Library Progress International
Vol.43, No.2, Jul-Dec 2023: P. 335-347

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

AI-DRIVEN APPROACHES FOR ENHANCING IOT SECURITY: A COMPREHENSIVE EVALUATION

Prof. Bhavesh Patel[1], Dr. Dhaval Jadhav[2]

[1]Assistant Professor, Shree Sitarambhai Naranjibhai Patel Institute of Technology & Research Centre, Umrakh
[2]Associate Professor, Vidyabharti Trust College of Master in Computer Application, Umrakh

How to cite this article: Prof. Bhavesh Patel, Dr. Dhaval Jadhav (2023) AI-DRIVEN APPROACHES FOR ENHANCING IOT SECURITY: A COMPREHENSIVE EVALUATION. *Library Progress International,* 43(2), 348-370

ABSTRACT:

As the Internet of Things (IoT) continues to expand ensuring cybersecurity has become paramount due to the rising frequency and sophistication of cyber-attacks. To address this challenge, integrating artificial intelligence (AI) technology with security protocols has emerged as a potential strategy for bolstering IoT cybersecurity defences. This review assesses the effectiveness of combining AI approaches with security mechanisms to mitigate cyber threats in IoT environments. First, the study assesses the effectiveness of AI-driven intrusion detection systems (IDS) in detecting and preventing hostile activity across various IoT network architectures. Second, it examines how AI methods like ML and DL detect unusual behaviour and potential cyber-attacks in real-time within IoT systems. Furthermore, the research looks at how AI-based security measures may adapt and scale to handle dynamic cyber threats and network infrastructures. Additionally, the study investigates the consequences of data privacy and ethical considerations when incorporating AI approaches into IoT security measures, addressing concerns about algorithmic bias and data privacy. Overall, this review sheds light on how AI approaches strengthen security mechanisms, reduce cybersecurity risks, and contribute to the evolving landscape of cyber defence measures in the realm of IoT.

Keywords: Anomaly Detection, Real-time threat detection, Intrusion Detection system, Data privacy.

INTRODUCTION

In recent years, the internet's rapid expansion and widespread acceptance of IoT have changed the way we interact, do business, and access information. However, in addition to these developments, the proliferation of cyber-attacks has presented substantial difficulties to the security and integrity of IoT systems. Cyber-attacks, ranging from malware infections to sophisticated hacking attempts, have become more common, diverse, and sophisticated, posing serious hazards to individuals, organisations, and nations alike [1].

To resist these emerging threats, existing security techniques are no longer enough. The rise of AI techniques, notably machine learning (ML) and deep learning (DL), has created new prospects for improving cybersecurity defences within IoT. AI algorithms can help security personnel detect, respond to, and mitigate cyberattacks in real time to analyse massive volumes of IoT data and identify patterns indicative of malicious behaviour [2].The relation between AI, ML and DL is shown in Figure 1.

Traditional IoT security methods need help to stay current with the ever-changing landscape of security risks. This needs a paradigm change towards more sophisticated and adaptable security solutions tailored to the IoT environment. AI techniques likeML and DL have enormous potential for improving cybersecurity defences by enabling proactive threat identification and response.

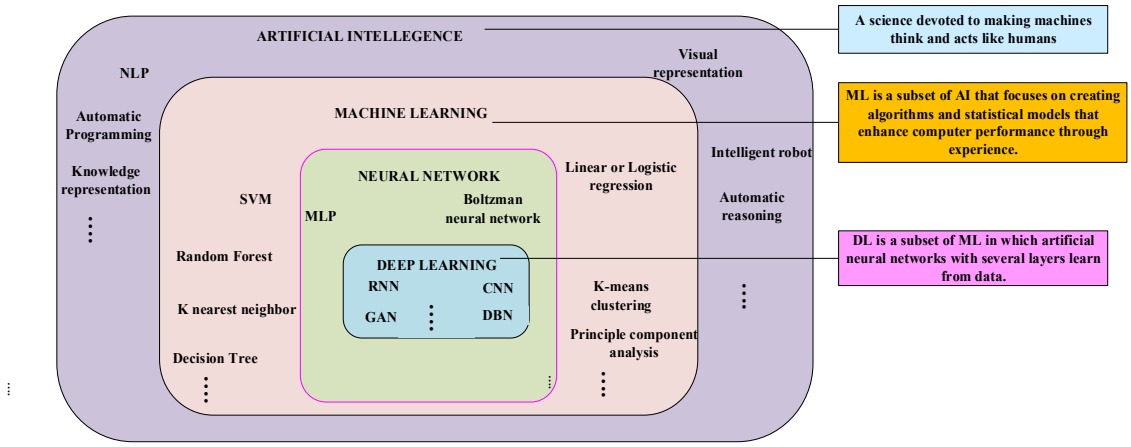

Figure 1: Relation between AI, ML and DL

AI algorithms enable security systems within IoT to analyse massive volumes of information, such as network traffic and user behaviour, with unprecedented speed and accuracy. AI-driven security methods,an IoT environment can proactively threat identification and response by recognising complicated patterns and minor anomalies that indicate malicious behaviour [3]. This proactive method not only enhances the effectiveness of security measures, but also shortens response times, reducing cyber-attacks impact on individuals, organisations, and critical infrastructure.

However, while AI has enormous potential for improving cybersecurity in IoT, its incorporation into security processes creates many ethical and privacy problems [4]. The primary problems include data privacy algorithmic discrimination, and legal consequences of AI-powered the making of decisions. Ensuring the proper and ethical use of AI-driven security mechanisms is critical to preserving trust and protecting the rights of persons and communities in the digital era.To overcome these issues, it is critical to establish strong governance frameworks and regulatory processes that promote openness, accountability, and fairness in using AI technology for IoT cybersecurity. Additionally, organisations must prioritize data protection and use privacy-preserving solutions to protect sensitive information while harnessing AI's capabilities for threat detection and mitigation.

1.1 SIGNIFICANCE OF CYBER SECURITY IN IoT

Nowadays, the proliferation of IoT has greatly expanded the number of users that utilise tools and programs that generate massive volumes of data, many of which are sensitive or confidential. As a result, [5] cyber security in IoT is becoming increasingly important in this day and age, as data theft on these systems increases. The tactics utilised by cyber attackers

through diverse attack approaches expand in volume and sophistication, causing numerous concerns.

1.2 ROLE AND NECESSITY FOR AI IN IoT CYBER SECURITY

In IoT, AI is crucial in modern cybersecurity, providing advanced capabilities to combat sophisticated and dynamic cyber threats. AI-driven solutions use ML and DL algorithms to process massive amounts of data from various points of view enabling AI systems to detect patterns of cyber threats with unprecedented accuracy, facilitating early threat identification and mitigation in IoT environment.AI in cybersecurity offers real-time threat detection and response by continuously monitoring network activities and analyzing data [6]. This proactive approach helps organizations identify anomalies and suspicious behaviour.In today's changing threat landscape, preventing possible breaches or cyberattacks is critical, as is drastically decreasing the impact of cyber disasters.

AI helps organisations predict and prepare for future cyber threatsby leveraging predictive analytics. This approach helps identify vulnerabilities and weaknesses in their IoT security infrastructure, decreasing the probability of effective assaults. AI-powered tools automate routine cybersecurity tasks, improving operational efficiency, reducing manual errors, and allocating human resources to strategic initiatives within IoT environments [7]. This automation also enables organizations to scale their cybersecurity efforts to meet the growing volume and complexity of cyber threats. Moreover, AI-driven cybersecurity solutions are adaptable to evolving threats, ensuring organisations remain resilient against the latest cyber threats. They continuously learn and update algorithms, enabling organizations to stay ahead of cybercriminals and mitigate new types of attacks.

1.3 INTEGRATION OF AI INTO IoT CYBERSECURITY STRATEGIES TO PREVENT CYBERATTACKS

AI has revolutionised cybersecurity in IoT by giving businesses strong tools to strengthen their defences against cyberattacks. AI-driven systems use ML algorithms to analyse large amounts of IoT data in real time, allowing for proactive threat detection and mitigation. AI systems can prevent cyberattacks by constantly tracking network activity, system logs, and user behaviour [8].Integrating AI into IoT cybersecurity methods provides great accuracy in detecting and responding to both known and unexpected threats. ML algorithms use historical data and attack signatures to detect typical cyber threats such as malware, phishing, and DOS assaults. AI-powered systems can potentially detect previously unknown risks by recognising unexpected patterns or abnormalities in network data or user behaviour [9].

Furthermore, AI enhances cybersecurity defences by enabling organizations to respond rapidly to emerging threats in real time. They automatically quarantine suspicious files, block malicious IP addresses, and alert cybersecurity teams to potential security incidents, reducing cyberattack risk [10].Moreover, AI enables organisations to stay ahead of cyber dangers by constantly learning and adapting to new threats. ML algorithms analyse fresh IoT data and update models to effectively detect emerging threats, ensuring resilience to cybercriminals' latest attack vectors and IoT security techniques.

1.4 APPLICATIONS OF AI IN IoT CYBERSECURITY

The use of AI to improve IoT cybersecurity is a game-changing strategy to defend against increasing cyber threats [11], [12]. AI serves a significant part in discovering vulnerabilities and threats in hardware security.Here's an overview of how AI is used to improve security in computer hardware.

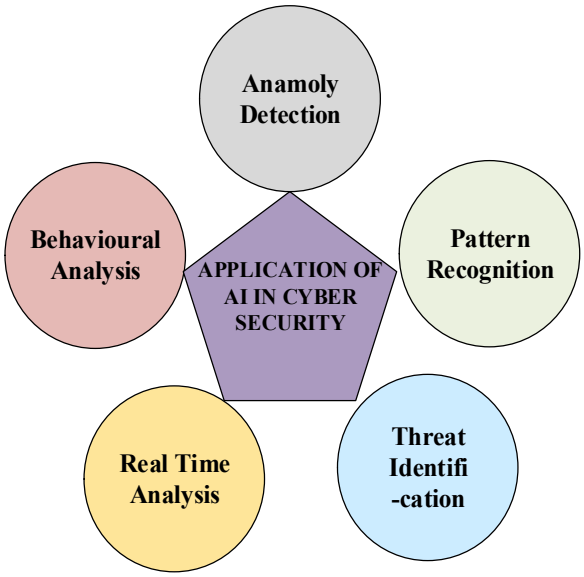

Figure 2: AI Application in cybersecurity

1.4.1 Anomaly Detection:

AI algorithms, specifically ML models, are used to provide a baseline of normal system behaviour, which can then be used to detect abnormalities that may suggest potential hardware-based vulnerabilities or attacks. This proactive approach is especially effective against novel and sophisticated attackers.

1.4.2 Behavioural Analysis:

AI systems analyse historical system behaviour patterns to identify deviations or irregularities that could signal hardware-based attacks. This behavioural analysis improves the ability to recognize subtle changes in hardware behaviour, resulting in more nuanced and adaptable security responses.

1.4.3 Pattern Recognition:

Neural networks, a subset of AI, are employed in hardware security to detect patterns and relationships in data. They excel in pattern recognition, allowing them to detect hardware-based vulnerabilities that may not be visible through traditional methods. Their adaptability enables them to learn and grow in response to new threats.

1.4.4 Threat Identification:

ML models are trained on a variety of datasets to detect and classify possible threats based on known hardware vulnerabilities and attack patterns. This proactive identification enables the adoption of targeted preventive actions, increasing the system's ability to detect known vulnerabilities and attack signatures.

1.4.5 Real Time Analysis:

AI systems examine hardware data instantaneously, detecting irregularities and triggering rapid responses to mitigate potential risks.This real-time analysis guarantees proactive security measures that respond to the dynamic nature of cyber threats while minimising the impact of hardware-based vulnerabilities and attacks.

1.5 STRUCTURE OF THE REVIEW

The interdisciplinary collaboration among cybersecurity specialists, ethicists, policymakers, and technologists is critical for establishing comprehensive approaches to AI-driven cybersecurity within IoT that balance innovation, ethics, and respect for individual rights. By embracing responsible AI practices and cultivating an ethical culture, we can maximise AI's potential to improve IoT cybersecurity defences while maintaining core values such as privacy, justice, and human dignity.This review offers a detailed assessment of the integration of AI techniques and security mechanisms in the field of IoT cybersecurity. Section 2 describes the background and motivation. The efficacy of the AI-driven IDS in the context of IoT is discussed in detail in section 3. Section 4 provides brief content on the adaptability and scalability of AI-based security mechanisms within IoT ecosystems. Implications for data privacy and ethical considerations are mentioned in section 5. Finally, section 6 provides conclusion of review.

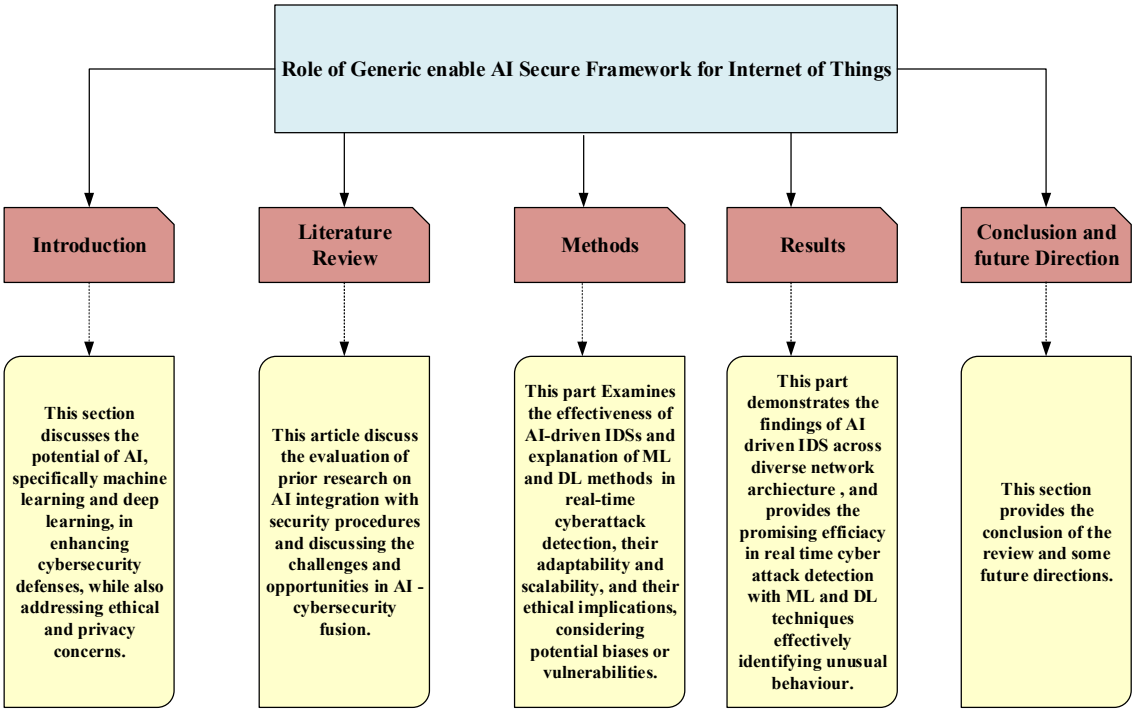

Figure 3: Taxonomy of the review

2. LITERATURE SURVEY

The growing reliance on digital technology and the spread of internet-connected gadgets have increased cyber risks, ranging from data breaches to ransomware attacks. Traditional cybersecurity solutions, while helpful in some cases, are struggling to keep up with cyber criminals changing techniques. Despite of this issue, there is an increasing interest in using AI approaches to improve cybersecurity defences.

AI, particularly ML and DL, has emerged as an effective technique for improving cybersecurity defences against a constantly changing landscape of cyber threats. ML and DL approaches allow security experts to analyse huge amounts of data, such as network traffic and user behaviour, at new speeds and accuracy [13]. These AI algorithms enable cybersecurity systems to identify and respond to possible threats in real time proactively. ML models can detect patterns indicating harmful activity, but DL algorithms can reveal hidden insights and

connections in complicated datasets, increasing the overall robustness of cybersecurity defences.

2.1 INTEGRATION OF AI TECHNOLOGY WITH IoT SECURITY PROCEDURES

The incorporation of AI in IoT cybersecurity implies a paradigm change towards more intelligent and adaptive security systems, delivering proactive threat detection and response capabilities that traditional security measures struggle to match.

The study by Konda [14] highlighted the complex nature of AI development and deployment, involving technical, ethical, and practical aspects. It emphasized the need to address ethical challenges to fully realize the potential of AI technology. A collaborative approach involving expertise from various fields, including computer science, ethics, law, and social sciences, is crucial for responsible AI development. This approach would harness the transformative power of AI while aligning it with ethical principles and societal improvement.A study by Iqbal et al. [15] explored the use of AI in military contexts, focusing on its role in cyberwarfare, autonomous weapon systems, surveillance, and predictive analytics. This research highlighted the effectiveness of AI in enhancing decision-making processes and the ethical and legal implications of AI deployment. It also examined how AI influences security policies, addressing concerns about accountability and transparency. The study also examined the potential impact of AI integration on the global balance of power, highlighting how varying access to AI capabilities may reshape international relations and geopolitical landscapes. These findings aim to inform policymakers, military strategists, and scholars about the opportunities and challenges of AI integration.

In response to the critical demand for safe and efficient services in the IoT ecosystem, Latif et al. [16] undertook a study to address IoT network management concerns, with a special emphasis on computation and energy scarcity issues.This study created an innovative architecture for IoT networks that utilises AI to improve security and energy efficiency. The architecture integrates blockchain and Software-Defined Networking technologies, resulting in efficient data analysis, security, and energy management. The cluster-based framework eliminates the Proof of Work component, resulting in significant energy savings and improved data transfer rates. The model outperformed conventional blockchain approaches and current routing protocols in terms of efficiency and performance. However, the architecture faces practical challenges in real-world implementation and scalability. Further research is needed to evaluate robustness and security consequences of integrating blockchain and SDN technologies into IoT networks.

Camacho et al. [17] investigated the multifaceted role of AI in cybersecurity, focusing on applications in domains such as threat detection, vulnerability assessment, incident response, and predictive analysis.It showed how AI systems can quickly identify security breaches and enable proactive defence mechanisms. However, challenges remain, such as ensuring equitable access, addressing data privacy and ethics, and reducing the environmental footprint of AI operations.

Yang et al. [18] investigated the e-government systems' security and privacy in smart cities and identified challenges. They used a distributed, secure, and secure framework utilising blockchain technology and AI. The framework aims to integrate e-government systems into smart city environments, ensuring user privacy and trust. However, the study acknowledges limitations, including scalability, interoperability, and regulatory compliance. Further research is needed to evaluate its effectiveness in diverse smart city contexts.Vegesna's [19] study explores AI's role in cybersecurity, evaluating models, algorithms, and technologies for threat identification, response, and recovery. However, limitations include theoretical frameworks.

Figure 4: AI and Cybersecurity [19]

The table 1 provides a structured overview of the studies on the Integration of AI technology with security procedures with their respective focus on various security measures.

Table 1: Overview of Integration of AI with IoT Security Procedure

REF	SECURITY CONTEXT	FOCUS
[14]	Understanding the complex nature of AI development	Addressing collaborative approach involving expertise in various fields.
[15]	Use of AI in Military	Role in technological warfare, driverless weapon systems, ethical and legal issues, and impact on global power balance.
[16]	IoT network management with AI	Addressing IoT network management issues through innovative AI architecture for security and energy efficiency, AI in the field of cybersecurity, focuses on identifying threats, risk assessment, incident response, and predictive analysis.And integrating blockchain and SDN technologies.
[17]	Multifaceted role of AI in IoT cybersecurity	Applications of AI in cybersecurity, highlighting its applications in threat detection, vulnerability assessment, incident response, and predictive analysis.
[18]	Security and privacy in smart cities	Focusing on the use of blockchain and AI in a decentralized, secure, and privacy-preserving framework.
[19]	Evaluation of AI's role in cybersecurity	algorithms, and technologies for threat identification, response, and recovery, limitations

2.2 CHALLENGES AND OPPORTUNITIES PRESENTED BY COMBINING AI AND CYBERSECURITY

Combining AI and cybersecurity within the realm of IoT creates a dynamic landscape with a mix of challenges and benefits. One major concern is the susceptibility of AI models to malicious attacks, in which adversaries exploit flaws to trick systems into making wrong conclusions. Protecting against such attacks demands strong defences and constant research into adversary resilience.

Furthermore, the convergence of AI and cybersecurity raises issues about data privacy, since AI-powered solutions frequently require access to sensitive data for training and analysis. Balancing data access with privacy restrictions is a complicated task for organisations looking to use AI in IoT cybersecurity. Furthermore, inherent biases in training data can spread to AI models, resulting in unfair or discriminating outcomes. Addressing prejudice and maintaining fairness in AI-powered cybersecurity systems is critical for preserving trust and integrity in decision-making processes.

Sontan et al. [20] study explored the transformative impact of AI techniques in cybersecurity, including threat detection, incident response, and vulnerability analysis.It explored vulnerability analysis using AI-driven methodologies, highlighting their ability to automate scanning, prioritize threats, and learn from historical data. AI-powered solutions improve cybersecurity scalability, accuracy, and adaptability. However, ethical and privacy considerations are crucial in deploying AI in cybersecurity operations, ensuring privacy rights and avoiding weaponization.

Mughal et al. [21] explored the use of AI in information security, highlighting its advantages and challenges. They discussed the dynamic nature of cyber threats and the limitations of traditional rule-based systems. AI can process large datasets, detect anomalies, automate threat responses, and provide real-time insights. However, the study highlighted the need for ethical frameworks and accountability mechanisms to ensure fair, transparent, and ethical AI use. The role of humans in information security is likely to evolve.The study by Zeadally et al. [22] highlighted the increasing complexity and scope of IoT cyber threats, emphasizing the need for a comprehensive understanding of these risks. It highlighted the need for new AI techniques to detect and mitigate threats, ranging from machine reasoning to human-like actions. Despite the study's limitations, it provides valuable insights into the evolving landscape of cyber threats and the role of AI in addressing them.

From the study, Aslam et al. [23] explored the symbiotic relationship between AI and cybersecurity, examined its applications, benefits, and limitations. It also explored the future trajectories of this dynamic field, considering ethical and strategic challenges. However, the study's limitations include focusing on theoretical frameworks and general trends, and not addressing the practical effectiveness of AI-driven cybersecurity solutions through extensive real-world implementations and empirical evaluations.

Despite these challenges, incorporating AI into IoT cybersecurity creates appealing prospects for better threat detection, automated incident response, and continuous learning. AI-powered systems can analyse massive volumes of data in real time, allowing organisations to detect and mitigate cyber risks at unprecedented speeds and precision. Furthermore, AI-powered automation streamlines incident response operations, decreasing response times and mitigating the effect of cyber-attacks. AI strengthens cybersecurity defences by constantly learning and adapting to changing threats, allowing organisations to remain ahead of adversaries' tactics and strategies. AI systems can use predictive analytics to find patterns and trends in previous data, allowing organisations to predict and prevent potential cyber risks proactively. As organisations traverse the difficult convergence of AI and cybersecurity, resolving these

challenges and capitalisingon the potential given by AI-driven solutions to boost cyber defences and protect digital assets.

Table 2: Challenges and Opportunities

Ref No	Challenges	Opportunities
[20]	Ethical and Privacy Considerations	Scalability, Accuracy and Adaptability
[21]	Need for Ethical Frameworks	Automation and real-time insights
[22]	Understanding cyber threats	-
[23]	-	Application and Future Trajectories

3. APPROACHES FOR ENHANCING CYBERSECURITY WITH AI

In recent years, incorporating AI technology into cybersecurity operations has emerged as a potential strategy for improving defence mechanisms against emerging cyber threats. AI-powered solutions provide increased capabilities for threat detection, response, and mitigation, increasing overall cybersecurity resilience. This section looks at the many strategies and techniques used to exploit AI in cybersecurity, to provide insights into the efficacy and adaptability of AI-based security solutions.

3.1 METHODOLOGIES FOR EVALUATING AI-DRIVEN INTRUSION DETECTION SYSTEMS

The evaluation of AI-driven IDS is a critical component of AI integration into cybersecurity. Methodologies for evaluating the efficacy of these systems include rigorous testing and validation procedures to establish their accuracy, efficiency, and dependability in identifying and mitigating cyber threats. These approaches may involve simulated attack scenarios, real-world data analysis, and comparisons with standard security procedures.Medjek et al. [24]developed an IDS using ML techniques to detect routing attacks against Routing Protocols for Low-power and Lossy Networks. They simulated various attacks and trained classifiers using features from various network topologies. However, there is a lack of exploration into alternative ML algorithms and a focus on classifier efficacy alone. Addressing these could improve the understanding of ML-driven IDS for RPL networks.

In their study, Vijay et al. [25] developed a groundbreaking approach to network management by combining an AI-driven IDS, a BAT optimization method, and a DCNN. The BATO-DCNN method enhances the convergence and accuracy of DCNN-based intrusion detection, achieving superior performance in complex search spaces and model parameter optimization. However, the approach faces limitations in generalizability across network architectures and computational overhead, which could be addressed through further empirical validation and optimization strategies.Panagiotou et al. [26] provided a comprehensive taxonomy of host-based IDS solutions, focusing on contemporary methodologies like Neural Network (NN) and DL. Their datasets offered valuable insights into intrusion detection research but may overlook alternative methodologies that may offer complementary insights or superior performance.

Wahab et al. [27] developed an AI-driven IDS framework to combat cyber threats in E-health and IoMT environments. The framework uses a hybrid model of long short-term memory and gated recurrent units. Evaluations were conducted using the CICDDoS2019 dataset and compared to classifiers like cu-GRU+DNN and cu-BLSTM. The study's effectiveness may be limited by the dataset's scope and metrics.Research by Yaseen et al. [28] explored the transformative impact of AI on cybersecurity, highlighting its role in threat detection and response. However, the study highlighted the limitations such as potential exploitation by malicious actors, limited datasets, ethical considerations, and potential vulnerabilities in AI models.

Liu et al. [29] developed a framework for Combined IDS datasets, SCVIC-CIDS-2021, to address the lack of datasets containing both network packet and host data. They developed a transformer-based deep learning model called CIDS-Net, which outperformed baseline models based solely on network flow features. The study highlighted the importance of incorporating host-based features in IDS for enhanced network security.

Summary:

From a thorough examination of approaches for evaluating AI-powered IDS. It includes research on ML techniques for detecting routing attacks, novel approaches that combine AI with optimisation methods and deep learning, a taxonomy of host-based IDS solutions, AI-driven IDS frameworks for specific environments, and discussions about AI's transformative impact and limitations in cybersecurity. The studies emphasised the significance of thorough testing and validation techniques for determining the accuracy, efficiency, and dependability of these systems in detecting and mitigating cyber threats. While some studies focused on the creation and evaluation of IDS frameworks adapted to specific contexts, such as E-health and the Internet of Medical Things (IoMT), others give extensive taxonomies of host-based IDS systems. Despite the progress made in using AI for IoT cybersecurity, the survey highlighted several challenges and limitations, such as the need for more research into alternative ML algorithms, generalizability across network architectures, computational overhead, ethical considerations, and the importance of incorporating both network packet and host data for comprehensive intrusion detection. Overall, this survey emphasises continuous efforts to enhance AI-driven IDS systems and emphasises areas.

3.2 AI METHODS FOR REAL-TIME DETECTION OF IoT CYBER THREATS

AI approaches such as ML and DL are critical for detecting cyber threats in real time in IoT landscape. ML algorithms analyse massive volumes of data to detect patterns and abnormalities that indicate malicious activity, whereas DL approaches as neural networks excel at digesting complicated data structures to reveal hidden dangers. These AI techniques enable cybersecurity systems to quickly recognise and respond to emerging attacks, reducing potential damage and downtime.

3.2.1 AI IN ML FOR SECURITY

In the field of IoT cybersecurity, several ML models play critical roles in strengthening defences against ever-changing threats. Among the most often used models are supervised learning, unsupervised learning, and reinforcement learningasrepresented in Figure 5. Supervised learning is the process of training a model on labelled data so that it can recognise patterns and make predictions based on instances encountered during training. In cybersecurity, this can be used to categorise emails as spam or valid, identify dangerous files based on recognised signatures, or detect odd behaviour in network traffic.

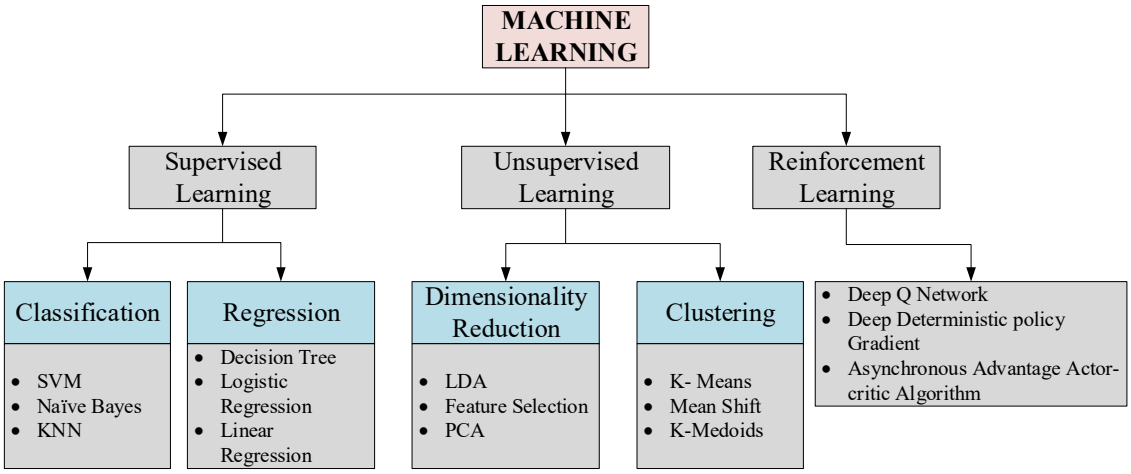

Figure 5: ML Approaches in AI for Cybersecurity

ML algorithms are data-driven systems that learn and adapt based on data. They enable computers to perform tasks like traffic detection without explicit information. They also enable efficient analysis of attacks and security events like spam mail, user identification, social media analytics, and attack detection. These algorithms enable efficient decision-making and efficient execution of tasks. From Figure 5., supervised learning utilizes labelled data, unsupervised learning uses unlabelled data, and semi-supervised learning combines both.

In their study, Alsarhan et al. [32] used SVM for intrusion detection in VANET. They integrated three intelligence optimization algorithms, GA, PSO, and Ant Colony Optimization, to improve the SVM classifier's accuracy. GA outperformed other optimization algorithms in performance. However, the study's limitations include generalizability and focusing on accuracy without considering other metrics or computational overhead.Sarker et al. [33] introduced the "IntruDTree" ML-based security model for intrusion detection. The model prioritizes security features and constructs a tree-based model using significant features. It shows effectiveness in prediction accuracy and reducing computational complexity. The model's effectiveness was evaluated on cybersecurity datasets and at the application level. However, limitations include generalizability and the need for further validation of diverse datasets and real-world applications.

Muneer et al. [34]research, highlighted the significant impact of machine learning on cyber security event detection. They argued that ML models can detect patterns, anomalies, and correlations in vast datasets, making them a promising advancement in information security. However, they warn against false positive or negative detections, which could compromise an organization's security. The study also acknowledges the need for rigorous evaluation and validation processes to ensure the effectiveness of ML in detecting real-world threats. The study presented by Arivudainambi et al. [35] introduced a hybrid approach of PCA and ANN for classifying malicious traffic whose results obtain better results with the advantage is capable of classifying the attacks more accurately in less time. In the study, Martin et al. [36] used ensemble classifiers for malware identification based on the merging of static and dynamic information, and while the experimental findings demonstrate good performance for the majority of the state-of-the-art algorithms tested, there is still potential for improvement over the Omni Droid dataset. This could assist researchers to train, test, and assess the efficacy of their algorithms. ML algorithms learn from data adapt accordingly and provide results based on data and examples.

Another study presented by Noor et al. [37], used ML classifiers such as NB, KNN, DT, RF and DL-based NN to detect 36 malware well-known threats, which automatedcyber threat attribution. From this evaluation, the experiment showed that ANN, SVM and RF are the best classifiers.However, the framework is dependent on threat data.Sahingoz et al. [38], provided a study for phishing detection from URLs using RF which was applied over NLP-based features. This research provides advantages such as language constructed in a language-independent way, faster execution, and robustness for the zero-day attack. However, it is the potential for false positives, leading to legitimate web paging being incorrectly added to the blacklist and inaccessible to users.

Toledo et al. [39] conducted a study to investigate the possibility of intercepting and classifying encrypted DNP3 traffic communication packets individually and performing a Peekaboo attack on encrypted IPSEC ESP DNP3 traffic using supervised ML models. They simulated two scenarios of encrypted DNP3 traffic:normal traffic without packet drops, and simulated Peekaboo attack scenarios where all packets are dropped and retransmitted with Urret messages. However, the study found that Peekaboo attacks can blind SCADA operators for some minutes and cause system disruptions.

Table 3: Meta-level study of chosen relevant literature on cyber security using ML classifiers

Ref No	ML Classifier	Problem solved	Domain Selected
[32]	SVM	Intrusion detection in VANET is a nonconvex and combinatorial problem	VANET
[33]	IntruDTree	Predicting high accuracy by reducing the computational cost with less number of features.	IoT
[35]	PCA and ANN	Malware traffic classification	Malicious traffic classification
[36]	Ensemble classifiers	Malware Detection	Android devices
[37]	NB, KNN, DT, RF and DL	Detection of 36 well-known threats	General
[38]	RF	Phishing Detection from URLs	Electronic commerce
[39]	DT, KNN, SVM, NB	Encrypted DNP3 traffic classification	Traffic Classification.

SUMMARY

AI combined with ML has proven useful in strengthening cybersecurity measures, providing increased capabilities for threat detection, categorization, and response. SL, USL, and RL are some of the most common ML approaches used in cybersecurity.Studies have proven effective in cybersecurity domains like intrusion detection, malware identification, phishing detection, and event analysis. Innovative approaches include intelligence optimization algorithms, tree-based models, and ensemble classifiers. However, challenges like false positives, data dependency, and sophisticated attack vulnerabilities persist. Rigid evaluation and validation processes are crucial for ensuring the dependability and efficacy of MLbased cybersecurity solutions. Hence, this study has to continue researchin DL algorithms are essential to address

existing challenges and further improve cybersecurity resilience in the ever-changing threat landscape.

3.2.2 AI IN DL FOR SECURITY

AI combined with DL has revolutionized security measures by processing complex data and extracting intricate patterns. DL is a method of learning representations with multiple concept levels, utilizing NNsto mimic the human brain. It can analyze data like text, images, and audio, while shallow learning models consist of a few hidden layers. DL can locate and learn representations from raw data, conduct training on features, and classification..ML methodologies are also used in DL, but other methods like Transfer Learning are also employed which is explained in Figure 6.

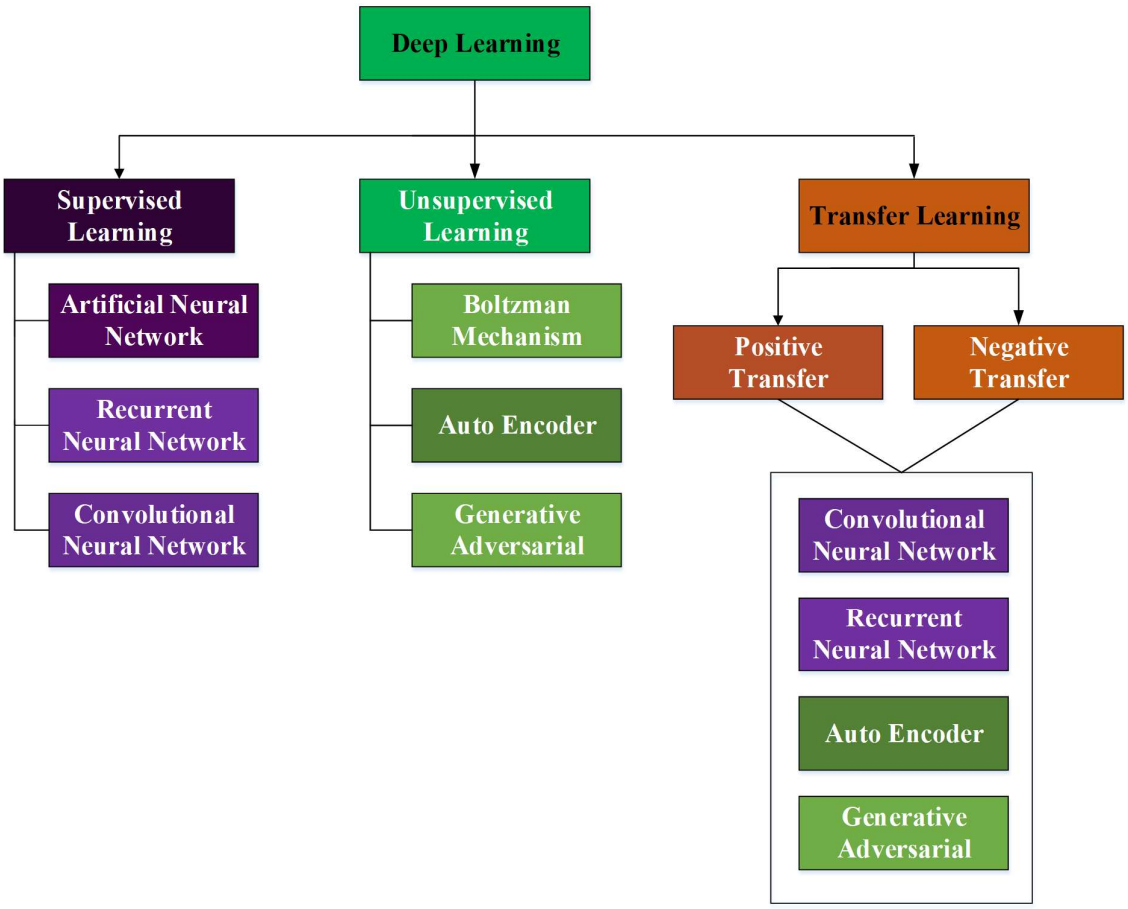

Figure 6: DL Approaches in AI for Cybersecurity

DL approaches, like as CNNs and RNNs, are effective in detecting malicious behaviours and anomalies in vast amounts of data, including network traffic logs and system data, and user behaviour data. This has led to significant advancements in threat detection, anomaly identification, and predictive analysis in cybersecurity.Furthermore, DL-based techniques enable real time monitoring and response to security incidents, which improves the overall cybersecurity posture. However, obstacles such as interpretability, adversarial attacks, and the

requirement for large-scale labelled datasets remain, emphasising the significance of continued research and development efforts to fully leverage AI in DL for security applications.

In their study, Keshk et al. [40] developed an Explainable ID Framework for IoT networks, utilizing an LSTM model to identify cyberattacks and provide explanations for their decisions. They introduced a new set of input features using the SPIP framework. The framework demonstrated high detection accuracy, efficient processing time, and superior interpretability.However, limited to confined to highlighting salient aspects and correlations, without identifying the underlying security flaws exploited.Sayegh et al. [41] have developed an advanced IDS for IoT networks, using LSTM and the SMOTE. The IDS effectively distinguishes between normal network traffic and potential malicious attacks. The study evaluated the IDS on three public datasets and found superior performance in detecting network intrusions. However, the focus on synthetic data generation may not fully capture real-world attack scenarios.

Ghanem et al. [42] used an intrusion detection method using the Hybrid Artificial Bee Colony algorithm and Monarch Butterfly Optimization. The technique enhances classification accuracy for malicious and non-malicious traffic in systems. The method is tested against nine other metaheuristic algorithms and demonstrated significant performance improvements. However, the feature selection technique has not been optimised, indicating potential for future research.Lee et al. [43] introduce Instruction2vec, anML method for static binary analysis. The framework models assembly code and learns software weakness code features through Text-CNN extraction. The authors compare Instruction2vec with Word2vec and Binary2img, focusing on Common Weakness Enumeration-121. However, the method's generalizability may require further validation and refinement.Thamilarasu et al. [44] presented an IDS for the IoT using a DL algorithm. This system identifies malicious traffic and promotes interoperability. It evaluated its adaptability and scalability but lacked discussion on potential challenges like false positives or computational complexity.

Alomari et al. [45] developed a robust malware detection system using DL and feature selection methodologies. They used two distinct malware datasets and trained dense and LSTM-based deep learning models. The study showed comparable performance to the original dataset, but its main limitation is its focus on general malware detection without mentioning the types of malware.Chaganti et al. [46] utilized a DL-based Bi-GRU-CNN model for detecting and classifying IoT malware. They also used ELF binary file byte sequences and RNN-based DL models. Their approach achieves better results in family classification but faces limitations due to imbalanced datasets.Xiao et al. [47] developed a CNN-IDS for network security, eliminating redundant features and extracting features from reduced-dimensional data. The model showed higher accuracy, lower false alarm rates, and improved timeliness compared to conventional algorithms. It also reduced classification time, meeting real-time system requirements However, it faces a limitation that R2L and U2R have low detection rates.

Papamartzivanos et al. [48] developed a new methodology to improve IDS by combining self-taught learning and MAPE-K frameworks. Their approach, which uses deep learning techniques, enables IDS to understand the attacks' nature. Experimentation validated the methodology, but it obtained low detection accuracy for U2R and R2L attacks. Mayuranathan et al. [49] developed a method for identifying DDoS attacks using Random Harmony Search and a DL-based classifier model. They integrated seven additional layers between visible and hidden RBM layers to improve detection rate. The study validated its effectiveness using the KDD'99 dataset, contributing to the advancement of IDS methodologies. However, the computational resources for IoT devicesare high.

Jiang et al. [50] have developed a novel approach to intelligent attack detection using LSTM-RNNs in a multi-channel framework. The method integrates data preprocessing, feature abstraction, and multi-channel training to achieve high detection rates. Although the model outperforms existing methods, but, itdoes not identify new types of attacks.Tian et al. [51] used an ID approach using an improved Deep Belief Network, simplifying data preparation and incorporating a sparsity penalty term for unsupervised training. This method addressed feature homogeneity and overfitting issues in IDSs. Even though, the accuracy of this model may be affected due to uncertainty of selecting parameters.Zhang et al. [52] introduced Tiki-Taka, a framework to evaluate the robustness of DL-based NIDS against adversarial manipulations and integrate defence mechanisms to enhance resilience. The study assessed five attack mechanisms against three NIDS models, revealing that defence mechanisms reduced attack success rates and achieved nearly 100% detection accuracy for most malicious traffic categories, including critical threats like botnets and DoS attacks.

Table 4: Meta-level study of chosen relatedworks on cyber security using DL classifiers.

Ref No	DL Classifier	Problem solved	Domain Selected
[40]	LSTM	Increase the understanding and clarity of IDS, and their performance.	VANET
[41]	LSTM+SMOTE+GAN	Imbalance data mitigation, and the elimination of extensive feature engineering.	IoT.
[42]	ABC+MBO+ANN	Detecting intrusions into network systems andimproving the accuracy and efficiency of classification.	IoT
[43]	CNN	Automated vulnerability detection	Software Engineering
[44]	DNN	Address assaults on IoT systems in real time using excellent defence and security.	Network systems.
[45]	Dense, LSTM based model	Large and high dimensional data has been addressed.	IoT
[46]	Bi-GRU -CNN, RNN	Identify the malware class by using an open source.	IoT Malware
[47]	CNN	Reduced the FAR and classification time.	Massive data environment
[48]	Autoencoder	achieved a high attack detection rate	ICT Infrastructure
[49]	RBM	Improved the performance of detecting attacks.	IoT
[50]	LSTM-RNN	Information Security problem Solved, achieved high detection rate.	Social Networks
[51]	CDBN	Increased FAR and classification accuracy	General
[52]	CNN, MLP, C-LSTM	defending against adversarial attacks	Network System

SUMMARY

AI in DL for cybersecurity is a crucial area of research, utilizing advanced DL techniques to enhance defences against evolving cyber threats. DL models, particularly NNs, are being used in IDSs and network Intrusion Prevention Systems.The accuracy and promptness of threat identification are improved by these models' superior ability to process massive amounts of network data and uncover complex patterns suggestive of hostile activity. Cybersecurity professionals can successfully defend against a variety of cyberattacks, such as malware, intrusion attempts, and DDoS, by utilizing techniques like CNNs, RNNs, and DBNs. Furthermore, DL-based cybersecurity systems become even more resilient against advanced evasion techniques used by cyber adversaries when adversarial training and defence mechanisms are integrated. Even with these improvements, research must continue to address issues like adversarial robustness, model interpretability, and DL approaches' scalability in complex and dynamic network environments.The combination of AI and DL has enormous potential to strengthen cybersecurity defences and protect vital digital assets from new threats as the cyber threat landscape changes.

3.3 ADAPTATION AND SCALABILITY OF AI-BASED SECURITY MEASURES

In the cybersecurity setting, the adaptability and scalability of AI-based security solutions provide a crucial edge in dealing with the dynamic nature of cyber threats and network architecture. Unlike traditional security systems, which may struggle to keep up with growing threats, AI algorithms provide a dynamic and flexible framework that constantly learns and changes based on new data and experiences. This feature allows security systems to anticipate future risks by recognising and mitigating previously unknown attack patterns.

The continual learning aspect of AI algorithms enables security systems to spot new trends and patterns of harmful activity, allowing them to adjust detection techniques in real time which helps keep ahead of cyber threats. As AI algorithms improve their understanding of network behaviour, they become better at distinguishing between true threats and false alarms, increasing performance of threat identification. From the above-mentioned survey of previous research studies, for instance, studies such as Alsarhan et al. [32] and Sahingoz et al. [38] show that ML classifiers such as SVM and RF can be used to detect intrusions and phishing, respectively. These models use data-driven methodologies to identify network traffic patterns and anomalies, resulting in efficient and language-independent solutions that can be quickly deployed to tackle emerging threats. Furthermore, ML-based security models, such as those introduced by Sarker et al. [33], demonstrate the scalability of AI-driven techniques by effectively handling massive amounts of data while reducing computational complexity. Furthermore, Toledo et al. [39] demonstrated the potential of ML in combating sophisticated attacks, such as Peekaboo attacks on encrypted communication channels, emphasising the adaptability of ML algorithms to changing threat landscapes.

Also, AI-based security measures that use DL algorithms demonstrate exceptional versatility and potential scalability in solving a variety of cybersecurity concerns. These models enable real-time monitoring and reaction to security issues, improving the overall cybersecurity posture. However, problems such as interpretability, adversarial assaults, and the requirement for large-scale labelled datasets remain, highlighting the significance of continued research and development efforts to fully realise the potential of AI in DL for refuge applications.Studies by Keshk et al. [40], Ghanem et al. [42], and Jiang et al. [50] show the adaptability of DL-based security measures by developing intelligent intrusion detection systems and advanced malware detection frameworks. These systems use DL algorithms to successfully identify cyber threats and improve classification accuracy for both harmful and non-malicious communications.

Furthermore, strategies such as feature selection methodology, self-taught learning, and multi-channel frameworks improve the adaptability of DL models to unique cybersecurity concerns.Furthermore, studies like Thamilarasu et al. [44], Zhang et al. [52] demonstrated the scalability of AIbased security measured by applying DL algorithms to IoT networks and NIDS to detect and classify malicious activity across large-scale environments.

Thus, the integration of AI in ML and DL techniques offers a promising way to improve cybersecurity measures. AI algorithms' adaptability and scalability enable efficient detection of cyber threats through supervised, unsupervised, and ensemble learning approaches. However, challenges like imbalanced datasets and computational resource requirements need ongoing research. DL techniques offer significant advancements in threat detection and anomaly identification, particularly in handling vast data volumes and evolving threat landscapes. Despite challenges like interpretability and identifying new types of attacks, DL models demonstrate remarkable adaptability and scalability, providing robust defence mechanisms against cyber threats.

4. EFFECTIVENESS OF AI-DRIVEN IoT SECURITY MEASURES

AI-powered security techniques have shown to be extremely effective in improving cybersecurity defences across multiple areas. These systems, which use complex algorithms and machine learning approaches, provide strong protection against emerging cyber threats.The following findings emphasised the need to harness AI technologies to improve cybersecurity defences and stay ahead of emerging threats.

4.1 FINDINGS FROM THE ASSESSMENTS OF AI-DRIVEN IDS

Several notable conclusions emerged while assessing AI-driven IDS across different network architectures. To begin, AI-powered IDS outperformed traditional rule-based systems in terms of detection capabilities, efficiently identifying and stopping hostile activity across a wide range of network infrastructures. The use of ML and DL techniques allowed IDS to analyse network traffic patterns and detect anomalies indicating cyber threats with high accuracy and efficiency. Furthermore, AI-powered IDS demonstrated the capacity to adapt and evolve in real-time, always learning from new data to increase detection skills and stay ahead of emerging threats. Overall, the examination demonstrated the efficiency of AI-driven IDS in strengthening cybersecurity defences through comprehensive threat detection and prevention methods. The evaluation of AI-driven IDS for the survey of some studies is an important aspect of AI incorporation into cybersecurity as mentioned in below Table 5. Methodologies for assessing the efficacy of these systems include rigorous testing and validation procedures to ensure their accuracy, efficiency, and dependability in detecting and addressing cyber threats.

Table 5: Results Obtained for AI-Driven -IDS

Study	**Method**	**Accuracy %**	**Precision %**	**Recall %**	**F1 %**
Vijay [25]	BATO-DCNN	42	48	49	45
Wahab [27]	**CuLSTM+GRU**	**99.01**	**98.80**	**99.12**	**99.04**
Tang [30]	GRU+RNN	89	91	92.50	94
Kim [31]	CNN	91.50	-	-	-
Liu [29]	XG Boost, RF	-	-	-	98.48

The results of these AI-driven IDS assessments show that these systems are successful at identifying and mitigating cyber threats across a wide range of network environments. These IDS solutions help to boost cybersecurity defences and protect vital assets from hostile activityby employing novel approaches and rigorous evaluations. Moreover, AI-driven IDS assessments are particularly effective in IoT environments, where interconnected devices and

complex data flow pose unique cybersecurity challenges. These systems [27] deliver robust threat detection and mitigation capabilities, enhancing visibility into network traffic. Advanced AI algorithms enable proactive identification of potential security breaches and swift responses to emerging threats. The adoption of AI-driven IDS systems represents a significant advancement in IoT cybersecurity, providing organizations with the necessary tools to defend against cyber threats in a dynamic digital environment.

4.2 RESULTS FROM EXAMINATION OF AI METHODS

The study of AI approaches for detecting anomalous behaviour and potential cyber-attacks in real-time produced encouraging results. ML and DL algorithms have shown to be extremely successful at detecting suspicious activity and anomalies in network traffic. AI-powered systems were able to detect tiny variations from typical behaviour, indicating potential cyber threats, by analysing massive volumes of data in real time. Furthermore, the utilisation of AI algorithms allows for speedy and accurate identification of known and unexpected attack patterns, allowing for fast response and mitigation measures. These findings emphasised the importance of AI in improving organisations' ability to recognise and respond to cyber threats proactively.The examination of AI methods such as ML and DL yielded significant insights into their effectiveness in enhancing security measures as represented in Table 6.

Table 6: Results from the examination of AI methods

Study	**AI Method**	**Method**	**Accuracy %**	**Precision %**	**Recall %**	**F1 %**
Alsarhan [32]	ML	GA-SVM	99			
Sarker [33]	**ML**	**IntruDTree**	**98**	**98**	**98**	**98**
Arivudainambi [35]	ML	PCA and ANN	99.52	-	-	-
Martin [36]	ML	Ensemble classifiers	89.7	89.7	-	-
Noor [37]	ML	NB	88	89	82	83
	ML	KNN	68	69	70	67
	ML	DT	82	76	74	73
	ML	RF	88	92	89	89
	DL	DLNN	94	90	89	89
Sahingoz [38]	ML	RF	97.98	97	-	98
Keshk [40]	DL	LSTM	87.3	78.7	87.6	82.9
Sayegh [41]	**DL**	**LSTM+SMOTE+GAN**	**98.31**	**97.87**	**98.74**	**98.30**
Ghanem [42]	**DL**	**ABC+MBO+ANN**	**98.58**	**96.63**	**-**	**-**
Lee [43]	DL	CNN	96.81	96.65	97.05	-
Thamilarasu [44]	DL	DNN	-	95	-	97
Alomari [45]	DL	Dense, LSTM based model	98.38	-	-	98.9
Chaganti [46]	**DL**	**Bi-GRU -CNN, RNN**	**100**	**99**	**99**	**99**
Xiao [47]	DL	CNN	92.2	-	-	-
Papamartzivanos [48]	DL	Autoencoder	77.99	-	99.6	-
Mayuranathan [49]	DL	**RHS-RBM**	**99.92**	**-**	**-**	**99.93**
Jiang [50]	DL	LSTM-RNN	98.94	-	-	-
Tian [51]	DL	CDBN	96.17	96.8	94.9	95.8
Zhang [52]	DL	CNN, MLP, C-LSTM	98.3	94.3	95.6	94.9

The aggregate results show that AI-driven IDS methodologies [33], [41],[42], [46] and [49] produce better results only when used in IoT environments compared with other domains. The distinct properties of IoT ecosystems, such as networked devices and complicated data flows, necessitate specialised cybersecurity solutions. AI-powered IDS solutions have proven extremely effective in tackling these difficulties, offering organisations sophisticated threat detection and mitigation capabilities that are suited to the IoT ecosystem.

This review emphasises the superiority of AI-driven Intrusion Detection System (IDS) approaches when applied to IoT environments against other domains. The distinct properties of IoT ecosystems, such as networked devices and complex data flows, necessitate specialised cybersecurity solutions. This study discusses how AI-powered IDS systems have been extremely effective in tackling these difficulties, offering organisations sophisticated threat detection and mitigation capabilities that are suited to the IoT ecosystem. This research emphasises the significance of incorporating AI technology, particularly within IoT cybersecurity policies, to successfully protect IoT deployments from future threats.

4.3 DATA PRIVACY AND ETHICAL CONSIDERATION

The evaluation of data privacy and ethical considerations in the integration of AI techniques into IoT security measures is an important part of this review. In today's digital landscape, when massive volumes of data are processed and analysed to detect and mitigate cyber dangers, protecting individuals' privacy rights and preserving ethical standards is critical.AI systems that train and make decisions based on previous data have the potential to perpetuate biases, leading to biased consequences. To address this, methods such as data preprocessing procedures, algorithm transparency, and continual monitoring and evaluation are critical, as AI models may unfairly target specific groups based on race, gender, or socioeconomic position.

Another significant consideration is data privacy which is critical for IoT cybersecurity, as organisations must follow tight standards to secure personal information and prevent unauthorised access. Highly secure encryption systems, restricting access, and data anonymization methods are used to safeguard sensitive information from potential security breaches.

Furthermore, ethical considerations include broader societal ramifications, such as the possible impact of AI-powered in IoT security measures on individual rights, liberties, and social norms. Ethical frameworks and guidelines can assist in the responsible expansion and arrangement of AI systems in cybersecurity by ensuring that they adhere to ethical values such as justice, transparency, accountability, and respect for human autonomy.

By addressing these data privacy and ethical concerns, organisations may foster trust and confidence in AI-powered within IoT security solutions among stakeholders such as users, regulators, and the general public. Furthermore, by incorporating fairness, transparency, and accountability principles into AI design and implementation, cybersecurity professionals can reduce the risks of algorithmic bias and data privacy breaches, ultimately increasing the effectiveness and acceptance of AI driven security solutions for safeguarding digital assets and protecting individual privacy rights.

5. CONCLUSION

The integration of AI into security mechanisms is a significant advancement in cybersecurity, especially in the IoT environment. Through this review, AI-driven Intrusion Detection Systems are crucial in detecting and preventing hostile activities across diverse network architectures. ML and DL methods have shown promise in real-time identifying unusual behaviour and

potential cyber-attacks. AI-based security measures in IoT environments are adaptable and scalable, enabling them to effectively handle dynamic cyber threats and evolving network infrastructures. However, concerns regarding data privacy and ethical considerations should be addressed in the deployment of AI-driven security measures. Ultimately, the IoT environment emerges as a pivotal domain of cybersecurity given its interconnected nature and proliferation of IoT devices. Future research should focus on refining AI algorithms for enhanced threat detection capabilities, addressing emerging cyber threats specific to IoT environments, and improving the transparency and interpretability of AI-based security systems. The IoT environment is a pivotal domain for future cybersecurity advancements, and it is essential to invest in robust frameworks for evaluating the efficiency and reliability of AI driven security measures in worldwide scenarios.

REFERENCES

1. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710.
2. Raparthi, M., Dodda, S. B., & Maruthi, S. (2020). Examining the use of Artificial Intelligence to Enhance Security Measures in Computer Hardware, including the Detection of Hardware-based Vulnerabilities and Attacks. *European Economic Letters (EEL)*, *10*(1).
3. Olabanji, S. O., Marquis, Y., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-Driven cloud security: Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science*, *17*(3), 57-74.
4. Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial intelligence: revolutionizing cyber security in the digital era. *Journal of Computers, Mechanical and Management*, *2*(3), 31-42.
5. Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), 491-497.
6. Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *Revista Espanola de Documentacion Cientifica*, *15*(4), 42-66.
7. Joseph, S. Role of Artificial Intelligence in Cybersecurity.
8. Repalle, S. A., & Kolluru, V. R. (2017). Intrusion detection system using ai and machine learning algorithm. *International Research Journal of Engineering and Technology (IRJET)*, *4*(12), 1709-1715.
9. Beshwari, F., Beshwari, M., & Beshwari, A. (2020). The Role of Artificial Intelligence in Mitigating Unknown-Unknown Risks. *The Role of Artificial Intelligence in Mitigating Unknown-Unknown Risks*, *64*(1), 13-13.
10. Sou, G. (2017). Big data management under internet engineering and information security threat. In *Proceedings of the World Congress on Engineering* (Vol. 1).
11. Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. *Minds and machines*, *29*, 187-191.
12. Akhtar, M., & Feng, T. (2021). An overview of the applications of Artificial Intelligence in Cybersecurity. *EAI endorsed transactions on creative technologies*, *8*(29).
13. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics*, *9*(7), 1177.

14. Konda, S. R. (2019). Ensuring Trust and Security in AI: Challenges and Solutions for Safe Integration. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY*, *3*(2), 71-86.
15. Iqbal, S., Rizvi, S. W. A., Haider, M. H., & Raza, S. (2023). Artificial Intelligence in Security and Defense: Explore the integration of AI in military strategies, security policies, and its implications for global power dynamics. *INTERNATIONAL JOURNAL OF HUMAN AND SOCIETY*, *3*(4), 341-353.
16. Latif, S. A., Wen, F. B. X., Iwendi, C., Li-Li, F. W., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer Communications*, *181*, 274-283.
17. Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.
18. Yang, L., Elisa, N., & Eliot, N. (2019). Privacy and security aspects of E-government in smart cities. In *Smart cities cybersecurity and privacy* (pp. 89-102). Elsevier.
19. Vegesna, V. V. (2023). Enhancing cyber resilience by integrating AI-Driven threat detection and mitigation strategies. *Transactions on Latest Trends in Artificial Intelligence*, *4*(4).
20. Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews*, *21*(2), 1720-1736.
21. Mughal, A. A. (2018). Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions. *Journal of Artificial Intelligence and Machine Learning in Management*, *2*(1), 22-34.
22. Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*, *8*, 23817-23837.
23. Aslam, M. (2024). AI and cybersecurity: an ever-evolving landscape. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(1), 52-71.
24. Medjek, F., Tandjaoui, D., Djedjig, N., & Romdhani, I. (2021). Fault-tolerant AI-driven intrusion detection system for the internet of things. *International Journal of Critical Infrastructure Protection*, *34*, 100436.
25. Vijay, G. S., Sharma, M., & Khanna, R. (2023). Revolutionizing network management with an AI-driven intrusion detection system. *Multidisciplinary Science Journal*, *5*.
26. Panagiotou, P., Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2021). Host-based intrusion detection using signature-based and AI-driven anomaly detection methods. *Information & Security: An International Journal*, *50*(1), 37-48.
27. Wahab, F., Zhao, Y., Javeed, D., Al-Adhaileh, M. H., Almaaytah, S. A., Khan, W., ... & Kumar Shah, R. (2022). An AI-driven hybrid framework for intrusion detection in IoT-enabled E-health. *Computational Intelligence and Neuroscience*, *2022*.
28. Yaseen, A. (2023). AI-DRIVEN THREAT DETECTION AND RESPONSE: A PARADIGM SHIFT IN CYBERSECURITY. *International Journal of Information and Cybersecurity*, *7*(12), 25-43.
29. Liu, J., Simsek, M., Kantarci, B., Bagheri, M., & Djukic, P. (2022, December). Collaborative feature maps of networks and hosts for ai-driven intrusion detection. In *GLOBECOM 2022-2022 IEEE Global Communications Conference* (pp. 2662-2667). IEEE.
30. T. A. Tang, D. McLernon, L. Mhamdi, S. A. R. Zaidi, and M. Ghogho, “Intrusion detection in sdn-based networks: deep recurrent neural network approach,” in Deep

Learning Applications for Cyber Security, p. 175195, Springer, Berlin, Germany, 2019.
31. J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," Electronics, vol. 9, no. 6, p. 916, 2020.
32. Alsarhan, A., Alauthman, M., Alshdaifat, E. A., Al-Ghuwairi, A. R., & Al-Dubai, A. (2023). Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 6113-6122.
33. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*, *12*(5), 754.
34. Muneer, S. M., Alvi, M. B., & Farrakh, A. (2023). Cyber Security event detection using machine learning technique. *International Journal of Computational and Innovative Sciences*, *2*(2), 42-46.
35. Arivudainambi, D., KA, V. K., & Visu, P. (2019). Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance. *Computer Communications*, *147*, 50-57.
36. Martín, A., Lara-Cabrera, R., & Camacho, D. (2019). Android malware detection through hybrid features fusion and ensemble classifiers: The AndroPyTool framework and the OmniDroid dataset. *Information Fusion*, *52*, 128-142.
37. Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, *96*, 227-242.
38. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345-357.
39. de Toledo, T. R., & Torrisi, N. M. (2019). Encrypted DNP3 traffic classification using supervised machine learning algorithms. *Machine Learning and Knowledge Extraction*, *1*(1), 384-399.
40. Keshk, M., Koroniotis, N., Pham, N., Moustafa, N., Turnbull, B., & Zomaya, A. Y. (2023). An explainable deep learning-enabled intrusion detection framework in IoT networks. *Information Sciences*, *639*, 119000.
41. Sayegh, H. R., Dong, W., & Al-madani, A. M. (2024). Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data. *Applied Sciences*, *14*(2), 479.
42. Ghanem, W. A. H. M., & Jantan, A. (2020). Training a neural network for cyberattack classification applications using hybridization of an artificial Bee colony and Monarch butterfly optimization. Neu-ral Process Lett 51: 905–946.
43. Lee, Y., Kwon, H., Choi, S. H., Lim, S. H., Baek, S. H., & Park, K. W. (2019). Instruction2vec: Efficient preprocessor of assembly code to detect software weakness with CNN. *Applied Sciences*, *9*(19), 4086.
44. Thamilarasu, G. and S. Chawla, Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. Sensors, 2019. 19(9): p. 1977.
45. Alomari, E. S., Nuiaa, R. R., Alyasseri, Z. A. A., Mohammed, H. J., Sani, N. S., Esa, M. I., & Musawi, B. A. (2023). Malware detection using deep learning and correlation-based feature selection. *Symmetry*, *15*(1), 123.
46. Chaganti, R., Ravi, V., & Pham, T. D. (2022). Deep learning based cross architecture internet of things malware detection and classification. *Computers & Security*, *120*, 102779.

47. Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, ‘‘An intrusion detection model based on feature reduction and convolutional neural networks,’’ IEEE Access, vol. 7, pp. 42210–42219, 2019
48. D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, ‘‘Introducing deep learning self-adaptive misuse network intrusion detection systems,’’ IEEE Access, vol. 7, pp. 13546–13560, 2019.
49. M. Mayuranathan, M. Murugan, and V. Dhanakoti, ‘‘Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment,’’ J. Ambient Intell. Hum. Comput., vol. 12, no. 3, pp. 3609–3619, 2019.
50. F. Jiang, Y. Fu, B. B. Gupta, Y. Liang, S. Rho, F. Lou, F. Meng, and Z. Tian, ‘‘Deep learning based multi-channel intelligent attack detection for data security,’’ IEEE Trans. Sustain. Comput., vol. 5, no. 2, pp. 204–212, Apr. 2020.
51. Q. Tian, D. Han, K.-C. Li, X. Liu, L. Duan, and A. Castiglione, ‘‘An intrusion detection approach based on improved deep belief network,’’ Appl. Intell., vol. 50, pp. 3162–3178, May 2020.
52. C. Zhang, X. Costa-Pérez, and P. Patras, ‘‘Tiki-taka: Attacking and defending deep learning-based intrusion detection systems,’’ in Proc. ACM SIGSAC Conf. Cloud Comput. Secur. Workshop, 2020, pp. 27–39.