities, particularly through various nature-inspired computing methods such as Computational Intelligence, Machine learning, Fuzzy logic, Deep learning, Immune systems, and Pattern recognition etc., which play a crucial role in detecting and preventing cybercrimes. AI enables the design of autonomous computing solutions that are capable of adapting to their context of use, employing different techniques such as "self-tuning, self-management, self-healing, self-configuration, and self-diagnosis" [1,3].

Regarding the future of cybersecurity, AI techniques emerge as a promising area of research focusing on enhancing security measures for cyberspace [4]. Therefore, this study aims at presenting the progress made thus far in utilizing different AI-based methods to address cybercrimes, demonstrating their effectiveness in detecting and preventing cyberattacks, and provide direction for upcoming studies.

2. Theoretical Framework

2.1. Digital Crimes: Issues and Challenges

Information and computing devices are increasingly becoming targets and tools for committing different form of digital crimes. Electronic devices and other high-tech products allow criminals to carry out inexpensive and effortless offenses. Nowadays, organization's databases, online computers, smartphones, and other information systems which are created for the betterment of society are becoming more vulnerable to criminal activities. Crimes against computing systems typically involve targeting organizational data, personal computers, emails, servers, bank accounts, websites, and digital records of both public and private institutions [5,6]. These offenses are also referred to as "Online crimes, Computer crimes, Cybercrimes, Online crimes, Internet crimes, or Network crimes" [7]. Cybercrimes encompass a range of offenses including computer trespassing', intellectual property rights being' misused, economic spying', online blackmail, global money laundering', non-delivery of' goods or services. and various other offenses facilitated by the Internet [8]. Though cybercrime is the most widely used term today, however, its precise definition remains elusive. Most definitions have been developed through experimentation. For instance, McGuire [9] in their work developed a helpful classification tool. The authors categorized cybercrime into "cyber-enabled crime" and "cyber-dependent crime". Cyber-enabled crimes are traditional offenses made easier by computer use. They argued that the range of cyber-enabled crimes is vast; ranging from white-collar crime like fraudulent financial transactions, identity theft, and theft of electronic information for profit, to drug trafficking, deviant voyeuristic activities, harassment, stalking, or other menacing behaviours. While these activities have always been considered criminal, they are now more accessible with a computer. While "Cyber-dependent crimes" on the other hand involves offenses that rely on cyber technology to exist [8]. Studies have shown that a cybercriminal can cause significant commercial harm using the internet. Indeed, it is now simpler and safer for a criminal to disrupt a business by corrupting its database with malware than by physically attacking it [10,11]. Cyber-dependent criminal activity was strongly felt globally in May 2015 when Cryptowall 3.0 ransomware began targeting businesses and wealthy individuals. Utilizing an exploit kit capable of exploiting applications vulnerabilities, the Cryptowall 3.0 searched for files on victims' computers, encrypted these files, deleted the originals, and demanded thousands of dollars in ransom money to return the files. It is estimated that these attacks affected hundreds of thousands of computers worldwide and caused nearly USD325 million in damages [8].

Every day, the volume of digital data stored and processed on computers and other computing systems grows exponentially as people communicate, share, work, shop, and socialize online. Language and geographical barriers have dissolved, and the virtual world has become more densely populated than ever. The concept of crime is inherent in human interactions, and cyberspace is not exempt from criminal activities and actors. Also, Folds contends that "most of the cybercrime we witness today simply reflects the migration of real-world crime to cyberspace, where criminals utilize it as a tool to commit traditional crimes in novel ways" [12].

2.2. Intrusion Detection and Prevention Systems, and Artificial Intelligence

In the context of intelligence computing, Dilek in their study stressed that AI can be defined in two distinct manners: (1) as a field of study focused on uncovering the nature of intelligence and crafting intelligent machines; or (2) as a discipline dedicated to devising techniques for solving complex problems that require some level of intelligence (e.g., making informed decisions based on vast amounts of data) [1]. With regards to applying AI to cyber defence, the authors primary interest lies in the latter definition. Research in AI centres around methods to enable machines (computers) to emulate intelligent human behaviours such as reasoning, learning, planning, and so forth [13].

The broad challenge of replicating intelligence has been broken down into specific sub-problems, each with particular attributes or capabilities expected of an intelligent system. According to Dilek [1], and Kushwaha [14], and the following attributes have garnered significant attention in research.

(1) Figuring stuff out, thinking, solving problems (such as with embodied agents, neural networks, and statistical methods in AI).
(2) Representing what we know (such as with ontologies).
(3) Understanding of Natural Language (i.e., machine translation, and information retrieval).
(4) Learning (i.e., machine learning).
(5) Planning (i.e., multi-agent planning and cooperation).
(6) Motion and Manipulation (i.e., navigation, planning, localization, mapping, and motion).
(7) Social Intelligence (i.e., simulation), and
(8) General Intelligence (i.e., Strong AI).

Computational models inspired by biological immune systems are known as AISs, which exhibit adaptability to changing environments and the ability to continuously and dynamically learn. Immune systems play a crucial role in identifying and addressing intruders within living organisms. Also, AISs are crafted to replicate natural immune systems, particularly in applications related to computer protection, including intrusion detection systems (IDSs) [15]. Furthermore, Genetic algorithms are other examples of an AI technique, based on the principles of evolutionary computation, mimicking the process of natural selection. Even when faced with intricate computing challenges, they provide resilient, adaptable, and efficient solutions. These algorithms can be utilized to generate classification rules for security attacks and develop specific rules for various security threats within IDSs [16].

Different methods have been devised to secure data over networks and the Internet, such as firewalls, antivirus software, secured protocols, and encryption. Nevertheless, adversaries continually devise new attack methods to compromise network systems. Thus, the need to have a robust intrusion detection and prevention system (IDPS), that can critically; monitor, detect, analyse, and respond to unauthorize activities [17]. Figure 1 depicts more robust IDPSs with advanced and traditional IDPSs components as per [1].

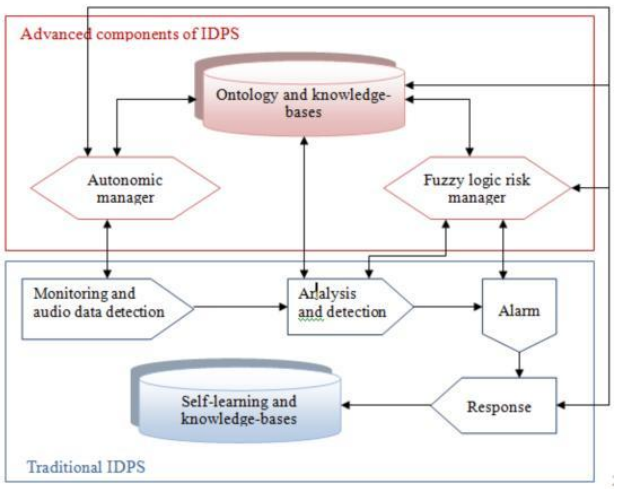

Figure 1. Advance IDPSs algorithms [1].

3. Methods

3.1. Study Design

The research is a literature review focusing on previous studies regarding cybersecurity, cybercrimes, and AI methods in order to provide progress made thus far in applying various AI techniques to address cybercrimes i.e., the effectiveness of AI methods in detecting and preventing cyberattacks. The subsequent subsections provide insight into the methodology employed for conducting the review.

3.2. Literature Search

After identifying the scope of our review, the authors initiated a search for related studies across several recognized scholarly databases. Due to the nature of our research topic, four scholarly databases were searched: ScienceDirect, IEEE Xplore, Web of Science, and Springer in order to locate articles relevant to our review topic.

3.3. Search Criteria

The authors commenced the search for related works by utilizing keywords that closely align with our review topics, such as "Cybersecurity", "Digital crimes", "Internet crimes", "Intrusion detection and prevention systems", "Intrusion detection and AI", "AI applications in cybersecurity", "Combat cybercrimes using AI" as per Mohammed [18]. A quite number of articles were extracted from the chosen databases for analysis.

3.4. Criteria for Selection

Given the intricate nature of the review topic (i.e., utilization of AI in cybersecurity), and scanty literature in the cybersecurity domain. Outcomes of the review databases searched produced only 437 relevant studies, which were organized and exported to a spreadsheet specially designed for the review purpose. Interestingly, there was no restriction on the publication period of the articles. During the second stage of our selection process, 285 articles were eliminated after reviewing their abstracts and titles as they were deemed irrelevant to our study. Additionally, studies written in languages other than English, lacking sufficient details regarding the application of AI in cybersecurity, and focusing excessively on cybersecurity aspects without discussing AI applications in cybersecurity were also excluded. The remaining 152 studies underwent further screening, after which 98 studies were also excluded due to inadequate details and precisions. Ultimately, 54 studies were thoroughly read and analysed in the review. Figure 2 depicts the review employed method.

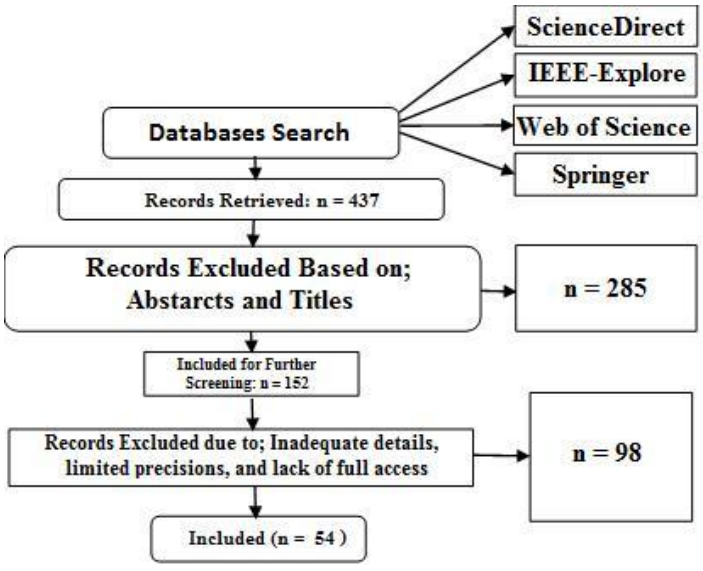

Figure 2. Algorithm of the review approach.

4. Results and Discussions

In this section, results concerning the progress made thus far regarding cybersecurity approaches, cybercrimes, and the application of AI to combat cybercrimes are offered.

4.1. Cybersecurity and Cybercrimes

Cybersecurity encompasses a variety of techniques and methods aimed at safeguarding computer systems and data from cyberattacks, preventing malicious software from taking control of system operations. Its focus lies on fortifying systems to eliminate vulnerabilities, combating cybercrime, and fostering a secure digital environment [19]. Additionally, it entails protecting information from theft, tampering, and unauthorized access, as well as safeguarding against natural disasters like dust and moisture [20]. Companies strive to ensure the integrity of data and information transfer processes between electronic devices, thwarting unauthorized third-party interference, alteration, or deletion of sensitive data.

Taddeo in their work stressed that confidentiality is imperative in such processes to ensure data transfer remains confidential and inaccessible to unauthorized individuals [21]. This is achieved through the utilization of different AI techniques that streamline the process, encrypt data, and securely transfer it to designated recipients [22]. Computer systems are characterized by their capacity to preserve data integrity, permitting alterations only by authorized individuals, alongside non-repudiation, which confirms task completion and prevents participants from denying transactions in the digital environment. The efficacy of computer systems is assessed through a series of robust security measures.

According to Mijwil [23], cybersecurity focuses mainly on safeguarding software and applications from vulnerabilities, which are perceived as weak points that can be exploited by cyber-attacks. While cyber criminals on the other hand target weaknesses in information systems by analysing system practices and user behaviour to exploit them for hacking purposes. Phishing, a form of fraudulent activity in cyberspace, aims to obtain valuable information beneficial to cybercriminals through sophisticated methods to gain control over both users and systems. Cybersecurity encounters numerous challenges in its operational practices. Experts organize information systems in cybersecurity, establishing best practices concerning their usage and work strategies. The shortage of cybersecurity experts is a major obstacle faced by companies, as a sufficient number of these specialists are essential for designing a secure digital environment [2]. However, studies have shown that "AI-based methods offer significant enhancements in detecting phishing and ransomware attacks compared to non-AI methods" [6]. For instance, by leveraging machine learning algorithms, AI can analyse vast datasets and identify subtle patterns indicative of malicious activity. These methods excel at recognizing evolving attack techniques and adapting to new threats in real-time. Additionally, AI algorithms can autonomously learn from past attacks, improving their accuracy and efficiency in detecting sophisticated phishing and ransomware attempts.

Jarrett contended that the increasing number of devices connected to the IoT amplifies the vulnerability to different form of attacks, threats spying, and network penetration [24]. Thus, recommended that companies should put in place robust protection majors and acquire the necessary technologies to confront the threat of cybercrime. Additionally, it is important not to utilize applications or programs from unlicensed or unofficial sources, as these may be a catalyst for hacking operations. Companies should implement specific strategies to safeguard data and information and create precise and thorough backup copies. Passwords should be complex and lengthy, and they should be changed every six months to a year to ensure the security of computer systems. By adhering to correct and precise procedures and exercising caution when using websites, the safety of the digital environment and the satisfaction of companies and customers are guaranteed.

Soni in their work stated that the "cybersecurity domain contributes to designing a flawless digital environment and preventing unauthorized access to this environment" [5]. The authors argued that these objectives can only be accomplished through the utilization of artificial intelligence techniques, which play a pivotal role in detecting and mitigating different attacks and threats. Consequently, the presence of various AI methods and effective measures regarding cybersecurity contribute to the formation of a secure digital environment.

4.2. Approaches to Combating Cybercrimes

Literature have shown that application of various artificial intelligence (AI) techniques in the cybersecurity domain plays a significant role in combating cybercrimes by shielding online systems, networks, and other sensitive information from disruption, illegitimate usage, destruction, disclosure, and/or alteration [5,10,22,23]. Cybercrime manifests in various ways, such as hacking, phishing, malware, and ransomware, and can result in severe repercussions for individuals and organizations. For instance, Mijwil in their study stressed for organizations to combat cybercrimes, the following cybersecurity approaches must be implemented; Regular security assessments, staff education, strong verification methods, robust intrusion and prevention systems (i.e., Network security), data encryption, incident response plan, cybersecurity threat intelligence, as well as consistently monitoring of the cyber threat environment and staying up-to-date on the latest strategies, tactics, and techniques employed by hackers [23].

In addition to the above-mentioned strategies, the authors equally emphasized the need for organizations to keep abreast of the most recent trends and best practices in cybersecurity, and be prepared to implement their cybersecurity strategies as needed in order to stay ahead of other emerging cybersecurity threats.

4.3. Roles of Artificial Intelligence in Combating Cybercrimes

Studies have shown that many organizations have begun to use different AI techniques such as artificial neural network (ANN), adaptive-neuro fuzzy inference system (ANFIS), intelligent agent applications (IAA), artificial immune system applications (AISA), ChatGPT, and other AIs applications to combat cybercrimes [1,25]. Thus, in this section, the review will present and debate the findings of prior studies regarding how different AI techniques are used to fight cybercrimes [26].

4.3.1. Combating Cybercrimes Using ANN

Abdullah in their study stressed that organizations are now using artificial neural networks (ANN) to fight cybercrimes [27]. The authors argued that ANN can be used to stop intrusions as the techniques can be employed to "spot DoS attacks, spam, computer worms, malware, and zombies. Also, Dilek and Mothukuri stressed that nowadays organizations use other AI techniques such as Data mining and Heuristics technology for anti-virus stuff [1,28]. For instance, some Intrusion Detection Systems (IDSs) used "mobile agent and smart agent tech to find sketchy cyber stuff". Singh stated that the "future of anti-virus is Heuristic Technology" which is like using special methods to figure out new viruses while scanning [2].

Sowjanya and Sungkur created NeuroNet, i.e., a neural network system that gathers and processes distributed data, coordinates core network device activities, searches for irregularities, issues alerts, and triggers countermeasures [29,30]. Their experiments highlight the robustness of the proposed NeuroNet system against low-rate TCP-targeted distributed DoS attacks. Also, Al-Janabi designed a neural network-based Intrusion Detection System (IDS) for prompt detection and classification of various attacks [31]. They developed the IDSs using neural network systems. Results of their experiments indicated that the proposed system has intrusion detection rates similar to other available IDSs, but it demonstrated at least 20.5 times faster detection of DoS attacks compared to other usual IDSs.

4.3.2. Combating Cybercrimes Using Intelligent Agent Applications (IAA)

Intelligent systems are AI applications that act on their own and chat h each other to swap info and team up to figure out and do the right things if something weird happens. Their ability to move and adjust in their surroundings, along with their collaborative nature, makes them suitable for combating cyber-attacks [32,33].

Kott and Heinl proposed an intelligent agent-based system approach to combat cyber intrusions [34,35]. The authors put their systems into action using "Programming of Logic" and applied it to automatically handle both the usual denial of service (DoS) and the distributed denial of service (DDoS) attacks without any human intervention. The results indicated that the agents' systems successfully detect and prevent different DoS and DDoS attacks. Also, Sarre in their study suggested a framework for adaptive and cooperative defence mechanisms against Internet attacks [8]. Their method relies on intelligent agent modelling and simulation, where collections of smart agents interact and adjust their setup and actions based on the network's condition

and the seriousness of attacks. They checked their method of examining DDoS attacks and defence apparatuses. The outcomes revealed that collaboration and the capacity to adjust in intelligent agent collections significantly improve defence effectiveness.

Chinedu and Zhang investigated how smart agent tech could make power grids work better and react faster, stopping known attacks and lessening or removing their effects [15,36]. They introduced an MLSM i.e., a prototype for Multi-Layered Security Model—that shields against wrong data and spots and recovers from unfamiliar attack tactics (like bad data from the internet or messing with the agents locally). Furthermore, Kotenko looked into the ways of using multiple agents to check and defend against botnets, which are quickly spreading online and being used for different cybercrimes like doing scans to find weaknesses, launching DDoS attacks, and sending loads of spam emails [37]. They explained how these systems are set up and put into action.

Madhok conducted a study to find the impact of intelligent agents in combating cybercrimes in banking industries [38]. The authors stressed that "intelligent malware and other advanced threats are increasing day by day this became necessary for the defence sector to use agent systems i.e., an autonomous entity which monitors through sensors and response upon an environment using actuators that is an agent with more advance intelligent [39]. Features that separate these Agent systems from the rest of other security tools are that intelligent agents can communicate among themselves in case they need to make plans or take some counter action for some threat in the system or network.

De Mello propose "a neural-symbolic BDI-agent based Multi-Context Systems (MCS) model to integrate these two methods". Results of their experiments show that the proposed agent can adapt and achieve high utility functions for dissimilar situations [40]. However, the authors argued that it is necessary to "consider the computational cost of using the NN's output in every reasoning cycle". In another study conducted by Herrero using flexible and adaptable "Mobile Visualization Connectionist agent-based IDS" [41]. The findings of their research indicated that the proposed Mobile Connectionist agent-based IDS can help in detecting intrusion in a changing networks environment. In their method, the smart agents utilized artificial neural networks to spot intrusions in a network. Additionally, Liu introduced an abstract model for anomaly detection in networks, influenced by the biological immune system, which relies on multi-agent technology [42]. They applied it to host and network layers in order to react to intrusions and reduce the harm and spread of infection.

Kotenko conducted a study based on multi-agent systems to investigate and defend against the widespread proliferation of botnets on the Internet [43]. These botnets are employed for a range of cybercrimes, including conducting vulnerability scans, executing distributed denial-of-service (DDoS) attacks, and sending large volumes of spam emails. The authors outlined the structure and technical aspects of these systems using various AI techniques.

4.3.3. Combating Cybercrimes Using Genetic Algorithm and Fuzzy Inference Systems

Few studies were conducted regarding the application of Genetic Algorithms and fuzzy systems in the cybersecurity domain. For instance, Chen in their study proposed a new fuzzy network intrusion detection method using class-association-rule mining in genetic network programming [32]. The results of their study suggested that the method is flexible and works well for both misuse and anomaly detection in networks. It can also handle databases with mixed attributes, including discrete and continuous ones, to find important class-association rules for better intrusion detection. Interestingly, their experiments and evaluation of the method showed that it gives high detection rates compared to other machine-learning techniques.

Cavus proposed an AI-based learning algorithm for user authentication and anomaly detectors that spot attacks using a genetic algorithm [44]. The authors applied the algorithm to a fake computer security system and proved how well it works for intrusion detection. Results of their work show that the proposed genetic algorithm if properly implemented can reduce attacks against financial institutions as the algorithm has the ability to handle velocity anomalies.

Khurana in their study came up with a fuzzy host-based intrusion detection system that uses data mining techniques and the services of the operating system calls [45]. Their simulation results showed that the system can boost performance, shrink database size, cut down time complexity, and reduce false alarm rates. Also, Masdari talked about a new fuzzy network intrusion detection method using class-association-rule mining in genetic network programming [46]. The study results show that their proposed approach is flexible and efficient for both misuse and anomaly detection in networks. Additionally, the approach can handle mixed databases with

both discrete and continuous attributes to find important rules for better intrusion detection. Their experiments and evaluation showed that the method gives high detection rates compared to other machine-learning techniques.

Abadeh designed and analysed different types of genetic fuzzy systems (GFSs) to handle intrusion detection issues as a new real-world application area that hasn't been tackled with GFSs before [47]. The resulting intrusion detection system should be able to identify both normal and abnormal behaviours in computer networks. They introduced three types of genetic fuzzy systems based on Michigan, Pittsburgh, and iterative rule learning (IRL) approaches to tackle intrusion detection as a high-dimensional classification problem. The experiments were carried out using DARPA datasets containing information on computer networks, containing both normal and intrusive behaviours.

Balan designed a fuzzy-based intrusion detection system for a "Mobile ad-hoc network" (MANET) [48]. The authors argued that "mobile ad-hoc networks do not use any proper infrastructure" so that it initiates a request for data transfer, thus, MANET is vulnerable to various types of attacks such as "black hole attacks", "warm hole attacks", and "grey hole attacks". The idea behind the authors' proposed systems is to have a system that detects when a node behaves maliciously using an intrusion detection system with fuzzy logic, and it can also determine the type of attacks. Results of the experiment clearly show that the system is robust enough to identify attacks such as a black hole, and grey hole attacks, and can prevent them using an effective node blocking mechanism, ensuring secure communication between nodes.

Though, the study succeeded in identifying the potential benefits of utilizing different AI-based approaches in combating cybercrimes. However, the authors discovered that utilization of AI in cybersecurity raises some ethical concerns and potential negative impacts. For instance, the authors discovered that: (i) utilization of AI-powered systems may inadvertently discriminate against certain groups or perpetuate biases present in training data; (ii) reliance on AI-based application may lead to over-reliance and human disengagement which in turn reduces human oversight and accountability; (iii) there's also the risk of adversaries exploiting AI vulnerabilities for malicious purposes, thus, amplifying cyber threats. Therefore, striking a balance between AI automation and human judgment is crucial to mitigate these ethical dilemmas and negative consequences.

4.3.4. Combating Cybercrimes Using ChatGPT

Advancements in artificial intelligence (AI) have changed lots of important areas by giving cheap, automated, and smart solutions Alawida [49]. Recently, there has been a significant breakthrough in natural language processing achieved by ChatGPT. Consequently, chatbot-driven AI technology now has the ability to interact and communicate with users, generating responses that resemble human conversation [50]. Al-Hawawreh conducted a study in an attempt to find out the practical applications and challenges of using ChatGPT to fight cybercrimes [51]. The authors stressed that ChatGPT has the potential to influence changes in the cybersecurity domain. They also argued that ChatGPT can be utilized as a chatbot-driven security assistant for penetration testing to analyse, investigate, and develop security solutions. However, in some studies, ChatGPT raises concerns about how the tool can be used for cybercrime and malicious activities [52,53]. Attackers can use such a tool to cause substantial harm by exploiting vulnerabilities, writing malicious code, and circumventing security measures on a targeted system.

Regarding the application of ChatGPT to fight cybercrimes, Elhanashi and Al-Hawawreh in their works argued that computer code has had a big impact on lots of important technologies and applications in our everyday lives [26,51]. The authors stressed that checking the code at every step of the software development life cycle (SDLC) to find any weaknesses, bugs, or security issues is important. For instance, Scanlon et al. in their study claimed that ChatGPT also plays a part in spotting vulnerabilities and fixing bugs in bits of code [54]. The authors used ChatGPT to check out a bunch of questions about code security and how well it works using Bitcoin data. Interestingly, the results of the tests showed that ChatGPT was able to spot a weakness in the extension of the TLS protocol code, which lets attackers get sensitive info from the server's memory. It also gave a detailed and simple explanation of the Bitcoin validation source code, which assesses the likelihood of blockchain attacks being low [55,56].

4.4. Ethical Considerations

Though, the study succeeded in identifying the potential benefits of utilizing different AI-based approaches in combating cybercrimes. However, the authors discovered that utilization of AI in cybersecurity raises some ethical concerns and potential negative impacts. For instance, the authors discovered that: (i) utilization of AI-powered systems may inadvertently discriminate against certain groups or perpetuate biases present in training data; (ii) reliance on AI-based application may lead to over-reliance and human disengagement which in turn reduces human oversight and accountability; (iii) there's also the risk of adversaries exploiting AI vulnerabilities for malicious purposes, thus, amplifying cyber threats. Therefore, striking a balance between AI automation and human judgment is crucial to mitigate these ethical dilemmas and negative consequences.

5. Conclusions, Recommendations, and Future Works

Cybersecurity is a significant issue as it tackles threats to information security. However, cyberattacks come in various forms, requiring countermeasures that stay updated with the latest trends. Since different cyber-attack approaches are constantly evolving, it's challenging to implement comprehensive measures. Therefore, this review aims to highlight the importance of safeguarding digital space using different methods, and how AI applications such as; ANN, Intelligent agents, Genetic algorithms, Fuzzy logics, ChatGPT, and other AI applications could be used to combat cybercrimes. Findings of the review indicates that AI-based intrusion detection systems (IDSs) are more robust and flexible compared to other conventional IDSs. Interestingly, the review results highlight how AI-based intrusion detection systems such as; ANN-based intrusion detection systems, intelligent agent-based intrusion detection systems, and Genetic fuzzy intrusion detection systems, and other machine learning detection systems can be used to assist security experts in analysing, designing, and developing security frameworks for combating cybercrimes. Just like other studies, the review too has some drawbacks. One major drawback of this study is that the review is limited to the databases used, and areas covered i.e., applications of AI-based techniques to fight cybercrimes. Thus, future works should investigate the negative effects of AI applications e.g., ChatGPT on the cybersecurity domain. Also, future works should enhance threat detection and response through advanced machine learning models by implementing AI-driven autonomous security systems, and improving privacy protection with AI-powered encryption. Furthermore, upcoming studies should tailor their efforts toward addressing ethical concerns surrounding AI decision-making in security contexts.

Author Contributions

Conceptualization: Y.B.M., M.S.B. and H.D.; methodology: M.S.B., Y.B.M. and H.D.; data curation: M.S.B., Y.B.M. and H.D.; formal analysis, Y.B.M., and H.D.; investigation, Y.B.M., and M.S.B.; resources, Y.B.M.; writing-original draft preparation: Y.B.M, M.S.B.; writing—review and editing: Y.B.M., H.D. and M.S.B.

Funding

This work received no external funding.

Institutional Review Board Statement

Not Applicable.

Informed Consent Statement

Not Applicable.

Data Availability Statement

The study data is available on request at Abubakar Tatari Ali Polytechnic, Bauchi-Nigeria, Department of Computer Science via the corresponding author.

Acknowledgments

The authors wish to extend their appreciation to Prof. Nadire Cavus, the Polytechnic Rector Dr. Hashim Sabo Bello, and TETFund for their contribution towards the success of this work.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. Available online: https://arxiv.org/abs/1502.03552 (accessed on 14 January 2024).
2. Singh, B.; Choudhary, R.; Sharma, A.; Sharma, P. Artificial Intelligence a Human Mind Tool Saving from Cybercrimes and Cyber Threats. *Int. J. Med. Toxicol. Legal Med.* **2022**, *25*, 37–46. [CrossRef]
3. Cavus, N.; Mohammed, Y.B.; Bulama, M.; Isah, M.L. Examining User Verification Schemes, Safety and Secrecy Issues Affecting M-Banking: Systematic Literature Review. *SAGE Open* **2023**, *13*. [CrossRef]
4. Cavus, N.; Mohammed, Y.B.; Gital, A.Y.; Bulama, M.; Tukur, A.M.; Mohammed, D.; Isah, M.L.; Hassan, A. Emotional Artificial Neural Networks and Gaussian Process-Regression-Based Hybrid Machine-Learning Model for Prediction of Security and Privacy Effects on M-Banking Attractiveness. *Sustainability* **2022**, *14*, 5826. [CrossRef]
5. Soni, V.D. Role of Artificial Intelligence in Combating Cyber Threats in Banking. *Int. Eng. J. Res. Dev.* **2019**, *4*, 7. [CrossRef]
6. Mohammed, Y.B.; Cavus, N.; Ya'u Gital, A.; Bulama, M.; Hassan, A. A Hybrid Soft Computing Approach for Prediction of Cloud-Based Learning Management Systems Determinants. *Int. J. Human–Computer Interact.* **2024**, 1–11. [CrossRef]
7. Wiafe, I.; Koranteng, F.N.; Obeng, E.N.; Assyne, N.; Wiafe, A.; Gulliver, S.R. Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access* **2020**, *8*, 146598–146612. [CrossRef]
8. Sarre, R.; Lau, L.Y.; Chang, L.Y. Responding to cybercrime: current trends. *Police Pract. Res.* **2018**, *19,* 515–518. [CrossRef]
9. Cyber crime: A review of the evidence. Available online: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence (accessed on 14 January 2024).
10. Zaytsev, O.A.; Pastukhov, P.S.; Fadeeva, M.Y.; Perekrestov, V.N. Artificial Intelligence as a New IT Means of Solving and Investigating Crimes. In Proceedings of the Institute of Scientific Communications Conference, Volgograd, Russia, 19–March 2020. [CrossRef]
11. Saponara, S.; Elhanashi, A.; Gagliardi, A. Reconstruct fingerprint images using deep learning and sparse autoencoder algorithms. In Proceedings of the Real-Time Image Processing and Deep Learning 2021, Florida, USA, 12–17 April 2021. [CrossRef]
12. Folds, C.L. How Hackers and Malicious Actors Are Using Artificial Intelligence to Commit Cybercrimes in the Banking Industry. PhD Thesis, Colorado Technical University, Colorado Springs, CO, USA, August 2022.
13. Taddeo, M. Three ethical challenges of applications of artificial intelligence in cybersecurity. *Minds Mach.* **2019**, *29*, 187–191. [CrossRef]
14. Kushwaha, N.S. Application of Artificial Intelligence Methods to the Prevention of Cybercrime. *Karnavati J. Multi. Stud.* **2023**, *1*, 1–32. [CrossRef]
15. Chinedu, P.U.; Nwankwo, W.; Masajuwa, F.U.; Imoisi, S. Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. *Rev. Int. Geog. Educ. Online* **2021**, *11*, 956–974. [CrossRef]
16. Yeoh, P. Artificial Intelligence: Accelerator or Panacea for Financial Crime? *J. Financial Crime* **2019**, *26*, 634–646. [CrossRef]
17. Pasha, S.A.; Ali, S.; Jeljeli, R. Artificial Intelligence Implementation to Counteract Cybercrimes Against Children in Pakistan. *Hum. Arenas* **2022**, 1–19. [CrossRef]
18. Mohammed, Y.B.; Karagozlu, D. A Review of Human-Computer Interaction Design Approaches towards Information Systems Development. *BRAIN. Broad Res. Artif. Intell. Neurosci.* **2021**, *12*, 229–250. [CrossRef]
19. Herath, T.B.; Khanna, P.; Ahmed, M. Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *J. Cybersecur. Priv.* **2022**, *2*, 1–18. [CrossRef]
20. Kabanda, S.; Tanner, M.; Kent, C. Exploring SME Cybersecurity Practices in Developing Countries. *J. Organiz. Comput. Electron. Commerce* **2018**, *28*, 269–282. [CrossRef]
21. Taddeo, M.; McCutcheon, T.; Floridi, L. Trusting Artificial Intelligence in Cybersecurity is a Double-Edged Sword. *Nat. Mach. Intell.* **2019**, *1*, 557–560. [CrossRef]
22. Wirkuttis, N.; Klein, H. Artificial Intelligence in Cybersecurity. *Cyber Intell. Secur.* **2017**, *1*, 103–119. [CrossRef]

23. Mijwil, M.; Aljanabi, M. Towards Artificial Intelligence-based Cybersecurity: the Practices and ChatGPT Generated Ways to Combat Cybercrime. *Iraqi J. Comput. Sci. Math.* **2023**, *4*, 65–70. [CrossRef]
24. Jarrett, A.; Choo, K.K.R. The Impact of Automation and Artificial Intelligence on Digital Forensics. *Wiley Interdiscip. Rev.: Forensic Sci.* **2021**, *3,* e1418. [CrossRef]
25. Kumar, S.; Gupta, U.; Singh, A.K.; Singh, A.K. Artificial Intelligence: Revolutionizing Cyber Security in The Digital Era. *J. Comput. Mech. Manage.* **2023**, *2*, 31–42. [CrossRef]
26. Elhanashi, A.; Lowe, D.; Saponara, S.; Moshfeghi, Y. Deep Learning Techniques to Identify and Classify COVID-19 Abnormalities on Chest X-Ray Images. In Proceedings of the Real-Time Image Processing and Deep Learning 2022, Orlando, FL, USA, 27 May 2022. [CrossRef]
27. Abdullah, F.M. Using Big Data Analytics to Predict and Reduce Cyber Crimes. *Int. J. Mech. Eng. Technol.* **2019**, *10*, 1540–1546. [CrossRef]
28. Mothukuri, R.; Basaveswararao, B.; Bulla, S. Judgement Classification Using Hybrid ANN-Shuffled Frog Leaping Model on Cyber Crime Judgement Database. *Rev. d'Intelligence Artif.* **2020**, *34,* 445–456. [CrossRef]
29. Sowjanya, S.M.; Ahmed, S.; Salman, S. ANN Based Cyber Threat Detection Utilising Event Profiles. *J. Algebraic Stat.* **2022**, *13*, 2410–2414. [CrossRef]
30. Sungkur, R.K.; Maharaj, M.S. Design and Implementation of a SMART Learning Environment for the Upskilling of Cybersecurity Professionals in Mauritius. *Educ. Inf. Technol.* **2021**, *26*, 3175–3201. [CrossRef]
31. Al-Janabi, S.T.F.; Saeed, H.A. A Neural Network Based Anomaly Intrusion Detection System. In Proceedings of the 2011 Developments in E-systems Engineering, Dubai, United Arab Emirates, 6–8 December 2011. [CrossRef]
32. Ahmad, F.; Abbasi, A.; Li, J.; Dobolyi, D.G.; Netemeyer, R.G.; Clifford, G.D.; Chen, H. A Deep Learning Architecture for Psychometric Natural Language Processing. *ACM Trans. Inf. Syst. (TOIS)* **2020**, *38*, 1–29. [CrossRef]
33. Oravec, J.A. Kill Switches, Remote Deletion, and Intelligent Agents: Framing Everyday Household Cybersecurity in the Internet of Things. *Technol. Soc.* **2017**, *51*, 189–198. [CrossRef]
34. Kott, A.; Theron, P. Doers, not Watchers: Intelligent Autonomous Agents are a Path to Cyber Resilience. *IEEE Secur. Privacy* **2020**, *18*, 62–66. [CrossRef]
35. Heinl, C.H. Artificial (Intelligent) Agents and Active Cyber Defence: Policy Implications. In Proceedings of the 2014 6th International Conference on Cyber Conflict (CyCon 2014), Tallinn, Estonia, 3–6 June 2014. [CrossRef]
36. Zhang, A.; Rau, P.-L.P. Tools or Peers? Impacts of Anthropomorphism Level and Social Role on Emotional Attachment and Disclosure Tendency Towards Intelligent Agents. *Comput. Hum. Behav.* **2023**, *138*, 107415. [CrossRef]
37. Kotenko, I. Agent-Based Modeling and Simulation of Network Infrastructure Cyber-Attacks and Cooperative Defense Mechanisms. In *Discrete Event Simulations*; Goti, A.; Publications: Verlag Österreich, Austria, 2010; 1, pp. 83–95. [CrossRef]
38. Madhok, E.; Gupta, A.; Grover, N. Artificial Intelligence Impact on Cyber Security. *IITM J. Manage. IT* **2019**, *7*, 100–107. [CrossRef]
39. Abdiyeva-Aliyeva, G.; Hematyar, M.; Bakan, S. Development of System for Detection and Prevention of Cyber Attacks Using Artificial Intelligence Methods. Isighn Proceedings of the 2021 2nd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 1–3 October 2021. [CrossRef]
40. De Mello, R.R.P.; de Santiago, R.; Silveira, R.A.; Gelaim, T.Â. Neural-symbolic BDI-Agent as a Multi-Context System: A Case Study with Negotiating Agent. *Expert Syst. Appl.* **2023**, *238*, 121656. [CrossRef]
41. Herrero, Á.; Corchado, E.; Wozniak, M.; Bae-Cho, S.; Petrović, S. Cybersecurity Applications of Computational Intelligence. *Neural Comput. Appl.* **2022**, *34*, 20447–20448. [CrossRef]
42. Liu, X.M. The Cyber Acumen: An Integrative Framework to Understand Average Users' Decision-Making Processes in Cybersecurity. In *Analyzing Human Behavior in Cyberspace*; Yan, Z.; IGI Global: Hershey, PA, USA, 2015; 1, pp. 192–208. [CrossRef]
43. Kotenko, I.; Konovalov, A.; Shorov, A. Agent-based Modeling and Simulation of Botnets and Botnet Defense. In Proceedings of the Conference on Cyber Conflict, Tallinn, Estonia, 15–18 June 2010.
44. Cavus, N.; Mohammed, Y.B.; Yakubu, M.N. An Artificial Intelligence-Based Model for Prediction of Parameters Affecting Sustainable Growth of Mobile Banking Apps. *Sustainability* **2021**, *13*, 6206. [CrossRef]
45. Khurana, K.; Sajja, P.S.; Bhatt, M.Z. Fuzzy Based Research Techniques for Intrusion Detection and Analysis: A Survey. *Int. Res. J. Eng. Technol.* **2016**, *3*, 1223–1227.
46. Masdari, M.; Khezri, H. A Survey and Taxonomy of the Fuzzy Signature-Based Intrusion Detection Systems. *Appl. Soft Comput.* **2022**, *92*, 106301. [CrossRef]
47. Abadeh, M.S.; Mohamadi, H.; Habibi, J. Design and Analysis of Genetic Fuzzy Systems for Intrusion Detection in Computer Networks. *Expert Syst. Appl.* **2011**, *38*, 7067–7075. [CrossRef]
48. Balan, E.V.; Priyan, M.; Gokulnath, C.; Devi, G.U. Fuzzy Based Intrusion Detection Systems in MANET. *Procedia Comput. Sci.* **2015**, *50*, 109–114. [CrossRef]

49. Alawida, M.; Mejri, S.; Mehmood, A.; Chikhaoui, B.; Isaac Abiodun, O. A Comprehensive Study of ChatGPT: Advancements, Limitations, and Ethical Considerations in Natural Language Processing and Cybersecurity. *Information* **2023**, *14*, 462. [CrossRef]
50. Fujima, H.; Kumamoto, T.; Yoshida, Y. Using Chatgpt to Analyze Ransomware Messages and to Predict Ransomware Threats. Available online: https://doi.org/10.21203/rs.3.rs-3645967/v1 (accessed on 14 January 2024).
51. Al-Hawawreh, M.; Aljuhani, A.; Jararweh, Y. Chatgpt for Cybersecurity: Practical Applications, Challenges, and Future Directions. *Cluster Comput.* **2023**, *26*, 3421–3436. [CrossRef]
52. Gupta, M.; Akiri, C.; Aryal, K.; Parker, E.; Praharaj, L. From Chatgpt to Threatgpt: Impact of Generative Ai in Cybersecurity and Privacy. *IEEE Access* **2023**, *2*, 11–20. [CrossRef]
53. Dash, B.; Sharma, P. Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review. *Int. J. Eng. Appl. Sci.* **2023**, *10*, 21–39.
54. Scanlon, M.; Breitinger, F.; Hargreaves, C.; Hilgert, J.-N.; Sheppard, J. ChatGPT for Digital Forensic Investigation: the Good, the Bad, and the Unknown. *Forensic Sci. Int.: Digital Invest.* **2023**, *46*, 301609. [CrossRef]
55. Okoli, C.; Schabram, K. A Guide to conducting a systematic literature review of information systems research. *SSRN Electron. J.* **2015**, *3*, 211–219. [CrossRef]
56. Keele, S. Performing systematic literature review in software engineering. In Proceedings of the 28th International Conference on Software Engineering, Shanghai, China, 20–26 May 2006. [CrossRef]