information

MDPI

Article

Insights into Cybercrime Detection and Response: A Review of Time Factor

Hamed Taherdoost [1,2]

[1] Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B 1V9, Canada; hamed.taherdoost@gmail.com
[2] GUS Institute, Global University Systems, London EC1N 2LX, UK

Abstract: Amidst an unprecedented period of technological progress, incorporating digital platforms into diverse domains of existence has become indispensable, fundamentally altering the operational processes of governments, businesses, and individuals. Nevertheless, the swift process of digitization has concurrently led to the emergence of cybercrime, which takes advantage of weaknesses in interconnected systems. The growing dependence of society on digital communication, commerce, and information sharing has led to the exploitation of these platforms by malicious actors for hacking, identity theft, ransomware, and phishing attacks. With the growing dependence of organizations, businesses, and individuals on digital platforms for information exchange, commerce, and communication, malicious actors have identified the susceptibilities present in these systems and have begun to exploit them. This study examines 28 research papers focusing on intrusion detection systems (IDS), and phishing detection in particular, and how quickly responses and detections in cybersecurity may be made. We investigate various approaches and quantitative measurements to comprehend the link between reaction time and detection time and emphasize the necessity of minimizing both for improved cybersecurity. The research focuses on reducing detection and reaction times, especially for phishing attempts, to improve cybersecurity. In smart grids and automobile control networks, faster attack detection is important, and machine learning can help. It also stresses the necessity to improve protocols to address increasing cyber risks while maintaining scalability, interoperability, and resilience. Although machine-learning-based techniques have the potential for detection precision and reaction speed, obstacles still need to be addressed to attain real-time capabilities and adjust to constantly changing threats. To create effective defensive mechanisms against cyberattacks, future research topics include investigating innovative methodologies, integrating real-time threat intelligence, and encouraging collaboration.

Keywords: cybersecurity; digital platforms; phishing detection; machine learning; threat intelligence

Citation: Taherdoost, H. Insights into Cybercrime Detection and Response: A Review of Time Factor. *Information* **2024**, *15*, 273. https://doi.org/10.3390/info15050273

Academic Editors: Abdelhamied Ashraf Ateya, Mohamed Hammad, Ahmed A. Abd El-Latif and Mohammed ElAffendi

Received: 31 March 2024
Revised: 23 April 2024
Accepted: 6 May 2024
Published: 12 May 2024

1. Introduction

A new era of cyber mobility brought about by expanding communication networks and the Internet has fundamentally changed how governmental and non-governmental organizations function. However, for many developed countries, the risk of cyberattacks has grown due to this greater dependence on integrated information-technology systems. Cyberattacks can target the vital infrastructure components of several countries due to the increasing interconnection and utilization of technology [1].

Technological developments in recent years have made it possible to comprehend the world's workings better, encouraging research into digital structures that can gather data from their surroundings and make decisions based on it. The main aim is to provide mathematical tools to analyze incoming data, identify patterns, and create prediction models for information that is not yet visible [2]. The capacity of firms to use information and communications technology to save expenses and boost productivity by giving clients access to information and services around the clock leads to prosperity. There are issues

in providing that availability. The perpetual availability of information implies that it is always open to assault [3].

Cyberdefenders are systematically disadvantaged in today's cyberwarfare. Attackers frequently only need to exploit a single security flaw to carry out an attack, and they may usually act at any time and from any location. Furthermore, the technical monocultures currently dominating information technology put these systems in high danger of assault. With many enterprises and individuals utilizing almost similar hardware, operating systems, and application software, cyber attackers have strong incentives to find and exploit flaws in these systems [4].

Cybercriminals have developed complex business strategies, using online anonymity to conduct lucrative unlawful operations. This has caused a paradigm change in cybersecurity techniques, emphasizing behavioral aspects [5,6]. The effective management of cyber hazards is hampered by a key barrier: the absence of data on cyber risk. This lack of data availability emphasizes the need for standardized databases, required reporting, and increased public knowledge to successfully combat cybercrime [7]. Riesco et al. [8] suggested using smart contracts and blockchain technology to encourage information sharing and create dynamic risk-management systems that may instantly reduce cyber risks. Using Python and Visual Studio Code for data analysis, Rana et al. [9] used malicious files as decoys to extract information from susceptible systems.

Cybersecurity analysts interact with risks, vulnerabilities, and threats regularly. As a result, they need a framework to rank the most important occurrences and assaults and choose the best course of action to counter them. Three things, nonetheless, could influence their choices: time, manual processes and methodologies, and subjectivity (Figure 1). These three variables can impact any cybersecurity analyst's performance, independent of their workplace [10].

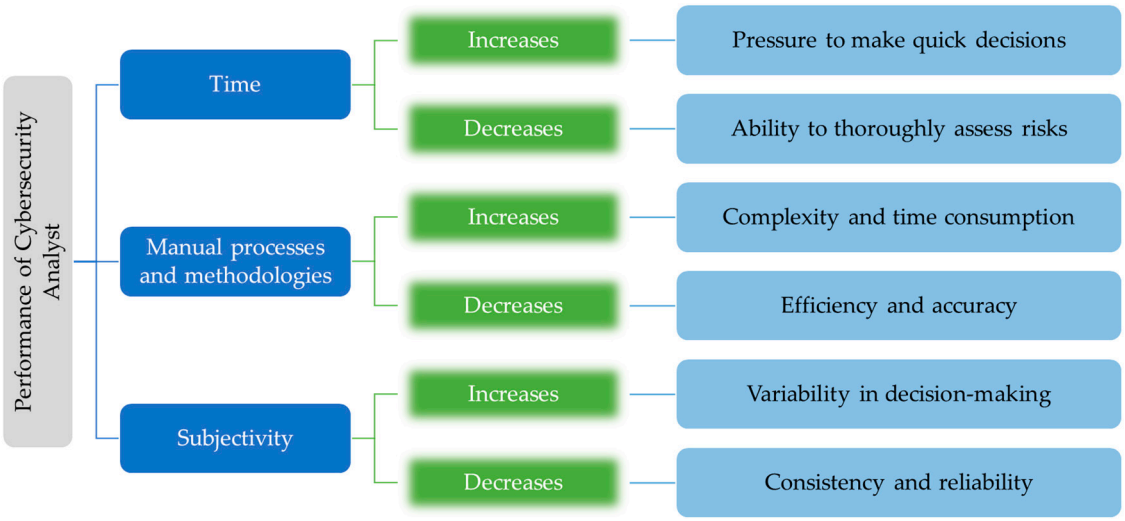

Figure 1. Impact of time, manual processes, and subjectivity on cybersecurity analyst performance.

Recent research has shed light on the time factor in cybercrime detection and response, emphasizing the critical role of response time in combating cyber threats. A study by Veena et al. [11] utilized machine-learning techniques and data from CBS open-data StatLine to identify and predict cybercrimes, highlighting the importance of timely detection based on crime-victim attributes. This approach underscores the significance of leveraging advanced technologies to enhance cybercrime detection efficiency and response effectiveness.

While previous studies have touched upon the significance of time-related metrics in cyber defense, only some have thoroughly examined the specific factors shaping detection time and response time. This research synthesizes models and theoretical frameworks to fill this gap in the literature and explain cybercrime detection and response difficulties.

It illuminates detection and response times through a systematic approach, emphasizing the need to use sophisticated technology to improve cyber defense efficiency and efficacy. Table 1 outlines the research objectives and corresponding questions for the study on cybercrime detection and response. By adhering to this structured approach, we aim to provide a comprehensive overview of the role of time-related metrics in cyber defense and offer valuable insights for cybersecurity practitioners, policymakers, and researchers.

Table 1. Research objectives and questions of the paper.

Research Objectives	Research Questions
To examine the importance of time-related metrics, specifically detection time and response time	What is the significance of detection time and response time in the context of cybercrime detection and response?
To identify and analyze the factors influencing detection time and response time in cyber-defense operations	What factors influence detection time and response time in cyber-defense operations?
To explore existing frameworks and models for measuring and evaluating time-related metrics.	What frameworks and models are available for measuring and evaluating time-related metrics in cybercrime detection and response?

2. Concepts

The Internet is a worldwide network of autonomous, globally linked networks. Even though it was first developed in 1994 to link government research centers, it has seen incredible development. It is now used by millions of people in government, academia, and public and commercial organizations for various reasons. The Internet has been constantly changing. The Internet has also shown many cyberattacks or attacks on its networks. Network security is critical because, as the Internet develops, enemies' attack strategies likewise change [12,13].

Modern crimes are spawned by the development of the Internet and associated technologies, including cybercrime. Because the origin of these crimes may be extremely difficult to establish, they may be classified as hybrid offenses as opposed to traditional criminal offenses like robbery and theft, which have a clear localization in both time and region of occurrence [14].

How can the proliferation of cybercrime be stopped? At some points, government surveillance can effectively discourage crime. In that sense, governmental and private law enforcement are vital, if not indispensable. In the near run, if police can identify the activity, criminal justice actions are typically a matter of "too little, too late". They rarely manage to block it beforehand [15]. Attackers can still breach security systems, destroying important data and having an adverse effect on the economy, even with ongoing security measures [16]. An adversary takes advantage of a user's vulnerability and manipulates them into revealing sensitive data [17].

An intrusion detection system (IDS) is required to protect against cyberattacks, given the accelerated advancements in information technology, network technology, computer security, and cybersecurity. Despite this, a constant stream of new developments and security enhancements are applied to the technology, permeating the security protocols to accomplish the same growth and enhancements [18]. Researchers have looked into several strategies, such as utilizing artificial intelligence and machine learning, to boost IDS performance. To improve intrusion detection, evolutionary algorithms, for instance, have been employed to create rules for classifying network traffic [19,20].

Cyber defenders need to stay one step ahead of these thieves to protect assets, data, and information against cutting-edge and growing cyber threats. This stage can only be reached when the cyber defender obtains sufficient data on threats, risks, vulnerabilities, assaults, and countermeasures before an event occurs. Timeliness is crucial in information-security risk management because pertinent information must be provided when needed so that appropriate action can be taken. For instance, countermeasures may be put in place, and an attacker can be stopped early if an organization is informed of an emergency danger as soon as feasible [21]. Time-related metrics are crucial in the context of cybersecurity for several reasons, as illustrated in Figure 2:

- Organizations may monitor cyber threats in real-time using time-related metrics, which enables timely security-event identification and response [22];
- Response time metrics offer useful insights into how rapidly companies can detect and address security breaches, which aids in assessing the effectiveness of incident-response procedures [22];
- Time-related metrics help detect new threats and vulnerabilities by monitoring changes in security events, vulnerabilities, and attack behaviors over time [23];
- These indicators let firms evaluate cybersecurity by comparing their performance to industry standards and best practices [24].

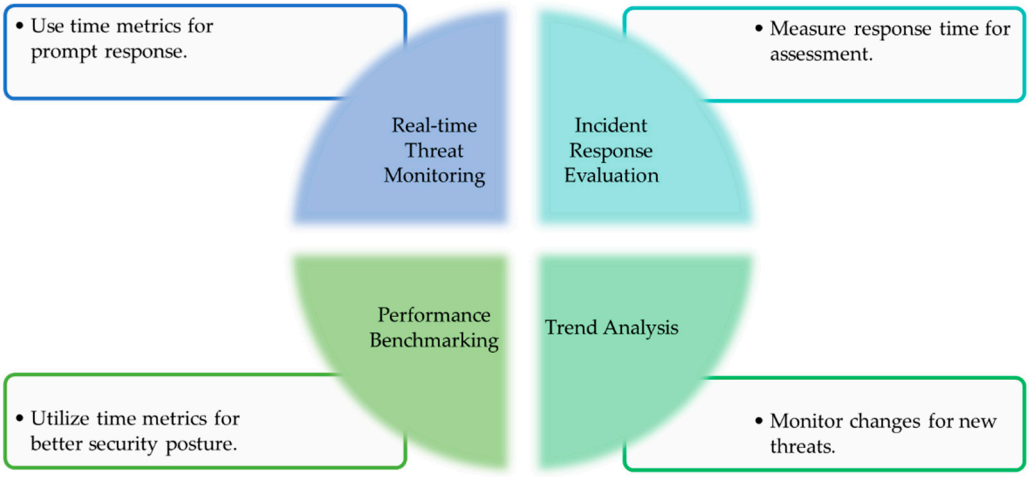

Figure 2. Time in cybersecurity strategies.

Organizations can bolster their cybersecurity stance using time-related metrics, enhance their capacity to respond to incidents, and proactively confront ever-changing cyber threats. These metrics furnish a quantitative foundation for assessing the efficacy of security measures and informing strategic choices aimed at fortifying cyber defenses.

The development of such models and the selection of simulations that assess cognitive burdens and reaction times to threats should involve stakeholders, such as users, managers, and developers. To practice real-world social engineering assault scenarios, stakeholders may also employ simulation. Furthermore, the budget could have an impact on vulnerability accounting. Businesses allocate very little money to cybersecurity [5].

Once an attacker has access to the network's first level, they will attempt to breach every defensive system level. To identify vulnerabilities before the attackers do, the defender needs to be more driven to investigate security at all levels utilizing tools [25].

The fact that cybercrime assaults may be operationalized and disseminated ahead of time indefinitely presents another practical challenge for investigators, making it even more difficult to establish a timeframe [26]. When victims do report cybercrimes to the authorities, they frequently wait to do so out of shame or a belief that they are more capable or driven to make things right than the police are. This prolongs the period between the incident and any potential evidence gathering [27]. Because they are ashamed of their actions or think they can manage the matter on their own, victims frequently put off reporting cybercrimes to the police. Law enforcement's capacity to gather pertinent evidence is hampered by the extended interval between the incident and reporting [28–30]. Law enforcement faces jurisdictional issues due to the internet and the transnational nature of cybercrime, which can involve offenses that transcend several regional boundaries [29,31].

In cybercrime, response time is a crucial factor that affects how events are handled and resolved. Incident reaction time is crucial to manage cyber problems effectively [32]. The field of restorative justice and cyber victimization emphasizes the importance of prompt reactions to cybercrimes to handle the aftermath and effects on victims properly [33]. In the context of cyber victim–offender panels, where prompt interventions can help heal

the pain caused by cybercrimes and reduce recidivism among offenders, it is important to understand the significance of quick reaction times.

Prompt action can lessen the negative effects of cybercrimes, including monetary losses, harm to one's reputation, and psychological distress [33,34]. Strong response mechanisms are required to safeguard privacy and data security against changing cyber threats [35]. The need for swift reactions to cybercrimes within a legal framework was shown by the study by Nugroho and Chandrawulan [36] synthesis of Indonesia's COVID-19 and cybercrime laws. This study highlighted the necessity of effective response systems to safeguard corporate and individual data, particularly in times of emergency, such as the COVID-19 pandemic. Protecting data security and privacy in the face of ever-evolving cyber threats requires the capacity to react quickly to cyber events.

One important factor that affects how successful cybersecurity measures are is the speed at which cybercrime is detected. In their systematic literature review, Abdullahi et al. [37] examined the application of artificial intelligence techniques to the identification of cybersecurity breaches within the domain of the Internet of Things (IoT). AI-based methods, including deep learning and machine learning, have demonstrated encouraging outcomes in the identification of diverse attack categories, such as probe, user-to-root (U2R), remote-to-local (R2L), and denial-of-service (DoS) attacks. Studies in this domain underscore the significance of promptly detecting and addressing cyber hazards to minimize harm. The application of data mining and machine-learning techniques to improve cybercrime detection skills has been the subject of several pieces of research. Gong and Lee [38] suggested a framework for real-time cyber threat detection, analysis, and response to enhance cybersecurity posture. They emphasized the need to shorten detection times. This approach provides a more comprehensive context of indications of compromise (IOCs) and improves cyber threat intelligence by utilizing cutting-edge technology such as neural networks and natural language processing.

Cybercrime prosecution presents several difficult issues, particularly in international and extraterritorial settings. There are legal and jurisdictional obstacles since the evidence needed to identify and prosecute cybercrime is frequently kept on private servers inside and outside the territorial state. To effectively address cyber threats, law enforcement agencies, and legislators must thoroughly understand the complexities of cybercrime prosecution. Due to resource limitations, Afzaliseresht et al. [39] brought attention to companies' need to look into many machine-generated danger alerts. Their suggested strategy seeks to increase awareness of possible risks and speed up reaction times by employing storytelling techniques to create reports in natural language. Using cutting-edge techniques like smart contracts and blockchain technology, businesses may improve knowledge sharing, expedite threat-intelligence exchange, and strengthen cybersecurity defenses.

3. Methodology

3.1. Data Sources and Analysis Methods

The study used a methodical search technique to locate pertinent journal articles on threat detection, incident response, cybersecurity, and cybercrime, particularly on reaction and detection times. On 28 March 2024, a mix of title, abstract, and keyword searches were performed in the Scopus database using the advanced query below:

(Title/abstract/Keywords ("Cybercrime" OR "Cybercrime" OR "Cybersecurity" OR "Cyber defense" OR "Incident response" OR "Threat detection" OR "Cyber incident") AND Title/abstract/Keywords ("Response time" OR "Detection time"))

To guarantee the authenticity and pertinence of the results, the search was restricted to records released in the years 2019 through 2024. The search results contained only journal publications classified as published in English. Reviews, books, book chapters, conferences, editorials, and other non-relevant document categories were filtered using exclusion criteria.

As shown in Figure 3, using the search criteria, 426 documents were found at first. Afterward, 97 documents were found after narrowing down the search results to contain

only journal publications. Of these, 26 publications satisfied further requirements listed as methods-proposing quantitative reports. However, several articles were not readily available because of the limitations of downloading them. Twenty-eight documents were retrieved for study after two more were found through supplemental searches.

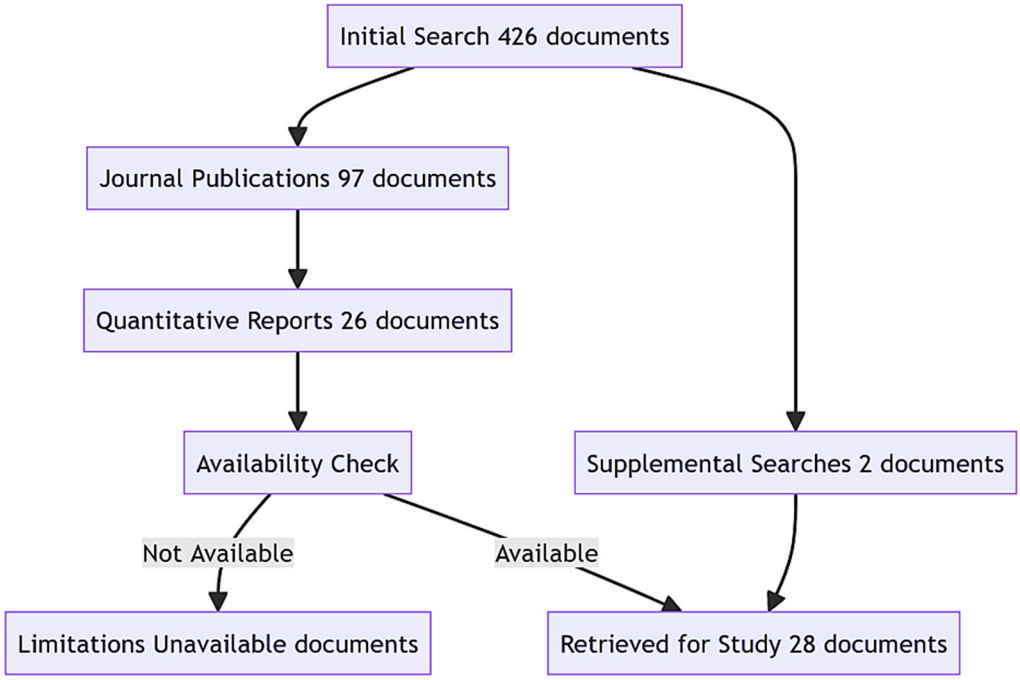

Figure 3. Papers collection method overview.

A methodical approach was used to examine the data, extract pertinent information from each document, concentrate on quantitative results, and suggest techniques for reaction and detection times in the context of cyber events. After that, data-synthesis techniques were used to find recurring themes, patterns, and revelations in the chosen publications.

3.2. Limitations of the Study

The search criteria mistakenly eliminated certain study types or articles that did not specifically include response time or detection time in their titles, abstracts, or keywords. Moreover, due to constraints, prejudice may have entered the selection process if certain publications were unavailable for download. Because this analysis relies only on the published literature, it is possible that unpublished or current research was overlooked. Even if every attempt was taken to guarantee that the search technique was thorough, it is still possible that some pertinent articles were overlooked. Recognizing the volume and variety of phishing attacks—Spear, Vishing, Email, Smishing, Angler, HTTPS, and Pharming—is also crucial. Each type has unique complications, which may affect detection times. This diversity may restrict the study's generalizability, thus applying conclusions to specific phishing attack circumstances with caution.

4. Results and Findings

An extensive overview of several pieces of research on cyber-defense operations and associated techniques is provided in this section. These studies provide important insights into crucial areas, including detection and reaction times, and the effectiveness of various cyber protection strategies through quantitative and comparative research.

A thorough method of assessing cybersecurity activities using both detection and reaction metrics is shown in Figure 4. It includes a wide spectrum of research on several facets of cyber defense, such as vulnerability management, intrusion prevention, phishing detection, and blockchain-based security solutions. The framework offers a comprehensive

viewpoint on the effectiveness of various cybersecurity tactics and their influence on lowering detection and reaction times in practical situations by combining the results of these investigations.

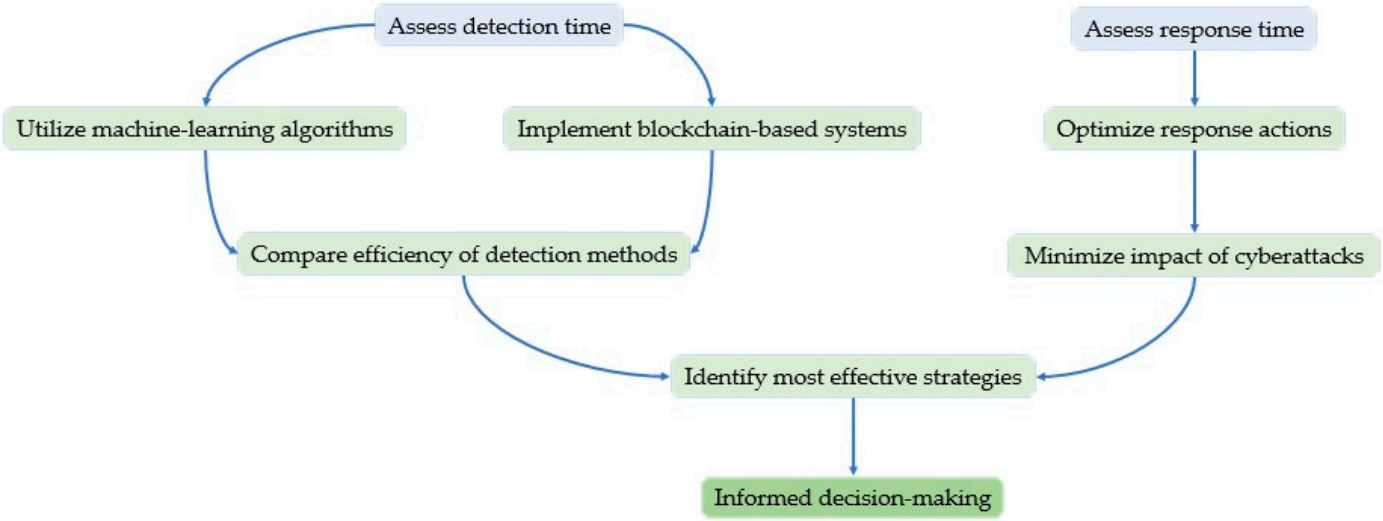

Figure 4. Cyber-defense operations.

4.1. Detection

The global economic expansion brought about by high technology has led to a change in phishing assaults in recent times. The surge in fraudulent losses across all categories in 2019 has been ascribed to the escalation of deception schemes, spoofing, and advanced cyberattacks like phishing. Phishing assaults will become more widespread; thus, to safeguard online user activity, a more effective phishing detection technique is needed [40]. Due to its dynamic assaulting techniques, phishing is a well-known cyberattack technique that has garnered substantial study attention in the cybersecurity arena over the last 20 years. Even though phishing has been combated using a variety of strategies, assaults have skyrocketed in the last several years. Machine learning has gained popularity in the current anti-phishing landscape, and methods such as deep learning have significantly enhanced the detection capabilities of anti-phishing software [41].

The research by Ariyadasa et al. [41] presented PhishDet, a novel approach to identifying phishing websites by employing URL and HTML data in conjunction with graph convolutional network and long-term recurrent convolutional network. PhishDet, the first of its type, achieved 96.42% detection accuracy, with a 0.036 false-negative rate, by utilizing the potent analytical and processing powers of graph neural network in the anti-phishing sector. It can fend off zero-day assaults effectively, and its 1.8-s average detection time is likewise reasonable. Adebowale et al. [40] focused on designing and developing a deep-learning-based phishing detection system that used website content such as text, graphics, and frames, as well as the universal resource locator, to meet this demand. A hybrid classification model known as the intelligent phishing detection system (IPDS) was constructed using the long short-term memory (LSTM) algorithm and the convolutional neural network (CNN). When applied to big-data sets, a detailed experimental investigation was carried out to assess and compare the efficacy of the IPDS in detecting phishing websites and phishing assaults. The model's accuracy rate was 93.28%, and its average detection time was 25 s, according to the data.

de Araujo-Filho et al. [42] examined generative adversarial networks (GANs), which offer a viable unsupervised method for identifying assaults through implicit system modeling. Additionally, GANs provide an alternative to LSTM networks by considering temporal relationships between data. Using temporal convolutional networks (TCNs) and self-attention, they provide a unique unsupervised GAN-based IDS that can identify

cyberattacks. The suggested IDS uses edge computing to bring computer resources closer to end nodes and is intended for edge servers. They demonstrated that their IDS is quicker by at least 3.8 times and more accurate than the two cutting-edge GAN-based IDS that serve as baselines. Maosa et al. [43] offered a framework for gathering data that reduces the requirement for long-term storage. Live-streaming methods transmit events in real time after they have been queued in memory up to a predefined threshold. They tested the framework in a real-time threat-detection system that uses machine learning. Compared to storage-based collection frameworks, our results provide a time gain of 300 milliseconds in the transmission time from event capture to analytics system; 95% of threats were detected, similar to the benchmark snort IDS.

Al-Haija [44] created and assessed an XSS detection solution for web applications based on machine learning. Specifically, they explore three types of supervised machine learning: hybrid (ensemble) learning of decision trees, optimizable naïve bays, and optimizable k-nearest neighbors. They used the XSS-Attacks-2019 dataset, which includes contemporary real-world traffic-subjected sorts of classes, normal (benign) or abnormal (XSS attack), to verify the effectiveness of the system. The trial results showed how dominant the hybrid-learning-based XSS detection system is. Accuracy, precision, and sensitivity were the top performance indicators, peaking at 99.8% with a very low detection time of 0.1031 ms. Using the Naive Bayes classifier with trust value when the parameters are set, a 99.7% accuracy was achieved by Sherubha and Mohanasundaram [45]. The work is expected to take around 27.35 s to complete. Based on the obtained data, it is now determined that the expected work performs better in accuracy, sensitivity, and specificity than the current procedures. The proposed NB-TV determines the likelihood of clone nodes occurring in the network based on variables like sequence number, SYN value, and frequency of IP-address occurrence.

Researchers have explored innovative solutions to address security challenges in critical infrastructure systems. Naeem et al. [46] described a smart memory forensics system that uses RGB visual pictures captured from the memory dump of suspicious processes to identify malicious assaults across high-availability servers. Second, local binary patterns (LBP) and gray-level co-occurrence matrices (GLCM) are used to record malware pictures' local and global features. Applying a cutting-edge t-distributed stochastic neighbor embedding approach (t-SNE) lowers the dimensionality of the data. It speeds up the discovery of new malware and its variations. The goal of an enhanced CNN model is to anticipate malicious files that might damage user devices or servers. They used a public data collection of 4294 harmful samples, including benign executables and malware variants, for their investigation. A baseline is created to compare the suggested model's performance with cutting-edge malware detection; the t-SNE dimensionality reduction approach and the coupled LBP + GLCM feature extraction increased the detection time by 73 times while increasing the detection accuracy by 98%.

Tolba and Al-Makhadmeh's [47] study introduces a cybersecurity-assisted authentication approach for smart grids to combat erroneous data flow. This approach uses information that has already been obtained to estimate the energy needs of the meters in advance. Authentication-dependent security is supplied based on the energy need and distribution method that has been pre-estimated. Up to the users' current connection time, variations in smart grid data for energy allocation are tracked based on network and end-user usage. By offering individual authentication for user verification and power sharing, this technique raises the detection rate of fake data. According to the results, the suggested solution reduced the detection time (4.67 s) without raising the end-user overload. Two-way authentication between the smart meter and the power-company security associate was the suggested approach by Chen et al. [48]. The suggested technique assessed how cyberattacks on the smart grid behaved. Attacks like retransmission and man-in-the-middle were taken into consideration. It was discovered that, by increasing secure connections, the suggested technique strengthens the trust between the smart grid and verified users and enhances both the power usage and detection time. The findings

demonstrated that the suggested algorithm's detection time grows with the false factor. The detection time increases by 1.4 s as the false factor rises from 0.1 to 0.3.

Today's most popular in-car network, the controller area network (CAN), is built without security or authentication features. Modern cars are excellent targets for cyberattacks since they have many networking technologies, including Bluetooth, Wi-Fi, and cellular radio, and are easily accessible from the outside world. Therefore, it is imperative to improve vehicle security by identifying and thwarting cyberattacks [49]. De Araujo-Filho et al. [49] offered a novel unsupervised intrusion prevention system (IPS) for CANs that can identify and block assaults without requiring information that is proprietary to automakers or altering the design of the electronic control units (ECUs). They assess which of the two machine-learning techniques is more accurate in detecting fuzzing and spoofing attacks while using the fewest bytes of data. Attacking frames can be identified sooner, and detection can begin sooner with fewer data bytes. The experiment outcomes demonstrate that, for the sorts of assaults considered, their suggested detection technique achieves accuracy levels over 99%, F1-scores above 97%, and detection durations below 80 µs. Yang et al. [50] used a sparse enhancement training technique to help the discriminator in the GAN correct the arbitration bias for false attack data every 100 steps, and they developed a new loss function for the generator in the GAN to improve its ability to make fake abnormal data. Furthermore, in building the GAN model, they use fewer convolution and de-convolution layers, which can theoretically lower the calculation time and cut the detection time to 0.12 ± 0.03 ms for a data block composed of 64 CAN messages.

The paper by Ilango et al. [51] proposes a feedforward–convolutional neural network (FFCNN), an AI-based anomaly detection system, to identify LR DoS assaults in IoT-SDN. The study uses the Canadian Institute of Cybersecurity Denial of Service 2017 (CIC DoS 2017) dataset. The important characteristics needed for identification are extracted by an iterative wrapper-based support vector machine (SVM) feature-selection process. The machine-learning methods J48, random forest, random tree, REP tree, SVM, and multi-layer perceptron (MLP) are used to compare the performance of the FFCNN. The metrics of accuracy, precision, recall, F1 score, detection time per flow, and ROC curves are used to assess the models' performance. Based on all measures, the empirical investigation demonstrates that FFCNN performs better than other machine-learning methods. The FFCNN model exhibits a detection time of 3.87 µs, which is notably quicker than the detection times of SVM (139.08 µs) and random forest (12.81 µs). Moreover, it maintains a high level of accuracy, whereas the detection times of J48 (2.04 µs), random tree (1.47 µs), REP tree (1.7 µs), and MLP (1.11 µs) are comparable. The primary reason for FFCNN's exceptional performance is the integration of CNN into the design.

To tackle security and privacy issues, a unique framework known as the BC-Trans network was suggested by Ingle and Ingle [52], which makes use of the advantages of both Blockchain technology and a transformer element. The transformer is essential in recognizing anomalous data, so the system can take preventative action against any dangers. A further security layer is added to the authentication process by introducing Hash-2 for IoT user verification. User passwords and information are safely stored using the Blockchain concept, guaranteeing a strong and impenetrable authentication system. CSE-CIC-IDS2018, a publicly accessible dataset, validates the suggested model. The suggested method performs well, showing detection times of 225.3 s, an accuracy of 99.25%, a precision of 99.53%, a recall of 99.32%, and an F1 score of 99.59%. The system's measurements improve as the output volumes rise, indicating adaptability and scalability.

4.2. Response

Safeguarding the privacy and integrity of sensitive user data, including passwords and PIN codes, poses a formidable obstacle for cybersecurity. Daily, billions of users are duped into entering sensitive information onto bogus logon pages. Phishing emails, enticing advertisements, click-jacking, malware, SQL injection, session hijacking, man-in-the-middle, denial of service, and cross-site scripting attacks are all methods of convincing

a user to visit a particular website. Phishing and web spoofing are forms of electronic deception in which an assailant creates a counterfeit version of a reputable website to obtain sensitive user data, including passwords. Researchers have suggested several security strategies as countermeasures to such exploits; however, these strategies encounter challenges related to latency and accuracy [53].

An improved deep-learning-based phishing detection method has been suggested by Prabakaran et al. [54] that combines the power of deep neural networks (DNN) and variational autoencoders (VAE) to identify fraudulent URLs efficiently. To improve phishing URL detection, the suggested system uses the VAE model to extract a raw URL's intrinsic properties by recreating the original input URL. Approximately one lakh of URLs were retrieved for testing purposes from the ISCX-URL-2016 dataset and the Kaggle dataset, two publically accessible datasets. The findings indicate that, compared to all previous models tested, the proposed model performs better, with a maximum accuracy of 97.45% and a faster reaction time of 1.9 s.

Shukla et al. [55] have created a real-time, highly scalable, feature-rich machine-learning-based anti-phishing detection method that uses HTTP headers—mostly security headers—extracted from web pages to determine if they are authentic or phished. Phishing websites are known to have a brief lifespan and are designed with a specific goal in mind, such as obtaining user credentials. The test results demonstrated a high accuracy of 97.8% and an average reaction time of 1.57 s. They have developed several datasets for various circumstances, such as a new dataset for testing undiscovered phishing assaults and a dataset for creating websites using phishing tools. The resulting data demonstrated 99% and 95% detection accuracy, respectively.

Phishing detection is challenging due to continually evolving assaults, despite prior attempts to lessen this common Internet menace. Its identification is made more challenging by the absence of a structured knowledge acquisition process and the need for continual learning assistance offered by current solutions. In this regard, SmartiPhish is presented by Ariyadasa et al. [56] as the first anti-phishing solution with integrated support for continuous learning and an inventive method for acquiring knowledge. SmartiPhish uses deeptiPhish, which uses deep learning and reinforces an effective phishing detection system. The deep-learning model predicts the likelihood of phishing attempts based on the URL and HTML content of a given online page. This probability is then sent to a reinforcement learning environment, which uses the website's popularity and past visits to determine the outcome. With a detection time of 4.3 s and an accuracy of 96.40%, SmartiPhish is quite effective. In an unbalanced setting, SmartiPhish functions admirably, and zero-day attack detection is fascinating.

Altamimi et al. [53] suggested and constructed a client-side defense mechanism that employs machine-learning methods to identify fraudulent websites and safeguard users against phishing attempts. PhishCatcher, a Google Chrome extension designed as a proof of concept, executes our machine-learning algorithm for categorizing URLs as trustworthy or dubious. The experimental outcomes demonstrate an exceptional precision of 98.5% and accuracy of 98.5%, respectively, derived from evaluations conducted on 400 legitimate and 400 classified phishing URLs. Furthermore, experiments were conducted on more than forty phishing URLs to determine the latency of our instrument. PhishCatcher exhibited an average response time of merely 62.5 ms.

The efficacy of a vulnerability management system that relies on network and port monitoring is enhanced in the paper by Basuki and Adriansyah [57] by integrating scenario planning and benchmarking models into the proposed method. Masscan can achieve response times of less than 2 s when performing network scanning to identify open ports on a subnet. Nmap can achieve response times of less than 4 s when scenario planning for detection on a single host. By integrating both models, a satisfactory optimization response time was achieved. The response time is under six seconds in total. With advancements in wireless communication networks and autonomous driving, such as the next-generation cyber–physical system (CPS), big-data analytics are becoming increasingly important to

achieve higher accuracy and reduced latency. However, a few issues, including confidentiality, safety, centralized control, and adversarial assaults, are not discussed in the available research [58]. Choi et al. [59] present an optimization approach for cyber-defense activities based on the information system's failure recovery time to improve cyber-resilience's reaction and recovery phases. The reaction times for different kinds of cyberattacks were established through training. Interestingly, there was a 17.8% drop in response time from the baseline.

Soundararajan et al. [58] proposed the BC-CS-AMSDAN-QFOMM-WCN, an adaptive multi-scale dual attention network with Quaternion fractional order Meixner moments for cybersecurity in wireless communication networks, as a solution to these problems. Initially, the cloud-layer difficulties are mitigated by the adaptive multi-scale dual attention network (AMSDAN) technique, which is provided at the edge layer. The AMSDAN is built in a blockchain environment to tackle the triple fundamental issues of mining, block creation, decryption, and encryption. During the encryption stage of a wireless communication network, a public and private key are assigned to each node using quaternion fractional order Meixner moments (QFOMM). The suggested BC-CS-AMSDAN-QFOMM-WCN method performs better than the current approaches, offering 23.31%, 11.03%, and 27.89% higher throughput and 36.51%, 13.09%, and 22.24% minimum delay, respectively. These approaches include Blockchain-based spectrum-sharing transactions for multi-operators wireless communication networks (BC-CS-SS-TSS-WCN), Blockchain and machine learning for wireless communications and networking systems (BC-CS-DAG-ML-WCN), and Blockchain-based privacy-preserving framework for emerging 6G wireless communications (BC-CS-B-RAN-WCN),

Vasylyshyn et al. [60] constructed a blockchain-based decoy system and ran controlled tests to measure network performance and evaluate the efficacy of attacker identification and cybercrime investigation. A blockchain-based method for detecting cybercrime using decoys is suggested. The methodology relies on the dynamic nature of the system's properties. Using such an approach, it is now feasible to create a system model that addresses the issue of intruders detecting decoys. The suggested approach minimizes the load instead of the traditional fixed solution. The findings show that, when decoys have dynamic features, services' response time is considerably lowered. Nginx is vulnerable because the dynamic host mining activities use up system resources. Along the X axis, a static host's average response time to Nginx is 1 to 2.5 Mbps faster than a dynamic host's. A DDoS assault starts to impact response time significantly at 2 Mbps. The dynamic host curve is always lower than the other, between 2 and 4 Mbps, indicating that a static host will take longer to load than a dynamic host. Methods for optimizing the four lightweight hash functions that reached the final stages of the NIST standardization competition—PHOTON-Beetle, Ascon, Xoodyak, and Sparkle—were proposed in a study by Lee et al. [61]. On a GPU platform, all four candidates attained high throughput for hashing (70 Gbps to 1000 Gbps), enabling the implementation of high-performance data integrity tests in IoT systems. Using ProjectQ, the implementation of these four hash functions on a quantum computer was evaluated.

To provide distributed dual-layer self-protection capabilities against distributed denial of service (DDoS) assaults, a novel cognitive closed-loop system is proposed by Benlloch-Caballero et al. [62]. For the distinct business roles of the stakeholders, digital service providers (DSPs), and infrastructure service providers (ISPs), respectively, the proposed system uses concurrent autonomous closed-loops in a novel way. This makes it suitable to offer multi-layer self-protection defense mechanisms across multiple administrative domains. After blocking 256 compromised devices, the system's efficacy against a large-scale assault was 78.12%, compared to 4.73% for the standalone version. Additionally, the isolated system needed 57 s to respond, but the suggested system only needed 18 s, resulting in a 316% performance improvement.

A unique digital forensic architecture for infrastructure-as-a-service (IaaS) clouds is proposed by Pourvahab and Ekbatanifard [63], utilizing Blockchain and software-defined

networking (SDN), two rapidly developing technologies. The evidence in this suggested forensic architecture is gathered and stored on a blockchain that several peers share. Secure ring verification-based authentication (SRVA) is suggested to guard against unauthorized user access. The harmony search optimization (HSO) technique is used to create secret keys optimally to fortify the cloud environment. The approach known as sensitivity-aware deep elliptic curve cryptography (SA-DECC) is introduced for encryption. The suggested digital forensic system takes 75 ms to react for 100 users, whereas the CFLOG system takes 100 ms to reply for 100 users. Consequently, the suggested digital forensic system outperforms the CFLOG system by 25%.

Nasir et al. [64] outlined our attempts to address this problem by creating an IDS integrated into an IoT device to improve visibility and strengthen the security of such devices. Their research framework, BTC_SIGBDS (Blockchain-powered, trustworthy, collaborative, signature-based botnet detection system), includes the device-level intrusion detection described here. To bolster defenses against new threats, they employ a trusted signature updating system and a signature-based detection technique. Using the ISOT, IoT23, and BoTIoT datasets, they have assessed the suitability and improved the capability of two of the most well-known signature-based IDS by creating custom signatures. With a peak alert of 1.5 million, more than the total number of alerts generated (about 0.34 million) with the default ruleset and a maximum processing time of 298.5 s, the assessment findings on the ISOT dataset using Snort demonstrate notable improvements. Suricata outperforms and reaches a 2.0 M peak alert with a 258.3-s maximum processing time. Regarding BoTIoT, both engines work better against DoS/DDoS assaults based on TCP and UDP, with peak warning percentages in the 90 s range.

In the work by Razaque et al. [65], software-defined networking (SDN) and virtual network function (VNF) technologies are combined to create virtual network function software-defined networking, or VNFSDN. VNFSDN is combined with the prioritized delegated proof of stake (PDPoS) consensus option to counter assaults. This version of blockchain technology solves the scalability problem by giving IoT devices a secure and flexible environment that can be swiftly scaled up or down to meet changing organizational demands. This allows IoT devices to make effective use of available resources. The PDPoS version gives IoT devices the ability to react proactively to possible security risks, minimizing or lessening the effects of cyberattacks. According to the results, the proposed VNFSDN has a 0.08 ms minimum response time. Li et al. [66] used fog/edge computing with federated learning (FL) to counter harmful coding. Their approach removes data and communication restrictions and trains a global optimal model based on scattered datasets of collaborators. Thorough analyses verify that the average cost is 2.7 times higher, the mitigation reaction time is 72% shorter, and the accuracy is 47% greater. Furthermore, the protocol assessment reveals that the FL's detection accuracy is almost 98%, nearly identical to centralized training.

5. Discussion

A quantitative analysis of the detection times for various cybersecurity solutions and IDSs from various manufacturers is given in Table 2. The detection time varies significantly throughout systems, ranging from milliseconds to seconds, depending on the specific approach and strategy employed. The Naive Bayes classifier with trust value and the smart memory forensics system are two instances of such systems. Both methods have rather quick detection rates; fractions of a second are used for detection. Conversely, more complex systems with longer detection times—measured in seconds—include the cybersecurity-assisted authentication for smart grids and the intelligent phishing detection system (IPDS).

Table 2. Time of detection in different approaches.

Study	Detection Method	Detection Time (s)	Change in Detection Time
Ariyadasa et al. [41]	PhishDet using Long-term Recurrent Convolutional Network	1.8	-
Adebowale et al. [40]	Intelligent Phishing Detection System (IPDS)	25	Increase
Tolba and Al-Makhadmeh [47]	Cybersecurity-assisted authentication for smart grids	4.67	Decrease
Chen et al. [48]	Two-way authentication for smart grids	Variable	Increase (1.4 s)
Sherubha and Mohanasundaram [45]	Naive Bayes classifier with a trust value	27.35	-
Al-Haija [44]	Machine-learning-based XSS detection system	1.031×10^{-4}	-
Naeem et al. [46]	Smart memory forensics system	73 times	Increase
de Araujo-Filho et al. [49]	Unsupervised intrusion prevention system (IPS) for CANs	$<80 \times 10^{-6}$	Decrease
Ilango et al. [51]	FeedForward–Convolutional Neural Network (FFCNN)	3.87×10^{-6}	-
Yang et al. [50]	Enhanced GAN-based IDS	0.12 ± 0.03	Decrease
Maosa et al. [43]	Framework for data gathering	300	Decrease
Ingle and Ingle [52]	BC-Trans Network	225.3	-

The time required to identify threats in cybersecurity operations may be affected by the volume and velocity of incoming data, the degree of automation in the detection process, the quality of the training data used to construct the detection model, and the complexity of the detection algorithm. Sophisticated machine-learning algorithms and deep-learning techniques may necessitate increased processing power and computing resources, potentially resulting in protracted detection durations. Conversely, systems that prioritize efficiency and quickness may be able to detect objects quicker. These systems may incorporate streamlined algorithms or optimized pipelines for data processing.

Reducing the time required to detect threats provides numerous benefits, such as an enhanced overall security stance, increased agility in addressing cyber threats, and reduced potential harm or impact from attacks. Organizations can identify and manage threats more quickly by reducing the time required for hackers to exploit vulnerabilities. This reduces the period during which malicious actors can exploit weaknesses. However, reducing the time required to detect something may increase the computational burden, false positives, and the possibility of missing more sophisticated or subtle attacks that require more time to detect.

However, delaying threat detection allows for a more thorough investigation and verification, reducing false positives, and improving threat detection precision. However, extending detection may delay cyber incident response, giving hackers more time to access networks and commit crimes. Prolonging detection time may also strain resources and operational efficiency, hindering the organization's capacity to manage and mitigate cyber threats. Detection speed and accuracy must be balanced to design successful cyber protection methods.

Table 3 provides a comparative analysis of response times across various cyber-defense systems and intrusion detection techniques. Response times range from fractions of a second to several seconds, depending on the complexity of the system and the efficiency of the detection methodology employed. For instance, systems like the Blockchain-based decoy system and the quantum programming algorithm demonstrate exceptionally fast response times, with most executions completing in less than a second. On the other hand, more complex systems like the Blockchain-transformer hybrid network and the adaptive multi-scale dual attention network exhibit slightly longer response times. However, they are still within acceptable limits for effective cyber-defense operations.

Table 3. Response time comparison of cybersecurity solutions.

Study	Proposed Methodology	Response Time Metrics
Prabakaran et al. [54]	Deep-learning-based phishing detection using DNN and VAE	1.9 s
Shukla et al. [55]	Machine-learning-based anti-phishing detection using HTTP headers	1.57 s
Ariyadasa et al. [56]	SmartiPhish: Anti-phishing solution with continuous learning	4.3 s
Altamimi et al. [53]	PhishCatcher: Client-side defense mechanism using machine learning	62.5×10^{-3} s
Basuki and Adriansyah [57]	Vulnerability management system with scenario planning and benchmarking	<6 s
Soundararajan et al. [58]	BC-CS-AMSDAN-QFOMM-WCN: Adaptive multi-scale dual attention network with Quaternion fractional order Meixner moments	36.51%, 13.09%, and 22.24% minimum delay
Vasylyshyn et al. [60]	Blockchain-based decoy system for detecting cybercrime	At 2 Mbps, a DDoS assault impacts response time, with dynamic hosts consistently faster than static hosts between 2 and 4 Mbps.
Lee et al. [61]	Optimization of lightweight hash functions for high-performance data integrity tests	Ranged from 70 Gbps to 1000 Gbps
Benlloch-Caballero et al. [62]	Cognitive closed-loop system for self-protection against DDoS attacks	18 s
Pourvahab and Ekbatanifard [63]	Digital forensic architecture for IaaS clouds using Blockchain and SDN	75×10^{-3} s
Nasir et al. [64]	BTC_SIGBDS: Blockchain-powered, Trustworthy, Collaborative, Signature-based Botnet Detection System	298.5 s
Razaque et al. [65]	Virtual network function software-defined networking (VNFSDN)	0.08×10^{-3} s
Li et al. [66]	Federated learning for harmful coding detection using fog/edge computing	72% shorter

Cyber-defense reaction time depends on the detection algorithm's computing complexity, the volume and velocity of incoming data, data processing and analysis pipelines, and detection automation. Systems prioritizing efficiency and speed, such as streamlined algorithms or enhanced data processing, have faster reaction times. Computing resources like memory and processing power can also affect reaction times, with faster systems analyzing and making judgments. Optimizing cyber-defense reaction time reduces attack damage, improves security, and speeds up threat identification and mitigation. By recognizing and addressing risks faster, firms may decrease the window of opportunity for attackers to exploit vulnerabilities. Reaction-time optimization has downsides, including higher false-positive rates, processing costs, and the risk of ignoring more complicated or subtle threats that require longer to identify and neutralize.

6. Conclusions and Future Work

The findings emphasize reducing detection and reaction times to improve cybersecurity. Supporting research demonstrates that solutions with high accuracy and short detection periods can stop phishing attempts. Machine-learning-based solutions have shown promise in reducing reaction time and improving detection precision.

Research on cybersecurity-assisted authentication for smart grids shows that faster attack detection speeds up reaction times, limiting their damage. Data from unsupervised intrusion-prevention systems for automotive control networks emphasizes early cyber threat identification for mitigation and response.

Although rapid detection provides agility in threat identification, as illustrated by the Naive Bayes classifier with trust value and the smart memory forensics system, it may necessitate greater computational resources. On the contrary, postponing detection

permits a more comprehensive verification process, which may result in a decrease in false positives but prolongs the timeframe during which cyber assailants can exploit vulnerabilities. Research has demonstrated the importance of response times, as evidenced by the implementation of streamlined algorithms and systems that prioritize efficiency in order to mitigate threats more quickly. To efficiently manage cyber risks while reducing operational burden and resource consumption, optimization endeavors must strike a balance between speed and precision.

Despite cybersecurity advances, many issues persist. The ever-changing cyber threat scenario needs continual detection and response protocol enhancement. Keeping cybersecurity systems scalable, interoperable, and resilient in the face of emerging threats is a problem for researchers and professionals.

Many strategies might be presented to overcome these obstacles and enable further research. Priority should be given to developing robust and adaptable cybersecurity systems that can quickly identify and respond to emerging cyber threats. Cybersecurity specialists, data scientists, and domain-specific experts must work together to solve complex cybersecurity problems by combining their skills and perspectives. Future cyber protection measures may benefit from combining blockchain, artificial intelligence, and peripheral computing. Secure and scalable cybersecurity systems can benefit from peripheral computing, which distributes processing power and storage over numerous devices.

Researchers can also seek funding and collaboration to expand their research. Collaborations with industry, government, and other academic institutions can also help cybersecurity researchers develop practical solutions and innovate. Researchers could assess commercialization and economic development possibilities to assist Commonwealth enterprises and communities. Technology transfer, entrepreneurship, and relationships with local firms and groups may be explored.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Bogatinov, D.S.; Bogdanoski, M.; Angelevski, S. AI-based cyber defense for more secure cyberspace. In *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*; IGI Global: Hershey, PA, USA, 2016; pp. 220–237.
2. Rodrigues, D.; de Rosa, G.H.; Passos, L.A.; Papa, J.P. Adaptive improved flower pollination algorithm for global optimization. In *Nature-Inspired Computation in Data Mining and Machine Learning*; Springer: Cham, Switzerland, 2020; pp. 1–21.
3. Morgan, G.; Gordijn, B. A care-based stakeholder approach to ethics of cybersecurity in business. *Ethics Cybersecur.* **2020**, *21*, 119–138.
4. Winterrose, M.L.; Carter, K.M.; Wagner, N.; Streilein, W.W. Adaptive attacker strategy development against moving target cyber defenses. In *Advances in Cyber Security Analytics and Decision Systems*; Springer: Cham, Switzerland, 2020; pp. 1–14.
5. Maalem Lahcen, R.A.; Caulkins, B.; Mohapatra, R.; Kumar, M. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity* **2020**, *3*, 10. [CrossRef]
6. Taherdoost, H.; Madanchian, M.; Ebrahimi, M. Advancement of Cybersecurity and Information Security Awareness to Facilitate Digital Transformation: Opportunities and Challenges. In *Handbook of Research on Advancing Cybersecurity for Digital Transformation*; IGI Global: Hershey, PA, USA, 2021; pp. 99–117.
7. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur.-Issues Pract.* **2022**, *47*, 698–736. [CrossRef]
8. Riesco, R.; Larriva-Novo, X.; Villagrá, V.A. Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information. *Telecommun. Syst.* **2020**, *73*, 259–288. [CrossRef]
9. Rana, M.U.; Ellahi, O.; Alam, M.; Webber, J.L.; Mehbodniya, A.; Khan, S. Offensive security: Cyber threat intelligence enrichment with counterintelligence and counterattack. *IEEE Access* **2022**, *10*, 108760–108774. [CrossRef]
10. Ayala, C.; Jiménez, K.; Loza-Aguirre, E.; Andrade, R.O. A Hybrid Recommender for Cybersecurity Based on Rating Approach. In *Advances in Cybersecurity Management*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 445–462.

11. Veena, K.; Meena, K.; Kuppusamy, R.; Teekaraman, Y.; Angadi, R.V.; Thelkar, A.R. Cybercrime: Identification and prediction using machine learning techniques. *Comput. Intell. Neurosci.* **2022**, *2022*, 8237421. [CrossRef] [PubMed]
12. Ramakrishnan, S.; Senthil Rajan, A. Network attack detection with QNNBADT in minimal response times using minimized features. In *Computer Networks and Inventive Communication Technologies*; Lecture Notes on Data Engineering and Communications Technologies; Springer: Singapore, 2022; pp. 563–579.
13. Taherdoost, H. Security and internet of things: Benefits, challenges, and future perspectives. *Electronics* **2023**, *12*, 1901. [CrossRef]
14. 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. Geogr. Educ. Online* **2021**, *11*, 956–974.
15. Sarre, R.; Lau, L.Y.-C.; Chang, L.Y. Responding to cybercrime: Current trends. *Police Pract. Res.* **2018**, *19*, 515–518. [CrossRef]
16. Azzedin, F.; Suwad, H.; Rahman, M.M. An Asset-Based Approach to Mitigate Zero-Day Ransomware Attacks. *Comput. Mater. Contin.* **2022**, *73*, 3003–3020. [CrossRef]
17. Biswas, B.; Mukhopadhyay, A.; Kumar, A.; Delen, D. A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. *Decis. Support Syst.* **2024**, *177*, 114102. [CrossRef]
18. Bafna, E. Real Time Cloud Based Intrusion Detection. In *Deep Learning Approaches to Cloud Security*; Wiley: Hoboken, NJ, USA, 2022; pp. 207–224.
19. Khraisat, A.; Alazab, A. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2021**, *4*, 18. [CrossRef]
20. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 20. [CrossRef]
21. Maleh, Y.; Alazab, M.; Tawalbeh, L.; Romdhani, I. *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*; CRC Press: Boca Raton, FL, USA, 2023.
22. Pendleton, M.; Garcia-Lebron, R.; Cho, J.-H.; Xu, S. A survey on systems security metrics. *ACM Comput. Surv. (CSUR)* **2016**, *49*, 62. [CrossRef]
23. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
24. Chaudhary, S.; Gkioulos, V.; Katsikas, S. Developing metrics to assess the effectiveness of cybersecurity awareness program. *J. Cybersecur.* **2022**, *8*, tyac006. [CrossRef]
25. Ait Maalem Lahcen, R.; Mohapatra, R.; Kumar, M. Cybersecurity: A survey of vulnerability analysis and attack graphs. In *Mathematics and Computing: ICMC 2018, Varanasi, India, 9–11 January 2018*; Selected Contributions 4; Springer: Singapore, 2018; pp. 97–111.
26. Dodge, C.; Burruss, G. Policing cybercrime: Responding to the growing problem and considering future solutions. In *The Human Factor of Cybercrime*; Routledge: London, UK, 2019; pp. 339–358.
27. UK HMIC. *Real Lives, Real Crimes: A Study of Digital Crime and Policing*; HMIC: London, UK, 2015.
28. Guedes, I.; Martins, M.; Cardoso, C.S. Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Secur. J.* **2023**, *36*, 472–497. [CrossRef]
29. Abu-Ulbeh, W.; Altalhi, M.; Abualigah, L.; Almazroi, A.A.; Sumari, P.; Gandomi, A.H. Cyberstalking victimization model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations. *Electronics* **2021**, *10*, 1670. [CrossRef]
30. Marttila, E.; Koivula, A.; Räsänen, P. Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. *Am. J. Crim. Justice* **2021**, *46*, 862–881. [CrossRef]
31. Miró-Llinares, F.; Moneva, A. Environmental criminology and cybercrime: Shifting focus from the wine to the bottles. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 491–511.
32. *Cost of a Cyber Incident: Systematic Review and Cross-Validation*; Cybersecurity & Infrastructure Security Agency: Washington, DC, USA, 2021.
33. Robalo, T.L.A.; Abdul Rahim, R.B.B. Cyber victimisation, restorative justice and victim-offender panels. *Asian J. Criminol.* **2023**, *18*, 61–74. [CrossRef]
34. Jansen, J.; Leukfeldt, R. Coping with cybercrime victimization: An exploratory study into impact and change. *J. Qual. Crim. Justice Criminol.* **2018**, *6*, 205–228.
35. Safitra, M.F.; Lubis, M.; Fakhrurroja, H. Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability* **2023**, *15*, 13369. [CrossRef]
36. Nugroho, A.; Chandrawulan, A.A. Research synthesis of cybercrime laws and COVID-19 in Indonesia: Lessons for developed and developing countries. *Secur. J.* **2023**, *36*, 651–670. [CrossRef]
37. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics* **2022**, *11*, 198. [CrossRef]
38. Gong, S.; Lee, C. Cyber threat intelligence framework for incident response in an energy cloud platform. *Electronics* **2021**, *10*, 239. [CrossRef]

39. Afzaliseresht, N.; Miao, Y.; Michalska, S.; Liu, Q.; Wang, H. From logs to stories: Human-centred data mining for cyber threat intelligence. *IEEE Access* **2020**, *8*, 19089–19099. [CrossRef]
40. Adebowale, M.A.; Lwin, K.T.; Hossain, M.A. Intelligent phishing detection scheme using deep learning algorithms. *J. Enterp. Inf. Manag.* **2020**, *36*, 747–766. [CrossRef]
41. Ariyadasa, S.; Fernando, S.; Fernando, S. Combining long-term recurrent convolutional and graph convolutional networks to detect phishing sites using URL and HTML. *IEEE Access* **2022**, *10*, 82355–82375. [CrossRef]
42. de Araujo-Filho, P.F.; Naili, M.; Kaddoum, G.; Fapi, E.T.; Zhu, Z. Unsupervised gan-based intrusion detection system using temporal convolutional networks and self-attention. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 4951–4963. [CrossRef]
43. Maosa, H.; Ouazzane, K.; Sowinski-Mydlarz, V. Real-time cyber analytics data collection framework. *Int. J. Inf. Secur. Priv. (IJISP)* **2022**, *16*, 1–10. [CrossRef]
44. Al-Haija, Q.A. Cost-effective detection system of cross-site scripting attacks using hybrid learning approach. *Results Eng.* **2023**, *19*, 101266. [CrossRef]
45. Sherubha, P.; Mohanasundaram, N. An efficient network threat detection and classification method using ANP-MVPS algorithm in wireless sensor networks. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 1597–1606. [CrossRef]
46. Naeem, M.R.; Khan, M.; Abdullah, A.M.; Noor, F.; Khan, M.I.; Khan, M.A.; Ullah, I.; Room, S. A malware detection scheme via smart memory forensics for windows devices. *Mob. Inf. Syst.* **2022**, *2022*, 9156514. [CrossRef]
47. Tolba, A.; Al-Makhadmeh, Z. A cybersecurity user authentication approach for securing smart grid communications. *Sustain. Energy Technol. Assess.* **2021**, *46*, 101284. [CrossRef]
48. Chen, T.; Yin, X.; Wang, G. Securing communications between smart grids and real users; providing a methodology based on user authentication. *Energy Rep.* **2021**, *7*, 8042–8050. [CrossRef]
49. De Araujo-Filho, P.F.; Pinheiro, A.J.; Kaddoum, G.; Campelo, D.R.; Soares, F.L. An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform. *IEEE Access* **2021**, *9*, 166855–166869. [CrossRef]
50. Yang, Y.; Xie, G.; Wang, J.; Zhou, J.; Xia, Z.; Li, R. Intrusion detection for in-vehicle network by using single GAN in connected vehicles. *J. Circuits Syst. Comput.* **2021**, *30*, 2150007. [CrossRef]
51. Ilango, H.S.; Ma, M.; Su, R. A feedforward–convolutional neural network to detect low-rate dos in iot. *Eng. Appl. Artif. Intell.* **2022**, *114*, 105059. [CrossRef]
52. Ingle, D.; Ingle, D. An enhanced blockchain based security and attack detection using transformer in iot-cloud network. *J. Adv. Res. Appl. Sci. Eng. Technol.* **2023**, *31*, 142–156.
53. Altamimi, A.B.; Ahmed, M.; Khan, W.; Alsaffar, M.; Ahmad, A.; Khan, Z.H.; Alreshidi, A. PhishCatcher: Client-Side Defense against Web Spoofing Attacks Using Machine Learning. *IEEE Access* **2023**, *11*, 61249–61263.
54. Prabakaran, M.K.; Meenakshi Sundaram, P.; Chandrasekar, A.D. An enhanced deep learning-based phishing detection mechanism to effectively identify malicious URLs using variational autoencoders. *IET Inf. Secur.* **2023**, *17*, 423–440. [CrossRef]
55. Shukla, S.; Misra, M.; Varshney, G. HTTP header based phishing attack detection using machine learning. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e4872. [CrossRef]
56. Ariyadasa, S.; Fernando, S.; Fernando, S. SmartiPhish: A reinforcement learning-based intelligent anti-phishing solution to detect spoofed website attacks. *Int. J. Inf. Secur.* **2024**, *23*, 1055–1076. [CrossRef]
57. Basuki, A.; Adriansyah, A. Response time optimization for vulnerability management system by combining the benchmarking and scenario planning models. *Int. J. Electr. Comput. Eng.* **2023**, *13*, 561–570. [CrossRef]
58. Soundararajan, S.; Nithya, B.; Nithya, N.; Vignesh, T. Block chain espoused adaptive multi-scale dual attention network with quaternion fractional order meixner moments encryption for cyber security in wireless communication network. *Wirel. Netw.* **2024**, 1–17. [CrossRef]
59. Choi, S.-H.; Youn, J.; Kim, K.; Lee, S.; Kwon, O.-J.; Shin, D. Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement. *Sustainability* **2023**, *15*, 13404. [CrossRef]
60. Vasylyshyn, S.; Susukailo, V.; Opirskyy, I.; Kurii, Y.; Tyshyk, I. A model of decoy system based on dynamic attributes for cybercrime investigation. *East.-Eur. J. Enterp. Technol.* **2023**, *1*, 121.
61. Lee, W.-K.; Jang, K.; Song, G.; Kim, H.; Hwang, S.O.; Seo, H. Efficient implementation of lightweight hash functions on GPU and quantum computers for IoT applications. *IEEE Access* **2022**, *10*, 59661–59674. [CrossRef]
62. Benlloch-Caballero, P.; Wang, Q.; Calero, J.M.A. Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. *Comput. Netw.* **2023**, *222*, 109526. [CrossRef]
63. Pourvahab, M.; Ekbatanifard, G. Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology. *IEEE Access* **2019**, *7*, 153349–153364. [CrossRef]
64. Nasir, M.H.; Arshad, J.; Khan, M.M. Collaborative device-level botnet detection for internet of things. *Comput. Secur.* **2023**, *129*, 103172. [CrossRef]

65. Razaque, A.; Yoo, J.; Bektemyssova, G.; Alshammari, M.; Chinibayeva, T.T.; Amanzholova, S.; Alotaibi, A.; Umutkulov, D. Efficient Internet-of-Things Cyberattack Depletion Using Blockchain-Enabled Software-Defined Networking and 6G Network Technology. *Sensors* **2023**, *23*, 9690. [CrossRef] [PubMed]
66. Li, J.; Lyu, L.; Liu, X.; Zhang, X.; Lyu, X. FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4059–4068. [CrossRef]