International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 7 No. 5 January – February - 2026

IOT, Smart Devices and Bias in AI Algorithm and Its Impact on Cyber Security

Miss. Sawant Shital Rangrao

Department of BCS, Sadguru Gadge Maharaj College, Karad

DOI - 10.5281/zenodo.18898380

Abstract:

Artificial Intelligence (AI) has redirect numerous industries, and its impact on cyber security is very great intense. This research paper explores the advancements in AI and its role in addressing challenges of cyber security. It examines the potential benefits of AI in threat detection, vulnerability assessment, incident response and predictive analytics. Additionally, the paper discusses the ethical implications and potential risks associated with AI in Cyber Security. Through an analysis of current research, case studies, and industry practices. This paper aims to provide the opportunities and challenges presented by the integration of AI in the field of cyber security.

Keywords: Cyber Security, Artificial Intelligence, Machine Learning, Deep Learning, Bio-Inspired Computing, Cognitive Science etc.

Introduction:

Cyber Security is subject to continuous and sophisticated attacks in today's fast changing digital environment, necessitating novel techniques to safeguard sensitive data and vital infrastructure.AI in Cyber Security holds the promise of enhanced threat detection, going beyond traditional signature-based methods. By leveraging machine learning algorithms and behavioural analysis, AI can uncover patterns and anomalies in vast datasets, enabling the identification of both known and previously unseen threats. This proactive approach allows organizations to respond swiftly and effectively, mitigating potential risks before they cause substantial harm.

In addition, the promise of AI also includes vulnerability analysis. AI-powered automated scanning and penetration testing can effectively find flaws in systems, networks, and applications. AI-driven techniques for prioritizing vulnerabilities and assessing risks enable business to make well-informed decisions, allocate resources effectively, and target serious vulnerabilities.AI integration may also help incident response, a critical component of cyber security. Organizations can quickly discover and respond to security breaches thanks to real-time event detection and AI's capacity to analyse massive amounts of data. One of AI's major capabilities, predictive analytics, may even predict prospective hazards, enabling proactive risk mitigation actions before they manifest. Although AI in Cyber Security has enormous promise, it is crucial to address ethical issues and possible hazards. Important issues that require attention include protecting privacy, making sure that data is protected, and getting rid of bias in AI systems. Another issue that calls for a strong counter measure is adversarial assaults, when AI itself may be tricked. In order to find patterns and signs of compromise, AI also helps with the analysis and correlation of enormous volumes of data from many sources, including log files, network traffic, and threat intelligence feeds. This information may be used to strengthen overall

cyber security resilience, establish more potent defensive measures, and fine-tune incident response procedures. Additionally, AI-powered systems may continually learn from and modify themselves in response to the changing threat environment and new attack methods, keeping up with the newest trends and assuring the efficacy of incident response.

AI-Based Threat Detection:

The advancement of AI-based threat detection in cyber security is incredible. Real-time security threat detection and response are made easier for enterprises. Threat detection used to be a laborious and manual procedure. However, thanks to artificial intelligence (AI), things are now simpler and quicker.

AI-powered threat detection systems keep an eye on user activity, system records, and network traffic using specialized algorithms and cutting-edge technologies. They can spot any unusual or suspect conduct that can point to a security problem by doing this. This is incredibly great since it enables businesses to quickly identify dangers as they emerge. The ability of AI-based threat detection to identify new and undiscovered dangers is one of its strongest features. Traditional threat detection techniques rely on pre-established rules and patterns, which means they may not catch newly emerging attack types. But AI is extremely intelligent and powerful because it can draw historical data and adjust to new dangers.

AI-based threat detections ability to lessen false alerts is yet another fantastic feature. Security programs may misidentify safe activities as threats, which can be extremely frustrating and wasteful. However, AI may learn from its errors and increase its accuracy, leading to fewer false alarms and improved resource management. Threat detection powered by AI also aids in responding to security problems. It may evaluate and rank warnings according to their seriousness and probable consequences. This enables security personnel to concentrate on the most significant dangers and respond quickly to stop any harm. Being one step ahead of hackers is like having a super-smart assistant.

However, deploying AI for threat detection is not without its difficulties. Making sure the AI algorithms are precise and dependable is a problem. We don't want the system to provide us with inaccurate information or fail to alert us to serious risks. The issues of privacy and ethics provide another difficulty. The data that AI systems utilize must be managed safely and ethically, therefore we must be cautious with it.

Top Cyber Threats in 2025:

Cyber threats in 2025 are evolving with greater precision and sophistication, using advanced technologies to exploit vulnerabilities. Here's a closer look at the top threats:

- AI-Powered Phishing Attacks: Instead of generic scam emails, hackers now use AI trained on public data to mimic trusted sources. These emails copy real writing styles, names, job titles, and past conversations to write messages. They

tailored these messages to you using real names, job roles, or even previous discussions. That's why it's getting harder to spot what's fake.

- Ransomware: Ransomware occurs when hackers lock your data and demand money to unlock it. AI helps attackers encrypt files faster and avoid detection. Some use tools like Evil Quest or Lock Bit that adapt in real time to bypass security. They also threaten to leak your private data if you don't pay up. So, it's about losing access and your information being exposed, too.
- Deep fake Scams: Attackers use AI to create fake videos and voice recordings from real samples that look and sound like someone you trust. It could be your manager asking for urgent help, but it's actually a video generated by AI that tricks you into taking action.
- Cloud vulnerabilities: Cloud vulnerabilities are opening new doors for cybercriminals. Hackers quickly target weak spots in these setups as more data shifts to services like Google Drive, Drop box, or AWS. AI tools like CloudSploit help them find and exploit security gaps. If a company doesn't set things up securely, attackers can break in, steal data, or lock out users.
- IoT Attacks: Hackers can easily hack devices like smart TVs, fridges, cameras, and even smart watches. These attacks are increasing because many of these devices have weak security. Hackers use AI to scan for open ports and take control of things like cameras or smart locks. They can use the device to break into other systems like the home Wi-Fi.

Following given comparison shows majors of AI-powered cyber-attacks and their counter measures to help you understand which security approaches work best against each threat.

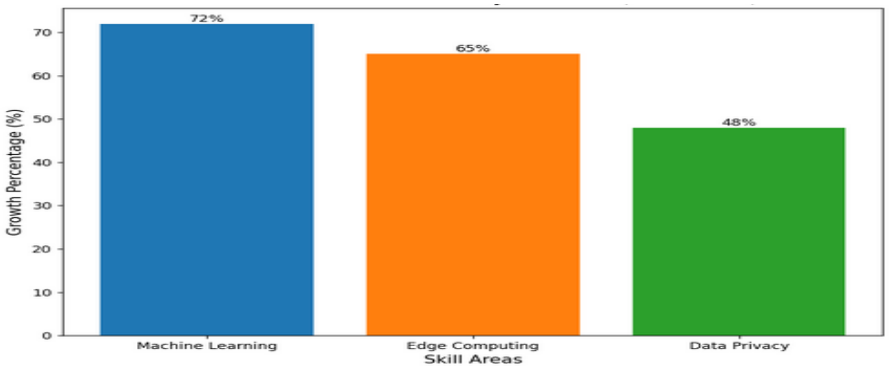
Threat	Target	What does it do?	Common Countermeasures
IoT Attacks	Smart devices (CCTV, wearables)	Takes control of unsecured devices, launches botnet attacks	Strong passwords, firmware updates, network segmentation
Cloud Vulnerabilities	Cloud storage and services	Exploits misconfigured cloud setups to access or leak data	Zero-trust access, proper configuration, encryption
Deepfake Scams	Humans (via media content)	Uses fake audio/video to impersonate trusted people	Deepfake detection tools, manual verification
Ransomware	Systems and files	Locks files and demands payment to restore access	Regular backups, endpoint protection, user training
AI-Powered Phishing	Individuals and employees	Sends realistic, personalised scam messages via email/text	Email filters, user awareness, multi-factor authenticati

Methodology:

Bibliometric Analysis:

Using Cite Space software, the analysis is based on a dataset consisting of 15,000 IoT job postings spanning the years 2020 to 2023. The analysis extracted keywords for skills and trends from the requirements for the skills. As per Statistics, Figure 1 can be seen that the demand for skills such as machine learning increased by 72%, edge computing increased by 65%, and data privacy increased by 48% between 2020 and 2023 [12]. Acknowledgments: Limitations: The study is based on analysing public postings and certain sectors or regions (e.g., non-English speaking localities) may unduly be under-represented. Moreover, trends across the entire IoT job market may be limited by data collection from a few platforms.

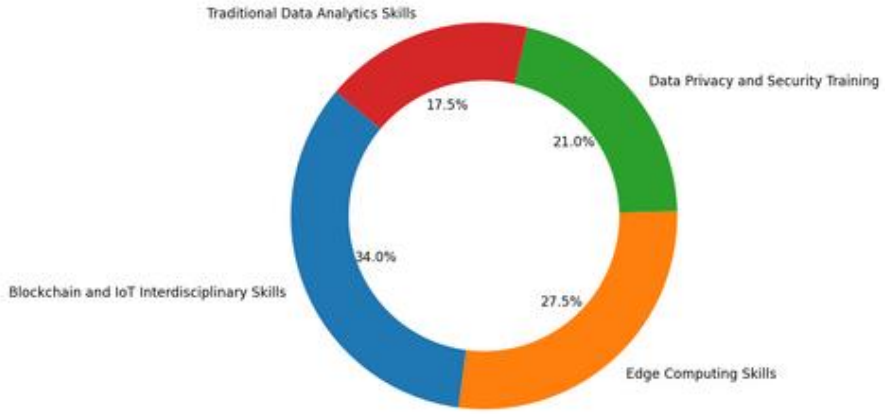
Figure 1: Skill Demand Growth in IoT Job Market (2020-2023)



Survey Research:

To gain insight into this dynamic landscape, researchers surveyed 1,200 Internet of Things (IoT) professionals from 12 countries to examine the shifting skill set and training requirements. The survey questionnaire covered aspects of skill utilizations, training needs and the impact of AI on IoT job markets. As indicated by the survey results, 73% of employers found it challenging to locate candidates having expertise in AI and IoT domain [13]. Likewise, researchers surveyed 1,500 IoT professionals across 15 countries to assess the influence of new technologies like blockchain and edge computing on the IoT jobs market. The survey shows that 68% of employers are struggling to hire candidates with multidisciplinary skills such as Blockchain and IoT. While 55% of companies expect edge computing skills to be a necessity within just a few years. Moreover, data privacy and security is top of the list in terms of urgent training needs according to 42% of employers, and one-third (35%) still see traditional data analytics skills as critical. Figure 2 shows the survey highlights the emerging trends in IoT employment market as well as the current skills demand and also reveals the impact of emerging technologies. [14] Limitations: While the survey sample is multinational, not all world's regions are equally represented (e.g. over-representation of developed economies). Self-selection bias might also play, too, since respondents might not proportionally represent people with strong opinions or specific organizational ties.

Figure 2: Key Trends in IoT Employment Market (2020-2024)



Curriculum Review:

Researchers assessed 50 university programs based on their relevance to the industry. The review looked at how many AI-related courses were in IoT programs and how well representative these programs were preparing students for the changing job market. Figure 3 can be seen 22% of the reviewed programs comprised AI modules relevant to IoT, and a whopping 85% of the programs did not comprise any course on ethical deployment of AI [13].

Limitations: The small sample size (n=50 programs) and geographic focus may limit conclusions. Furthermore, particularly with regards to skill development, the review did not incorporate the role of vocational training institutions, potentially missing alternative educational pathways.

Figure 3:

Category	Inclusion (%)	Exclusion (%)
AI Modules Tailored for IoT	22	78
AI Ethics Deployment Courses	15	85

Comparison of AI-Related Course Inclusion in IoT University Programs While the mixed-methods approach strengthens the study's validity, several limitations warrant acknowledgment:

Data was collected over the period 2020–2023, but rapid developments in technology (e.g., generative AI) may already change skill needs beyond this time frame. Because job postings and surveys focused at high-level skill categories, more nuanced sub-skills (e.g. programming languages, or frameworks) may have been under-represented. These data only establishes correlations between emerging technologies and current skill demands; establishing causation requires longitudinal studies of the impact of these technologies. These limitations indicate where future research can expand geographic coverage, employ real-time data streams, and integrate qualitative interviews for contextual depth.

AI in Security Concerns:

In order to evaluate enormous volumes of data, find patterns, and make choices in real-time, AI's work model for resolving security risks uses sophisticated algorithms and machine learning approaches. AI-powered systems are capable of continually monitoring a variety of data sources, including user activity, network traffic, and system logs. AI systems may learn from previous data and identify anomalies or patterns that differ from typical behavior by applying machine learning techniques.

AI-based systems may proactively identify possible security issues and threats in the context of cyber security. AI algorithms can identify suspicious actions or behaviors, such as anomalous data transfers, illegal access attempts, or odd user activity, by continually monitoring network traffic. AI may also examine user behavior and system data to find signs of compromise and potential security holes.

Artificial intelligence (AI) systems have the ability to detect possible security incidents and inform users while automatically reducing the risk. AI algorithms, for instance, can start a response sequence that isolates impacted computers, blocks suspect network traffic, or

alerts security staff if a malicious action is discovered.

Assessment of vulnerabilities is essential for guarantee and safety of digital systems. Artificial intelligence (AI) has recently shown itself to be a potent ally in the field of vulnerability assessment, allowing businesses to more quickly and accurately detect and prioritize risks. Artificial intelligence (AI is used to fuel automated scanning and penetration testing systems for vulnerability assessment. These instruments can do thorough analysis of software, networks, and systems, looking for any potential vulnerabilities and security problems. These evaluations may be carried out more quickly and at a bigger scale by using AI algorithms, allowing businesses to cover a wider attack surface and spot weaknesses that might otherwise go undetected.

Prioritizing vulnerabilities according to risk is one of the main advantages of AI in vulnerability assessment. AI-driven algorithms assess each vulnerability's severity and possible effects while taking into account its exploitability, prospective attack vectors, and the system's criticality. As a result, businesses are able to concentrate their resources more wisely, concentrating on the vulnerabilities that represent the most risk. Additionally, AI is capable of on-going learning and adaptation in response to the changing threat environment and new attack methods. AI-powered vulnerability assessment solutions can enhance their detection capacities over time by utilizing machine learning techniques, keeping up with the most recent attack trends and developing vulnerabilities.

Ultimately, by proactively detecting and fixing vulnerabilities, the inclusion of AI in vulnerability assessment helps businesses to improve their security posture. AI makes vulnerability assessments more thorough and efficient by utilizing automation, scalability, and sophisticated analytics. This helps enterprises remain one step ahead of possible attackers and fortify their entire protection against cyber threats. AI-powered vulnerability assessment tools will become more successful at protecting digital systems as a result of continued research and development in this area.

Automated scanning, risk prioritization, contextual analysis, adaptive scanning, integration with threat intelligence, remedial recommendations, continuous monitoring, cooperation, scalability, and efficiency are just a few benefits provided by AI-powered vulnerability assessment solutions. These solutions improve vulnerability assessments' efficiency, accuracy, and efficacy, allowing businesses to proactively find and fix vulnerabilities and fortify their cyber security defences.

AI-Powered Incident Response:

Effective incident response is essential for recognizing and managing security issues in the quickly developing field of cyber security. However, conventional approaches to incident response frequently rely on labour-intensive, error-prone manual analysis and human interaction. Fortunately, the development of artificial intelligence (AI) has completely changed the way that businesses can identify, assess, and react to security problems in real time.

Real-time issue detection includes many improvements such as AI makes incident response. AI systems can continually monitor network traffic, system records, and user activity to spot abnormalities and possible security problems by using machine learning algorithms and sophisticated analytics. This proactive strategy enables firms to see risks as they emerge, cutting down on the amount of time attackers spend inside systems and lowering the incident's potential effect.

Incident response enables due to AI which provides better the ability threat intelligence. A variety of data sources, including threat intelligence feeds and security incident reports, may be analysed and correlated by AI algorithms to find trends and similarities that may point to the involvement of certain threat actors or attack operations. As a result, companies are better able to understand the tactics, methods, and procedures (TTPs) used by attackers, which helps them to develop more effective to define plans and preventative measures for upcoming occurrences.

Another potent for AI skill crisis response is predictive analytics. AI systems can prospective security risks and weaknesses by examining past data and patterns. Organizations are able to prevent or reduce future occurrences by deploying patches, putting in place extra security measures, or changing system configurations thanks to this foresight. On the other hand, predictive analytics aids in spotting trends and patterns linked to certain attack vectors, assisting businesses in effectively allocating resources and enhancing their overall security posture.

By automating analysis and decision-making, it also dramatically improves incident response's speed and effectiveness. AI-powered systems quickly determine the breadth and severity of an issue by analysing and correlating massive amounts of data from numerous sources, including log files, network traffic, and threat intelligence feeds. The system may perform specified actions like isolating impacted systems, blocking suspicious traffic, or starting remediation operations without needing human participation by implementing automated incident response workflows. This automation quickens the reaction time to incidents, lowers the chance of human mistake, and provides uniform and standardized answers for all occurrences.

Large-scale security data sets may also be correlated and analysed with the help of AI. It gets harder for human analysts to comprehend and make sense of the massive volumes of data in today's digital environment as a result of the exponential rise of data. Big data is best handled by AI-powered platforms, which allow businesses to see abnormalities, linkages, and trends that human analysts would miss. The accuracy and efficiency of incident response initiatives are improved by this comprehensive examination of data from many sources. Incident response enabled by AI also makes post-incident analysis and learning easier. AI systems may find trends, signs of breach, and emerging attack methods by collecting and analysing data from security occurrences. This information may be utilized to strengthen overall cyber security resilience, establish more potent defensive measures, and fine-tune incident response procedures.

However, there are difficulties in putting AI-powered incident response into practice. It's essential to ensure the precision and dependability of AI algorithms to prevent false positives or false negatives, which can reduce the efficiency of incident response. To achieve precise detection and analysis, the training data used to create AI models must be extensive and representative of many incident kinds. Additionally, as incident response frequently entails managing sensitive information, firms must carefully consider data privacy and security when implementing AI technologies. AI-powered incident response requires careful consideration of data security and regulatory compliance.

The ethical aspect of AI-powered incident response is also crucial. To gain trust and guarantee ethical use of AI, transparency and accountability in AI algorithms and decision-making processes are crucial. Due to the possibility of AI algorithms may unintentionally reinforce pre-existing biases or discriminate

against particular people or groups, organizations must also address concerns of justice and bias. To address these ethical issues and guarantee the right and moral applications of AI in incident response, it is essential to put in place systems for human oversight and validation.

Application of AI in Social Media:

Social media platforms have developed into a breeding ground for a number of security issues, such as fraudulent accounts, cyber bullying, hate speech, and the dissemination of false information. By monitoring user behavior and content, spotting and throughout harmful activity, and ensuring user safety, artificial intelligence (AI) can play a significant part in resolving these problems.

AI-powered systems is used sentiment analysis and natural language processing to spot potentially dangerous information, such hate speech or abusive language. It also detect or eliminate harmful content by examining the context and sentiment of posts and comments, therefore shielding people from harashment or cyber bullying. Additionally, AI has the ability to spot trends in automated both activity and fraud account activity, which assist in stopping the spread of false information and guarantee the validity of user interactions.

Application Of AI in Mobile Applications:

With the processing of private and confidential financial information, mobile applications have become an indispensable part of our everyday life. They provide particular security difficulties, such as mobile malware, data leaks, and phishing attempts. By examining user behavior, spotting suspicious activity, and guarding against unwanted access, artificial intelligence (AI) which improve the security of mobile applications.

Mobile application user interactions, such as use trends, access requests, and login attempts, may be examined by AI-powered systems. AI may detect abnormalities in user behavior, such as strange activity patterns or unwanted access attempts, and can then inform users or enact extra security measures based on these findings. The AI system recognizes an abnormality, such as a user of an app suddenly starting to access sensitive data without a good purpose and either request extra authentication or even stop the suspicious behavior.

By analysing characteristics of known malicious activities, AI algorithms identify and block suspicious app installations or URLs that leads phishing websites. This proactive approach improves the security of mobile applications and shields users from potential threats.

Challenges And Opportunities:

Challenges:

Industry Challenges of Integrating Ai into IoT One of the most pressing issues faced, is a lack of professionals with interdisciplinary knowledge. In one case, smart city project deployment was delayed by 30% and the overspend was 25% due to lack of expertise in optimization of AI algorithms, IoT protocols (like MQTT, LoRa) and the design of edge computing [15]. Cyber security threats for AI-powered IoT systems in manufacturing. In a case study, one of the automotive plants discovered that thieves breached IoT sensors, listing real-time production data, to access the raw data applied for intellectual property. The company had to spend an extra 15% to enable end-to-end encryption as well as blockchain-based audit trails [16]. As AI rapidly involves, we will develop skill ourselves continuously. A textile manufacturer, for instance, faced difficulties in integrating AI-driven predictive maintenance with its legacy IoT devices, which led to a process of retraining staff

and upgrading systems that took around six months [17].

Opportunities:

AI capabilities-AI-IoT synergy can deliver transformative benefits across sectors: For example, in semiconductor factories, AI-IoT synergy is utilized to analyse equipment vibration data collected through edge sensors. With machine learning models, we were able to predict failures 48 hours in advance, resulting in a 40% reduction in downtime and a 12% improvement in yield rates [18]. In smart buildings, AI algorithms use IoT occupancy sensors to optimize HVAC systems. The International Energy Agency says 20% energy savings [19]. By utilizing usage patterns of NLP-based AI and IoT, a smart home device company was able to customize their voice assistant interactions, achieving a 35% increase in customer satisfaction [20]. An AI vision systems provider integrated its solution on IoT (Internet of Things) cameras for a food packaging firm to detect defects in real-time, reducing product recalls by 22 percent and saving $2.8 million in two years [21].

Future Directions and Recommendations:

The incorporation of Artificial Intelligence (AI) in cyber security has opened up exciting future possibilities. As technology advances, organizations and policymakers must explore and maximize the potential of AI while also addressing the challenges associated with its implementation.

Looking ahead, AI has the potential to revolutionize cyber security in a number of emerging areas. Internet of Things (IoT) security is one such area. As connected devices proliferate, securing the IoT ecosystem becomes increasingly important. By analysing large volumes of data from interconnected devices, detecting anomalies, and identifying potential threats, AI plays a critical role in this domain.

Secondly, it stands to gain significantly from AI developments is cloud security. Protecting sensitive data kept in cloud settings is crucial given the increasing dependence on cloud computing. By maximizing resource distribution, spotting and preventing unwanted access attempts, and detecting harmful activity, AI may improve cloud security. Organizations may improve their defensive mechanisms, guarantee data privacy, and boost overall cloud security by utilizing AI-powered products.

Furthermore, autonomous systems present particular cyber security difficulties that AI can successfully solve. Securing these systems from cyber-attacks becomes essential as autonomous technology such as drones, autonomous cars, and other devices proliferate. To defend autonomous systems from possible threats, AI can offer real-time threat detection, anomaly identification, and automated reaction capabilities. This can ensure the integrity and dependability of these systems and allow for the safe and secure functioning of autonomous technology.

AI-driven cyber security solutions must be developed through collaboration between government, business, and academic institutions. Organizations may hasten the development of AI technologies and their applications in cyber security by establishing collaborations and knowledge-sharing. In addition to fostering interoperability and efficiency across industries, this partnership may result in the formation of standardized procedures, standards, and assessment criteria for AI-based cyber security solutions.

Conclusion:

A new age of protection against changing cyber threats has begun with the incorporation of artificial intelligence (AI) in cyber security.

Organizations have the chance to improve their security posture and protect their digital assets by utilizing AI's skills in threat detection, vulnerability assessment, and incident response. Organizations can discover both known and unexpected threats in real-time thanks to AI-based threat detection, enabling proactive security actions. AI-driven vulnerability assessment improves the effectiveness of locating and ranking vulnerabilities. Rapid identification, reaction, and mitigation of security issues are made possible by AI-powered incident response, reducing the potential effect.

However, ethical issues, privacy worries, and possible threats related to AI algorithms must be addressed in order to apply AI in cyber security responsibly. Privacy protection, fairness, and prejudice reduction are to be addressed. Future applications of AI in cyber security have enormous promise. Cyber security defences may be strengthened by investigating developing fields like IoT security, cloud security, and autonomous systems. In order to create standards, laws, and support research to maximize the advantages of AI while minimizing threats, collaboration between politicians, industry professionals, and academics is essential. Organizations may create a more secure digital future by embracing AI's potential while solving its problems. The use of AI in cyber security marks a huge advancement in fending off online attacks and safeguarding vital data in our increasingly linked environment.

References:

1. John McCarthy, Artificial Intelligence logic and formalizing common sense, Stanford University, CA, USA 1990
2. **"Exploring Emerging Cybersecurity Risks from AI-Driven IoT Systems"** (Journal of Theoretical and Applied Information Technology (JATIT)): This paper examines how AI algorithms and IoT device security interact, highlighting new threats from their convergence, such as data breaches and AI model poisoning.
3. R.A.R. Ashfaq, X.Z. Wang, J.Z. Huang, H. Abbas, Y.L. He, Fuzziness based semi-supervised learning approach for intrusion detection system,. Information Science, 2017, 378, 484-497.
4. A.H. Hamamoto, L.F. Carvalho, L.D.H. Sampaio, T. Abrao, M.L. Proenca, Network anomaly detection system using genetic algorithm and fuzzy logic,. Expert System Application. 2018, 92, 390-402.
5. S. Smadi, N. Aslam, L. Zhang, Detection of online phishing email using dynamic evolving neural networks based on reinforcement learning,. Decision Support System, 2018, 107, 88-102.
6. **The Impact of Artificial Intelligence on IoT Application Technology Talent Demand** : **Author**: Zijie SuAuthors Info & ClaimsDEAI '25: Proceedings of the 2nd Guangdong-Hong Kong-Macao Greater Bay Area International Conference on Digital Economy and Artificial Intelligence July 2025
7. https://www.balbix.com/insights/artificial-intelligencein-cybersecurity/.