JETNR
Journal of Emerging Trends and Novel Research
JETNR.ORG | ISSN : 2984-9276
An International Open Access, Peer-reviewed, Refereed Journal

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: IMPACT, LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

Sunriz Islam[1], Md. Abul Hayat[2], Md. Fokhray Hossain[3]
1Department of Telecommunication and Electronics Engineering, Hajee Mohammad Danesh Science and Technology University
2, 3Department of computer science and engineering, Daffodil International University.

***Abstract**:* Artificial intelligence (AI) is an effective technology that cybersecurity teams may use to better the security posture against a variety of security challenges and cyberattacks. AI helps these teams automate repetitive processes, faster threat detection and response, and improve the accuracy of their actions. This study explores the complex relationship between cybersecurity awareness and AI, examining the potential benefits and drawbacks of using AI to support cybersecurity awareness campaigns. This study paper seeks to offer a thorough grasp of the impact of AI on cybersecurity awareness by a detailed examination of current advancements, case studies, and professional viewpoints.

Keywords: Cyberattacks, Cyber security Awareness, Internet of Things (IoT), IoT Data Security, IoT Data Security, Cybersecurity Education, Cyber Threats, Cybersecurity Policy.

INTRODUCTION

A collection of technologies, procedures, and practices that guard networks, hardware, software, and data against intrusion, damage, and unauthorized access are collectively referred to as cybersecurity [1]. Technological advancements in the digital economy and infrastructure aggravate resulting in a notable increase in cyberattacks that carry grave implications. Additionally, researchers track the evolution of nation-state-affiliated criminal advertising in addition to the increasing sophistication of cyberattacks, which are developing new and intrusive ways to target even the most observant of targets [2]. The amount, scope, and impact of cyberattacks are increasing because of this growth, making intelligence-driven cybersecurity necessary to manage huge data and offer a dynamic defense against changing cyberattacks. To identify, prevent, detect, address, and record cyberattacks to avoid future security incidents, advisory organizations like the National Institute of Standards and Technologies (NIST) are also pushing for the use of more proactive and adaptive approaches [3]. They do this by moving toward real-time assessments, continuous monitoring, and data-driven analysis.

Artificial Intelligence (AI) is a fascinating instrument that can offer analytics and intelligence to defend against constantly changing cyberattacks by quickly analyzing millions of events and monitoring a broad range of cyberthreats to predict and address issues before they arise. Because of this, AI is being incorporated into cybersecurity systems more and more and used for a range of purposes, such as automating security chores or assisting human security teams in their work. Many studies to address issues linked to the identification, protection, detection, reaction, and recovery from cyberattacks have been conducted because of the extended field of cybersecurity and the increasing excitement of researchers from both AI and cybersecurity industries.

AI and cybersecurity awareness together represent a significant breakthrough in how companies defend themselves against the barrage of cyberthreats. This combination has the potential to improve user training and response capabilities while revolutionizing threat detection. Although AI is becoming more and more prevalent in cybersecurity awareness, its impact and limitations are complicated and require careful study. [4]. AI's tailored user education approach also holds great potential for creating a workforce that is security-aware by customizing training materials to meet unique learning requirements and knowledge gaps. These outcomes show how AI can raise cybersecurity awareness and act as a crucial barrier against a dynamic landscape of online threats [5]. Furthermore, the vulnerability of AI systems to hostile attacks highlights a dangerous flaw in which the very instruments of defense could be employed against the defenders. Justice and ethical concerns are brought up by data bias, particularly when AI decisions inadvertently support biased results.

To maximize AI's advantages and minimize its disadvantages as organizations manage these intricate relationships, it's necessary to strike a balance between the technology's promise and its limitations [6]. In recent years, several evaluations on AI applications and cybersecurity have been published [7–10]. To the best of our knowledge, there isn't, however, a thorough analysis that covers current research to explain the specifics of how AI techniques are used and the cybersecurity operations they cover. Therefore, to serve as a resource for upcoming scholars and practitioners, our goal was to present a thorough analysis, an overview of AI use cases in cybersecurity, limitations, and a discussion of the research problems associated with the adaptation and use of AI for cybersecurity. A comparison of the study and review articles over the past few years is displayed in Table 1.

Table 1: Comparison of this review with existing studies.

References	Taxonomy	Use case identification	Classification of defense solution based on the Function	AI domain	SLR	Coverage	Research gaps	Purpose
Wiafe et al. [7]	No	No	No	Yes	Yes	IEEE & ACM digital library	No	Provides an overview of existing research on AI for cybersecurity
Zhang et al. [8]	No	No	No	No	Yes	Google Scholar, SpringerLink, ScienceDirect, IEEE & ACM digital library	No	Provides a review constrained to the application of AI in the areas of user authentication, dangerous behavior monitoring, network situation awareness, & identification of abnormal traffic
Torres et al. [9]	No	No	No	No	No	Nill	No	Reviews the application of machine learning techniques in spam,

								malware, and phishing detection
Truong et al. [10]	No	No	No	No	No	Nill	No	Reviews the application of AI techniques in intrusion, malware, APT and phishing detection
Proposed Study	Yes	Yes	Yes	Yes	Yes	Scopus Database	Yes	Explores research from 2010 to February 2022 related to AI applications for cybersecurity from a descriptive point of view, and a detailed state-of the-art analysis

2. BACKGROUND

The analysis of the background data about the major ideas of this review, including the operational definition of cybersecurity using the NIST cybersecurity framework, is the focus of this part [3]. Use the AI taxonomy put forward by AI Watch [11] to make sense of the various ways AI is being applied to cybersecurity.

2.1. Cybersecurity

Cybersecurity is the field of safeguarding programs, networks, and systems from online threats. Typically, the goals of these cyberattacks are to disrupt regular corporate operations, obtain, alter, or delete sensitive data, or use ransomware to demand money from customers [12]. To prevent damage, unauthorized use or modification, or exploitation of information and communication systems and the data they contain, cybersecurity implements policies, processes, and technical methods. The situation is made more complicated by the speed at which technology is developing and changing as well as the way that cyberthreats are changing so quickly. AI-based cybersecurity solutions have emerged in response to this unprecedented challenge, assisting security teams in effectively mitigating risks and enhancing security. A widely recognized and unified taxonomy is required to analyze the literature on using AI for cybersecurity because of the diversity of AI and cybersecurity. Researchers and practitioners will be able to better grasp the technical processes and services that require AI to be improved to execute cybersecurity with the aid of this organized taxonomy.

For this reason, the solution categories required to protect, detect, react to, and fight against cyberattacks were understood using a well-known cybersecurity framework that was proposed by NIST [3]. The fundamentals of the NIST cybersecurity framework outline how to strengthen an organization's cybersecurity. The four main components of the framework are the following: categories, subcategories, informative references, and functions. The discovered AI use cases were categorized using the first two tiers of the NIST architecture, which are made up of 23 solution categories and 5 cybersecurity functions. The functions offer a thorough overview of the cybersecurity lifecycle management process. An excellent place to start looking for AI use cases to strengthen cybersecurity is the solution categories provided under each function. The primary goal of choosing these two levels is to offer a simple and understandable classification system for grouping the AI for cybersecurity literature that is currently available into the relevant solution category. According to Fig. 1, the suggested taxonomy includes a third level that is in line with the first two levels by outlining AI-based use cases for every cybersecurity framework level.

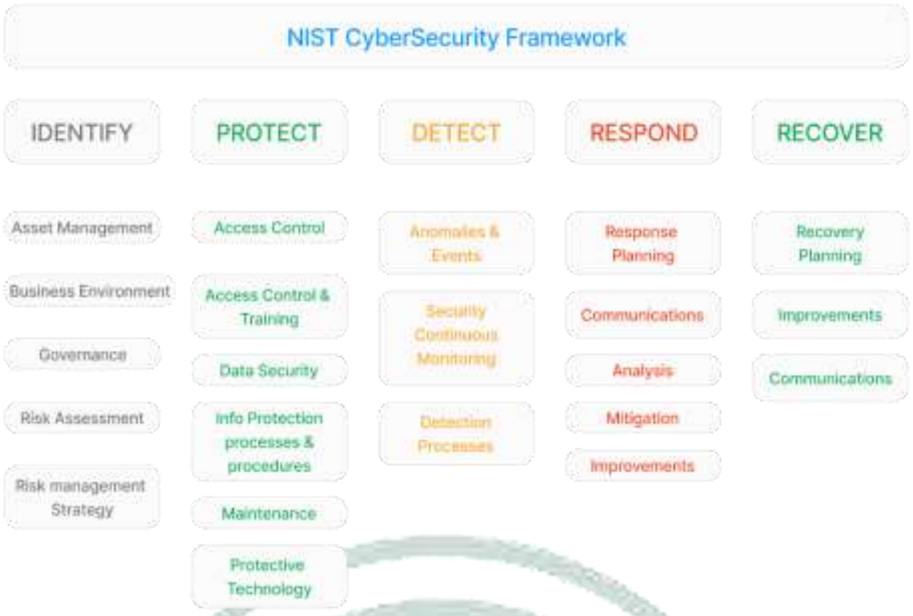


Figure 1: NIST cybersecurity framework.

Cybersecurity is a broad area that encompasses several academic fields. It is composed of seven primary pillars:

- Network Security
- Cloud Security
- Endpoint Security
- Mobile Security
- IoT Security
- Application Security
- Zero Trust

2.2. Artificial intelligence

Artificial intelligence leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind. Artificial intelligence (AI) has been a game-changer in cybersecurity. By offering cutting-edge methods for identifying and reducing cyberthreats, it has completely changed how cybersecurity is approached [13]. AI is becoming a more important tool in cybersecurity strategies for many businesses, and its application in this field is growing quickly.

The size of the global AI in cybersecurity market is anticipated to increase at a compound annual growth rate (CAGR) of 23.3% from $8.8 billion (about $27 per person in the US) (about $27 per person in the US) in 2020 to $38.2 billion (about $120 per person in the US) (about $120 per person in the US) by 2026, according to a report published by MarketsandMarkets.

Traditional cybersecurity mostly depended on signature-based detection methods prior to the development of AI. These systems functioned by comparing the signatures of malicious code or recognized threats in an incoming traffic database. The system would provide an alert and take appropriate action to block or isolate the threat when a match was discovered. Because lawful traffic may be mistakenly identified as malicious if it happens to exhibit characteristics like those of a recognized threat, signature-based detection systems may produce many false positives. This resulted in security analysts devoting a substantial amount of effort to the investigation of false positives, potentially draining available resources. Manual analysis was also used in traditional cybersecurity. Security alarms and logs would be manually examined by security analysts who would search for trends or clues that might point to a security breach.

AI-based cybersecurity solutions are different from conventional methods in several ways. As we just saw, signature-based detection systems, which were limited to detecting known threats, were a major component of traditional cybersecurity tactics. This implied that novel and unidentified dangers might go unnoticed. On the other hand, AI-based solutions make use of machine learning algorithms that are capable of real-time threat detection and response for both known and unexpected threats. To find patterns that are hard for people to see, machine learning algorithms are trained on enormous volumes of data, including historical threat data and data from the network and endpoints. This makes it possible for AI-based systems to recognize dangers and take appropriate action in real-time, all without requiring human involvement. Machine learning algorithms, for instance, can examine network traffic patterns to spot unusual activity that might point to a cyberattack. They can then notify security staff or even initiate automatic actions to mitigate the threat.

The fact that AI-based solutions are built to continuously learn and adapt sets them apart from conventional methods in yet another aspect. The application of AI to cybersecurity signifies a significant change in the way businesses handle cybersecurity. AI domains include, but are not limited to, fuzzy logic, case-based reasoning, genetic algorithm, Bayesian optimization, evolutionary algorithm, planning graph, artificial neural network, deep learning, support vector machine, natural language processing, text mining, sentiment analysis, image processing, sensor networks, object recognition and speech processing. This allows businesses to better protect sensitive information and vital systems.

3. RESEARCH METHODOLOGY

To identify prospective research gaps and highlight emerging areas of knowledge, the SLR attempts to locate, assess, and interpret all the available research in the field of interest. It offers a top-notch, transparent, and repeatable review to condense the numerous researches works. For the following reasons, this study uses an SLR methodology: (i) AI for cybersecurity is a broad topic with a lot of literature; (ii) it tries to address research issues; and (iii) the rigor and reproducibility it offers to produce an objective scientific investigation. A detailed description of the SLR technique is provided below.

3.1. Selection of bibliometric database

Web of Science (WoS) and Scopus are the two most widely used bibliometric databases. Because of has nearly 60% greater coverage than the WoS, the Scopus database was selected for this investigation [14]. Furthermore, because of its more comprehensive coverage, sophisticated search filters, and data analysis grids, Scopus provides superior data management.

3.2. Search strategy

To perform a thorough literature evaluation of the influence of AI on cybersecurity, a comprehensive search for terms relevant to cybersecurity and AI was conducted between November 2021 and February 2022. Well-defined search criteria were used to search, as indicated in **Table 2**. The logical operator was used to combine keywords related to cybersecurity with artificial intelligence. The studies that are connected to any of the terms in each field were found by using the logical OR operator inside the various keywords. In particular, the cybersecurity keywords were extracted from the NIST cybersecurity framework, and the AI keywords match the taxonomy presented by AI Watch.

Table 2: Search string

AI Keywords	Cybersecurity Keywords
("cognitive computing" OR "algorithmic intelligence" OR "neural networks" OR "predictive modeling" OR "automated learning" OR "natural language processing" OR "text analysis" OR "pattern recognition" OR "feature extraction" OR "data mining techniques" OR "sentiment detection" OR "computer vision" OR "data filtering" OR "GAN applications" OR "deep neural networks" OR "reinforcement learning" OR "data-driven approaches" OR "topic modeling" OR "machine reasoning" OR "optimization techniques" OR "computational intelligence" OR "machine perception" OR "automated decision-making" OR "semantic analysis" OR "knowledge discovery" OR "automated problem-solving" OR "intelligent agents")	("cybersecurity") AND ("threat modeling" OR "security policy" OR "security awareness" OR "digital forensics" OR "incident handling" OR "cybersecurity governance" OR "compliance management" OR "security risk assessment" OR "security metrics" OR "security controls" OR "automated vulnerability" OR "vulnerability" OR "fuzzing" OR "penetration" OR "identity and access management" OR "cloud security" OR "IoT security" OR "endpoint security" OR "network security" OR "data protection" OR "secure coding" OR "security architecture" OR "security awareness" OR "risk mitigation" OR "security auditing" OR "security training" OR "security assessment" OR "cybersecurity standards" OR "security best practices" OR "ethical hacking")

3.3. Criteria for inclusion and exclusion

After the search phase, the studies that were found were filtered to exclude any irrelevant research. To locate the relevant publications that deal with the study topics, inclusion and exclusion criteria used to the earlier stage collected studies.

Inclusion Criteria:

1. Articles included in the review must be written in English.
2. Only full research papers, excluding presentations or supplements to posters, are considered.
3. Emphasis on artificial intelligence (AI) as a primary focus or significant inclusion in the methodology is required.
4. The selected articles should directly address one or more of the research questions posed in this study.
5. In cases where studies appear in multiple journals or conferences, only the most recent version is considered.

Exclusion Criteria:

1. Studies not presented in the English language are excluded.
2. Articles offering a comprehensive review or survey of AI in various cybersecurity domains are not included.
3. Duplicate articles, representing the same work by authors in different conferences or journals, are filtered out.
4. Articles providing a comparative analysis of different AI models or existing cybersecurity techniques are excluded.
5. Articles focused on enhancing the security of AI techniques to resist attacks are not considered.
6. Papers providing sole recommendations, guidelines, or principles for cybersecurity (non-scientific) are excluded.
7. Editorials, books, chapters, summaries of workshops, and symposiums are not included in the review.
8. Studies lacking sufficient information are excluded.
9. Studies for which a full text cannot be located are not considered.

4. CYBERSECURITY USES THE MOST RECENT AI DEVELOPMENTS

Cybersecurity literature is arranged on the first level according to five main functions: identify, protect, detect, respond, and recover, demonstrate in **figure1**. These five cybersecurity functions range from the use of AI to stop security attacks to a more sophisticated mechanism that actively searches for new threats and counterattacks.

4.1 Threat Detection and Prevention

An organization's capacity to keep an eye on activities within its IT environment and identify actual security incidents is known as threat detection. The capacity to stop specific risks before they harm the environment or infiltrate it is known as threat prevention. Real-time threat detection is a prerequisite for preventing threats, therefore the two go hand in hand. Carrying out a comprehensive risk assessment is the first step towards danger detection and prevention. Finding potential risks, weaknesses, and threats that might affect the organization's information systems is part of this process. This entails determining possible points of attack, estimating the probability of a breach, and analyzing the possible consequences for the company. Once the risks have been identified, it is critical to assess and rank them according to likelihood of occurrence and possible impact. This will assist companies in concentrating their efforts on resolving the biggest dangers and weaknesses first. There are several techniques for prioritizing risks, including qualitative analysis, quantitative risk assessments, and combinations of the two.

4.2 Behavioral Analytics

The tracking, gathering, and evaluation of user data and behaviors using monitoring systems is known as user behavior analytics (UBA). Since users are only one type of entity with observable behaviors on contemporary networks, UBA is frequently referred to as user and entity behavior analytics (UEBA). Processes, apps, and network devices are examples of additional entities. To detect traffic patterns brought on by user behavior, both benign and malevolent, UBA technologies examine past data logs, including network and authentication logs gathered and kept in log management and security information and event management (SIEM) systems [15]. The main purpose of UBA and UEBA systems is to give cybersecurity teams useful information when they see anomalous activity.

For UEBA to function, it must gather a variety of data, including user roles and titles, access, accounts, and permissions; user activity and location; and security alerts. The study considers variables including the resources consumed, the length of sessions, connectivity, and peer group activity to compare aberrant behavior to. This data can be gathered from both past and present activity. When modifications are made to the data, such as promotions or new permissions, it also updates automatically. The typical behaviors that UBA and UEBA systems keep an eye on are those linked to certain attacks or other security incidents. Brute-force assaults, inappropriate data access, data loss, unauthorized users moving laterally, and dubious actions by privileged users who might be malevolent insiders are among the behaviors that are monitored.

UBA systems can decrease false positives and give cybersecurity teams more precise, actionable risk intelligence by utilizing machine learning algorithms.

4.3 Predictive Analysis

Predictive analytics analyzes prior data and forecasts future events by using several methods, including statistical modeling, machine learning, and data mining. Network managers can take proactive steps to stop problems before they start by utilizing this potent technology to obtain insightful information on the security, performance, and overall health of their networks. Predictive analytics is a tool that AI uses to forecast possible dangers based on past data and new patterns. AI can identify weaknesses that could be exploited in the future by analyzing large datasets, which enables enterprises to take preventive measures.

4.4 Automated Incident Response

Automation, artificial intelligence, and machine learning are all applied to the incident response process, which is incident response automation. By using automation to eliminate many of the conventional pain points from an organization's incident response process, automated incident response essentially increases efficiency.

The following are some advantages of automating incident response:

1. Considerably quicker correction and response
2. Less work for the incident responders and security personnel
3. Reduced MTR, or mean time to resolution
4. Increased awareness of the IT infrastructure
5. Decreased possibility of human error
6. Improved and more successful reaction techniques
7. Reduced expenses

Cyber threat intelligence and data from inside your own company power incident response automation. Large amounts of data are ingested, orchestrated, and analyzed by it for insights that enable it to handle and minimize catastrophes significantly faster than any person. An automated incident response platform may use the following tools to gather data:

- Network and application logs
- Intrusion prevention and intrusion detection systems
- External threat intelligence
- Identity and Access Management (IAM) tools
- Endpoint protection tools
- Data feeds from SIEM/SOAR
- Third-party sources such as vendors and business partners

4.5 Security Information and Event Management (SIEM)

A security system called security information and event management, or SIEM, assists companies in identifying and resolving any security threats and vulnerabilities before they have an opportunity to interfere with day-to-day operations. SIEM solutions assist business security teams in identifying abnormalities in user behavior and in automating many of the laborious tasks related to threat detection and incident response using artificial intelligence (AI) [16].

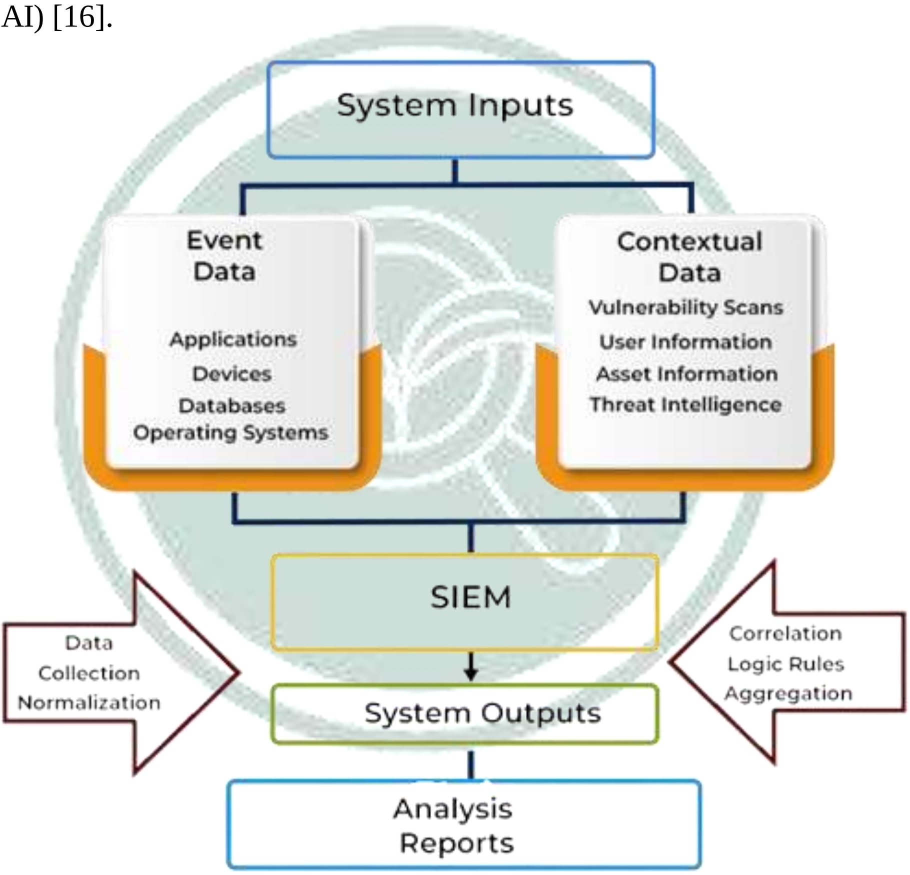


Figure 2: Architecture of SIEM

All SIEM solutions, at their most basic, carry out some degree of data consolidation, aggregation, and sorting operations to detect threats and fulfill data compliance obligations. While the capabilities of certain systems differ, the majority provide the same essential features.

Log Management: Event data is ingested by SIEM from a variety of sources throughout the whole IT infrastructure of a company, including cloud and on-premises settings. Real-time event log data is gathered, correlated, and analyzed from users, endpoints, apps, data sources, cloud workloads, networks, and security hardware and software like firewalls and antivirus programs.

Event Correlation and Analytics: Any SIEM solution must provide event correlation. By applying sophisticated analytics to recognize and comprehend complex data patterns, event correlation offers valuable information that can be used to promptly identify and address possible security risks to a company. By offloading the laborious manual workflows connected to the in-depth analysis of security events, SIEM solutions greatly increase the mean time to detect (MTTD) and mean time to response (MTTR) for IT security teams.

Incident Monitoring and Security Alerts: Security teams use SIEM to compile their analysis into a single, central dashboard from which they can monitor activity, prioritize warnings, spot dangers, and start responding or fixing issues. To assist security analysts in identifying patterns or spikes in suspicious behavior, the majority of SIEM dashboards also feature real-time data visualizations. Administrators can be promptly warned and take appropriate action to reduce vulnerabilities before they materialize into more serious security issues by using predefined, customized correlation criteria.

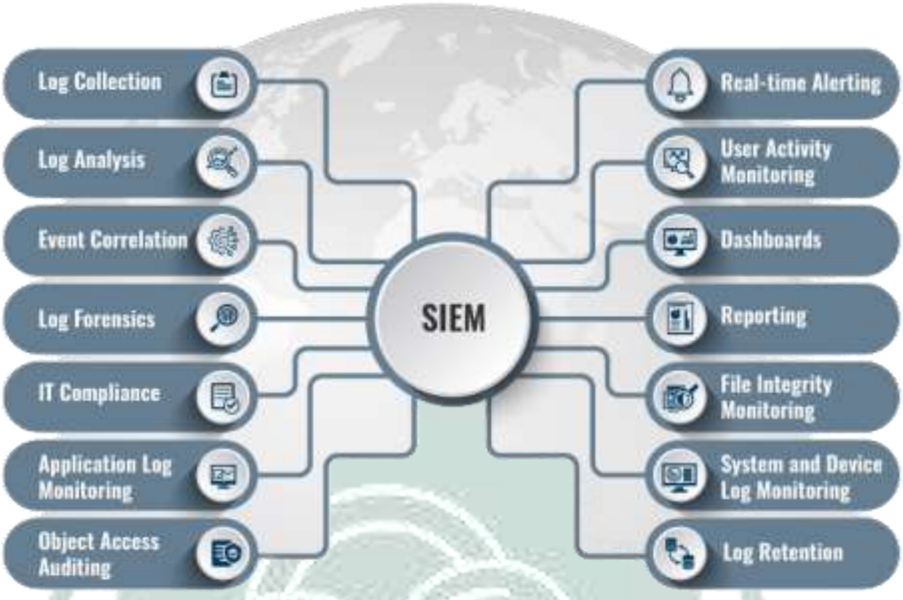


Figure 3: Components and Capabilities of SIEM

Benefits of SIEM

- Real-time threat recognition
- AI-driven automation
- Improved organizational efficiency
- Detecting advanced and unknown threats
- Conducting forensic investigations
- Assessing and reporting on compliance
- Monitoring Users and Applications

Future SIEM systems will rely more and more on AI as cognitive skills enhance the system's ability to make decisions. Additionally, it will enable systems to expand and adjust as endpoint counts rise. Artificial Intelligence (AI) presents the possibility of a solution that supports more data types and a sophisticated understanding of the threat landscape as it changes, as IoT, cloud computing, mobile, and other technologies increase the amount of data that a SIEM tool must consume.

4.6 Endpoint Security

Preventive endpoint protection and a novel type of continuous detection and response capabilities are combined in endpoint security. Systems for securing endpoints are engineered to promptly identify, evaluate, prevent, and mitigate active threats. They must work together with other security technologies to accomplish this, providing administrators with visibility into sophisticated threats to expedite the timeframes it takes to detect and address them. Traditional antivirus software has given way to endpoint security, which now offers complete defense against sophisticated malware and emerging zero-day threats.

For several reasons, an endpoint protection platform is essential to business cybersecurity. In today's corporate environment, data is a company's most important asset, and losing access to our data itself might put the entire enterprise at risk of going bankrupt. Additionally, as hackers constantly devise new methods to obtain access, steal data, or coerce staff members into disclosing important information, the danger landscape is growing more complex. When you consider the potential, the expense of shifting resources from achieving business objectives to countering threats, the damage a large-scale breach would do to one's reputation, and the real monetary cost of noncompliance, it's simple to understand why endpoint protection platforms are now considered essential for protecting contemporary businesses [17].

An endpoint is a device that is connected to a network. The number of unique devices linked to an organization's network can easily reach the tens (or even hundreds) of thousands, given the increasing prevalence of BYOD (bring your own device) and IoT (Internet of Things).

Endpoints can include the gadgets that are more widely recognized, like: Tablets, Mobile devices, ATM machines, Smart watches, Servers, Medical devices etc.

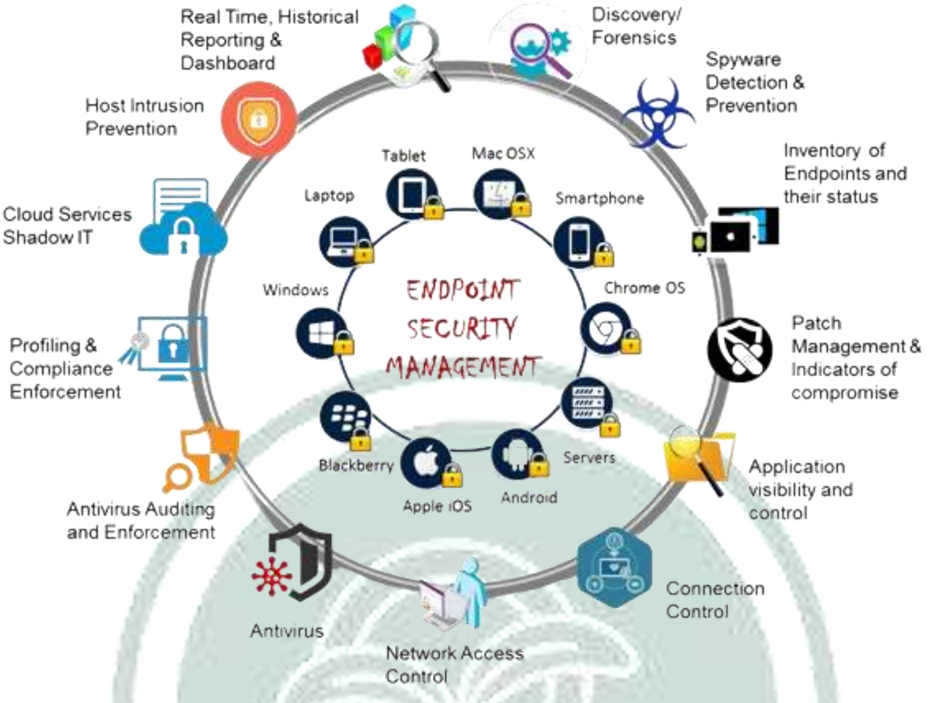

Real Time, Historical Reporting & Dashboard
Discovery/ Forensics
Spyware Detection & Prevention
Inventory of Endpoints and their status
Patch Management & Indicators of compromise
Application visibility and control
Connection Control
Network Access Control
Antivirus
Antivirus Auditing and Enforcement
Profiling & Compliance Enforcement
Cloud Services Shadow IT
Host Intrusion Prevention
Tablet
Mac OSX
Smartphone
Chrome OS
Servers
Android
Apple iOS
Blackberry
Windows
Laptop
ENDPOINT SECURITY MANAGEMENT

Figure 4: Endpoint Security Management

Endpoint security components

- Using machine learning classification to quickly identify zero-day threats
- Preventive web security to guarantee secure online browsing
- To stop data loss and exfiltration, data classification and loss prevention are necessary.
- Firewall integrated to prevent malicious network assaults
- Email gateway to stop attempts at social engineering and phishing that target your staff
- Encryption of disks, emails, and endpoints to stop data theft
- Protection against unintentional and intentional acts with insider threat intelligence

Endpoint security vs Network security: Antivirus software is made to protect a single endpoint and provides visibility into it, often only from that endpoint. On the other hand, endpoint security software views the business network holistically and provides a single point of access to all connected endpoints.

Table 3: Enterprise vs. Consumer Endpoint Protection

Protection of Enterprise Endpoint Security	**Protection of Consumer Endpoint Security**
Consumer Endpoint Security Protection	Only a few single-user endpoints must be managed.
Improved at overseeing various endpoint collections	Necessary for managing a limited quantity of endpoints with a single person
Central management hub software	Endpoints individually set up and configured
Remote administration capabilities	Rarely requires remote management
Configures endpoint protection on devices remotely	Configures endpoint protection directly to device
Deploys patches to all relevant endpoints	User enables automatic updates for each device
Requires modified permissions	Uses administrative permissions
Ability to monitor employee devices, activity, and behavior	Activity and behavior limited to sole user

4.7 Network Security

Network security is the process of preventing theft, misuse, and unauthorized access to the underlying networking infrastructure. To ensure that people, devices, apps, and applications operate securely, a secure infrastructure must be built. Several levels of defense are combined in the network and at the edge to create network security. Policies and controls are implemented at each tier of network security. Network resources are accessible to authorized users, but bad actors are prevented from executing threats and exploits. The digital age has changed the globe. Our way of living, working, playing, and learning has evolved. Any company that wants to provide the services that both clients and staff require needs to safeguard its network. Additionally, network security aids in preventing attacks on proprietary data. In the end, it safeguards your reputation.

Types of network security

Firewalls: Network traffic is managed by firewalls using pre-established security rules. Firewalls are an essential component of everyday computing since they filter out malicious communications. Firewalls play a major role in network security, particularly Next Generation Firewalls, which concentrate on thwarting malware and application-layer attacks.

Workload security: Workloads migrating across various clouds and hybrid environments are safeguarded by workload security. The greater attack surfaces of these dispersed workloads need to be safeguarded without compromising the business's agility.

Zero Trust Network Access (ZTNA): According to the zero-trust security methodology, a user should only be granted the access and authorization necessary for them to carry out their duties. Compared to standard security solutions, such as VPNs, which give users complete access to the target network, this is a fundamentally different approach. Software-defined perimeter (SDP) solutions, sometimes referred to as zero trust network access (ZTNA), allow people who need that access to carry out their job responsibilities to have specific access to an organization's applications.

Email Security: Any procedures, goods, and services intended to keep your email accounts and content safe from outside threats are referred to as email security. Although the built-in email security mechanisms of most email service providers are intended to keep you safe, they might not be sufficient to prevent hackers from accessing your data.

Data Loss Prevention (DLP): To prevent sensitive information from being exposed outside of an organization, particularly regulated data like personally identifiable information (PII) and compliance-related data like HIPAA, SOX, PCI DSS, etc., data loss prevention, or DLP, is a cybersecurity methodology that combines technology and best practices.

Sandboxing: Sandboxing is a cybersecurity technique in which files are opened or code is performed on a host computer that simulates end-user operating environments in a secure, isolated environment. To keep threats off the network, sandboxing watches the code or files as they are opened and searches for harmful activity. Before the files reach an unwary end user, malware, for instance, can be safely recognized and prevented in formats like PDF, Microsoft Word, Excel, and PowerPoint.

Cloud Network Security: These days, workloads and applications are not just hosted locally in a data center on-site. To keep up with the shift of application workloads to the cloud, modern data center protection demands increased adaptability and creativity. Firewall-as-a-Service (FWaaS) deployments in private, public, hybrid, and cloud environments are made possible by software-defined networking (SDN) and software-defined wide area network (SD-WAN) solutions.

VPN: The connection between an endpoint and a network, frequently via the internet, is encrypted using a virtual private network. IPsec or Secure Sockets Layer is typically used by a remote-access VPN to authenticate communication between a device and the network.

Access control: Your network should not be accessible to every user. You need to identify every user and every device to keep out any attackers. You can then put your security policies into effect. Noncompliant endpoint devices might either have their access restricted or blocked. Network access control (NAC) is this process.

Application security: Whether it is purchased or developed by your IT department, any software that powers your company must be secured. Unfortunately, any program could have security flaws that hackers could use to access your network. Application security includes the software, hardware, and procedures you employ to plug those gaps.

Behavioral Analytic: Normal behavior must be recognized to identify anomalous network behavior. Using behavioral analytics, activities that are out of the ordinary are automatically detected. It will then be easier for your security staff to spot possible issues and swiftly eliminate risks if there are signs of compromise.

Data loss prevention: Employers are responsible for ensuring that personnel do not transmit confidential information outside of the network. Data loss prevention (DLP) technology can prohibit users from sending, downloading, or even printing important documents in an unsafe way.

Mobile device security: Mobile apps and gadgets are becoming a more frequent target for cybercriminals. Ninety percent of IT businesses might enable corporate applications on personal mobile devices during the next three years. Naturally, you must manage which devices are able to connect to your network. Additionally, you must set up their connections to allow private network traffic.

Security information and event management: SIEM Products compiles the data required by the security team to recognize and address risks. These goods are available in multiple formats, such as server software and appliances that are both virtual and physical.

Wireless security: Wired networks offer greater security than wireless ones. Installing a wireless LAN might be likened to placing Ethernet ports everywhere, including the parking lot, if strict security measures are not taken. Products made specially to safeguard wireless networks are required to stop an exploit from spreading. Strong network security will prevent ransomware, viruses, worms, trojans, spyware, and adware.

4.8 Cloud Security

The cybersecurity guidelines, best practices, controls, and technology used to safeguard data, applications, and infrastructure in cloud settings are collectively referred to as cloud security [18]. Cloud security specifically aims to provide disaster recovery, access management, data governance and compliance, storage and network protection against external and internal threats. The collection of cybersecurity safeguards used to safeguard cloud-based infrastructure, data, and applications is known as cloud security. This involves protecting cloud environments against internal risks, illegal access, and online attacks by implementing security policies, practices, controls, and other technologies including identity and access management and data loss prevention systems.

The primary focus of cloud security is on integrating policies, procedures, and technological tools to guarantee data security, facilitate regulatory compliance, and give users and devices control over privacy, access, and authentication.

Cloud service providers (CSPs) usually operate under a shared responsibility paradigm, which implies that you, the client, and the cloud provider share responsibility for putting cloud computing security into practice. In general, the customer is required to secure everything that operates "in" the cloud, including network controls, identity and access management, data, and applications, but the CSP is always in charge of the cloud and its fundamental infrastructure. Depending on the cloud computing service model you choose and the service provider, different shared responsibility models apply; the more the provider handles, the more they may safeguard.

Cloud computing service models are Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). Businesses can enhance their overall security posture by taking advantage of the numerous benefits that cloud computing security offers. The best cloud providers include multi-factor authentication, encryption, zero-trust network architecture, identity and access management, and continuous logging and monitoring in addition to secure-by-design infrastructure and layered security that are integrated into the platform and its services. Additionally, you can automate and manage security on a massive scale with the aid of the cloud. Other common cloud security benefits include Greater visibility, Centralized security, Reduced costs, Data protection, Cloud compliance and Advanced threat detection.

Most businesses will probably encounter cloud security issues, such as: Lack of visibility, Misconfigurations, Access managements, Dynamic workloads, Compliance.

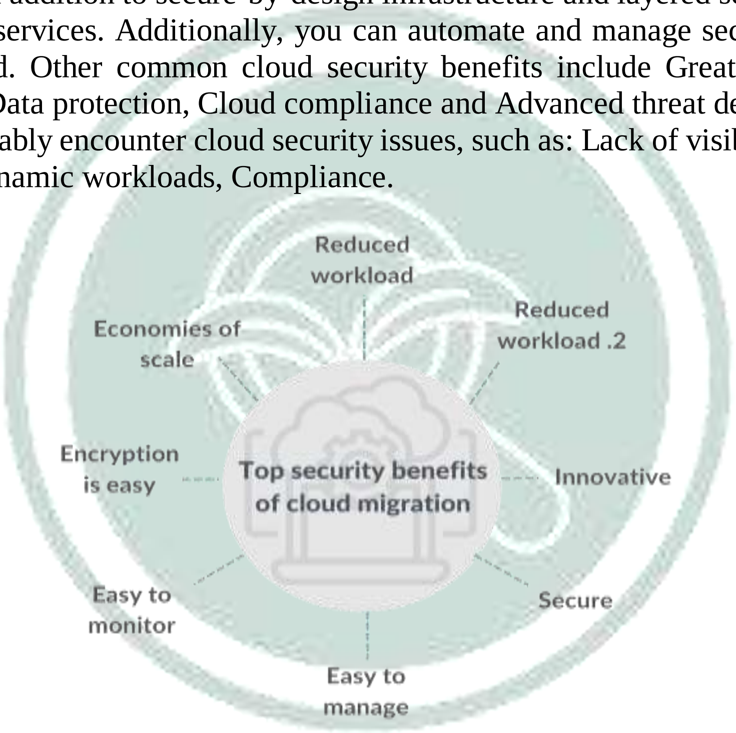


Figure 5: Benefits of Security in Cloud Computing

As new security risks surface, cloud security is always changing and adapting. Because of this, there are a wide variety of cloud security solutions on the market right now; and the list below is by no means exhaustive:

- Identity and access management (IAM)
- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Public key infrastructure (PKI)

4.8 Vulnerability Assessment and Management

The process of testing to find and classify security flaws in order of severity within a certain time limit is called a vulnerability assessment. A focus on thorough coverage and a range of automated and manual procedures may be used in this process [19]. Vulnerability assessments employing a risk-based methodology can focus on several technology levels; host, network, and application-layer assessments are the most popular types.

There are two ways to characterize a vulnerability:

1. A weakness in software architecture or a defect in the code that can be used to hurt people. An authenticated or unauthenticated attacker may be the source of the exploit.
2. A security breach might arise from a vulnerability in internal controls or a gap in security processes that can be exploited.

There are three primary objectives of a vulnerability assessment:

1. Find weaknesses that range from serious design errors to straightforward configuration errors.
2. To make it easier for developers to find and replicate the findings, document the vulnerabilities.
3. Provide instructions to help developers fix the vulnerabilities that have been found.

Vulnerability management involves the ongoing process of recognizing, evaluating, addressing, and reporting security vulnerabilities in systems and associated software. While it bears resemblance to vulnerability assessment, the crucial distinction lies in its continuous nature. Unlike vulnerability assessment, which primarily identifies and categorizes risks in network infrastructure, vulnerability management extends the process by incorporating decisions on whether to remediate, mitigate, or accept these risks. Additionally, vulnerability management encompasses broader concerns such as general infrastructure enhancement and comprehensive reporting.

The vulnerability management cycle includes vulnerability assessments, and the virtual machine (VM) cycle needs to be a crucial element of your NetOps team's security plan. Today's organizations just cannot afford to overlook the security vulnerabilities in their network architecture. Teams struggle to maintain network visibility as networks get more complicated. Threat actors seeking to take advantage of system vulnerabilities will find this to be the perfect scenario. Often, risks and attacks go unnoticed until they've caused irreparable damage at considerable cost to the organization.

Benefits of virtualization go beyond security. For instance, doing routine assessments of the hardware and software on your network can assist your team in locating out-of-date software or possible updates that could enhance both the overall security and efficiency of the network. Additionally, VM can assist your company in adhering to internal and external compliance standards. Your company can avoid fines and other penalties for noncompliance by routinely detecting and mitigating risks using vulnerability assessments and the virtual machine cycle.

With the obvious benefits, it should be clear that vulnerability assessment and vulnerability management are crucial to reducing overall risk in an organization's infrastructure.

4.9 Phishing Detection

Phishing is a cybercrime that involves using fake emails, texts, and websites to get sensitive data, including credit card numbers and passwords, among other personal information. Phishing assaults have grown more complex because of the expansion of the internet and online transactions, making it more challenging for people to identify them and stay clear of them. The process of spotting phishing assaults early on, alerting administrators and users, and, ideally, reducing the threat is known as phishing detection. Phishing detection is always changing because attackers are always coming up with new strategies.

When it comes to identifying phishing websites, machine learning can be a useful tool. Machine learning algorithms can differentiate between authentic and fake websites by use of extensive dataset training. As a result, efficient phishing detection systems that can recognize and alert users to potentially hazardous websites may be developed.

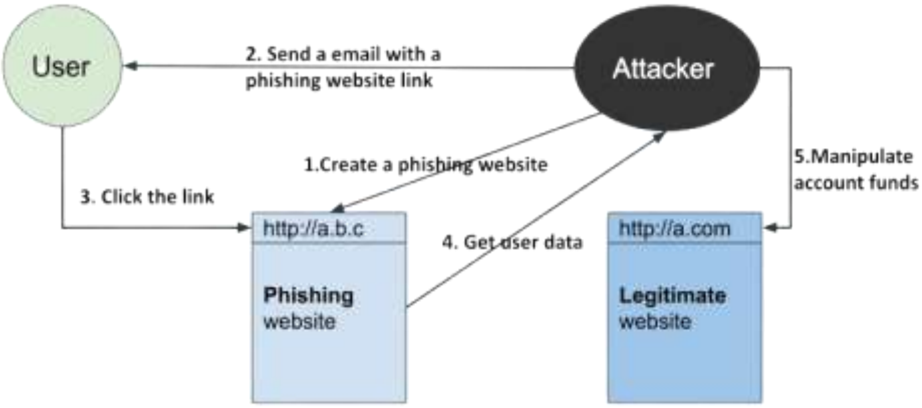


Figure 6: Phishing life cycle

Machine learning can help detect phishing attacks by leveraging its ability to learn patterns and identify anomalies in data. It can be applied to build models that automatically distinguish between dangerous and legitimate websites, emails, and other types of correspondence. ML can be applied in several ways to identify phishing attack.

Domain analysis: ML models may detect anomalies and disparities that might point to a phishing attempt by examining the SSL certificates and domain data of websites. Red flags include, but are not limited to, a short domain registration period, a freshly registered domain, and the absence of an SSL certificate.

URL analysis: To identify suspicious elements like abnormally long URLs, the use of special characters, or the existence of several subdomains, machine learning models can examine the structure and content of URLs. These features may assist in the model's ability to distinguish between trustworthy and fraudulent websites.

Text analysis: Machine learning can analyze text on webpages or in emails to find patterns that are frequently connected to phishing scams. These consist of suspicious terms, expressions, or connections that could indicate a phishing attempt.

Email header analysis: Machine learning (ML) may look at email headers to find sender information that raises red flags, such spoofing email addresses, anomalies in the "from" or "reply-to" sections or using public email services for messages that are supposedly official.

Behavior analysis: Using data from mouse movements, click patterns, and keystroke dynamics, machine learning (ML) can be used to examine user behavior and spot variations from the norm that can point to a phishing attempt.

Image analysis: Machine learning (ML) models, like convolutional neural networks (CNNs), can be trained to examine images on websites, like banners and logos, and identify if they are original artwork or have been altered. This might assist in locating fake websites that are employed in phishing scams.

Anomaly detection: Machine learning models can be taught to identify typical activity patterns and highlight deviations or abnormalities that might indicate a phishing attempt. Unusual email sending behaviors, unexpected network traffic, or other anomalous occurrences can be examples of this.

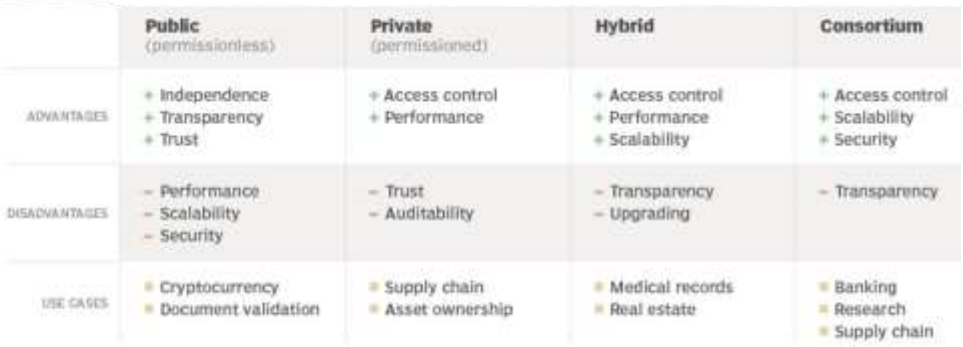
Real-time detection: Since machine learning models can collect and evaluate data instantly, they can be used to quickly identify phishing assaults as soon as they happen. Such attacks can do less damage if they are met with swift action.

ML can be a useful tool for detection and prevention of phishing attacks by combining various methods. But it's crucial to keep in mind that no solution is flawless, and for strong security, a multi-layered strategy combining ML and conventional security measures is necessary.

4.10 Blockchain Security

A blockchain network's entire risk management system is called blockchain security, and it uses cybersecurity frameworks, assurance services, and best practices to mitigate the risk of fraud and attacks. The various types of blockchains can be broadly categorized by their forms of access control.

- There are no limitations on who can access or publish new blocks on a public blockchain, also known as a permission less blockchain. Participants in blockchains may remain anonymous.
- The publication of new blocks is restricted to a private blockchain, commonly referred to as a permissioned blockchain. It may also limit who is able to access the blockchain. Every user on the blockchain needs to be verified and identified. A consortium blockchain or an individual can oversee such a blockchain.
- Interoperable public and private blockchains, or a blockchain of blockchains, are referred to as hybrid blockchains.



	Public (permissionless)	Private (permissioned)	Hybrid	Consortium
ADVANTAGES	+ Independence + Transparency + Trust	+ Access control + Performance	+ Access control + Performance + Scalability	+ Access control + Scalability + Security
DISADVANTAGES	- Performance - Scalability - Security	- Trust - Auditability	- Transparency - Upgrading	- Transparency
USE CASES	▪ Cryptocurrency ▪ Document validation	▪ Supply chain ▪ Asset ownership	▪ Medical records ▪ Real estate	▪ Banking ▪ Research ▪ Supply chain

Figure 7: Types of blockchain technology

Compared to private blockchains, public blockchains are much easier for attackers to target and breach since they are intrinsically open to all users and do not require user identification. The blockchain isn't perfect. Cybercriminals have ways to take advantage of blockchain's weaknesses and do serious harm. Here are four methods blockchain technology can be attacked by hackers.

Phishing attacks: Phishing is a fraudulent attempt to get login credentials from a user. Emails seeming to be from reputable sources are sent by scammers to wallet key owners. The emails employ fictitious hyperlinks to request users' credentials. Both the user and the blockchain network may suffer damages if credentials and other private data are compromised.

Routing attacks: Blockchains depend on large-scale, real-time data transmission. Data that is being transferred to internet service providers can be intercepted by hackers. Blockchain users are usually blind to the threat posed by a routing attack, so everything appears to be normal. On the other hand, fraudsters have secretly taken advantage of currency or private information.

Sybil attacks: Hackers generate and utilize many fictitious network identities in a Sybil attack to overwhelm the network and bring down the entire system. Sybil is the name of a well-known fictional character who has been diagnosed with multiple identity disorder.

51% attacks: A significant amount of processing power is needed for mining, particularly for large-scale public blockchains. However, a miner or group of miners might obtain more than 50% of the mining power in a blockchain network if they could muster enough resources. Possessing more than half the power entitles one to alter and control the ledger. Private blockchains are not vulnerable to 51% attacks.
It is essential to take action to guarantee the security of your blockchain design and surroundings in the modern digital world.

4.11 Supply chain risk management

Decisions on risks that are especially connected to recognizing, evaluating, and controlling supply chain risks are supported by supply chain risk management. A supply chain's ability to effectively address cybersecurity threats depends on thorough analysis of the risks and weaknesses, economical methods for managing supply chain risk, and a measurement of the supply chain's cyber resilience. Artificial intelligence (AI) techniques are being actively used by researchers to automate threat analysis and prediction [20], optimal cybersecurity investment [21–23], and supply chain cyber resilience evaluation [24].

A secure integrated network connecting the subsystems of the incoming and departing chains is necessary for cyber supply chain security. To minimize the disturbance to the organization, it is crucial to comprehend and anticipate risks using both internal and threat intelligence resources. Using machine learning approaches, Yeboah-ofori et al. integrated cyber threat intelligence data to forecast cyberattack patterns on cyber supply chain systems [20].

In Industry 4.0 supply chain cybersecurity, optimizing cybersecurity spending is crucial for prompt detection, mitigation, and budget-balancing of security breaches. To balance supply chain cybersecurity, Sawik [21-23] suggested many approaches to identify the best cybersecurity investment with a constrained budget and a portfolio of security measures.

To reduce or restrict the impact of a potential cybersecurity event, the protect function aids in the planning and implementation of suitable safeguards. To proactively defend against both internal and external cyber threats, this consists of a variety of technical and administrative safeguards. By authenticating users, devices, and other assets, tracking user behavior, automating access control, providing adaptive training, preventing data leakage and integrity monitoring, automating information protection and processes, and offering proactive security solutions, artificial intelligence (AI) can increase the system's resilience. **Table A1** provides an overview of all primary studies that concentrate on the protect function. Demonstrated in the Appendix section are the solution categories and a thorough synopsis of the AI use cases in each category.

4.12 IoT Security: IoT security is built on a cybersecurity approach that prevents cyberattacks on connected IoT devices and the weaker networks they link to. There is no built-in security for Internet of Things devices. IoT devices function unnoticed by traditional cybersecurity systems and transmit data over the internet in an unencrypted manner, so IoT security is necessary to assist prevent data breaches.

Unfortunately, the majority of IoT devices cannot have security software installed on the devices. When connected to a network, spyware from IoT devices may even come pre-installed. Network security is crucial for IoT security because of this. Many IoT device connections and the devices that are interacting over the network are not identified by many network security solutions. These and other significant IoT security issues are demonstrated in the fig below.

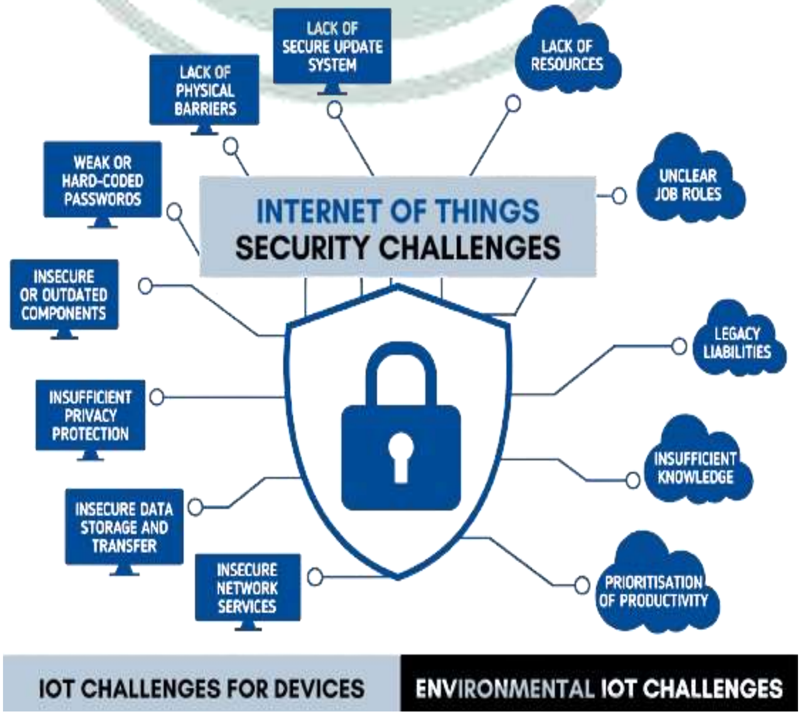

INTERNET OF THINGS
SECURITY CHALLENGES
LACK OF SECURE UPDATE SYSTEM
LACK OF PHYSICAL BARRIERS
LACK OF RESOURCES
WEAK OR HARD-CODED PASSWORDS
UNCLEAR JOB ROLES
INSECURE OR OUTDATED COMPONENTS
LEGACY LIABILITIES
INSUFFICIENT PRIVACY PROTECTION
INSUFFICIENT KNOWLEDGE
INSECURE DATA STORAGE AND TRANSFER
INSECURE NETWORK SERVICES
PRIORITISATION OF PRODUCTIVITY
IOT CHALLENGES FOR DEVICES
ENVIRONMENTAL IOT CHALLENGES

Figure 8: IoT challenges for devices and environment

Based on Infocomm Media Development Authority’s (IMDA) IoT cybersecurity guide, the recommendations for securing your devices revolve around 4 fundamental design principles:

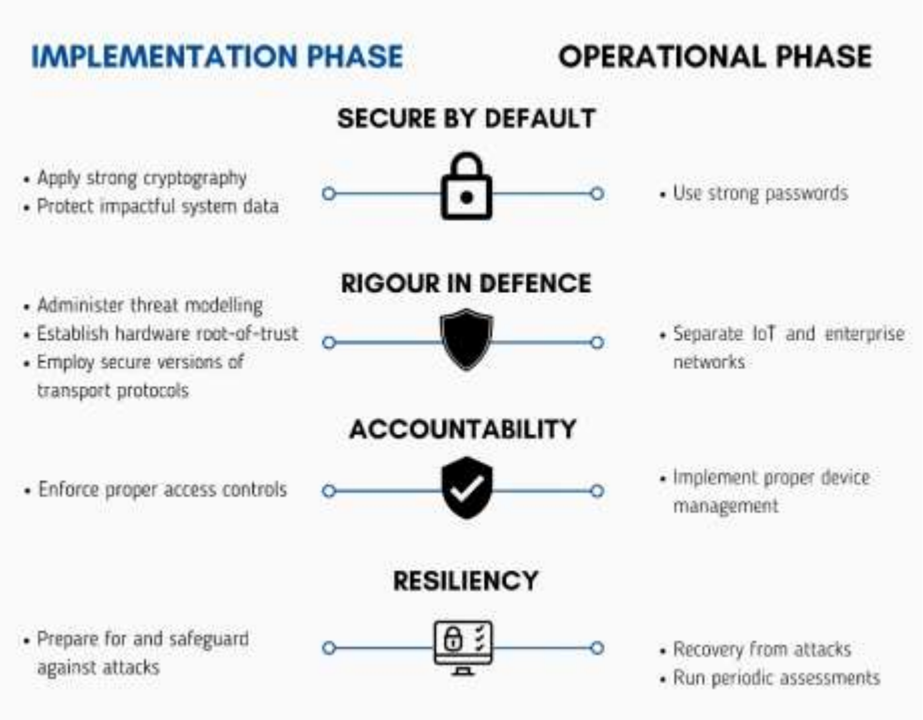

IMPLEMENTATION PHASE
OPERATIONAL PHASE
SECURE BY DEFAULT
• Apply strong cryptography
• Protect impactful system data
• Use strong passwords
RIGOUR IN DEFENCE
• Administer threat modelling
• Establish hardware root-of-trust
• Employ secure versions of transport protocols
• Separate IoT and enterprise networks
ACCOUNTABILITY
• Enforce proper access controls
• Implement proper device management
RESILIENCY
• Prepare for and safeguard against attacks
• Recovery from attacks
• Run periodic assessments

Figure 9: IoT security recommendations

5. LIMITATION OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

This paper provides valuable information on the intersection between cybersecurity and AI techniques, along with the identification of research gaps to feed future research. Artificial intelligence (AI) is not as concerned about cyber security as it could be. Because AI tends to produce false positives and negatives, actual threats could go unnoticed or get overwhelmed by pointless alerts, undermining user confidence and decreasing operational efficacy. Adversarial attacks can leverage AI weaknesses to take over systems intended to enhance security, potentially leading to breaches. In addition, AI may be less effective if it relies too heavily on historical data, which might reinforce impacts and prevent it from adapting to fresh, innovative attack methods. Artificial intelligence still requires human knowledge since AI finds it difficult to comprehend contextual nuances and can erroneously interpret user behaviors and intentions. Ultimately, despite AI's tremendous potential, overcoming its present limitations requires careful balancing.

6. CONCLUSION

This paper examines the various artificial intelligence (AI) strategies utilized in the cybersecurity field and the cybersecurity operations that have benefited from AI technology. AI's processing power has made it feasible to identify potential threats in advance, and its tailored advice promotes a Cyberwar culture. Nevertheless, this progress is not without its challenges. Biases, adversarial flaws, and false positives can undermine effectiveness and confidence. The right mix between AI's advantages and human abilities must be found to optimize its benefits and minimize its disadvantages. The development of artificial intelligence (AI) in cybersecurity has been examined in relation to various roles, categories of solutions, particular use cases, and AI approach types.

The analysis findings showed that while there are more publications now than ever before, to put useful AI-based cybersecurity solutions into practice, greater focus needs to be placed on gathering and presenting historical data pertaining to various cybersecurity functions. The classification of the major research to combine the current state of the literature in this field and understand the significance of AI for cybersecurity is the key contribution of this work. The paper also suggests future research routes to tackle new problems related to the effective application of AI in cybersecurity.

REFERENCES

[1] Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar, Secure framework against cyber-attacks on cyber-physical robotic systems, J. Electron. Imaging 31 (6) (2022), 061802-061802.

[2] P. Chithaluru, A.T. Fadi, M. Kumar, T. Stephan, Computational intelligence inspired adaptive opportunistic clustering approach for industrial IoT networks, IEEE Internet Things J (2023), https://doi.org/10.1109/JIOT.2022.3231605.

[3] M. Barrett, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2018.

[4] Rawindaran, Nisha, Ambikesh Jayal, and Edmond Prakash. 2022. "Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime".

[5] SELVI, C.S., Sripada, R.N. and Widjaja, G., Impact and limitations of artificial intelligence in cyber security awareness.

[6] Kaur, R., Gabrijelčič, D. and Klobučar, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, p.101804.

[7] I. Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver, Artificial intelligence for cybersecurity: a systematic mapping of literature, IEEE Access 8 (2020) 146598–146612.

[8] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo, Artificial intelligence in cyber security: research advances, challenges, and opportunities, Artif. Intell. Rev. 55 (2022) 1029–1053.

[9] J. Martínez Torres, C. Iglesias Comesana, ˜ P.J. García-Nieto, Machine learning techniques applied to cybersecurity, Int. J. Mach. Learn. Cybern. 10 (10) (2019) 2823–2836.

[10] T.C. Truong, I. Zelinka, J. Plucar, M. Candík, ˇ V. Sulc, ˇ Artificial intelligence and cybersecurity: past, presence, and future, in: Artificial intelligence and evolutionary computations in engineering systems, 2020, pp. 351–363.

[11] S. Samoili, M.L. Cobo, E. Gomez, G. De Prato, F. Martinez-Plumed, B. Delipetrev, A.I. Watch, Technical report, Joint Research Center (Seville site), 2020.

[12] What is Cybersecurity? – Cisco, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html, 16/12/2023

[13] Sonya Moisset, How Security Analysts Can Use AI in Cybersecurity, https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/, 16/12/2023

[14] D. Zhao, A. Strotmann, Analysis and visualization of citation networks, Synthesis lectures on information concepts, retrieval, and services, 7 1 (2015) 1–207.

[15] Peter Loshin, what is User (and Entity) Behavior Analytics (UBA or UEBA)? https://www.techtarget.com/searchsecurity/definition/user-behavior-analytics-UBA, 16/12/2023

[16] What is Security Information and Event management (SIEM)? https://www.ibm.com/topics/siem, 17/12/2023

[17] What Is Endpoint Security? How It Works & Its Importance, https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security/, 17/12/2023

[18] What Is Cloud Security? | Google Cloud, https://cloud.google.com/learn/what-is-cloud-security, 17/12/2023

[19] What Is a Vulnerability Assessment and How Does It Work? https://www.synopsys.com/glossary/what-is-vulnerability-assessment.html, 17/12/2023

[20] A. Yeboah-Ofori, S. Islam, S.W. Lee, Z.U. Shamszaman, K. Muhammad, M. Altaf, M.S. Al-Rakhami, Cyber threat predictive analytics for improving cyber supply chain security, IEEE Access 9 (2021) 94318–94337.

[21] T. Sawik, A linear model for optimal cybersecurity investment in industry 4.0 supply chains, Int. J. Prod. Res. 60 (4) (2022) 1368–1385.

[22] T. Sawik, B. Sawik, A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value, Int. J. Prod. Res. 60 (21) (2022) 6556–6572.

[23] T. Sawik, Balancing cybersecurity in a supply chain under direct and indirect cyber risks, Int. J. Prod. Res. 60 (2) (2022) 766–782.

[24] S. Rahman, N.U. Hossain, K. Govindan, F. Nur, M. Bappy, assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: a model to generate cyber resilience index of a supply chain, CIRP J. Manuf. Sci. Technol. 35 (2021) 911–928.

[25] A.I. Siam, A. Sedik, W. El-Shafai, A.A. Elazm, N.A. El-Bahnasawy, G.M. El Banby, A.A. Khalaf, F.E. Abd El-Samie, Biosignal classification for human identification based on convolutional neural networks, Int. J. Commun. Syst. 34 (7) (2021) 1–22.

[26] J.M. Jorquera Valero, P.M. Sanchez ´ Sanchez, ´ L. Fern´ andez Maimo, ´ A. Huertas Celdr´ an, M. Arjona Fern´ andez, S. De Los Santos Vílchez, G. Martínez P´erez, Improving the security and QoE in mobile devices through an intelligent and adaptive continuous authentication system, Sensors 18 (11) (2018) 3769.

[27] P.M. S´ anchez, A. Huertas Celdran, ´ L. Fern´ andez Maimo, ´ G. Martínez P´erez, G. Wang, Securing smart offices through an intelligent and multi-device continuous authentication system, in: International Conference on Smart City and Informatization, 2019, pp. 73–85.

[28] A.G. Martín, M. Beltran, ´ A. Fern´ andez-Isabel, I.M. de Diego, an approach to detect user behaviour anomalies within identity federations, Comp. Security 108 (2021), 102356.

[29] H. Alobaidi, N. Clarke, F. Li, A. Alruban, Real-world smartphone-based gait recognition, Comput. Secur. 113 (2022), 102557.

[30] K.A. Rahman, D. Neupane, A. Zaiter, M.S. Hossain, Web user authentication using chosen word keystroke dynamics, in 18th IEEE International Conference on Machine Learning and Applications (ICMLA), 2019, pp. 1130–1135.

[31] A. Shaout, N. Schmidt, Keystroke identifier using fuzzy logic to increase password security, in: 21st International Arab Conference on Information Technology (ACIT), 2020, pp. 1–8. R. Kaur et al. Information Fusion 97 (2023) 101804 27

[32] A. Hafeez, K. Topolovec, S. Awad, ECU fingerprinting through parametric signal modeling and artificial neural networks for in-vehicle security against spoofing attacks, in 15th International Computer Engineering Conference (ICENCO), 2019, pp. 29–38.

[33] G. Baldini, R. Giuliani, M. Gemo, F. Dimc, On the application of sensor authentication with intrinsic physical features to vehicle security, Comput. Electr. Eng. 91 (2021), 107053.

[34] Y. Cui, F. Bai, R. Yan, T. Saha, R.K. Ko, Y. Liu, Source Authentication of distribution synchrophasors for cybersecurity of microgrids, IEEE Trans. Smart Grid 12 (5) (2021) 4577–4580.

[35] M. Benedetti, M. Mori, On the use of Max-SAT and PDDL in RBAC maintenance, Cybersecurity 2 (1) (2019) 1–25.

[36] M. Abolfathi, Z. Raghebi, H. Jafarian, F. Banaei-Kashani, A scalable role mining approach for large organizations, in: Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics, 2021, pp. 45–54.

[37] S.S. Chukkapalli, S.B. Aziz, N. Alotaibi, S. Mittal, M. Gupta, M. Abdelsalam, Ontology driven AI and access control systems for smart fisheries, in: Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, 2021, pp. 59–68.

[38] B. Leander, A. Cau ˇ ˇsevi´c, H. Hansson, T. Lindstrom, ¨ Access control for smart manufacturing systems, in: European Conference on Software Architecture, 2020, pp. 463–476.

[39] Z. Tan, R. Beuran, S. Hasegawa, W. Jiang, M. Zhao, Y. Tan, Adaptive security awareness training using linked open data datasets, Educ. Inf. Technol. 25 (6) (2020) 5235–5259.

[40] F. Nembhard, M. Carvalho, T. Eskridge, A hybrid approach to improving program security, in: IEEE Symposium Series on Computational Intelligence (SSCI), 2017, pp. 1–8.

[41] T.Espinha Gasiba, U. Lechner, M. Pinto-Albuquerque, Sifu-a cybersecurity awareness platform with challenge assessment and intelligent coach, Cybersecurity 3 (1) (2020) 1–23.

[42] D.C. Le, N. Zincir-Heywood, Anomaly detection for insider threats using unsupervised ensembles, IEEE Trans. Netw. Service Manag. 18 (2) (2021) 1152–1164.

[43] J. Kim, M. Park, H. Kim, S. Cho, P. Kang, Insider threat detection based on user behavior modeling and anomaly detection algorithms, Appl. Sci. 9 (19) (2019) 4018.

[44] T. Al-Shehari, R.A. Alsowail, An insider data leakage detection using one-hot encoding, synthetic minority oversampling and machine learning techniques, Entropy 23 (10) (2021) 1258.

[45] K. Alzhrani, E.M. Rudd, T.E. Boult, C.E. Chow, Automated big text security classification, in: IEEE Conference on Intelligence and Security Informatics (ISI), 2016, pp. 103–108.

[46] Y. Guo, J. Liu, W. Tang, C. Huang, Exsense: extract sensitive information from unstructured data, Comput. Secur. 102 (2021), 102156.

[47] H. Li, J. Wu, H. Xu, G. Li, M. Guizani, Explainable intelligence-driven defense mechanism against advanced persistent threats: a joint edge game and AI approach, IEEE Trans. Dependable Secure Comput. 19 (2) (2022) 757–775.

[48] A.A. Alghamdi, G. Reger, Pattern extraction for behaviours of multi-stage threats via unsupervised learning, in: International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020, pp. 1–8.
[49] L. Gallo, A. Maiello, A. Botta, G. Ventre, 2 Years in the anti-phishing group of a large company, Comput. Secur. 105 (2021), 102259.
[50] D. Wu, W. Shi, X. Ma, A novel real-time anti-spam framework, ACM Trans. Internet Technol. (TOIT) 21 (4) (2021) 1–27.
[51] E.S. Gualberto, R.T. De Sousa, T.P. Vieira, J.P. Da Costa, C.G. Duque, The answer is in the text: multi-stage methods for phishing detection based on feature engineering, IEEE Access 8 (2020) 223529–223547.
[52] M. Nguyen, T. Nguyen, T.H. Nguyen, A deep learning model with hierarchical lstms and supervised attention for anti-phishing, in 1st Anti-Phishing Shared Task Pilot at 4th ACM IWSPA, 2018, pp. 29–38.
[53] D. Cohen, O. Naim, E. Toch, I. Ben-Gal, Website categorization via design attribute learning, Comput. Secur. 107 (2021), 102312.
[54] C. Marques, S. Malta, J.P. Magalh˜ aes, DNS dataset for malicious domains detection, Data Br 38 (2021), 107342.
[55] B. Yu, J. Pan, D. Gray, J. Hu, C. Choudhary, A.C. Nascimento, M. De Cock, Weakly supervised deep learning for the detection of domain generation algorithms, IEEE Access 7 (2019) 51542–51556.
[56] J. Spaulding, A. Mohaisen, Defending internet of things against malicious domain names using D-FENS, in: IEEE/ACM Symposium on Edge Computing (SEC), 2018, pp. 387–392.
[57] P.L. Indrasiri, M.N. Halgamuge, A. Mohammad, Robust ensemble machine learning model for filtering phishing URLs: expandable random gradient stacked voting classifier (ERG-SVC), IEEE Access 9 (2021) 150142–150161.
[58] R. Vinayakumar, K.P. Soman, P. Poornachandran, evaluating deep learning approaches to characterize and classify malicious URL's, J. Intell. Fuzzy Syst. 34 (3) (2018) 1333–1343.
[59] W. Li, J. Jin, J.H. Lee, Analysis of botnet domain names for IoT cybersecurity, IEEE Access 7 (2019) 94658–94665.
[60] B. Alotaibi, M. Alotaibi, Consensus and majority vote feature selection methods and a detection technique for web phishing, J. Ambient. Intell. Humaniz. Comput. 12 (1) (2021) 717–727.
[61] Y. Qin, B. Hoffmann, D.J. Lilja, Hyperprotect: enhancing the performance of a dynamic backup system using intelligent scheduling, in: IEEE 37th International Performance Computing and Communications Conference (IPCCC), 2018, pp. 1–8.
[62] P.M. Van de Ven, B. Zhang, A. Schorgendorfer, ¨ Distributed backup scheduling: modeling and optimization, in: IEEE INFOCOM 2014-IEEE Conference on Computer Communications, 2014, pp. 1644–1652.
[63] Z. Zeng, Z. Yang, D. Huang, C.J. Chung, LICALITY–Likelihood and criticality: vulnerability risk prioritization through logical reasoning and deep learning, IEEE Trans. Netw. Service Manag. 19 (2) (2021) 1746–1760.
[64] J. Yin, M. Tang, J. Cao, H. Wang, apply transfer learning to cybersecurity: predicting exploitability of vulnerabilities by description, Knowl. Based Syst. 210 (2020), 106529.
[65] J. Yin, M. Tang, J. Cao, H. Wang, M. You, A real-time dynamic concept adaptive learning algorithm for exploitability prediction, Neurocomputing 472 (2022) 252–265.
[66] T. Bai, H. Bian, M.A. Salahuddin, A. Abou Daya, N. Limam, R. Boutaba, Rdp-based lateral movement detection using machine learning, Comp. Commun. 165 (2021) 9–19.
[67] N. Afzaliseresht, Y. Miao, S. Michalska, Q. Liu, H. Wang, From logs to stories: human-centred data mining for cyber threat intelligence, IEEE Access 8 (2020) 19089–19099.
[68] G. De la Torre-Abaitua, L.F. Lago-Fern´ andez, D. Arroyo, A compression-based method for detecting anomalies in textual data, Entropy 23 (5) (2021) 618.
[69] T. Eljasik-Swoboda, W. Demuth, leveraging clustering and natural language processing to overcome variety issues in log management, in: ICAART, 2020, pp. 281–288.
[70] D. Sisiaridis, O. Markowitch, Reducing data complexity in feature extraction and feature selection for big data security analytics, in 1st International Conference on Data Intelligence and Security (ICDIS), 2018, pp. 43–48.
[71] P.F. De Araujo-Filho, A.J. Pinheiro, G. Kaddoum, D.R. Campelo, F.L. Soares, an efficient intrusion prevention system for CAN: hindering cyber-attacks with a lowcost platform, IEEE Access 9 (2021) 166855–166869.

[72] C. Constantinides, S. Shiaeles, B. Ghita, N. Kolokotronis, A novel online incremental learning intrusion prevention system, in 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2019, pp. 1–6.
[73] S.M. de Lima, H.K. Silva, J.H. Luz, H.J. Lima, S.L. Silva, A. de Andrade, A.M. da Silva, Artificial intelligence-based antivirus in order to detect malware preventively, Prog. Artif. Intell. 10 (1) (2021) 1–22.
[74] P. Marques, M. Rhode, I. Gashi, Waste not: using diverse neural networks from hyperparameter search for improved malware detection, Comput. Secur. 108 (2021), 102339.
[75] P. Karuna, H. Purohit, S. Jajodia, R. Ganesan, O. Uzuner, Fake document generation for cyber deception by manipulating text comprehensibility, IEEE Syst. J. 15 (1) (2020) 835–845.

APPENDIX

Table A1: An overview of the primary research that concentrated on the role of protection.

Solution Category	Use Case	Contribution	AI domain	Author
Identity Management, Authentication and Access Control	AI-supported user authentication	Physical biometric-based authentication	Learning	Siam et al. [25]
		Behavioral biometric-based authentication	Learning	Valero et al. [26], Sanchez et al. [27], Martin et al. [28]
		Behavioral biometric-based authentication	Perception	Alobaidi et al. [29]
		Multifactor authentication	Reasoning	Rahman et al. [30], Shaot & Schmidt [31]
	AI-supported device authentication	Sensor identification & authentication	Learning	Hafeez et al. [32], Baldini et al. [33]
		Source authentication of distributed Synchrophasors	Learning	Cui et al. [34]
	Automated access control	Role-based access control	Planning	Benedetti and Mori [135], Abolfathi et al. [136]
		Attribute-based access control	Planning	Chukkapalli et al. [137]
		Attribute-based access control	Reasoning	Leander et al. [38]
Awareness and Training	Adaptive security awareness and training	Adaptive cybersecurity training	Communication	Tan et al. [39]
		Recommender system for secure coding	Communication	Nembhard et al. [140]
		Secure coding awareness	Learning	Gasiba et al. [41]
Data Security	Data leakage prevention	Monitoring data access, data movement and user activity	Learning	Le and Zincir-Heywood [42], Kim et al. [43], Al-Shehari et al. [44]
		Automated data sensitivity detection	Communication	Alzhrani et al. [45], Guo et al. [46]
		Advanced persistent threat detection	Learning	Li et al. [47], Alghamdi & Reger [48]

	Intelligent e-mail protection	Malicious spam email detection	Learning	Gallo et al. [49]
		Malicious spam email detection	Communication	Wu et al. [50].
		Phishing email detection	Communication	Gualberto et al. [51], Nguyen et al. [52]
	Malicious domain blocking & reporting	Website design features for malicious website detection	Learning	Cohen et al. [53]
		Domain-based features for malicious website detection	Learning	Marques et al. [54], Yu et al. [55], Spaulding & Mohaisen [56]
		URL-based features for malicious website detection	Learning	Indrasiri et al. [57], Vinayakumar et al. [58]
		Hybrid features for malicious website detection	Learning	Li et al. [59], Alotaibi [60]
Information Protection Processes & Procedures	AI-powered backup	Dynamic backup scheduling	Reasoning	Qin et al. [61]
		Intelligent backup scheduling	Learning	Van de Ven et al. [62]
	AI-enhanced vulnerability management plan	Context-based vulnerability risk scoring	Reasoning & Learning	Zeng et al. [63]
		Vulnerability exploitation trends	Learning	Yin et al. [64]
	Log analysis	Vulnerability exploitation trends	Communication	Yin et al. [65]
Protective Technology		Evidence extraction	Learning	Bai et al. [66]
		Data presentation technique	Communication	Afzaliseresht et al. [67]
		Handle variety & interoperability issue	Communication	Torre-Abaitua et al. [68], Eljasik-Swoboda and Demuth [69]
		Automated security analysis of heterogenous log data	Learning	Sisiaridis and Markowitch [70]
	IPS	IPS for electronic control units	Learning	De Araujo-Filho et al. [71]
		IPS for IoT network	Learning	Constantinides et al. [72]
	Anti-virus/Anti-malware	Analysis of modus operandi of malware	Learning	De Lima et al. [73]
		Dynamic data analysis	Learning	Marques et al. [74]
	Protection by deception	Decoy text generation	Planning	Karuna et al. [75]