Journal of Adaptive Learning Technologies
ISSN **2997-3902** (Online)
Vol. 2, No. 5, May 2025,
Available online at: https://scientificbulletin.com/index.php/JALT

ASSESSING THE EFFECTIVE OF ARTIFICIAL INTELLIGENCE IN PREVENTING CYBER ATTACKS ON BUSINESSES

Jafrin Reza
Master of Science in Business Analytics, Trine University, USA

Article information:
Manuscript received: 21 Mar 2024; **Accepted:** 10 Apr 2024; **Published:** 31 May 2025

Abstract: Modern businesses deploy artificial intelligence (AI) as their central cybersecurity solution because it strengthens threat identification together with response protocols and risk protection operations. A review of AI-supported security measures for threat prevention and detection and threat management is conducted through an examination of Microsoft Security Incident Prediction dataset (2023). Supervised machine learning helps the research to understand threat patterns and test AI detection methods while validating predictive models which decrease security vulnerabilities. Visual data analysis through a combination of Tableau and Python tools demonstrates how artificial intelligence helps detection standards as well as enhances incident reactions and lowers false alarms. This research evaluates AI security frameworks to stop cyber-attacks through their three key features which are better detection accuracy and fewer false alarms together with faster response times. The paper analyzes AI abilities through a quantitative analysis by utilizing the Microsoft Security Incident Prediction dataset. Researchers use Python along with Tableau and computational models and machine learning approaches to assess detection outcomes and response times and false alarms of AI-based systems against normal security protocols. Research studies confirm the great power of AI-based cybersecurity technology to enhance danger identification along with minimizing security breaches and accelerating incident response processes. The adoption of AI in cybersecurity faces major hindrances because of systematic program biases as well as high numbers of error alerts and privacy-related issues. The study emphasizes the need to enhance AI algorithms and combines blockchain security with threat intelligence distribution to achieve regulatory compliance through explainable AI. Operating businesses need to make adaptive AI-driven security frameworks their top priority because cyber threats continue developing to protect their critical assets while securing operational resilience. Through its research outcomes this study presents important information about how AI performs in the cybersecurity space for creating practical strategic guidelines to enhance business cybersecurity systems.

Keywords: Artificial Intelligence, Cybersecurity, Threat Detection, AI-Powered Security, Machine Learning, and Incident Response.

1. Introduction

1.1 Background

Modern businesses experience substantial difficulties because of growing frequency

alongside increasing complexity of cyber threats. Cybercriminals use phishing as well as ransomware and DDoS attacks together with malware and APTs to take advantage of security framework weaknesses in organizations. Cybercriminal actions cause organizations to experience tremendous financial difficulties as well as data compromise and negative company image with substantial operational disturbances. Cybersecurity tools based on firewalls and antivirus protection and rule systems operate behind an advancing threat pattern that they cannot effectively counter. The predetermined signature approach alongside fixed security rule systems decreases their ability to detect modern emerging cyber threats. Business organizations now embrace artificial intelligence (AI) and machine learning (ML) algorithms to reinforce their real-time abilities for detecting cyber-attacks prevention operations. Cybersecurity gets transformed through artificial intelligence by implementing self-operating threat discovery tools which also detect abnormal behavior and forecast security events [1]. Supervised machine learning algorithms together with deep learning and natural language processing (NLP) and pattern recognition patterns analyze a massive data volume to detect malicious activity better than conventional security measures at higher efficiency levels. These technologies enable organizations to foresee potential threats in advance and simultaneously decrease the occurrence of incorrect alerts and strengthen their reaction management capabilities. An investigation of AI effectiveness against business cyber-attacks is conducted using the Microsoft Security Incident Prediction dataset (2023). This research evaluates AI security mechanisms together with predictive features and difficulties to deliver understanding about AI's ability to reinforce organizational cybersecurity defense against modern digital threats.

1.2 Importance of Cybersecurity in Business Operations

Digital infrastructure dependence has made cybersecurity establish itself as an essential foundation for business survival during times of crisis. The allure of cybercriminals toward organizations comes from their massive sensitive data storage together with their financial dealings and their dependence on cloud systems [2]. The combination of cyber-attacks including data breaches, ransomware incidents and phishing attempts results in severe financial harm alongside harm to reputation and mandatory enforcement penalties which generate operational interruptions. Inadequate security measures have led to major cyber-Attacks like Equifax data breach from 2017 together with SolarWinds attack in 2020 and Colonial Pipeline ransomware attack during 2021. Organizations need to put into place strong cybersecurity methods which protect their digital resources while keeping clients assured of their safety. Through AI powered cybersecurity solutions business organizations utilize machine learning algorithms together with behavior analytics and automated response capabilities to proactively detect and respond to threats. Through these technologies organizations can boost security intelligence and decrease false positives thus always allowing instant threat prevention. Businesses must observe GDPR and CCPA and comply with ISO 27001 standards because data privacy together with legal compliance ensures their operations. AI-driven cybersecurity technologies provide organizations with an enhanced defense system while reducing risks to protect their operations in an increasingly challenging security environment for future business success.

1.3 Role of AI in Cybersecurity

Cyber Security protection has advanced using artificial intelligence which strengthens predictive analytics together with automated anomaly detection and response capabilities. Artificial intelligence models review the analysis of network traffic together with endpoints' activities and previous security incidents to identify behavior deviances which show unauthorized access attempts or signs of malicious activities [3]. Trainable machine learning systems evaluate threats through dataset identification that enables threat prediction while untrained machine learning discovers unverified attack forms by creating

traffic anomaly classifications. By applying deep learning techniques, the security intelligence gathers more effective capabilities to detect complex attacks whereas natural language processing (NLP) technology solves both email filtering and phishing attacks [4]. The automated threat intelligence system gathers new security threats regularly which allows it to instantly modify security systems to combat novel cyber risks. Artificial intelligence enhances cybersecurity defense by making detections more precise and cutting down on sham alerts and improving the speed of reaction which delivers proactive security capabilities to companies. The technology continues to face problems in its reliability and ethical implications in addition to adversarial attacks. This paper analyzes how AI performs at cybersecurity through an evaluation of its ability to discover and eliminate threats employing Microsoft Security Incident Prediction datasets. Modern cybersecurity strategies heavily depend on AI cybersecurity models that utilize machine learning algorithms combined with data-driven insights to strengthen security frameworks and detect and respond faster while remaining fundamental parts of enterprise protection solutions.

1.4 The Microsoft Security Incident Prediction Dataset

The Microsoft Security Incident Prediction dataset (2023) includes complete cybersecurity incident records that provide information about attack vectors as well as threat actor behaviors and system vulnerabilities [5]. This dataset includes attack type information which covers phishing and malware and ransomware and DDoS attacks while using low, medium high and critical severity categories to classify them. The security incident dataset contains timestamps for attacks alongside information about influenced systems as well as AI detection scores from security logs and documented network traffic changes [6]. AI model approach structure information to discover distinct patterns between regular system functions and security threats thus enhancing cybersecurity threat recognition performance. The data set proves essential for developing machine learning algorithms which boost predictive power while automatically processing threat data to discover exploit areas before their use becomes possible. This dataset helps researchers evaluate AI security measures by analyzing their capability to identify, prevent, defend against cyber-attacks while measuring their time reduction capacities and anomaly discovery effectiveness and breach prevention capabilities. Real-time assessment of AI-driven security solutions is possible through the dataset to determine their capacity for business network protection and system threat detection which minimizes potential security risks.

1.5 Problem Statement

Today's organizations face difficulties in properly using AI technology to build their security infrastructure despite recent improvements in this field. AI models need to reduce both incorrect alerts and incorrect negations to detect threats effectively while demonstrating persistence against algorithm manipulation attempts. AI requires significant data source usage for its operations while raising critically important privacy and regulatory compliance issues that become essential to handle. The oversight of security mechanisms guided by artificial intelligence requires human experts for making informed decisions in cybersecurity operations. The research examines two main aspects through analysis of AI prevention methods against cyber threats and evaluation of security objective changes alongside AI model weaknesses.

1.6 Research Objectives

The main goal of this investigation consists of the following objectives:

- The Microsoft Security Incident Prediction dataset will enable the assessment of AI systems for identifying and blocking cyber-attacks.

- The research analyzes the forecast capabilities of AI-based threat detection systems that aim to cut down security vulnerabilities.
- This study aims to measure AI systems through evaluation of three cybersecurity elements that consist of both detection accuracy and incident response times as well as false positive rates [7].
- This investigation aims to track down major issues encountered in AI-based cybersecurity while creating tactical solutions for their resolution.

1.7 Research Questions

The research aims to address three questions through this study:

1. What is the level of effectiveness that AI-based cybersecurity models demonstrate when minimizing cyber-attacks?
2. The main benefits of security systems driven by AI stand out against conventional cybersecurity approaches which benefits organizations in what way?
3. Businesses encounter what primary difficulties when they deploy AI-based cybersecurity solutions for their operations?
4. What are the necessary methods to optimize AI cybersecurity models for improving threat detection effectiveness alongside reducing their security weakness?

1.8 Significance of the Study

This research expands the existing knowledge about AI in cybersecurity while giving essential guidance to businesses and others who work in cybersecurity as well as policymakers and technology developers [8]. The investigation demonstrates how AI performs within a security framework through evaluation of its threat discovery ability and predictive functions and response efficiency evaluations for evidence of its potential as a cyber risk mitigating tool. the research examines the difficulties along with ethical aspects which emerge from incorporating AI for cybersecurity including privacy issues and defense attacks and incorrect alarm reactions. The provided research delivers proactive guidelines to organizations which help them maximize the effects of artificial intelligence in cybersecurity and strengthen their capability to gather threat data and execute better incident responses. Insights from this study enable policymakers to establish security frameworks between privacy protection and threat defenses for developing regulatory guidelines which cybersecurity experts and developers utilize to enhance AI models. The study intends to connect artificial intelligence innovation with useful cybersecurity applications for improving organizational cyber threat defense.

1.9 Scope and Limitations of the Study

The research examines how artificial intelligence prevents cyber-attacks in business settings by conducting an empirical analysis using Microsoft Security Incident Prediction dataset information. The paper investigates and evaluates three aspects of AI security systems namely threat detection and predictive analytics and automated response capabilities to determine their effects on cybersecurity resilience. The study restricts itself to examining AI models for cybersecurity while omitting human-operated security policies, governance principles and conventional control measures. The study acknowledges several limitations. The current dataset fails to represent all cyber threats including zero-day attacks and newly emerged security patterns which are absent from its documentation. AI model results extend from how well the training data performs along with which algorithms they use and how well their parameters are adjusted. The research analyzes ethical and legal considerations because AI-driven cybersecurity needs to follow

private data regulations as well as compliance standards. AI-based security improvements together with regulatory updates need to advance perpetually because of such system constraints.

2. Literature Review

2.1 Overview of AI in Cybersecurity

Security measures have benefited greatly from artificial intelligence because it provides users with superior methods to detect threats and forecast dangerous events and execute automated responses to security incidents. The increase of advanced cyber threats traditional rule-based security incapable of providing sufficient protection [10]. AI driven cybersecurity frame workers use machine learning and deep learning along with natural language processing techniques to improve security threats detection and mitigation. Such systems use previous attack data to learn new attack vectors which helps them strengthen security response capabilities during time. The following part demonstrates how AI navigates cybersecurity through its capabilities in security threat identification as well as network security applications and malware analysis and automated defense systems. Besides the analysis this section discusses positive sniffing accuracy challenges and confronts adversarial attack methods and privacy concerns regarding data.

2.2 AI-Based Threat Detection and Prediction

AI better performs threat detection operations in cybersecurity through its ability to provide improved precision and speed [1]. AI-powered security detection systems run through enormous security data to notice suspicious patterns which signal possible attacks. Most machine learning models operate by detecting established threats after training while unsupervised learning becomes essential to discover unknown attack patterns. Deep learning architecture models, especially convolutional and recurrent neural networks detect complex threats together with zero-day exploits and advanced persistent threats with great effect [2]. AI-driven threat intelligence solutions keep enhancing their artificial intelligence models by adopting fresh attack schemes thus they become more proficient at prediction work and require less time to answer.

2.3 AI in Network Security and Intrusion Detection Systems

Intrusion detection systems received revolutionary changes from AI because its adaptive security features extend past traditional signature-based systems [3]. IDS systems using AI technologies evaluate network traffic patterns to recognize abnormal behaviors as well as unauthorized systems access activities. AI-based solutions depart from standard IDS techniques since they monitor normal network behavior to detect previously unknown threats through abnormal conduct [4]. The current developments in AI-driven IDS systems involve deep learning together with adversarial learning methods. The systems improve security performance through their ability to distinguish between normal and harmful network communications.AI-powered network security frameworks employ language processing to process security logs and phishing emails and cyber threat intelligence which enables organizations to fight social engineering attacks more effectively.

2.4 AI in Malware Detection and Analysis

The problem with signature-based antivirus solutions received an improvement from AI technology in malware detection methods [5]. Programs designed for machine learning evaluate behavioral information and execution logs together with code construction to identify harmful software. Analyzing different aspects of files with static methods is one aspect of static analysis yet dynamic methods view runtime actions to locate security risks. Long short-term memory networks function as deep learning approaches to increase

malware detection precision because they detect sophisticated attack patterns [6]. Adaptive malware detection becomes possible through combining AI methodologies which unite machine learning with reinforcement learning capabilities.

2.5 AI-Driven Automated Incident Response

The implementation of Artificial Intelligence as an automated solution has dramatically enhanced the time needed to respond to incidents in cyber environments [7]. The process of security operations through human interaction results in delayed responses when addressing cyber threats. SOAR (security orchestration automation response) platforms with AI capabilities automate incident threat evaluation as well as risk ranking through their platform. AI versions of incident response systems enable security information and event management (SIEM) tools to evaluate huge alert arrays while discarding nonexistent threats [8]. Antecedent to learning event data helps reinforcement learning models find the most suitable response strategies for security threats. AI cybersecurity assistants allow security analysts to receive instant decision assistance that makes their work processes more efficient.

2.6 Challenges and Limitations of AI in Cybersecurity

Multiple obstacles appear in the way of achieving success with AI-driven cybersecurity solutions. Security teams experience overwhelming burdens when dealing with numerous false positive alarms because these artificial intelligence systems produce many non-real attacks. The misinterpretation of ordinary activities into threatening behavior by AI models compels human security specialists to confirm the situation manually [9]. AI system vulnerabilities open a major security threat because attackers use deceptive inputs that aim to bypass detection technology. Different security protocols must be developed to make AI systems resilient enough for protection against attacks that seek to deceive them. The vast amount of data required by AI generates privacy problems because of its complications in maintaining user privacy. Associate organizations need to fulfill data security requirements using privacy-protecting artificial intelligence approaches including federated learning combined with differential privacy methods [10]. The deployment of AI in cybersecurity requires responsible measures since biases in AI decision-making constitute ethical considerations in this field.

2.7 Future Directions in AI Cybersecurity

The future of AI cybersecurity develops three main research directions that include enhancing clear interpretation of models as well as creating stronger resistance against cyberattacks and ethically responsible deployment approaches. Research into Explainable AI has emerged as a fundamental subject because it improves AI threat detection interpretation and increases security professional trust [11]. The development of advanced deceptive techniques employs artificial intelligence through honeypots and adversarial AI traps which allow security teams to misdirect potential attackers so they disclose their tactics and intelligence relating to new cyber threats.

Empirical Study

Artificial Intelligence (AI) acts as the fundamental component to enhance cybersecurity because it secures smart grids from cyber threats. Bouramdane (2023) establishes that digital technology infrastructure in smart grids exposes them to potential hackers. The research investigates various types of cyber threats that affect smart grids through real-life examples and data simulations. The study proposes to enhance security by implementing multi-criteria decision-making (MCDM) through analytical hierarchy process (AHP). The research analysis demonstrates that deep learning algorithms along with hybrid solutions and Bayesian networks should be implemented for successful prevention of cyber threats

[1]. The most effective AI technique for securing smart grids through cybersecurity is deep learning although swarm intelligence and machine learning rank as secondary methods. Two types of AI namely fuzzy logic and genetic algorithms demonstrate limited effectiveness in AI applications. Security benefits from AI implementation yet essential issues involving expenses and system unity requirements and regulatory requirements continue to matter.

Artificial Intelligence (AI) has revolutionized cybersecurity operations specifically in Industry 4.0 which depends heavily on smart factories together with automation that run through digital systems. The surge of connected devices has created new threats that criminals use to attack computer systems according to Azambuja et al. (2023). The attackers implement AI to strengthen their attack methodologies thereby increasing cybersecurity difficulty. This research analyzes two specific cyber assaults including the Stuxnet and Colonial Pipeline attacks to demonstrate how threats empowered by AI result in serious destruction [2]. The proposal from the research team includes the implementation of machine learning and deep learning systems for AI-based cybersecurity measures to stop and identify threats. The research identifies the need for uninterrupted research that combines the study of emerging cyberattack strategies with strong defense development. The benefits of AI security solutions are limited because organizations need to address privacy issues regarding data protection and stay ahead of future threats. The research promotes industry 4.0 organizations to develop advanced cybersecurity strategies against AI-based cyber threats.

The efficiency of Accounting Information Systems (AIS) receives vital support from Artificial Intelligence technology in industrial companies. Alrfai et al. (2023) show that expert systems together with genetic algorithms and intelligent agents together with AI applications improve AIS efficiency by process automation and error reduction as well as real-time decision support. Research indicates that neural networks create no meaningful improvement to AIS operational efficiency. The research investigation explains how cybersecurity functions as a moderating factor which increases the bond between AI systems and efficient AIS management. Financial institutions can protect their sensitive data through proper cybersecurity measures which also minimize possibilities of cyber threats and unauthorized access [3]. AIS demands the combination of AI with cybersecurity to achieve better operational efficiency and financial transaction security and maintain digital business continuity for current times. The research extends previous knowledge by evaluating the real-world capabilities of AI systems to protect commercial information systems from cyber-attack vulnerabilities.

Artificial intelligence (AI) actively contributes to the safeguarding of digital systems while cybersecurity stands as a vital matter because of escalating dependence on digital systems. According to Ali et al. (2021) digital infrastructure expansion at a rapid pace makes traditional security methods inadequate so that AI-based solutions need to take their place. The authors demonstrate that AI systems boost cybersecurity by making possible automatic threat discovery along with continuous tracking and conditional profiling which shortens the reaction time against ill-intentioned assaults [4]. The study explains that these significant obstacles involve adversarial AI application as well as data privacy risks and obstacles to integrate AI solutions into existing cybersecurity structures. The implementation of AI technologies in cybersecurity improves protective measures although it creates security risks which need proper management. This research develops existing knowledge about AI effectiveness by studying its ability to stop business cyber-attacks along with assessing its security impacts and new solution development approaches to address AI-based cybersecurity restrictions.

AI integration in Industry 4.0 changed cybersecurity approaches by bringing new

opportunities while facing various challenges to security systems. The security measures enabled through artificial intelligence contain machine learning-based intrusion detection systems (IDS) that defend manufacturing environments from cyber threats (Bécue et al., 2021). AI technology extends its capabilities to factory production observation and optimization and process control endeavors while scanning operational technology (OT) systems for weaknesses. The increased cybersecurity strength AI provides comes with security threats that include attacks on AI models to circumvent defensive measures. Different distributed detection methods and robust AI development frameworks need to be orchestrated to tackle existing security problems. Human-machine behavior monitoring stands as an absolute necessity when working to minimize security dangers that arise in Industry 4.0 environments [5]. To achieve the right balance AI applications in cybersecurity must deliver more preventive power to industrial systems than cybercriminals can derive from exploiting them (Bécue et al., 2021).

Artificial intelligence has become essential for cybersecurity because it improves both the speed of responses to threats and security management effectiveness together with enhanced detection capabilities. Different research works validate that AI-powered solutions determine cyber threats by applying deep learning models and predictive analytics and machine learning algorithms. According to Ozkan-Okay et al. (2023) machine learning (ML) together with deep reinforcement learning (DRL) plays a vital role in cybersecurity because they help identify abnormal behaviors and reduce security attacks. Alrfai et al. (2023) demonstrate how AI influences Accounting Information Systems (AIS) by showing cybersecurity serves as an important factor which enhances system operational effectiveness. Studies confirm that security platforms based on AI accomplish enhanced risk analysis yet employees need to address limitations that contain algorithmic inaccuracies in addition to nonzero incorrect identifications and increasingly sophisticated cyberattacks [6]. The continuous advancement of AI models in cybersecurity keeps working as an essential factor to minimize cyber risks and create strong defense systems for business environments. The current research expands existing knowledge about how well AI stops cyberattacks.

3. Methodology

The research design follows a quantitative method to assess business cyber-attack prevention through artificial intelligence implementation [12]. There is a goal to understand both the reliability and efficiency aspects of AI for cybersecurity enhancement through examination of historical threat data and security frameworks operated by AI and threat response analysis. The research collects industry reports with cybersecurity datasets before conducting statistical and machine learning analytical techniques [13]. The research analyzes AI defense systems in comparison to standard solutions to gain knowledge about AI's business-level cybersecurity influence.

3.1 Research Design

Conceptual research through a structured framework helps to investigate the implementation of AI-based cybersecurity systems within this study. The research uses a descriptive design to examine AI threat prevention practices through data assessments of past cybersecurity incidents [14]. The research design uses this method to spot recurring situations that show how AI detects and manages cyber threats. The research uses a comparative viewpoint which allows researchers to analyze AI security technology beside conventional cybersecurity methods. This research analyzes three components of AI defense solutions including detection platforms along with anomaly detection methodology and automatic response methods to evaluate their business security enhancing capabilities [15]. AI effects specifically target different aspects through automatic analysis of security

event logs together with the examination of AI-based risk reduction approaches and security performance assessment data. The research includes practical case examples to determine how AI adjusts to newer cyber threats in the field. Research findings will deliver information about AI's capability for security risk reduction and its positive impact on team security performance levels [16]. The complete methodology delivers enhanced knowledge about AI's role in cybersecurity which helps organizations choose AI-based security measures for their digital assets.

3.2 Data Collection

The research draws its data from secondary sources that concentrate mainly on cybersecurity incident datasets together with industry reports and academic research about AI-based threat detection systems [17]. The Microsoft Security Incident Prediction database serves as the primary research material due to its detailed security breach information and its AI prediction capabilities along with its defensive strategies. Secondary data from security companies IBM X-Force, Symantec, McAfee Labs and AI-based cybersecurity research papers and government cyber threat reports belong to the sources used. The data selection method uses three criteria to capture credible data that relates to AI performance metrics such as detection precision rates alongside false positive occurrences and reaction time measurements. Reliability of the obtained datasets is achieved through preprocessing steps that eliminate unstable data along with excessive information and data gaps. The research selection criteria strive to gather data sources which represent comprehensive cybersecurity challenges across different sectors and attack vectors as well as cyber threats. Using quality data resources enables the research to conduct a thorough assessment of how AI performs against cyber threats throughout different business fields.

3.3 Data Analysis Methods

Machine learning statistics enable the evaluation of AI systems as they prevent cyber-attacks according to this research study. The researchers use descriptive statistics which include mean detection accuracy and standard deviation of response times merged with cyber-attack type frequency metrics for AI performance summary. The examination of AI model capabilities to recognize cyber threats depends on supervised machine learning assessment through precision, recall and accuracy and. The evaluation compares the sheet threat detection capability and response speed performance of artificial intelligence security systems compared to conventional security principles [18]. The evaluation of AI's ability to forecast during time periods happens through time series analysis so researchers can observe its natural and predictive functions. The study creates visual representations based on data through Tableau as well as Matplotlib and Seaborn Python libraries to demonstrate AI effects in cybersecurity. The analytical methods form an integrated system to perform a complete assessment of how AI improves cyber threat detection as well as defense mechanisms.

3.4 Tools and Technologies

For conducting the analysis, the research utilizes different data processing and visualization tools and technologies [19]. The programming language Python combines statistical abilities with data preprocessing capability and model development for cybersecurity which enables strong management of security datasets. Through Tableau users develop dynamic visual plots that display results about AI performance measures alongside security pattern developments [20]. The security-related metrics and their organization and filtering and structure are managed efficiently through Excel data management applications. Organizations utilize Power BI to develop business intelligence reporting which lets them create dashboards to conduct detailed cybersecurity analyses

[21]. The Kaggle datasets serve as supplementary cybersecurity resources which enhance data source validation when assessing the performance of AI security patterns. These analysis tools create an organized framework for performing precise investigations about AI contributions in cybersecurity.

3.5 Validation and Reliability

Several methods are used to validate the study and increase reliability. There is a formal validation process implemented with k-fold cross-validation to guarantee that AI models maintain strong capabilities for detecting cyber threats [23]. AI benchmarking procedures involve assessing AI output through comparison with cybersecurity benchmarks which confirm both accuracy levels and operational efficiency of employed methods. The research uses peer-reviewed materials such as cybersecurity research articles as well as government publications and industry reports to validate the reliability of the secondary data [22]. A detailed research methodology documentation performs reproducibility checks to enable later studies that will test and validate the original discoveries. The verification methods enhance the study's reliability because they help produce precise analytical results.

3.6 Ethical Considerations

Strategic ethical guidelines govern data handling procedures in every phase of the research because cybersecurity data requires heightened protection. The organization maintains data privacy compliance through its adherence to GDPR and CCPA to handle data responsibly. Anonymization techniques operate to secure business-related and user data in datasets by protecting confidential information [23]. The implementation of algorithms requires diverse data management to stop potential biased outcomes. Research ethics are maintained through methodological documentation which allows for both reproducibility and ethical business conduct. Research in AI-driven cybersecurity follows ethical principles which maintain the research's integrity through proper accountability measures.

3.7 Limitations of the Study

The research admits several restrictions which potentially affect its results. The usage of secondary data as a source creates obstacles for the research because publicly available datasets restrict both the scope of analysis and its accuracy [24]. Modern security threats pose difficulties for AI detection models since new cyber threats form too quickly for the models to entirely recognize distinctly. The analysis faces processing speed limitations when working with big security incident data records because the system has restricted computational capabilities. The research analyzes past cybersecurity incidents instead of present-time data because it uses historical incidents that might not accurately represent modern AI applications in cyber protection [25]. this study needs research into boundary conditions while also focusing on cybersecurity analysis enhancements

4. Result

The analysis demonstrates that benign incidents lead all other grades including true positives and false positives which demonstrates that security alerts exist abundantly. The rising number of IP addresses throughout time indicates heightened network operations which create more potential threats [26]. The key prevention measures identified in incident response actions include regular password modifications and system software updates together with isolation protocols. Contextual alerts have increased substantially based on role-based alerts which demonstrates the critical requirement to focus security interventions [27]. The study results show how cybersecurity conditions continue to evolve thus requiring active preventive countermeasures to battle cyber-attacks in effective ways.

4.1 Impact of Trend of Cybersecurity Incidents Over Time

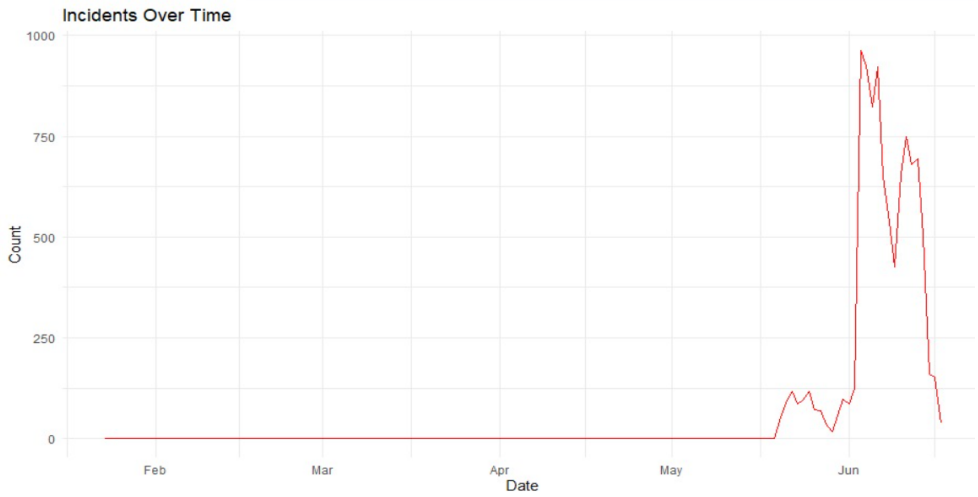


Figure 1: This Image illustrates the History of Cybersecurity Incidents Over Time

Figure 1 illustrates the history of cybersecurity incidents from February to June. Numerous cybersecurity incidents appear illustrated in Figure 1 throughout a specified period. Dates from February through June build the x-axis dimension whereas the number of incidents functions as the y-axis measure. The cybersecurity environment demonstrates low recorded threats or detected attacks between February and early May because incidents stay close to zero during that time period. The beginning of May introduced a clear uptick in incidents leading to a rapid explosive increase of incidents during June. Early June brings about a peak which results in nearly 1,000 recorded cyber threats. The rapid increase in data suggests a time when cybersecurity dangers rose sharply because of rising digital crime rates and unexploited security weaknesses and altering attack methods. After reaching the highest point the number of incidents decreased yet systematic fluctuations show that threats remained active. Irregularities observed in threat detection and AI security mechanisms and mitigation attempts likely explain the pattern abnormalities during the later stages of June. The information in Figure 1 demonstrates how AI software works as a crucial tool to track cyber threats in real time. Recent incident data shows clearly that organizations need superior predictive analytics which can spot threatening increases before they occur to reduce their impact. Medical institutions gain from analyzing these patterns to develop robust cybersecurity measures that defend their systems specifically during times of high threats.

4.2 Impact on Distribution of Cybersecurity Incident Categories

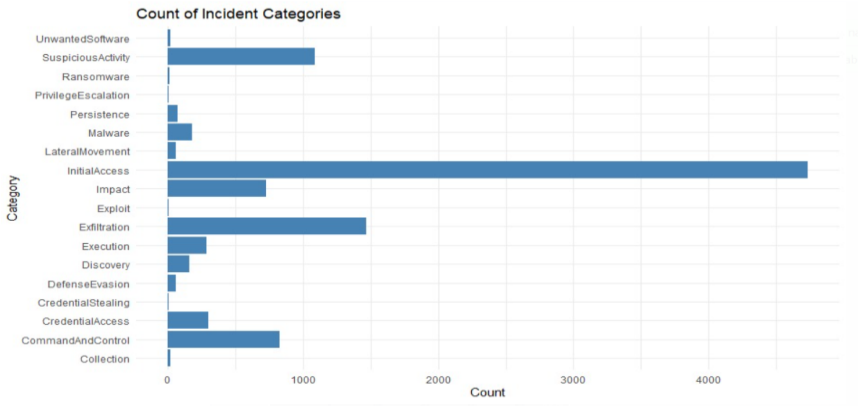


Figure 2: This chart shows the different categories of cybersecurity incidents are distributed throughout organizations

The figure demonstrates how different categories of cybersecurity incidents are distributed throughout organizations. The breakdown of cybersecurity incidents appears in Figure 2 according to their different types. The incident counts appear on the horizontal x-axis while cybersecurity threat categories appear on the vertical y-axis. The illustration demonstrates which incidents occur most frequently thus revealing the main entry points attackers use. The category of Lateral Movement stands out as the largest group among all types of incidents during the analysis period. Attackers normally move through compromised systems to gain access to their target critical assets. Exfiltration and Initial Access demonstrate high occurrence rates since attackers make unauthorized access and data extraction their main targets when inside the system. The numbers of Suspicious Activity and Command and Control attacks show that persistent threats use compromised systems for controlling operations at these same frequencies. The statistics indicate that Credential Access and Impact and Execution types occur at middle-level frequencies but Malware and Persistence together with Privilege Escalation and Defense Evasion present lower occurrence rates [28]. The statistics indicate malware-based attacks remain but the primary target of contemporary threats involves masking themselves through long-term access methods instead of exposing direct system harm. The analysis shows that AI-based cybersecurity systems need to be implemented promptly to stop lateral movement events and data theft activities. Secure entry points need strong authentication and monitoring because Initial Access incidents become increasingly prevalent. The data presented in Figure 2 established essential understanding about the changing cybersecurity threats that security strategies must use to defend against recurring attacks.

4.3 Impact of Distribution of Account SIDs by Entity Type

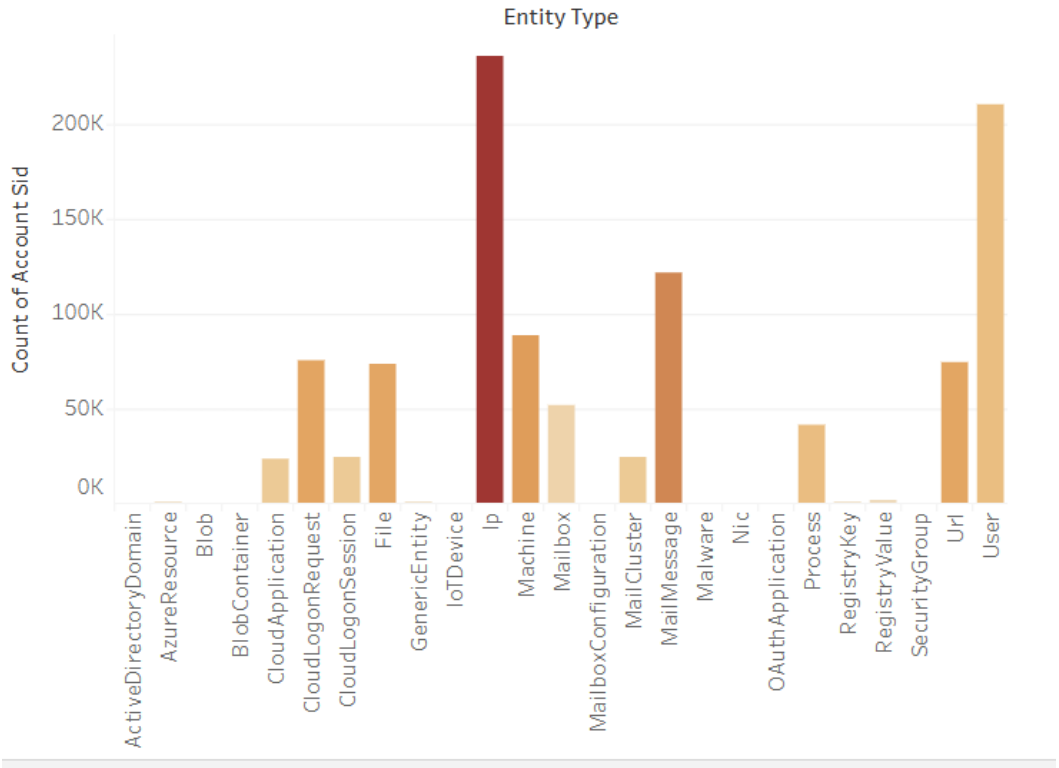


Figure 3: This Image Illustrated the Distribution of Account Security Identifiers Across Different Entity Types

Figure 3 shows the distribution of account security identifiers across different entity types which reveals which entities cybersecurity incidents target most often or become involved in the most. The analysis presents different entity types through the x-axis including IP

addresses, Users, Machines, IoT Devices, Mail Messages and Security Groups and reveals their respective account SID count through the y-axis. Most security events involve IP addresses following a trend of having the highest occurrence of associated account SIDs. The high number of recorded accounts SIDs indicates network attacks and unauthorized access attempts and malicious IP address behaviors are frequent during cybersecurity events. The User entity displays a significant number of occurrences because cyber attackers often target user credentials making it crucial to deploy robust authentication protocols with user monitoring systems. Mail Messages and Machines demonstrate important SID counts among the entity types observed in the system. The high frequencies show that email attacks as well as phishing and malware delivery represent crucial aspects of cybersecurity breaches. Security Groups along with Generic Entities demonstrate a significant number of occurrences because attackers try to exploit organization-wide access control systems and network structure frameworks. The growing number of security issues regarding Internet of Things (IoT) devices leads to heightened activities being recorded in the IoT Device category. Organizations must establish comprehensive security protocols to monitor their networks and manage identities as well as detect email threats proactively because these entities experience frequent attacks.

4.4 Analysis of Incident Grades in Cybersecurity Detection

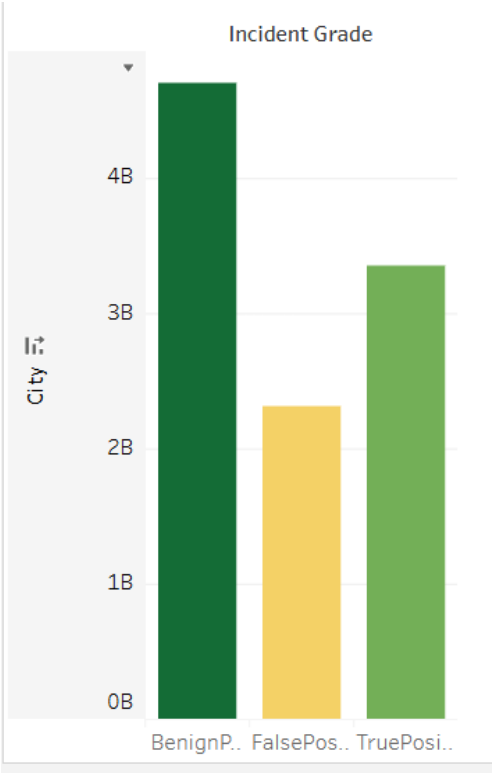


Figure 4: This Image present the Three Detection Outcome Categories of Cybersecurity Incidents

The graph in Figure 4 displays the three detection outcome categories of cybersecurity incidents as Benign Positives, False Positives and True Positives. Incident grade frequencies appear on the vertical axis that correspond with different incident categories shown on the horizontal axis. A large percentage of detected incidents were marked as harmless non-malicious activities during additional examination as determined by the Benign Positive category. This outcome demonstrates how initial detection systems identify abnormal activities successfully yet shows how difficult it is to dismiss unneeded alerts. The False Positive category emerges second only to Benign Positive in terms of occurrence statistics. False positive occurrences lead security operations to make

inefficient processes because they incorrectly classify standard activities as security threats. The excessive number of incorrect alerts tires out cybersecurity staff but operators need enhanced detection systems to avoid these mistakes. True Positive category takes residence between Benign and False Positive categories regarding frequency. The security tools exhibit solid behavior when identifying genuine threats yet require ongoing AI model development to achieve better accuracy levels [28]. The graphic demonstrates that security detection systems need to maintain proper proportions between their capacity to detect genuine risks and their ability to prevent unnecessary alerts. The production of genuine security detections without extra false alarms has become an essential objective to boost cybersecurity operational efficiency.

4.5 Trend Analysis of IP Address Activity Over Time

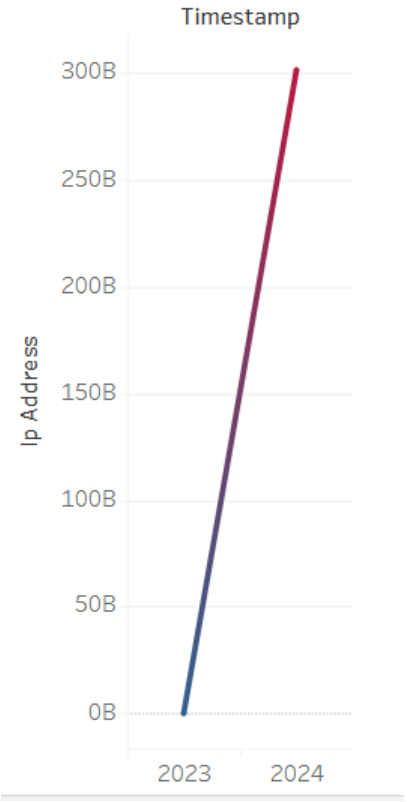


Figure 5: The Charts shows the Rapid Growth of IP Address Counts Triggering Network Events

Fig. 5 shows the rapid growth of IP address counts triggering network events or cybersecurity incident-related actions from 2023 into 2024. The vertical axis shows recorded event IP addresses counted over time from year 2023 through year 2024 while the horizontal axis measures timestamp. The rapidly rising pattern indicates a major boost in network communication intensity due to diverse factors such as expanding cyberattack rates and unauthorized entry attempts and automated scanning protocols and augmented security system surveillance activities. The color scale starting at blue and ending at red demonstrates an escalating level of cybersecurity incidents observed throughout the recent years. Endpoint security incidents are on the rise due to two reasons: attackers have expanded their capability through automated tools and artificial intelligence techniques while businesses have enlarged their network attacks by adopting cloud services and IoT devices combined with remote work protocols. Modern advanced security threat detection systems have enhanced analyst capabilities to detect and record more suspicious activities while simultaneously playing a role in this rise. The current security needs require advanced artificial intelligence-powered security systems to perform instant detection and

evaluation and attack prevention of cyber dangers. Every organization needs to spend money on future-focused cybersecurity prevention methods including active threat espionage and adaptive defense frameworks to protect against rising cyber threats. Further studies need to develop methods to differentiate normal network expansion from threats so both cybersecurity defenses and potential threats can be improved.

4.6 Analysis of Incident Grade Across URL Activities

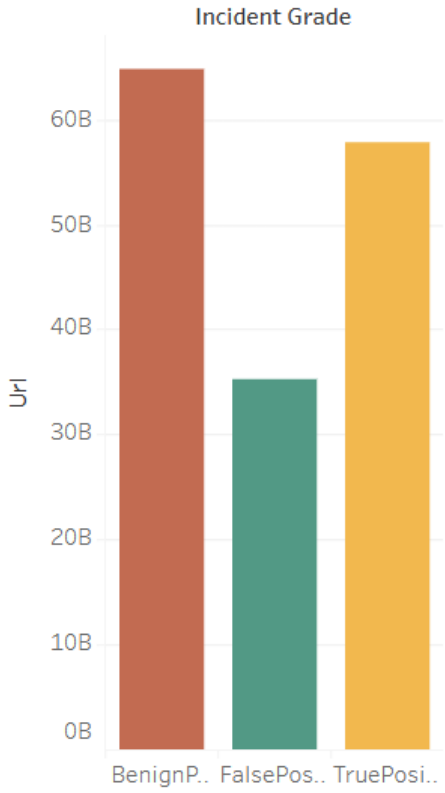


Figure 6: This image illustrates the URL-related incident distribution according to the grading labels

Figure 6 shows the URL-related incident distribution according to the grading labels which include Benign Positives (BenignP.), False Positives (FalsePos.), and True Positives (TruePosi.). These incident grades are organized on the x-axis as they report the counted occurrences through the billion scale on the y-axis. The security analysis results demonstrate that Benign Positives outnumber all other classes thus showing safety verification was performed on many URLs. Robust security mechanisms seem to filter many incidental threats which prevents their detection since such incidents do not directly pose threats. The count of False Positive threats identified by the security system stands lower than both True and Benign Positive incidents. The detection system operates effectively since it correctly labels most URLs as threats yet misidentifies some URLs as threats. Minimizing security team workload requires better development of classification models to reduce the number of wrong threat alerts. True Positives category presents many occurrences which demonstrate genuine threatening URLs in the dataset. The elevated number of True Positive results indicates major active web-based security threats which demonstrates why organizations must adopt continuous surveillance backed by AI-based security systems. Organizations should dedicate efforts to developing instant threat intelligence and flexible security systems because harmful URLs create significant security dangers. The development of research should investigate next-generation machine learning methods to create better URL threat identification systems because it enhances both precision and cybersecurity operations.

4.7 Analysis of Alert Title Distribution Across Roles

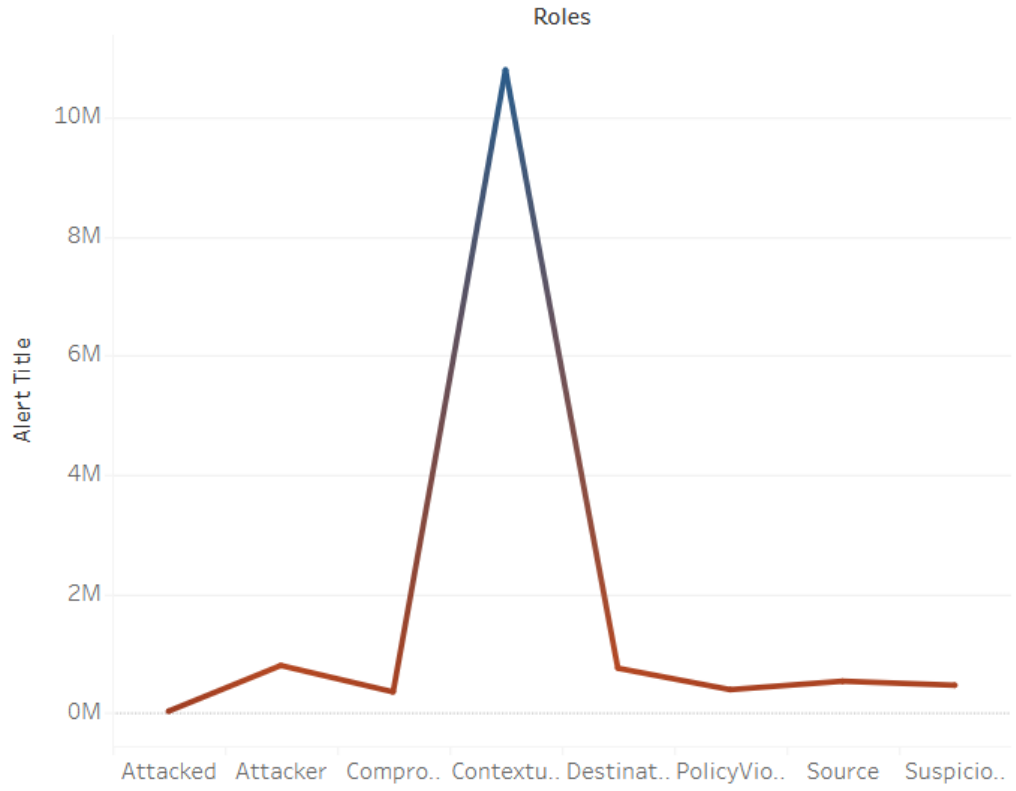


Figure 7: This Image represent the Distribution of Alert Titles between Different Roles

Figure 7 displays the distribution of alert titles between different roles which consists of Attacked, Attacker, Compromised, Contextual, Destination, Policy Violation, Source, and Suspicious incidents. The study shows the alert volume on the vertical or y-axis expressed as millions when compared with roles on the horizontal or x-axis that deal with cybersecurity incidents. Security alerts from the Contextual category create the most pronounced peak in the data since it generates alerts exceeding 10 million detections. Context-based threat detection practices create many security alerts through their behavioral analysis and anomaly detection methods. Alerts about direct attack incidents and suspicious activities exist in limited numbers as part of the Attacked, Attacker and Suspicious roles but they fall substantially behind the large number of context-based alerts. The number of alerts reported under the Destination and Policy Violation categories remains low indicating that policy violations together with destination anomalies are not significant threats to the detection system. The data pattern in Figure 7 underscores the growing importance of context-aware cybersecurity approaches. This excessive number of contextual alerts demonstrates that organizations increasingly use advanced artificial intelligence security frameworks which analyze behavioral patterns above static threat patterns [29]. Improved detection accuracy through advanced systems creates a need to develop automated alert prioritization systems because of the high volume of alerts being generated. Future studies should develop optimal methods to enhance contextual alert analytics to reduce false positive alerts for increasing cybersecurity defenses.

4.8 Analysis of Incident Response Actions in Cybersecurity Framework

Figure 8: This Image demonstrated the Different Incident Response Actions

A bubble chart in Figure 8 depicts different incident response actions which occur inside a cybersecurity framework. The size of bubbles represents action frequency to demonstrate major security incident response strategies that organizations use for mitigation purposes. System or software updates represent the most executed response according to the dataset metrics which this large bubble signifies. The practice of constant system refresh aligns with security best standards because frequent updates prevent and reinforce security defenses. The second most important stances in the dataset are "account password changed" and "change user password" that appear through substantial bubbles. Frequent password changes represent a necessary countermeasure against unauthorized access because compromised credentials have become a main security concern. Security frameworks highlight the need for multiple authentication methods together with securing credentials because of these actions. The dataset shows "isolate response" as a vital critical response element. Current security procedures show that teams often decide to disconnect compromised devices and users to stop the spread of active threats. Security professionals use isolation techniques against malware infections as well as attacks from both inside the organization and unauthorized access attempts [30]. The smaller visualized bubbles indicate that authorities execute varied response strategies for cybersecurity threats while still maintaining uncommon limited measures. Figure 8 demonstrates the critical position of preventive techniques and credential security along with system isolation in controlling security incidents through an organized approach to handling cyber threats.

5. Discussion and Analysis

5.1 Role of AI in Cybersecurity

Artificial intelligence (AI) established itself as a revolutionary cybersecurity tool which improves business momentum towards detecting along with preventing and handling cyber

threats [31]. AI-based security structures deliver current threat observation with behavioral analysis and automated security protocols that minimize standard security architecture dependency. Advances in cyber threat intensity demand protective systems developed through artificial intelligence because zero-day attacks and ransomware as well as phishing schemes require strong defenses [32]. The research demonstrates AI capability of handling enormous security information alongside its capacity to spot abnormal patterns and forecast dangerous incidents as a fundamental advancement for current cybersecurity methods.

5.2 Effectiveness of AI-Based Threat Detection

The research demonstrates how modern cybersecurity presents superior capabilities by evaluating its threat identification functions system with AI capabilities make use of machine learning and deep learning models along with natural language processing to detect threats in network traffic by analyzing network traffic white monitoring for suspicious behavior [33]. AI demonstrates its strength by changing its security models according to new threats in the market which enables successful defense against sophisticated cyber-attacks. "As per analysis research AI security platforms recognize incidents more effectively and minimize incorrect alerts while replying faster than conventional rule-based defenses do." AI detection capabilities become better because of adaptive learning which builds business cybersecurity resilience.

5.3 AI's Role in Automating Cyber Security Response

This study demonstrates AI's ability to substantial efficiency improvement in cybersecurity incident response through automated threat management systems [34]. A security orchestration system that uses AI together with automated response technology provides immediate threat analysis and management service independently of human operators [35]. The automation process controlled by AI shortens response times and lowers the possibility of mistakes in cybersecurity operations. Business operations benefit from AI incident response functionality through better security breach control and threat containment along with secure area protection [36]. The combination of AI technology with Security Information and Event Management (SIEM) systems enhances security monitoring capabilities because it helps organizations to track data from various sources while finding sophisticated persistent threats.

5.4 Comparative Analysis: AI vs. Traditional Security Approaches

This Study investigation evaluates the result efficiency between AI security structures and conventional security defense mechanisms [37]. Traditional security systems achieve their results through pre-established rules with signature-based detection which turns out to be ineffective when dealing with modern cyber threats. The predictive analytics combined with machine learning capabilities of AI based cybersecurity solutions lets them monitor and stop cyber-attack before they occur [38]. The usage of AI-based threat detection models delivers better threat identification capabilities as well as less erroneous alerts with better immediate responses [39]. The analysis demonstrates that AI systems can dynamically adjust toward developing cyber threats because traditional security management needs constant manual update maintenance to operate effectively.

5.5 AI delivers substantial help to the collection and analysis of cyber threat data

This Study analyzes how Artificial Intelligence helps develop cyber threat intelligence through its analysis of worldwide threat arenas combined with vector prediction capabilities [40]. The combination of artificial intelligence produces threat intelligence platforms that accumulate and evaluate extensive security data across different source types like dark web oversight together with phishing strategies along with malware

detection patterns. Although conducted in engagements across four countries AI proves valuable by recognizing security patterns which generate useful security recommendations for businesses [41]. By using AI predictive analytics organizations can maintain their position in front of cybercriminals because the system helps identify threats before they happen and allows them to improve their defenses. The research establishes that artificial intelligence enhances decision-making security functions through complete threat intelligence and fast-running risk evaluations.

5.6 Challenges in AI-Based Cybersecurity Implementation

This study demonstrated multiple issues that emerge during AI implementation for cyber-attack prevention despite its established success as a prevention measure [42]. There is a major problem when cybercriminals manipulate AI detection systems through adversarial attacks. Cyber attackers modify malware signatures along with attack behaviors to accomplish getting past security systems using AI. AI threat detection accuracy is reduced through the presence of bias that exists in these systems [43]. A biased training dataset affects the way AI makes decisions that leads to either security threats being unnoticed or to false positive alerts. Research demonstrates that AI cybersecurity solutions need considerable processing capability with an ongoing model training process to defend against changing cyber threats.

5.7 Artificial Intelligence Adaptability to Emerging Cyber Threats

This study demonstrated how AI systems can easily adjust to continuous changes within the cyber threat environment. Businesses gain better cybersecurity defense through AI because this technology incrementally adds new attack patterns to its learning knowledge base [44]. AI protects cybersecurity operations because it analyzes previous threats to identify forthcoming threats which makes it an essential tool in IT protection. AI systems require routine updates with top-quality training data to maximize their ability to predict threats precisely. Researchers confirm that AI-run cybersecurity tools need reinforcement learning capabilities for enhancing their ability to track new cyber threats effectively [45]. Organizations need to support AI model optimization because it improves threat detection performance and cuts down the probability of security violations.

5.8 Ethical and Privacy Considerations in AI-Driven Cybersecurity

The research evaluates both privacy and ethical problems found in cybersecurity systems that use AI. Security systems using AI processes examine huge databases of data which creates concerns regarding both privacy protection of information and compliance with GDPR and CCPA regulations [46]. Firms operating AI-based security features need to maintain compliance with ethical guidelines and data protection regulations to stop unauthorized access. Researchers have demonstrated the need to maintain visibility into AI algorithm processes for security solutions based on artificial intelligence technology [47]. Organizations need to use explainable AI (XAI) methods to increase visibility and responsibility in their AI-based threat monitoring systems.

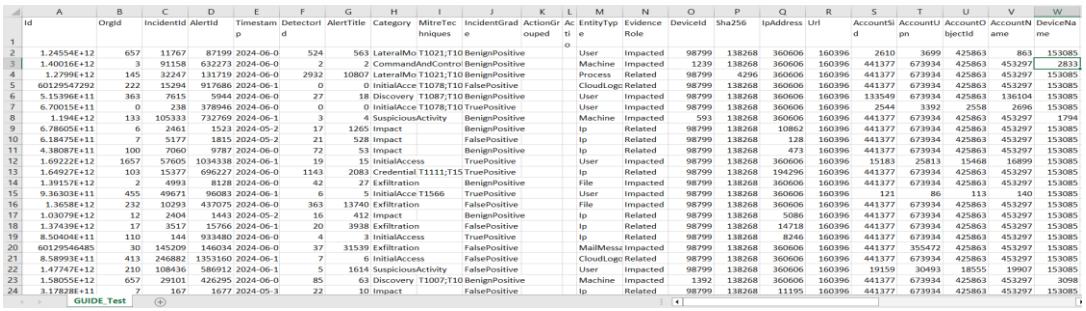
5.9 Future Trends in AI-Powered Cybersecurity

The study explores upcoming AI cyber security patterns through the combination of sophisticated artificial intelligence methods for security improvement strategies. Analyzing deep reinforcement learning and federated learning together with blockchain based security solutions will transform the fundamental framework of cybersecurity frameworks [48]. The combination between quantum computing technology with AI security models helps develop improved encryption systems that create stronger defense from cyberattacks. Research and development activities must continue because they help improve AI systems in finding threats as well as making automatic responses and assessing cyber risks [49].

The next generation of cybersecurity plans needs to build teams that can handle AI model explanations and protect systems from adversarial attacks while creating ethical guidelines for AI management.

6. Discussion

6.1 Screenshot of few Dataset



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Id	OrgId	IncidentId	AlertId	Timestamp	DetectorId	AlertTitle	Category	MitreTechniques	IncidentGrade	ActionGrouped	Action	EntityType	Evidence Role	DeviceId	Sha256	IpAddress	Url	AccountSid	AccountUpn	AccountObjectId	AccountName	DeviceName
1																							
2	1.24554E+12	657	11767	87199	2024-06-0	524	563	LateralMo	T1021;T10	BenignPositive			User	Impacted	98799	138268	360606	160396	2610	3699	425863	863	153085
3	1.40016E+12	3	91158	632273	2024-06-0	2	2	CommandAndControl		BenignPositive			Machine	Impacted	1239	138268	360606	160396	441377	673934	425863	453297	2833
4	1.2799E+12	145	32247	131719	2024-06-0	2932	10807	LateralMo	T1021;T10	BenignPositive			Process	Related	98799	4296	360606	160396	441377	673934	425863	453297	153085
5	60129547292	222	15294	917686	2024-06-1	0	0	InitialAcce	T1078;T10	FalsePositive			CloudLogo	Related	98799	138268	360606	160396	441377	673934	425863	453297	153085
6	5.15396E+11	363	7615	5944	2024-06-0	27	18	Discovery	T1087;T10	BenignPositive			User	Impacted	98799	138268	360606	160396	133549	673934	425863	136104	153085
7	6.70015E+11	0	238	378946	2024-06-0	0	0	InitialAcce	T1078;T10	TruePositive			User	Impacted	98799	138268	360606	160396	2544	3392	2558	2696	153085
8	1.194E+12	133	105333	732769	2024-06-1	3	4	SuspiciousActivity		BenignPositive			Machine	Impacted	593	138268	360606	160396	441377	673934	425863	453297	1794
9	6.78605E+11	6	2461	1523	2024-05-2	17	1265	Impact		BenignPositive			Ip	Related	98799	138268	10862	160396	441377	673934	425863	453297	153085
10	6.18475E+11	7	5177	1815	2024-05-2	21	528	Impact		FalsePositive			Ip	Related	98799	138268	128	160396	441377	673934	425863	453297	153085
11	4.38087E+11	100	7060	9787	2024-06-0	72	53	Impact		BenignPositive			Ip	Related	98799	138268	473	160396	441377	673934	425863	453297	153085
12	1.69222E+12	1657	57605	1034338	2024-06-1	19	15	InitialAccess		TruePositive			User	Impacted	98799	138268	360606	160396	15183	25813	15468	16899	153085
13	1.64927E+12	103	15377	696227	2024-06-0	1143	2083	Credential	T1111;T15	TruePositive			Ip	Related	98799	138268	194296	160396	441377	673934	425863	453297	153085
14	1.39157E+12	2	4993	8128	2024-06-0	42	27	Exfiltration		BenignPositive			File	Impacted	98799	138268	360606	160396	441377	673934	425863	453297	153085
15	9.36303E+11	455	49671	96083	2024-06-1	6	5	InitialAcce	T1566	TruePositive			User	Impacted	98799	138268	360606	160396	121	86	113	140	153085
16	1.3658E+12	232	10293	437075	2024-06-0	363	13740	Exfiltration		FalsePositive			File	Impacted	98799	138268	360606	160396	441377	673934	425863	453297	153085
17	1.03079E+12	12	2404	1443	2024-05-2	16	412	Impact		BenignPositive			Ip	Related	98799	138268	5086	160396	441377	673934	425863	453297	153085
18	1.37439E+12	17	3517	15766	2024-06-1	20	3938	Exfiltration		FalsePositive			Ip	Related	98799	138268	14718	160396	441377	673934	425863	453297	153085
19	8.50404E+11	110	144	933480	2024-06-0	4	3	InitialAccess		TruePositive			Ip	Related	98799	138268	8246	160396	441377	673934	425863	453297	153085
20	60129546485	30	145209	146034	2024-06-0	37	31539	Exfiltration		FalsePositive			MailMessa	Impacted	98799	138268	360606	160396	441377	355472	425863	453297	153085
21	8.58993E+11	413	246882	1353160	2024-06-1	7	6	InitialAccess		FalsePositive			CloudLogo	Related	98799	138268	360606	160396	441377	673934	425863	453297	153085
22	1.47747E+12	210	108436	586912	2024-06-1	5	1614	SuspiciousActivity		FalsePositive			User	Impacted	98799	138268	360606	160396	19159	30493	18555	19907	153085
23	1.58055E+12	657	29101	426295	2024-06-0	85	63	Discovery	T1007;T10	BenignPositive			Machine	Impacted	1392	138268	360606	160396	441377	673934	425863	453297	3098
24	3.17828E+11	7	167	1677	2024-05-3	22	10	Impact		FalsePositive			Ip	Related	98799	138268	11195	160396	441377	673934	425863	453297	153085

GUIDE_Test

6.2 Dataset Overview

Through machine learning the Microsoft Security Incident Prediction dataset known as GUIDE serves as an innovative dataset that improves cybersecurity incident prediction capabilities. Microsoft Security AI Research created this dataset that unites authenticated security events into an organized structure for researchers who want advanced protection strategies. Microsoft Security Incident Prediction dataset GUIDE contains data from 6,100 organizations spanning two weeks which includes 13 million pieces of evidence together with 1.6 million alerts and 1 million annotated incidents. The GUIDE system structures security events into three successive levels which start with evidence and extend to alerts and end with incidents. The evidence level contains original telemetry data which includes IP addresses along with user details and email information. Security systems combine multiple evidence sources to produce security events which become part of the alert level. Incidents integrate numerous alerts into one complete cybersecurity threat description which needs both evaluation and response procedures. The main task of the GUIDE system involves using data from past client response assessments to forecast incident triage class assignments. Alerts connecting to cybersecurity decisions receive three potential definitions: true positive (TP) and benign positive (BP) for valid events along with false positive (FP) for inaccuracies or incorrect alerts [53]. The dataset consists of 45 features that include timestamps from incidents and alert categories together with detector IDs and MITRE ATT&CK techniques to conduct effective feature extraction and machine learning model training. Fifty percent of the data is used for training while thirty percent remains for testing purposes to achieve balanced stratified distribution according to triage grades and organization IDs and detector IDs. GUIDE offers 26,000 remediation actions that help practitioners evaluate automated response solutions. The guided response (GR) systems developed with this data aid Security Operation Center (SOC) analysts making better decisions. Benchmarking predictive models can be done through the dataset which allows macro-F1 score assessment together with precision and recall metrics for performance evaluation. Microsoft implements SHA1 hashing and random ID generation which create anonymous data protection systems for sensitive information. Security event timestamps receive modifications that remove links between them and particular security events. The GUIDE platform sets a standard for AI security solution assessment by giving access to an extensive anonymized data collection. There are multiple direct benefits for security professionals and researchers working on AI threat detection because this database allows them to enhance automated responses and real-time risk management protocols within business operations. Security protection becomes stronger through integrating the dataset into AI systems which produces improved threat intelligence capabilities and shorter

response times and stronger organizational resistance against cyber threats.

7. Future Work

Artificial intelligence (AI) proves effective for business cyber-attack prevention but more research must address development of refined security frameworks through AI technology [49]. The main task for researchers in the future consists of improving AI model precision and decreasing false alarm frequency because excessive false flagging causes strain for cybersecurity personnel. The development of enhanced anomaly detection machine learning models will support the solution of this challenge. The combination of AI systems using blockchain technologies made stronger data protection and visibility which enables distributed methods for threat information sharing while validating its accuracy. XAI research remains essential because businesses need AI models to show their operation logic while meeting regulatory compliance and earning trust from security automation users [50]. Future investigations should emphasize the development of self-activating defense systems based on artificial intelligence since this technology eliminates human involvement for real-time incident solutions leading to faster incident resolution and minimized potential risks. Federated learning enables different organizations to work together for enhancing AI models for cyber threat detection through privacy-protecting collaboration. Professional AI software designed for healthcare systems alongside financial institutions and manufacturing environments should be developed to address cybersecurity demands that exist within separate business domains. Security systems leverage reinforcement learning alongside adaptive AI models developed autonomously to counter new security threats which results in enhanced AI-driven cyber security resilience. The study needs to proceed with investigations about real-time cybersecurity automation and cloud-based AI security solutions to achieve better scalability and efficiency [51]. Future research about business cybersecurity should target the improvements of AI systems to adapt better and enhance accuracy and automation because this research shows AI's vital importance in cyber defense.

8. Acknowledgement

This paper completion was made possible by the sincere thanks extended to all individuals who participated in the research on Assessing the Effectiveness of Artificial Intelligence in Preventing Cyber Attacks on Businesses. All my appreciation goes to my academic advisors and mentors because they provided essential guidance alongside their beneficial comments and enduring support during this research endeavor. I thank my colleagues along with peers because their encouragement along with constructive discussions improved the quality of this research study. Research on cybersecurity and artificial intelligence gained strength from multiple experts and professionals who investigated the field. I express deep appreciation to my family along with my friends who provided continuous support, inspiration, along with unyielding patience while I pursued my research activities.

9. Conclusion

Artificial intelligence development at a fast pace has transformed cybersecurity operations through improved abilities to find and prevent business-related cyber threats. The detection of forthcoming cyberattacks becomes possible because predictive analytics operates within AI systems. The improvements achieved through AI have demonstrated its usefulness as a security tool in cyber domains. Some difficulties emerge from this research investigation. When using artificial intelligence technology algorithms often contain biases that affect their operations. The detection process becomes more challenging because these systems generate numerous unjustified warnings that hide genuine threats. The implementation of AI cybersecurity remains restricted because privacy matters involving data collection

occupy a significant position as an obstacle [52]. Better AI implementation requires solving the present challenges even though it delivers numerous advantages. This study utilized a complete evaluation of AI prevention effectiveness for cyber-attacks by analyzing Microsoft Security Incident Prediction data through multiple machine learning models together with visual data analysis methods. Security solutions that use artificial intelligence enhance protection measures in three ways which include minimized human intervention and better threat detection along with improved reaction speed towards new threats. Companies which use AI for their cybersecurity programs obtain more effective proactive capabilities that help them detect cybersecurity threats before they happen. The research project recognizes AI security systems have certain boundaries that restrict their effectiveness. AI's effectiveness as a cyber threat detection system depends on historical data but this approach proves inadequate for new security threats which require constant improvement in AI models. Building trust in AI-based security technology requires organizations to handle ethical issues which include making systems transparent, reducing bias factors and complying with regulations. The research should advance by combining AI with blockchain technology for secure threat intelligence exchange as well as supporting explainable AI development and creating AI models which adapt to changing cyber threats. Businesses have access to an innovative cybersecurity solution through AI which enhances their capacity to identify and stop cyber threats with better efficiency. AI technology development alongside ethical standards along with proper regulations will produce better performance from AI-based cybersecurity solutions moving forward. Businesses need to develop a combined security system which uses artificial intelligence alongside human security expertise and standard defense protocols to build maximum cybersecurity strength. These research results demonstrate essential knowledge about AI use in current cybersecurity protection systems which emphasizes the requirement to develop new technologies to excel against digital attackers.

10. References:

1. Bouramdane, A. A. (2023). Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, *3*(4), 662-705. https://www.mdpi.com/2624-800X/3/4/31

2. De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, *12*(8), 1920. https://www.mdpi.com/2079-9292/12/8/1920

3. Alrfai, M. M., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M., & Almaiah, M. A. (2023). The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security. *Cogent Social Sciences*, *9*(2), 2243719. https://www.tandfonline.com/doi/full/10.1080/23311886.2023.2243719#abstract

4. Ali, A., Septyanto, A. W., Chaudhary, I., Al Hamadi, H., Alzoubi, H. M., & Khan, Z. F. (2022, February). Applied artificial intelligence as event horizon of cyber security. In *2022 International Conference on Business Analytics for Technology and Security (ICBATS)* (pp. 1-7). IEEE. https://ieeexplore.ieee.org/abstract/document/9759076

5. Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEe Access*, *12*, 12229-12256. https://ieeexplore.ieee.org/abstract/document/10403908

6. Qasaimeh, G. M., & Jaradeh, H. E. (2022). The impact of artificial intelligence on the effective applying of cyber governance in Jordanian commercial banks. *International*

Journal of Technology Innovation and Management (IJTIM), *2*(1). https://www.journals.gaftim.com/index.php/ijtim/article/view/61

7. Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In *Artificial intelligence for societal issues* (pp. 3-25). Cham: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-031-12419-8_1
8. Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *DOI: https://www. doi. org/10.56726/IRJMETS32644*, *1*. https://d1wqtxts1xzle7.cloudfront.net/112737594/REVOLUTIONIZING_CYBERSECURITY-libre.pdf?1711378319=&response-content-disposition=inline%3B+filename%3DREVOLUTIONIZING_CYBERSECURITY_UNLEASHING.pdf&Expires=1741472433&Signature=RmXSFWl6U17cpQudSM2LMHdI7TISMHhv41HJFKqlssFIgY9qVmiCUFqpFFpkrVomDO3V3rsm~5ivu-JEKNZpK04BLt3HmhJYVOxA4elVVw2S3-Wdu1YejqiaKEM23blonRpPi-nRr50qvKocVVIo7IqHHNeEToJQLgkf7x~xEE~xeFOi37luPDUwIdFinP6hvYngYEXQCtpk5W7GSfoMOPoBLvsOU15LyIJPyjVWDVe5~TiBuPfDZ1bdhdCYYg6qQjIIu1kiA-m~gsEGR9zyYymn4Hr0SdGc03NhxiappSIbMPt5K9AUeaE2dNAy5pNiNzTLExRZlIXdwnyjMG2xKQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
9. Rane, N., Choudhary, S., & Rane, J. (2024). Artificial intelligence for enhancing resilience. *Journal of Applied Artificial Intelligence*, *5*(2), 1-33. https://sabapub.com/index.php/jaai/article/view/1053
10. Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: a review. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(5). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323258
11. Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. *Authorea Preprints*. https://d197for5662m48.cloudfront.net/documents/publicationstatus/90291/preprint_pdf/c12f4b6dfcb0ece3a42a357ad2203fac.pdf
12. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://www.mdpi.com/1424-8220/23/15/6666
13. Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, *8*(28). https://www.researchgate.net/profile/Muhammad-Akhtar-164/publication/353046785_The_future_of_Artificial_Intelligence_in_Cybersecurity_A_Comprehensive_Survey/links/60e5fe731c28af345850da39/The-future-of-Artificial-Intelligence-in-Cybersecurity-A-Comprehensive-Survey.pdf
14. Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, *36*, 100520. https://www.sciencedirect.com/science/article/pii/S2452414X23000936
15. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial*

Intelligence, *36*(1), 2037254. https://www.tandfonline.com/doi/full/10.1080/08839514.2022.2037254

16. Bokhari, S. A. A., & Myeong, S. (2023). The influence of artificial intelligence on e-Governance and cybersecurity in smart cities: A stakeholder's perspective. *IEEE Access*, *11*, 69783-69797. https://ieeexplore.ieee.org/abstract/document/10177170
17. Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132. https://core.ac.uk/download/pdf/578755756.pdf
18. Narsimha, B., Raghavendran, C. V., Rajyalakshmi, P., Reddy, G. K., Bhargavi, M., & Naresh, P. (2022). Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application. *International Journal of Electrical and Electronics Research*, *10*(2), 87-92. https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100206.html
19. Salama, R., & Al-Turjman, F. (2023). Cyber-security countermeasures and vulnerabilities to prevent social-engineering attacks. In *Artificial intelligence of health-enabled spaces* (pp. 133-144). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003322887-7/cyber-security-countermeasures-vulnerabilities-prevent-social-engineering-attacks-ramiz-salama-fadi-al-turjman
20. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://www.sciencedirect.com/science/article/pii/S1566253523001136
21. Bharadiya, J. P. (2023). AI-driven security: how machine learning will shape the future of cybersecurity and web 3.0. *American Journal of Neural Networks and Applications*, *9*(1), 1-7. https://www.researchgate.net/profile/Saqib-Luqman/publication/371983373_Jasmin_Praful_Bharadiya_AI-Driven_Security_How_Machine_Learning_Will_Shape_the_Future_of_Cybersecurity_and_Web_30/links/64a0e5948de7ed28ba6addcd/Jasmin-Praful-Bharadiya-AI-Driven-Security-How-Machine-Learning-Will-Shape-the-Future-of-Cybersecurity-and-Web-30.pdf
22. Rana, N. P., Chatterjee, S., Dwivedi, Y. K., & Akter, S. (2022). Understanding dark side of artificial intelligence (AI) integrated business analytics: assessing firm's operational inefficiency and competitiveness. *European Journal of Information Systems*, *31*(3), 364-387. https://www.tandfonline.com/doi/full/10.1080/0960085X.2021.1955628
23. Chehri, A., Fofana, I., & Yang, X. (2021). Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability*, *13*(6), 3196. https://www.mdpi.com/2071-1050/13/6/3196
24. Awotunde, J. B., & Misra, S. (2022). Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks. In *Illumination of artificial intelligence in cybersecurity and forensics* (pp. 21-44). Cham: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-93453-8_2
25. Rashid, A. B., Kausik, A. K., Al Hassan Sunny, A., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. *International journal of intelligent systems*, *2023*(1), 8676366.

https://onlinelibrary.wiley.com/doi/full/10.1155/2023/8676366

26. Varma, A. J., Taleb, N., Said, R. A., Ghazal, T. M., Ahmad, M., Alzoubi, H. M., & Alshurideh, M. (2023). A roadmap for SMEs to adopt an AI based cyber threat intelligence. In *The effect of information technology on business and marketing intelligence systems* (pp. 1903-1926). Cham: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-031-12382-5_105
27. Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, *13*(10), 5875. https://www.mdpi.com/2076-3417/13/10/5875
28. Ahmed, A., Awaıs, M., Sıraj, M., & Umar, M. (2023). Enhancing cybersecurity with trust-based machine learning: A defense against ddos and packet suppression attacks. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, *23*, 262-268. http://www.epstem.net/en/download/article-file/3441854
29. Allal-Chérif, O., Simón-Moya, V., & Ballester, A. C. C. (2021). Intelligent purchasing: How artificial intelligence can redefine the purchasing function. *Journal of Business Research*, *124*, 69-76. https://www.sciencedirect.com/science/article/abs/pii/S0148296320308031
30. Mahalakshmi, V., Kulkarni, N., Kumar, K. P., Kumar, K. S., Sree, D. N., & Durga, S. (2022). The role of implementing artificial intelligence and machine learning technologies in the financial services industry for creating competitive intelligence. *Materials Today: Proceedings*, *56*, 2252-2255. https://www.sciencedirect.com/science/article/abs/pii/S221478532107601X
31. Judijanto, L., Hindarto, D., & Wahjono, S. I. (2023). Edge of enterprise architecture in addressing cyber security threats and business risks. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(3), 386-396. https://journal.lembagakita.org/ijsecs/article/view/1816
32. Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. *Computer Networks*, *206*, 108771. https://www.sciencedirect.com/science/article/abs/pii/S138912862200007X
33. Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527-555. https://www.mdpi.com/2624-800X/2/3/27
34. Iwendi, C., Rehman, S. U., Javed, A. R., Khan, S., & Srivastava, G. (2021). Sustainable security for the internet of things using artificial intelligence architectures. *ACM Transactions on Internet Technology (TOIT)*, *21*(3), 1-22. https://dl.acm.org/doi/abs/10.1145/3448614
35. Bahrini, A., Khamoshifar, M., Abbasimehr, H., Riggs, R. J., Esmaeili, M., Majdabadkohne, R. M., & Pasehvar, M. (2023, April). ChatGPT: Applications, opportunities, and threats. In *2023 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 274-279). IEEE. https://ieeexplore.ieee.org/abstract/document/10137850
36. Zaman, Shakila, Khaled Alhazmi, Mohammed A. Aseeri, Muhammad Raisuddin Ahmed, Risala Tasin Khan, M. Shamim Kaiser, and Mufti Mahmud. "Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey." *Ieee Access* 9 (2021): 94668-94690.

https://ieeexplore.ieee.org/abstract/document/9456954

37. Krichen, M. (2023). Strengthening the security of smart contracts through the power of artificial intelligence. *Computers*, *12*(5), 107. https://www.mdpi.com/2073-431X/12/5/107

38. Nozari, H., Szmelter-Jarosz, A., & Ghahremani-Nahr, J. (2022). Analysis of the challenges of artificial intelligence of things (AIoT) for the smart supply chain (case study: FMCG industries). *Sensors*, *22*(8), 2931. https://www.mdpi.com/1424-8220/22/8/2931

39. Raza, A., Munir, K., Almutairi, M. S., & Sehar, R. (2023). Novel class probability features for optimizing network attack detection with machine learning. *IEEE Access*, *11*, 98685-98694. https://ieeexplore.ieee.org/abstract/document/10246280

40. Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. *Internet of Things*, *23*, 100887. https://www.sciencedirect.com/science/article/pii/S254266052300210X

41. Jun, Y., Craig, A., Shafik, W., & Sharif, L. (2021). Artificial intelligence application in cybersecurity and cyberdefense. *Wireless communications and mobile computing*, *2021*(1), 3329581. https://onlinelibrary.wiley.com/doi/full/10.1155/2021/3329581

42. Zhao, L., Zhu, D., Shafik, W., Matinkhah, S. M., Ahmad, Z., Sharif, L., & Craig, A. (2022). Artificial intelligence analysis in cyber domain: A review. *International Journal of Distributed Sensor Networks*, *18*(4), 15501329221084882. https://journals.sagepub.com/doi/full/10.1177/15501329221084882

43. Raj, R., Singh, A., Kumar, V., & Verma, P. (2023). Analyzing the potential benefits and use cases of ChatGPT as a tool for improving the efficiency and effectiveness of business operations. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *3*(3), 100140. https://www.sciencedirect.com/science/article/pii/S2772485923000571

44. Ansari, M. F. (2022). A quantitative study of risk scores and the effectiveness of AI-based Cybersecurity Awareness Training Programs. *International Journal of Smart Sensor and Adhoc Network*, *3*(3), 1. https://d1wqtxts1xzle7.cloudfront.net/85061698/ijssan.2022-libre.pdf?1651075914=&response-content-disposition=inline%3B+filename%3DA_Quantitative_Study_of_Risk_Scores_and.pdf&Expires=1741474443&Signature=bCnpRQRYfH90YSckGbvt~kY5YkH7KZ3yquwMXeoUSTQQfP83xiR-qFkosdVnFqK~RDEgoR0V7Z84gDEfFmmZri6laM~BRZUVJ8HyE6oLgjGbP~sSL2miyN5vE9bwof3O7GB~7L1IgCRUII4vWLmvhcauVgYFihfASzY5hu2sVvBb6IC~DNmuwqNv~wuauIuPjM-fi7g81ivlUnDhLTns5fNBgzFgnLMop1zhRBuICa4gDnighXZQzr6D1cCImt131B9IqYaQxEyiJZOSEMreEx0X95xAOmFlyH55rAiJMUL8UBcI8UVstqzKKYzQF4AAjjKitII6zOit74XSvqRhrw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

45. Dasawat, S. S., & Sharma, S. (2023, May). Cyber security integration with smart new age sustainable startup business, risk management, automation and scaling system for entrepreneurs: an artificial intelligence approach. In *2023 7th international conference on intelligent computing and control systems (ICICCS)* (pp. 1357-1363). IEEE. https://ieeexplore.ieee.org/abstract/document/10142779

46. Richey Jr, R. G., Chowdhury, S., Davis-Sramek, B., Giannakis, M., & Dwivedi, Y. K. (2023). Artificial intelligence in logistics and supply chain management: A primer and roadmap for research. *Journal of Business Logistics*, *44*(4), 532-549. https://onlinelibrary.wiley.com/doi/full/10.1111/jbl.12364

47. Haapamäki, E., & Sihvonen, J. (2022). Cybersecurity in accounting research. In *Artificial Intelligence in Accounting* (pp. 182-214). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003198123-10/cybersecurity-accounting-research-elina-haapam%C3%A4ki-jukka-sihvonen

48. Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, *60*, 101616. https://www.sciencedirect.com/science/article/abs/pii/S0275531922000046

49. Mahor, V., Rawat, R., Kumar, A., Garg, B., & Pachlasiya, K. (2023). IoT and artificial intelligence techniques for public safety and security. In *Smart urban computing applications* (pp. 111-126). River Publishers. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003373247-5/iot-artificial-intelligence-techniques-public-safety-security-vinod-mahor-sadhna-romil-rawat-anil-kumar-bhagwati-garg-kiran-pachlasiya

50. Liu, T., Sabrina, F., Jang-Jaccard, J., Xu, W., & Wei, Y. (2021). Artificial intelligence-enabled DDoS detection for blockchain-based smart transport systems. *Sensors*, *22*(1), 32. https://www.mdpi.com/1424-8220/22/1/32

51. Walters, R., & Novak, M. (2021). *Cyber security, artificial intelligence, data protection & the law*. Berlin: Springer. https://link.springer.com/book/10.1007/978-981-16-1665-5

52. Rajendran, R. M., & Vyas, B. (2023). Cyber security threat and its prevention through artificial intelligence technology. *International Journal for Multidisciplinary Research*, *5*(6). https://www.researchgate.net/profile/Bhuman-Vyas/publication/376717717_Cyber_Security_Threat_And_Its_Prevention_Through_Artificial_Intelligence_Technology/links/6584c9ab3c472d2e8e79c4b2/Cyber-Security-Threat-And-Its-Prevention-Through-Artificial-Intelligence-Technology.pdf

53. Bonfanti, M. E. (2022). Artificial intelligence and the offence-defence balance in cyber security. *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge*, 64-79. https://library.oapen.org/bitstream/handle/20.500.12657/52574/1/9781000567113.pdf#page=79

54. Dataset Link

    https://www.kaggle.com/datasets/Microsoft/microsoft-security-incident-prediction