Proceedings of International Conference on "Recent Innovations in Engineering, Technology & Science for Sustainable Development (RIETSSD-2026)"
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

From Rule-Based Systems to Artificial Intelligence: A Comparative Review of Modern Cyber Security Approaches

Tanvi Thakur[1], Namrata Kashyap[2]

[12]Assistant Professor, School of Computer Application & Technology, Career Point University, Kota, India

[1]tanvi.thakur@cpur.edu.in; [2]namrata.kashyap@cpur.edu.in

Abstract: Cybersecurity has become a multifaceted, dynamic, and hostile problem because many critical systems and infrastructures were becoming digitized and transformed in response. Although the concept of artificial intelligence (AI) has become a potent tool in cyber defense enabling better anomaly detection, predicting threats, and automating responses, it equally brings forth novel threats through creation of more dynamic, evasive and scalable attacks. In this review, the author focuses on the emerging dual role of the AI in cybersecurity and the development of AI as the device that may be both defensive and a threat multiplier. The paper employs a systematic literature review approach to generalize findings of the recent empirical research, surveys, and models of the key cybersecurity aspects. It will analyze the AI-based anomaly detection, the threat detection using deep learning, and the automated defense, and critically evaluate the data quality, practice of evaluation, and reproducibility. The results indicate that anomaly detection is the heart of the AI-based cybersecurity infrastructures; nevertheless, the majority of existing technologies are based on simplistic threat models, unrealistic datasets, and accuracy focused performance metrics that prevent real-world applications. The review also finds structural gaps between research findings and operational needs with methodological weakness and overperformance assertions. To provide the comprehensive socio-technical lens on AI-driven cybersecurity, the work sheds light on the benefits and risks of artificial intelligence as well as the structural constraints of AI-enabled cyber defense mechanisms in general, and proposes research directions in this area, to ensure the future of AI-driven cybersecurity predictability, authenticity, and reliability.

Keywords: AI in cybersecurity, Artificial Intelligence in digital security, Threat detection, Anomaly Detection, Automated Incident Response, Malware Analysis.

Proceedings of International Conference on "Recent Innovations in Engineering, Technology & Science for Sustainable Development (RIETSSD-2026)"
Career Point International Journal of Research (CPIJR)
 | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

I. INTRODUCTION

Due to the rapid growth of digitalization across the various sectors has increase the cybersecurity challenges[1]. Resolving those challenges through manually will difficult and time-consuming. To overcome from the difficulties in cybersecurity challenges, the role of AI is very important; through it, we go smoothly and tackle the challenges easily. Challenges like Network Issues, System Failures, Data Breaches, Insider Threats, Hacking, Bugging, etc. Cybersecurity is the study and application of technical and analytical mechanisms for detecting, analyzing, and preventing adversarial or accidental threats that target the system, network, and Cyber Physical Infrastructures.

Cybersecurity and Artificial Intelligence

Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc.

Table 1. Some types of Cyber Security

Injection attacks	It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

DNS Spoofing	Data is introduced into a DNS resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer.
Session Hijacking	It is a security attack on a user session over a protected network.
Virus	It is a type of malicious software program that spreads throughout the computer files without the knowledge of the user.
Worm	It is a type of malware whose primary function is to replicate itself to spread to uninfected computers.
Trojan horse	It is a malicious program that causes unexpected changes to computer settings and unusual activity, even when the computer should be idle.

Cybersecurity systems detect, examine, and fix potential system weaknesses and vulnerabilities before hackers or malicious software exploit them. An organization, its employees, and the processes and technologies must come together to create a solid cybersecurity layer that protects it from potential attacks.

Advantages of Cybersecurity:

(i) Data Safety from Hackers
(ii) Safeguarding Online Transactions
(iii) Preventing Identity Theft
(iv) Mitigation of Financial Losses
(v) Decreased Data Theft Hazard
(vi) System Availability and Improved Data
(vii) Protect Business Reputation
(viii) Assist Remote Working
(ix) Compliance with Regulations
(x) Cyber Posture is Improved
(xi) Handles Data Management
(xii) Improve Customer's and Stakeholders' Trust
(xiii) Defence Against Malware
(xiv) Recovery of the System

Disadvantages of Cybersecurity:

(i) Cost
(ii) Complexity
(iii) False Sense of Security
(iv) Privacy Concerns
(v) User Inconvenience
(vi) Skill Shortage
(vii) Potential for Human Error
(viii) Constantly Evolving Threats
(ix) Impact on Performance
(x) International Scope
(xi) Need for Constant Monitoring
(xii) Regular Updates
(xiii) Slowing Down the System

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

Artificial Intelligence is a field of research in computer science that develops and studies methods and software that enable machines to perceive their environment and use learning and intelligence to take actions that maximize their chances of achieving defined goals.

Table 2. Forms of AI

Traditional AI	Traditional AI, or classical AI, involves methods that humans explicitly program.
Machine Learning	Machine Learning (ML) is a subset of AI that involves creating models that can learn from data.
Large Language Models (LLMs) and Their Applications	Large language models, the most common example of generative AI, are systems trained on massive datasets and designed to process and analyze vast amounts of natural language data and then use that information to generate humanlike responses to user prompts.

The functioning of AI systems can vary greatly depending on their specific purpose and underlying technology, but here's a general overview of how AI works:

1. *Inputs*

- Inputs deal with the data and information that an AI system uses for analysis and processing.
- Inputs can be text, images, audio, video, the data of sensors, or others.
- Inputs stress the function of the system and determine the quality of the AI system's performance.

2. Processing

- Processing data is an action that incorporates the data manipulation, analysis, and interpretation by the software AI algorithms.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

- AI algorithms represent a multitude of methods, including machine learning, deep learning, natural language processing, and computer vision, among many others, which permit processing of the data.
- Tasks like matching, categorization, regression, clustering, prediction, etc., are some of the techniques that may be involved in the process.

3. Outcomes

- The outputs (the results or responses) by the AI system are interpreted by the way it tackles the input data.
- It can be difficult to predict the exact outcome in this kind of task as well as it depends on the particular issue or goal of the system.
- Examples of outcomes can be forecasts, suggestions, categorizations, generated info, or substances, etc.

4. Adjustments

- Adjustments are often used to describe AI's ability to learn, grow, and make improvements through attention to data and customer feedback.
- AI systems normally contain kinds of mechanisms to learn from their experience, and better themselves instead of making mistakes, by updating their models or parameters.
- Changes can range from retraining of machine learning models, fine-tuning of the algorithms, updating of procedures of decision-making, to running special procedures, and so on.

5. Assessments

- Measurements consist of the consideration of both the performance, reliability, fairness, and ethical aspects of AI systems.
- Assessment metrics may include accuracy, precision, recall, F1 score, fairness metrics, interpretability, robustness, etc.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

- Evaluation of AI deployments that are sensitive to risks and concerns of stakeholders assists them in making suitable decisions for AI systems.

Advantages of AI:

- Reduction in Human Error
- Enhances decision-making
- Works 24/7 without fatigue
- Increases efficiency and automation
- Improves personalization in user experiences

Disadvantages of AI:

- Lack of human creativity and emotional intelligence
- Risk of job displacement
- Privacy and security concerns
- Ethical concerns and AI bias
- Potential for misuse in deepfakes and misinformation

Challenges of Cyber Security

- Security Vulnerability In Cloud Computing Environment
- Ransomware Attacks Are Aiming At Critical Business Functions
- Growing Trend Of IoT (Internet of Things)Device Usage
- Lack Of Phishing Attacks Awareness
- Unmanaged Access Privileges Within The Organizations
- Serverless App Vulnerability
- Supply Chain Vulnerability
- Increase In Use Of Artificial Intelligence

Table 3. Comparison of Rule-Based Security and AI-Driven Security

Dimension	**Rule-Based Security**	**AI-Driven Security**
Patterns of security	Deterministic, rule-based, signature-driven	Data-driven, probabilistic, learning-based
Threat Awareness Requirement	Attacks must be known beforehand (known signatures)	Capability to detect uncharacterized and zero-day attacks.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

Dimension	Rule-Based Security	AI-Driven Security
Zero-Day Attacks	Handled Poorly	Strong – detects deviations from learned normal behavior
Response to Polymorphic Malware	Ineffective – minor changes evade detection	centrally based on behavior, not structure.
Insider Threat Detection	Limited – assumes external attackers	Stronger – models user behavior and deviations
Multi-Stage / APT Detection	ineffective at correlated time-based anomalies	temporal and collective anomaly detection.
The ability to respond to Changing Threats	A rule has to be updated manually by hand	A model only has to be retrained and learns.
Scalability	rule explosion in large systems	High – handles large, high-dimensional datasets
False Positive Management	Often rigid – high false positives under dynamic conditions	Context-aware but may still suffer if poorly trained
Explainability	High – rules are human-readable	Variable Deep learning models can be opaque.
Computational Cost	Low to moderate	needs training, monitoring, and retraining.
Data Dependency	does not need huge datasets	can be performed based on data quality and realism.
Stability to Adversarial Adaptation	attackers can learn and evade rules with minimal effort	initially strong and susceptible to adversarial ML.
Evaluation Practices	Simple metrics (rule hits, alerts)	Metrics (precision, recall, robustness, drift)
Real-World Deployment Risk	Stable but limited effectiveness	Powerful, but weak when datasets and evaluation are faulty.
Strategic Role	Baseline defense and compliance	Force multiplier to provide scalable and proactive defense

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

Sun et al. (2017) and Li and Liu (2021) provide the increasing magnitude and complexity of cyberattack cases against critical infrastructure and organizational systems in the framework of survey studies and review analysis, respectively[2,5].

Kaur and Ramkumar (2021) and Admass et al. (2023) indicate in their review of cybersecurity research surveyed that lone attacks have way since been shifted to massive, organized attacks. Newer cyber threats are often perpetrated not only by nation-states but also by certain criminal gangs offering them, malicious insiders, facilitating access, private actors, and automated or AI-enabled opponents aiding reconnaissance or persistence. These attacks often focus on critical infrastructure, organizations and interconnected socio-technical systems and in such cases, digital failures can explode into major economic disruption and physical impact. The long-standing security assumptions, i.e. well-defined network boundaries, geographically limited threats, and defense mechanisms that typically remained constant, are becoming ineffective in this dynamical environment. The breaking down of these boundaries reveals inherent gaps in traditional, perimeter-based frameworks of cybersecurity.

According to Scholz et al., the modern cyber threats are becoming progressively interdependent, with the lack of digital systems disrupting organizational and cyber-physical systems. Studies on security of critical infrastructures reveal how coordinated cyber attacks may spread through the internet over cyber-physical systems resulting in a widespread disruption of service[3]. The research on organizational and insider threat also highlights the significance of human behavior, institutional structures and governance failures as the key factors in promoting cybersecurity vulnerability[1,3]. Meanwhile, the development of artificial intelligence has realized both highly effective methods of threat detection, anomaly analysis, and automated response, and at the same time, more adaptive and evasive attack methods[6,9,10]. Altogether, these results imply that cybersecurity should be interpreted as the socio-technical and strategic issue, not the technical one that is defined in a very specific manner.

Irrespective of this increasing awareness, there is still a significant gap in the way the issue of cybersecurity is presented and resolved. The review articles of Kaur and Ramkumar (2021) and Jonas et al. (2023) give more emphasis on technical and cryptographic solutions, and little is said on the impact of macro-organizational and systemic issues on cyber threats. Little focus is given to the application of organizational resilience, economic asymmetries and

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

geopolitical factors into the cybersecurity models. Consequently, most of the solutions that have been suggested have been found to be too rigid to operate in dynamic and adversarial environments in which attackers keep changing their tactics.

To address these constraints, this paper will analyze cybersecurity in the context of a growing and dynamic cyber threat environment, with respect to its macro-level aspects. In particular, the paper summarizes the literature to show how cyber threats have evolved beyond individual technical occurrences to be systemic and multi- actor processes that cross conventional security lines. This study contends that flexible and systemic cybersecurity defense methods are needed, as opposed to rigid controls by locating cybersecurity in the context of organisations, economies, and geopolitics. By doing so, the paper can contribute to a more comprehensive notion of cybersecurity and offer a conceptual framework of designing resolute security measures that would be applicable to digital infrastructures that are more interdependent and integrated in the present digital world.

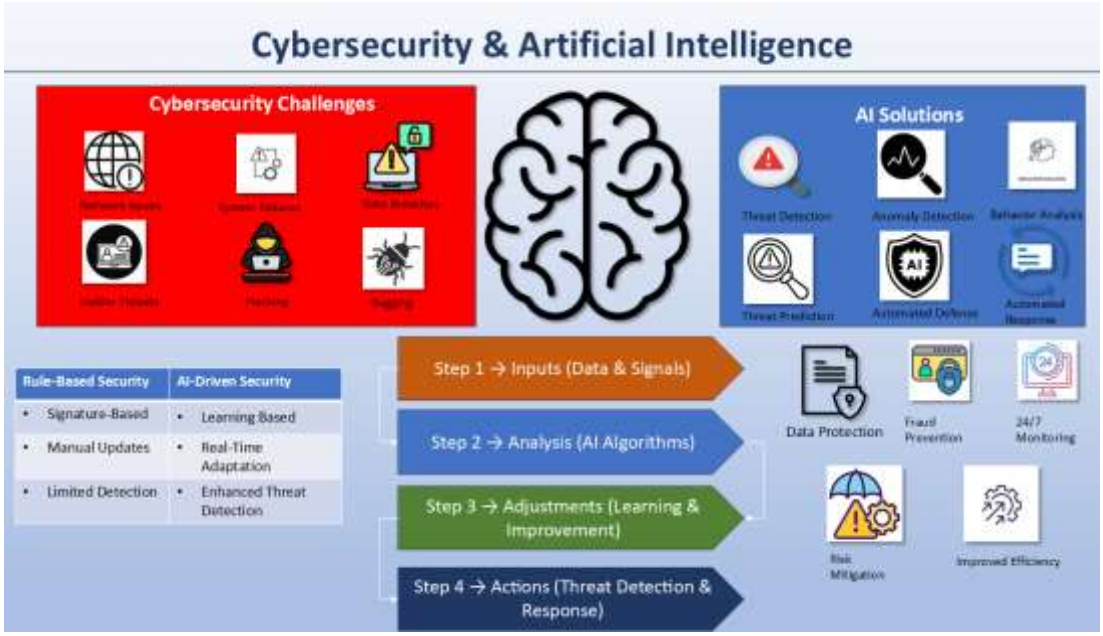

Fig 1: Artificial Intelligence in the Contemporary Cybersecurity architectures

II. LITERATURE REVIEW

The initial cybersecurity studies and practice were heavily based on the defense mechanisms that relied on rules and signature-detection schemes (like firewall, intrusion detection system, and antivirus virus detection software). These methods were based on a set of rules,

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

recognized attack signatures and staged assumptions of how an attacker would behave. Although useful in identifying formerly seen threats, studies done concerning the insider threat detection, further demonstrate such constraints, where deterministic models do not identify deviant behavioural nuances in adversarial worlds (Yuan and Wu3).

Unlike in signature-based systems of intrusion detection in the dawn of times, Ucci et al.9 demonstrate that polymorphic malware and zero-day malware easily evade rule-based detectors. The signature-based mechanisms presuppose the prior knowledge of the patterns of attacks, so it is inherently reactive, not proactive. The once-established defenses fail as quickly as attackers keep using polymorphic and metamorphic malware whereby the malware dynamically changes its structure in order to avoid detection3,9. Malware analysis studies note that they can make small changes to malicious code to avoid signature-based detection without changes to the underlying malicious behavior. This forms a basic flaw of definition detection rules when dealing with an environment where attackers constantly evolve.

The empirical research conducted on insider threat detection and advanced persistent threats indicates that the traditional security models are not capable of detecting multi-stage attacks that occur over time, in a coordinated and well-organized manner3,7. Rule-based systems are generally emerging with a design approach of detecting external intrusion usually on the basis of malicious activity whose source is external to the organization. The insider threats, however, are largely seen in deviant behavioral aspects as opposed to clear boundary violations, which is why posing a challenge to detect by some set of rules3. On the same note, an increasing number of high-tech attacks take the form of a multi-phase campaign, with innocent actions that may seem innocent given individual context but that in the long run turn out to be dangerous. According to the survey studies conducted by Chandola et al. (2009) and Yuan and Wu (2020), deterministic detection systems do not have the contextual sensitivity to be able to correlate the distributed and temporally separated security events.

Simultaneously, cryptographic security studies show an increasing threat to the fixed cryptographic security solutions. Even though encryption can be described as the essential component of cybersecurity, various side-channel attacks, Advanced persistent threats (APTs), and the expected effects of quantum computing4,5 are gradually diminishing its efficiency. Side-channel attacks rely on physical or implementation level properties, but not cryptographic vulnerabilities, making mathematically sound algorithms practically susceptible. Besides, APTs usually circumvent cryptographic protection completely, using

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

human, organizational, or supply-chain weaknesses. Commenting on cybersecurity practices using review-based assessments, Kaur and Ramkumar (2021) and Admass et al. (2023) observe that the cryptographic strength is not a sufficient condition to be secure in the working environment4,6.

According to constituents the argument by Scholz et al.1 is that reactive security models are structurally ill-suited to adversaries who maintain the best strategies in reaction to defenses established. Conventional defenses use a model of static threats where strategy of attacks does not change significantly with time. Conversely, the contemporary attackers observe, test, and respond to deployed security mechanisms and proactively apply the automation and artificial intelligence to do this more quickly. This has developed an asymmetric relationship whereby those defending themselves have to work to prevent an enormous pool of potential attacks, whereas the attacker has to work to find only one vulnerability. Consequently, the traditional and rule-based security will deteriorate as it is launched, especially in large-scale of high-value systems.

Unlike the initial rule based intrusion detection systems, Scholz et al.1 and Chandola et al. show that deterministic defenses do not work well against zero-day as well as insider attacks which dynamically evolve with respect to controls deployed. Concurrently, the literature recognizes the fact that deterministic controls still have a value in the detection of known attacks and also in operational stability within controlled environments[1]. Although traditional approaches are still needed as the baseline controls, the use of traditional approaches in solitude as is being highlighted in the literature as limiting. This understanding has fueled an increasing move towards learning based, system oriented and adaptive security strategies. Nonetheless, the current reviews tend to review such newer methods separately without adequately comparing them to the hierarchy of failures of classical defenses. This disconnect explains the necessity to have a thorough examination in place that critically looks at the reasons why the traditional models of cybersecurity have not worked, and the emerging paradigms are trying to cover these gaps (albeit to no avail).

Proceedings of International Conference on "Recent Innovations in Engineering, Technology & Science for Sustainable Development (RIETSSD-2026)"
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

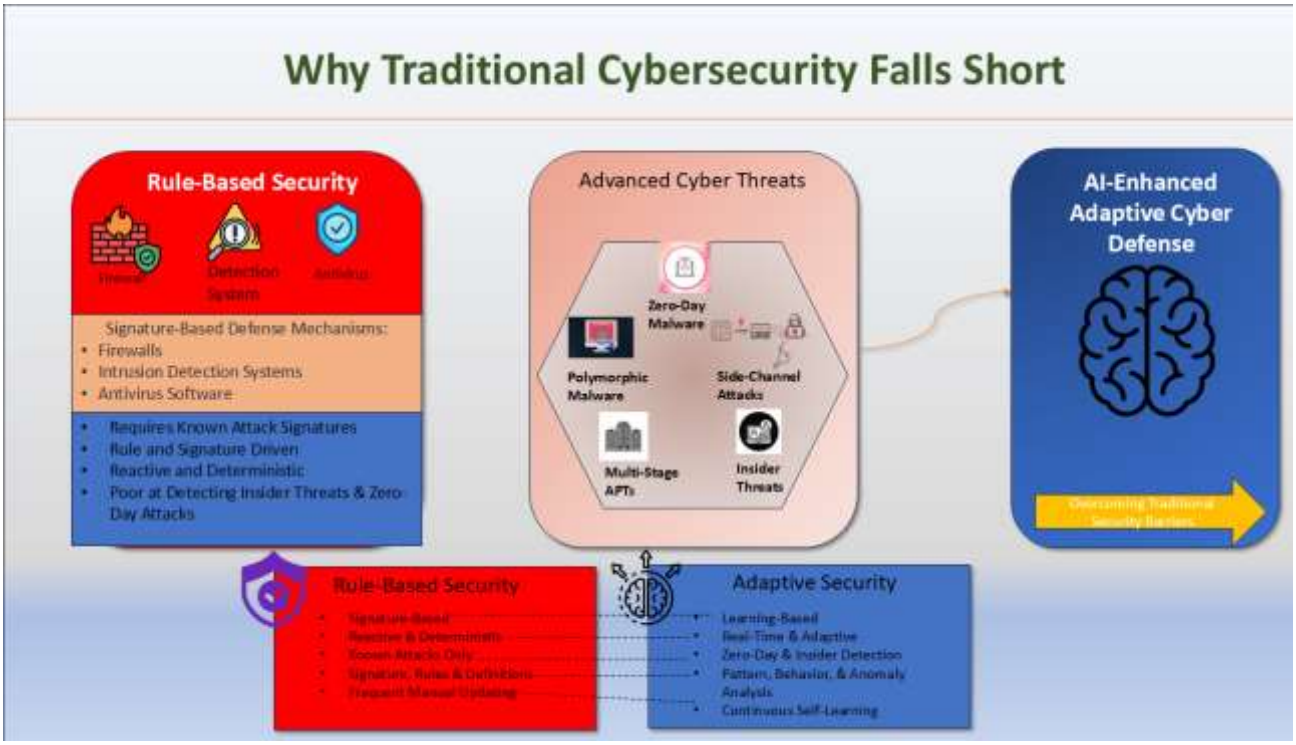

Fig 2: Comparison of standard and Artificial Intelligence-based cybersecurity models.

III. METHODOLOGY

Research Design

This paper is a literature review approach to the application of artificial intelligence in cybersecurity support, and it will discuss the enhancement of defensive functions of the anomaly detection, threat prediction, and automated response to cybercrime by artificial intelligence. A transparency and reproducibility, as well as comprehensive coverage of the relevant research, were attained with the help of the systematic review process. The system review method is in line with the best data on systematic reviews of cybersecurity and information systems research.

Data Sources and Search Strategy

In order to have a comprehensive search to come up with a wide and representative sample of relevant studies, a thorough search in multiple leading academic databases was made in:

(i) IEEE Xplore Scopus

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

(ii) Web of Science

(iii) SpringerLink

(iv) ScienceDirect

(v) ACM Digital Library

(vi) Google Scholar (It is taken as an auxiliary source).

Keywords and Search Strings

Maximization of coverage was achieved by use of the Boolean operator and combination of keywords. The search strings that were representative were:

(i) artificial intelligence AND cybersecurity

(ii) machine learning AND intrusion detection

(iii) "network security" AND artificial intelligence-based anomaly detection.

(iv) threat prediction" AND machine learning

(v) Artificial intelligence-based cybersecurity systems.

(vi) BEHAVIORal analysis AND cyber threat detection.

(vii) And the phrase "automated cyber defense" and AI.

Title, abstract, and keywords search terms were used. The search was restricted to English-based publications.

Study Selection and Sampling Process

Initial Retrieval

Total records located: some 200-250 papers in all databases (prior to removal of duplicate entries).

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

Screening and Filtering

The method of sample was a multi-stage filtering method:

(i) Eradication of duplicates between databases.

(ii) Relevance screening Title and abstract relevance to AI-based cybersecurity defense.

(iii) Shortlisted articles review - The full text of shortlisted articles will be reviewed.

The final sample of review after the screening was about 40-50 high-relevance studies, which also met rigorous standards of review.

Inclusion and Exclusion Criteria

Inclusion Criteria

The studies were covered in case they met the following criteria:

(i) Interested in AI or machine learning to use in cybersecurity.

(ii) Attack defensive functions, including:

- · Anomaly detection
- · Threat prediction/ forecasting.
- · Intrusion detection
- Full-automated response or decision support.

(iii) Utilized either an empirical, experimental, survey-based or review research.

(iv) Published either by peer-reviewed journals or reputable conferences.

(v) Published in the past 10-15 years, to be updated on the recent AI trends.

Exclusion Criteria

Research has been filtered out unless it:

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

(i) Only centered on cryptography with no elements of AI.

(ii) Handled offensive AI methods with no defensive connotation.

(iii) Peer-reviewed, opinion pieces, or editorials were not present.

(iv) Should have had more of a methodology.

(v) Were not full texted or written in English.

Data Extraction

The data extraction template was structured and it would be used to extract:

(i) Date of publication (authors, date, location).

(ii) Methods of AI (e.g., machine learning, deep learning, GANs).

(iii) Application field of cybersecurity (e.g., malware detection, insider threat, intrusion detection)

(iv) Kind of Data to analyse (system logs, malware binaries, user behaviour, network traffic)

(v) Method of evaluation (quantitative or qualitative or both)

(vi) Reported results in terms of accuracy of detecting, prediction capability and response efficiency.

(vii) Applicable organizational or practitioner perspectives.

Data Analysis and Thematic Synthesis

The thematic analysis method of data analysis which entails the use of deductive and inductive codes was used to analyze the extracted data.

The areas that deductive coding is focusing on were:

(i) Better accuracy in the detection of anomalies.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

(ii) Threat prediction and forecasting based on AI.

(iii) Speed and fastness in automation.

New patterns that had been uncovered in the inductive coding included:

(i) Previously unknown attacks detected.

(ii) Detection of minor displays of deviant behavior.

(iii) High-dimensional and large-scale cybersecurity data mishandling.

The studies were then categorized according to the AI capabilities such as detection, prediction and response automation. The comparisons between studies were performed in order to find the prevailing trends, the commonalities of benefits, and the limitations were reported.

Methodological Rationale

In doing so, the method can be used to identify and synthesize research on AI-related cybersecurity through consistency. The approach combines empirical research findings, surveys, and frameworks, which explains why the methodology assists in the combined thinking about the impact of AI on improving scalability, intelligence, and adaptability in cyber defense. The focus on technical performance and organizational confidence is used to guarantee that the review will capture not merely the algorithmic effectiveness, but the practical applicability as well.

Summary

To conclude, this approach gives a clear and strict basis of the analysis of AI as a cybersecurity enabler. Using systematic sampling, systematic data collection, and thematic synthesis, the study will be in a good position to show how the AI-driven techniques can enhance capabilities of conventional defenses and how the shortcomings of conventional, rule-based security models may be mitigated.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

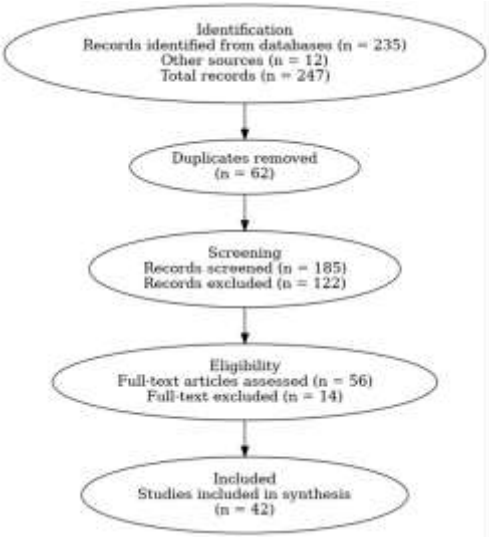

Fig 3: Illustrating the study selection process for the systematic review of artificial intelligence–based cybersecurity defense mechanisms.

IV. Results and Discussion

Results: Anomaly Detection as the Core AI-Based Defense Mechanism

Research Question (RQ)	Key Findings	Interpretation (What it Means)	Implications
RQ1: How does anomaly detecting contribute to AI-powered cybersecurity systems?	Most AI-based security solutions rely on anomaly detection in order to detect intrusion, insider threats, malware, and fraud.	Anomaly detection operates as the main analytical cybersecurity AI engine since it allows detection of attacks without prior knowledge of them.	Affirms anomaly detection as the basic mechanism of AI-based cyber defense architectures.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

RQ2: To what extent do existing methods of detecting anomalies handle cyber threats in real-life situations?	Majority of systems also concentrate on point anomalies, contextual and collective anomalies are under-represented although their occurrence is common in real attacks.	Research focus does not match operational threat realities, which limits real-life effectiveness.	Enhances the importance of context-dependent and sequence-based detectors.
RQ3: How does deep learning and GAN-based techniques affect the detection of abnormalities?	On high-dimensional and data, deep learning and GAN-based models demonstrate good results, particularly on the unseen attacks.	Substantial AI models enhance the detection but add vulneracity to an unstable training and openness.	Also denounces that performance gains should be offset with strength and interpretability.
RQ4: How can we explain the existing gap between research on anomaly detection, and operational requirements in cybersecurity?	In current studies, simplified threat modeling, unrealistic data sets and accuracy based evaluation prevail.	The difference is more of concept and not of strict technical nature-security is being understood as pattern recognition as opposed to adversarial behavior.	Adversarial, temporal and system level evaluation Calls.

Proceedings of International Conference on "Recent Innovations in Engineering, Technology & Science for Sustainable Development (RIETSSD-2026)"
Career Point International Journal of Research (CPIJR)
 | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

Conclusion: Data, Evaluation, and Reproducibility Challenges

Research Question (RQ)	Summary Conclusion	Evidence Review	Deployability
RQ5: What implications do dataset constraints have on the AI-based cybersecurity research?	The quality of datasets is the significant bottleneck of the effectiveness of AI-related security.	Reviewed studies are dominated by small samples, artificial data, and unavailability of public data.	Causes overfitting, bad generalization and unreliability in deployment.
RQ6: Do the existing evaluation practices provide adequate practices to deploy cybersecurity in the real world?	The current indicators of evaluation usually exaggerate performance of the system.	Accuracy-based metrics are unconcerned with class imbalance, false positives and concept drift.	Gives false positives which do not work when operationalized.
RQ7: How reproducible is the AI-based research on cybersecurity?	The field does not have high reproducibility.	Minimal datasets and source codes do not allow cross-study validation.	Cripples confidence, slows adoption of industrial means and reduces adoption of indusries.

Career Point International Journal of Research (CPIJR)
 | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

RQ8: What are the implications on the wider issues of AI-driven cybersecurity adoption?	AI improves defensive intelligence but is weak in terms of methods.	Excessive reliance on data realism and rigor of evaluation among studies.	In practice, AI is not supposed to substitute but complement traditional security measures.

Future Research Directions

Research Gap Determined	RQ connection	Future Research Suggestion
Excessive use of point anomaly detection	RQ2	Design context aware and group-based anomaly detection models.
Unrealistic datasets	RQ5	Generative large-scale, longitudinal,

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

		adversarial realistic datasets.
Weak assessment procedures	RQ6	Embrace soundness-, expense-, and drift-carrying evaluation measures.
Low reproducibility	RQ7	Compel to publish data, code and benchmark standards.
Field studies and hybrid security tests fragile deployment	RQ8	Perform longitudinal field experiments and hybrid security test.

V. CONCLUSION

This review explored the changing place of artificial intelligence in cybersecurity by thematically synthesizing current studies on the topic, although it pays specific attention to the systems issue of structural constraints that constrain the real capabilities of AI-based security systems. The results indicate that although AI has been put at the center of contemporary cybersecurity, particularly, in areas of anomaly detection, threat forecasting, and autonomous response systems, the outcomes of its practical application are limited by an ongoing lack of research quality and transparency and insufficient verification of research outputs. The literature review demonstrates that a significant percentage of AI-focused cybersecurity models are tested using small or artificially balanced data and honest orders of experiment, which restrict their generalization to dynamic, real-life attack situations7,9, which cast serious doubts on their applicability in dynamic and adversarial settings.

One of the major findings that can be drawn after conducting this review is the widespread impact of the limitations of datasets. Most of these studies are based on small or artificially balanced datasets and not on the extreme imbalance of classes and behavioural variation encountered in real-world cyber environments. The absence of publicly available, longitudinal and adversarially realistic data, further fringe the credibility of reported performance gains and limits meaningful cross study comparison. Consequently, both

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

detection accuracy and robustness are frequently exaggerated at the expense of showing the reality about the challenges of operation of deployed security systems.

Systematic weaknesses of evaluation methods are closely associated with the data restriction. The review identifies the heavy use of traditional accuracy-based measures that cannot include false positives, concept drift, and the economic costs of the security operations. When assessing systems by disregarding the real-world limitations like the changing behavior of attackers, and the distorted data distributions, most assessments present a partial and over-optimistic view of system functionality. Such a lack of alignment between laboratory performance and systematic dependability is a major impediment to the uptake of AI-inspired cybersecurity solutions.

On a practical view, the findings have a critical significance on the researchers and practitioners. Organizations implementing AI-driven security applications must be critical in the interpretation of reported performance indicators and must focus on the implementation of solutions that are confirmed through realistic scenarios. It is recommended to practitioners that they should consider layered security strategies where the AI is added in-and-is-not-replaced by the traditional controls but should invest in continuous monitoring and model modification to address performance degradation with time. To the developers, it is critical to have transparency in the source of data, assessment protocols and model incompatibility in the formation of trust and responsible deployment.

Although this review has its contributions, it has a number of limitations. To start with, the analysis is limited by the accessibility and quality of the existing studies with many of them not being adequately detailed in methodology or not providing reproducible data. Second, the review summarizes the findings in various domains, but it has not shown in an empirical manner how certain AI can be applied in the real world. Lastly, thely development of cyber threats and AI methods implies that certain results could be irrelevant as other methods and datasets are created.

Future studies should overcome these limitations by focusing on data realism, evaluation rigour and reproducibility. These comprise the creation of massive, publicly available, and time-changing datasets, that reflect authentic attack conduct and organizational scenes.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

Assessment systems must not rely on the tenets of accuracy but rather be delivered in the form of holistic evaluation systems that include robustness, interpretability, economic cost, and adversarial resilience. Also, the focus should be made more on the longitudinal studies and real-life deployments to comprehend the behavior of AI-based systems with the adaptive attacker over time.

To conclude, although artificial intelligence has an impressive service of strengthening cybersecurity, the results of using it are directly related to how well the data is collected, how practices are evaluated, and whether the research is transparent. To help fill that research-to-reality gap, it is vital to address these structural issues in order to help future researchers generate more reliable and effective solutions to cybersecurity issues.

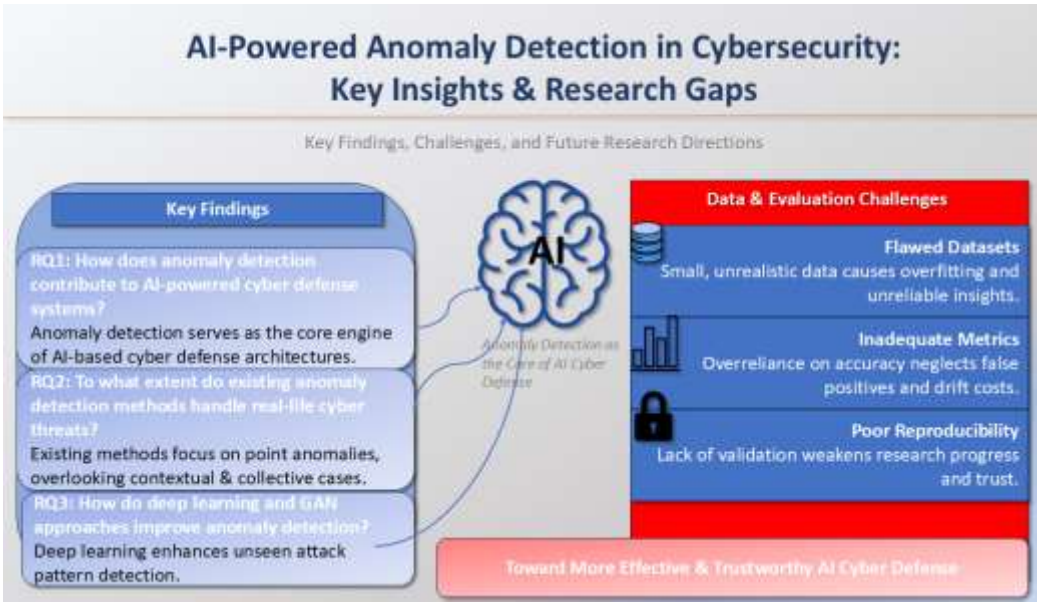

Fig 4: Greater Success and Reliable AI Cyber Defense.

REFERENCES

1. K. Shehzadi, T. Abbas, and A. Zainab, “A survey of intrusion detection in smart grid systems: Comparative analysis of rule-based, machine learning and deep learning approaches,” International Journal of Security and Networks, vol. 20, no. 2, pp. 145–162, 2025

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

2. S. Reynaud and A. Roxin, "Review of explainable artificial intelligence for cybersecurity systems," Journal of Cybersecurity and Privacy, vol. 5, no. 1, pp. 1–22, 2025.
3. F. Uccello, M. Pawlicki, S. D'Antonio, and R. Kozik, "Comparative analysis of AI-based methods for enhancing cybersecurity monitoring systems," in Artificial Intelligence Applications in Cybersecurity, Springer, pp. 101–118, 2025.
4. S. Muneer, U. Farooq, and A. Athar,"A critical review of artificial intelligence–based approaches in intrusion detection: A comprehensive analysis," Security and Communication Networks, vol. 2024, Article ID 3909173, pp. 1–28, 2024.
5. Z. Huma and J. Muzaffar, "Hybrid AI models for enhanced network security: Combining rule-based and learning-based approaches," Global Perspectives on Machine Reasoning, vol. 3, no. 1, pp. 1–15, 2024.
6. S. Sathyakala and E. Anbalagan, "Comparative analysis of cyber security threat detection based on artificial intelligence approaches," IEEE Access, vol. 12, pp. 45678–45692, 2024.
7. D. Jonas, N. A. Yusuf, and A. R. A. Zahra, "Enhancing security frameworks with artificial intelligence in cybersecurity," International Journal of Advanced Computer Science and Applications, vol. 14, no. 11, pp. 1–9, 2023
8. W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," Journ al of Information Security and Applications, vol. 75, Art. no. 103504, 2023.
9. S. Muneer, U. Farooq, and A. Athar, "Artificial intelligence–based intrusion detection systems: A review of traditional and modern approaches," Journal of Information Security and Applications, vol. 72, pp. 103421–103436, 2023.
10. I. H. Sarker, "Machine learning and artificial intelligence in cybersecurity: A comprehensive survey," Journal of Network and Computer Applications, vol. 198, pp. 103271–103295, 2022.
11. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, pp. 102419–102436, 2022.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

12. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets, and challenges," Cybersecurity, vol. 5, no. 1, pp. 1–22, 2022.
13. J. Kaur and K. R. Ramkumar, "The recent trends in cybersecurity: A review," Journal of King Saud University – Computer and Information Sciences, vol. 33, no. 5, pp. 456–472, 2021.
14. Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cybersecurity: Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8185, 2021.
15. I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: An overview of security intelligence modeling, techniques, and research directions," SN Computer Science, vol. 2, no. 3, pp. 1–18, 2021.
16. S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," Computers & Security, vol. 94, Art. no. 101784, 2020.
17. I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: An overview from machine learning perspective," Journal of Big Data, vol. 7, no. 1, pp. 1–29, 2020.
18. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets, and challenges," Cybersecurity, vol. 3, no. 1, pp. 1–21, 2020.
19. R. W. Scholz, R. Czichos, P. Parycek, and T. J. Lampoltshammer, "Organizational vulnerability of digital threats: A first validation of an assessment method," Future Generation Computer Systems, vol. 87, pp. 629–649, 2019.
20. D. Ucci, L. Aniello, and R. Baldoni, "Survey of machine learning techniques for malware analysis," Computers & Security, vol. 81, pp. 123–147, 2019.
21. I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: An overview from machine learning perspective," Journal of Big Data, vol. 6, no. 1, pp. 1–29, 2019.
22. H. Zenati et al., "Adversarially learned anomaly detection," in Proc. IEEE International Conference on Data Mining (ICDM), 2018, pp. 727–736.
23. C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," International Journal of Electrical Power & Energy Systems, vol. 99, pp. 45–56, 2017.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20694811

24. V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.