International Journal of Current Research and Applied Studies, (IJCRAS)

ISSN: 2583-6781

available at https://ijcras.com/

Volume 5 Issue 2 March-April 2026, Page 31-41

To cite this article: Yashasvi Sharma (2026). THE RISE OF AI-DRIVEN CYBER ATTACKS AND THE NEED FOR AI-POWERED DEFENSE, International Journal of Current Research and Applied Studies (IJCRAS) 5 (2): Article No. 142, Sub Id 251

THE RISE OF AI-DRIVEN CYBER ATTACKS AND THE NEED FOR AI-POWERED DEFENSE

Yashasvi Sharma

Independent Researcher
Orcid ID: https://orcid.org/0009-0002-2830-667X

DOI : https://doi.org/10.61646/IJCRAS.vol.5.issue2.142

ABSTRACT

The advancement of artificial intelligence (AI) enables cybercriminals to execute complex automated cyberattacks that evade detection. AI-powered threats easily bypass traditional security systems which rely on rule-based detection and signature-based defenses. The integration of machine learning (ML) technology with deep-fake technology along with automated hacking tools allows cybercriminals to create sophisticated phishing attacks and malware distribution tactics that evade both detection and prevention systems.

Phishing attacks using AI technology have become a dominant threat because attackers employ natural language processing (NLP) together with generative AI to produce highly individualized phishing emails that appear genuine. The success of AI-powered phishing attacks stems from their ability to mimic human communication methods which makes them more difficult to detect than basic phishing attempts. Through behavioral analysis of public data AI systems execute massive social engineering attacks that identify specific targets for their attacks. (Guembe et al., 2022). The development of malware using AI represents a significant threat to security systems. Real-time adaptive malware from AI evades both traditional signature-based and heuristic detection methods. Self-mutating malware operated by cybercriminals alters its code structure automatically to evade both antivirus software and endpoint security systems. AI-driven cyberattacks now improve brute-force attacks through their ability to predict password patterns which leads to security weaknesses in authentication systems.

The defense against evolving threats now utilizes artificial intelligence solutions developed by organizations. Through its ability to analyze big data sets AI detects unknown threats by finding patterns and delivering automated incident response and threat detection and anomaly detection capabilities. The analysis of attack patterns by machine learning algorithms allows the prediction of potential vulnerabilities which remain unexploitable. The real-time monitoring provided by AI-driven Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) solutions enables security incidents to be detected and mitigated in real-time.

Behavioral analytics and fraud prevention heavily depend on AI technology. Organizations monitor irregular activities by utilizing user and entity behavior analytics (UEBA) systems. AI systems use detected abnormal login attempts, privilege escalations, and access patterns to activate alerts and implement security measures such as MFA and access restrictions.

AI cybersecurity applications are demonstrated through various case studies. Financial institutions that implement AI-powered fraud detection systems have achieved over 80% reduction in unauthorized transactions. Through endpoint protection systems AI helps governments track cyber espionage threats and tech companies safeguard their cloud environments.

AI cybersecurity offers excellent protection yet it faces multiple barriers which include false positives along with adversarial AI attacks and ethical challenges. The fight against future cyber threats will increasingly depend on AI-powered cybersecurity solutions because of developing AI capabilities that will create resilient digital defense systems.

Keywords: AI-driven cyberattacks, AI-powered cybersecurity defense, machine learning in cybersecurity, AI phishing and malware detection, behavioral analytics in cyber defense

1. INTRODUCTION

Artificial intelligence (AI) has made rapid progress which transformed cybersecurity through new opportunities and security challenges. AI security solutions enhance threat detection capabilities and improve incident response and cyber resilience for organizations. Cybercriminals have started using AI to develop advanced automated attacks which evade traditional security measures. The cybersecurity industry maintains a continuous battle between AI-powered attacks and AI-based defensive systems. (Ghadge, 2024)

AI serves malicious purposes through its implementation in phishing campaigns with AI enhancement and intelligent malware and deepfake-based social engineering attacks. AI enables attackers to perform automated, large-scale cyberattacks and generate realistic impersonations while manipulating security algorithms. Security mechanisms based on traditional rules and human intervention fail to match the speed of these continuously evolving threats.

Organizations implement AI-driven cybersecurity solutions to detect and respond to cyber threats in real

time as they fight against emerging security challenges. Machine learning (ML) algorithms process large security data sets to detect unusual patterns, which enables automatic threat response and reduces the security team workload. AI security tools improve authentication processes, network monitoring capabilities, and fraud detection systems, that results in cybersecurity systems that adapt and become more proactive.

The research investigates how AI-powered cyberattacks are increasing in number and the attack methods used by cybercriminals, as well as the protective measures based on AI that defend against these threats. AI-driven cybersecurity strategies demonstrate their effectiveness through real-world examples, which show their ability to protect organizations from complex cyberattacks. Security strategies for the future need to understand how AI affects cybersecurity because both attackers and defenders use AI to achieve their goals.

2. THE EVOLUTION OF AI-DRIVEN CYBER ATTACKS:

2.1 AI-Powered Phishing and Social Engineering

The effectiveness of phishing and social engineering attacks has dramatically increased because of AI integration. The traditional phishing messages contained standard templates that made them detectable by security systems. AI-powered phishing uses machine learning (ML) algorithms to process large data sets, which enables attackers to create personalized attacks that match individual user behavior patterns, writing styles, and online activities. Through natural language processing (NLP) models, attackers create realistic emails and text messages and deepfake voice recordings that duplicate actual human voices. AI systems enable cybercriminals to perform massive targeted phishing attacks through automated processes, which shorten the time needed for these operations. The danger of spear-phishing attacks increases when AI creates messages that seem genuine because they target specific individuals or organizations. AI-enhanced phishing scams now threaten users with technical expertise because traditional email filters and awareness training no longer provide sufficient protection. Organizations need to implement AI-based threat detection systems which examine message metadata and sender reputation and content anomalies to prevent phishing attempts from reaching users. (Haber & Rolls, 2024)

2.2 Adversarial Machine Learning (AML) Attacks

The technique of Adversarial Machine Learning (AML) enables cybercriminals to deceive AI-powered security systems through manipulation of training data or input samples. AI-powered security solutions which include IDS, malware classifiers and facial recognition systems use ML models to detect threats. The attackers take advantage of model weaknesses through adversarial examples which are specially designed inputs that make AI systems produce incorrect classifications. An attacker could alter malware to make it resemble normal software thus avoiding detection systems. AI-based facial recognition systems become mislead by small pixel modifications in images. AML attacks pose a significant threat because they utilize AI intelligence to evade traditional cybersecurity defenses. (Kalin, 2022) Researchers fight AML threats by creating strong AI models which detect adversarial manipulation through adversarial training and anomaly detection and continuous model updates. (Kerwin, 2017)

2.3 Deepfake and Synthetic Identity Fraud

The AI-powered generative models behind deepfake technology allow cybercriminals to generate realistic fake videos and images and voice recordings. The deepfakes serve as tools for identity fraud and financial fraud and misinformation campaigns. The attackers use digital evidence manipulation to create fake CEO and government official impersonations while conducting voice phishing (vishing) scams through synthetic voice generation that replicates real voices. The combination of authentic and fabricated personal details which criminals call synthetic identities helps them evade identity checks to create fake bank accounts and obtain loans. The detection of deepfake-based fraud remains challenging because AI systems keep enhancing the authenticity of synthetic media. AI-based attacks now compromise traditional identity verification methods which include biometric authentication. Organizations need to implement deepfake detection technologies which include AI-based video forensics and blockchain-based identity verification and multi-factor authentication (MFA) to validate digital interactions. (Leander, 2024)

2.4 Automated Network Exploitation

AI bots operated by cybercriminals perform large-scale network vulnerability scanning and exploitation through unprecedented means. AI technology enables attackers to perform vulnerability identification automatically which speeds up their ability to scan thousands of systems at once. AI network exploitation tools analyze system configurations through machine learning to detect weak security controls before selecting high-value targets. The bots possess the ability to modify their attack methods through real-time feedback which enables them to choose the most successful techniques. The AI system can modify its attack plan automatically after encountering a blockage to attempt another approach. Cybercriminals have started using automated penetration testing tools which were created for ethical hacking purposes to perform brute-force attacks and credential stuffing and lateral movement within networks. Organizations need to establish continuous network monitoring and AI-based threat detection and zero-trust security models to verify access requests before granting permissions for protection against AI-driven exploitation.

3. AI-POWERED DEFENSE STRATEGIES

3.1 AI-Driven Threat Detection and Response

Modern cybersecurity depends heavily on machine learning (ML) algorithms which monitor extensive data sets to identify potential cyber threats through anomaly detection. ML-based systems differ from traditional security protocols because they learn from historical patterns and real-time activities to detect new threats. AI security tools can detect security breaches early through their capability to identify abnormal system behavior patterns.

ML models use pattern recognition to examine user conduct and network data and system logs in order to detect irregularities. An AI security system identifies suspicious login attempts when users attempt to access their accounts from unfamiliar locations or through unauthorized devices thus indicating account compromise. The system detects data exfiltration attempts through the identification of large sensitive information transfers to external servers which indicates a potential breach. (Waizel, 2024) AI systems identify malware through system interaction analysis which helps detect behaviors that match malicious

software patterns. (Ahmed, Islam, Shatabda, & Islam, 2022)

ML-driven cybersecurity provides real-time threat detection as its primary substantial benefit. AI enables organizations to automate threat detection and response which shortens the time needed to contain an attack because traditional security solutions struggle with quick responses to new evolving threats. The detection of anomalies through AI leads to immediate security protocol activation which includes access revocation and device isolation and security team alerts for prompt response.

AI enhances cybersecurity resilience through its ability to learn from new threats and modify its detection models which leads to improved protection over time. The proactive security approach reduces the probability of data breaches and insider threats and malware infections which keeps security teams ahead of developing cyberattacks. AI-driven anomaly detection functions as an essential defensive tool for organizations to protect against increasingly complex cyber threats.

3.2 Automated Incident Response

AI-powered Security Orchestration, Automation, and Response (SOAR) platforms transform cybersecurity operations through automated threat detection and containment and remediation processes. These systems use artificial intelligence and machine learning to analyze large security data sets in real time for threat identification and automatic response without human intervention. SOAR platforms integrate with multiple security tools to streamline incident response operations which shortens both response time and required effort for cyber threat management.

SOAR platforms deliver their greatest benefit through AI-driven playbooks which enable automated response capabilities. The detection of security threats by these playbooks leads to automatic action selection through predefined rules and current risk evaluation processes. The AI-powered SOAR system detects compromised devices and instantly cuts their network connection to stop malware spread and unauthorized access. The system will automatically cut off access and implement extra authentication protocols when it detects stolen or compromised credentials. The system executes these actions at a speed that minimizes attacker opportunities to exploit system vulnerabilities. (Giusti Gestri, 2019)

AI-driven SOAR platforms possess a vital capability to stop malicious activities while they happen in real time. The system blocks traffic from known malicious IP addresses and domains immediately when an attack starts from these sources thus preventing data exfiltration and additional infiltration attempts. The system's proactive approach reduces the likelihood of ransomware attacks and phishing campaigns and other cyber threats from becoming major incidents.

SOAR platforms enhance incident response speed and operational efficiency while improving overall cybersecurity resilience through their automated security processes. Organizations benefit from AI handling basic security incidents so their teams can concentrate on complex threats thus maintaining continuous protection against evolving cyber risks with minimal service interruptions.

3.3 Predictive Threat Intelligence

AI predictive analytics transforms cybersecurity operations by processing large datasets to detect security threats before they occur. AI learns from historical cyber incidents and hacker strategies and malware behaviors to enable organizations to take security actions before attacks happen. Security teams use predictive capabilities to detect minor indicators of compromise and early-stage attacks which enables them to take defensive measures before threats grow more dangerous.

AI systems that analyze worldwide threat intelligence enable organizations to detect industry-wide and geographic attack patterns, which guide them in developing suitable security measures. AI systems detect increasing ransomware threats against particular sectors, so cybersecurity teams receive warnings to strengthen their defenses and install security patches before attacks happen. AI systems detect modifications in hacker tactics including new phishing methods which lead to recommendations for security protocol adjustments. (Zhou, Guo, He, Zhao, & Bazzi, 2019)

The predictive approach both improves threat mitigation and optimizes resource allocation. Security teams should focus on fixing critical vulnerabilities because this approach decreases the probability of successful cyberattacks. AI-driven predictive analytics serves as a vital security tool to prevent cyberattacks because it helps organizations stay ahead of threats and prevent attacks before they happen thus strengthening their cybersecurity resilience.

3.4 Zero Trust AI Security Models

AI systems function as essential components for Zero Trust architecture development because they eliminate automatic trust for all entities regardless of their network position. The Zero Trust security model requires continuous verification of user identities and device integrity and network behaviors before granting access to sensitive resources whereas traditional security models depend on perimeter defenses. AI improves this model through real-time risk assessment which uses behavioral analytics and anomaly detection and contextual awareness to evaluate every access request.

Machine learning algorithms in AI systems detect abnormal user behavior patterns which include non-standard login locations, irregular access times and unauthorized device usage to trigger additional security protocols that include step-up authentication and access revocation. AI systems check device health status to verify security policy compliance before granting access. AI-driven Zero Trust security provides essential protection against insider threats, credential theft and lateral movement attacks because it performs real-time risk assessments. (Rane, Choudhary, & Rane, 2023)

3.5 AI-Driven Deception Technology

AI-powered deception security solutions employ advanced honeypots and decoy systems with fake credentials to mislead attackers away from critical assets. The deceptive environments created by AI systems mimic real systems to trick cybercriminals into interacting with false data which AI continuously

monitors their behavior. AI analyzes attack patterns to collect valuable intelligence about hacker tactics and procedures which organizations use to improve their security posture before attacks occur.

AI improves deception techniques through real-time threat assessments which trigger dynamic trap adaptations. Automated decoys create simulated versions of legitimate user behavior and application weaknesses and sensitive information to draw attackers into revealing their attack methods. AI-driven deception systems enhance attack attribution capabilities which allow organizations to identify cybercriminals and forecast upcoming threats. The approach both disrupts active attacks and enables organizations to take proactive measures against threats which decreases data breach risks. Organizations achieve a strategic cyber defense and intelligence gathering advantage through the integration of deception security with AI. (Tiham, Fahim, Julcarnine, & Usman, 2024)

4. CASE STUDIES AND INDUSTRY APPLICATIONS:

4.1 Case Study 1: AI-Powered Phishing Defense in Financial Institutions

A multinational bank used AI-driven phishing detection tools to fight against increasing email-based cyber threats. The system used machine learning algorithms and natural language processing (NLP) to analyze incoming emails in real time for detecting suspicious links and malicious attachments and fraudulent sender patterns. The AI solution continuously adapted to new phishing techniques, reducing false positives and enhancing accuracy. The bank achieved a 70% success rate in blocking phishing attempts which stopped credential theft and unauthorized access. The bank achieved enhanced cybersecurity posture through automated threat analysis and email filtering which protected customer data and created a safer digital banking environment.

4.2 Case Study 2: AI-Enhanced Ransomware Mitigation

A healthcare provider implemented AI-based endpoint protection as a defense mechanism against the increasing ransomware threats. The system employed machine learning algorithms to track device behavior while detecting anomalies and identifying malicious activities in real time. The AI solution detected ransomware attempts through its analysis of file access patterns and system modifications before encryption started. The system used automated response mechanisms to isolate infected endpoints and neutralize threats which stopped patient data breaches from occurring. (Chaithanya & Brahmananda, 2022) The proactive security measures cut down both system downtime and data loss which maintained operational continuity. The healthcare provider used AI-driven threat detection to enhance its cybersecurity framework and protect sensitive medical records from ransomware attacks.

5. CHALLENGES AND LIMITATIONS:

5.1 AI Arms Race

The ongoing advancement of artificial intelligence (AI) creates an ongoing battle between cybercriminals and security professionals in the AI arms race. Cybercriminals use AI-powered malware together with deepfake technology and automated phishing attacks to evade standard security protocols. Cybersecurity teams need to continuously innovate by developing advanced AI-powered defense systems which detect and eliminate new security threats. AI security solutions need to learn autonomously while adapting to

threats so they can fight autonomous cyber threats in real-time. The ongoing battle between attackers and defenders requires ongoing research together with AI cybersecurity investments and organization-wide collaboration for threat intelligence sharing to enhance defensive AI models. (Sharma, Yashasvi, 2025)

5.2 Data Privacy Concerns

AI security solutions need extensive datasets to train their models and detect threats properly. The heavy dependence on large datasets for AI systems creates ethical and compliance issues regarding user privacy and data protection standards including GDPR and CCPA. Organizations need to establish rigorous data governance policies which guarantee AI security models maintain privacy protection standards. The combination of differential privacy with anonymization and secure federated learning techniques enables organizations to reduce risks without compromising AI threat detection capabilities. Organizations worldwide will continue to face the essential challenge of protecting privacy while maintaining security as AI security systems advance. (Maher, Bhable, Lahase, & Nimbhore, 2022)

6. FUTURE PROSPECTS:

The future of AI-driven cybersecurity will emphasize autonomous intelligent and resilient defense mechanisms because cyber threats continue to advance in complexity. Organizations will transform their digital asset protection through three major developments: federated learning and AI-powered autonomous security agents and quantum-resistant AI encryption. The cybersecurity landscape must evolve through continuous innovation and adaptation and collaboration to maintain robust security defenses because cybercriminals use AI to develop advanced attack strategies.

6.1 Federated Learning in Cybersecurity

Traditional AI models depend on centralized datasets to train and improve threat detection algorithms. Multiple organizations can train AI models collaboratively through federated learning without sharing sensitive data. The decentralized system provides better privacy and security because it enables AI systems to learn from worldwide cyber threats without revealing protected or regulated data. The future of threat intelligence sharing depends on federated learning because it enables companies and governments and cybersecurity firms to unite their efforts for strengthening defenses against new attacks.

6.2 AI-Powered Autonomous Security Agents

AI-powered autonomous security agents self-learning AI systems will dominate future cybersecurity by detecting and responding to cyber threats autonomously in real time. These AI agents differ from conventional security software because they function autonomously without human involvement for updates and operate continuously to adapt to emerging attack patterns. These security agents use machine learning together with behavioral analysis and predictive analytics to prevent attacks before they occur thus minimizing the need for reactive cybersecurity measures.

6.3 Quantum-Resistant AI Encryption

With the emergence of quantum computing, conventional encryption algorithms are at risk of being

broken by quantum attacks. AI-driven cybersecurity must evolve to develop quantum-resistant encryption techniques that can withstand attacks from quantum computers. AI will play a significant role in designing and optimizing cryptographic algorithms that can protect sensitive data from future post-quantum threats. Organizations will need to adopt AI-driven cryptographic models that ensure long-term data security in an era where quantum decryption capabilities become a reality.

7. CONCLUSION:

The development of artificial intelligence (AI) enables cybercriminals to perform sophisticated and large-scale evasive attacks through AI-driven techniques. AI-powered cyber threats including automated phishing campaigns along with AI-enhanced malware and adversarial machine learning have made traditional security measures inadequate against these emerging risks. Organizations need to implement AI-powered defense systems which provide real-time threat detection and automated response and predictive intelligence capabilities to fight evolving threats. AI technology delivers its greatest cybersecurity impact through real-time data analysis which detects abnormalities to identify potential threats. AI-driven attacks evade traditional security systems that operate through static rules and signature-based detection methods because these systems cannot adapt to AI-driven threats. AI security tools employ machine learning algorithms together with behavioral analytics to monitor network activities for abnormal behavior and detect login patterns which might indicate potential intrudings before they grow worse. AI learns from previous cyber incidents to boost its effectiveness in protecting against future cyber threats. AI-based cybersecurity frameworks decrease the duration of both threat detection and response operations for cyberattacks. Security teams using traditional methods face challenges from the overwhelming number of security alerts which creates delays and exposes systems to higher risk. AI-powered Security Orchestration, Automation, and Response (SOAR) systems can detect threats autonomously while taking actions to neutralize them without human interference. Security logs undergo analysis by these systems while they correlate threat intelligence to trigger immediate security countermeasures which include device isolation, access privilege revocation and security patch deployment. The automated system reduces human mistakes while speeding up incident handling and maintaining constant defense against AI-based cyberattacks. (Ike et al., 2021) AI-driven cybersecurity uses predictive threat intelligence to anticipate attacks before they occur instead of depending on reactive security measures. AI algorithms analyze worldwide threat patterns to recognize new cyberattack trends while identifying previously undiscovered vulnerabilities and forecasting the upcoming attack vectors used by cybercriminals. Through this intelligence organizations can strengthen their security defenses ahead of time to decrease the chances of attack success. The adoption of AI in cybersecurity presents multiple obstacles for organizations to overcome. The main issue in the AI arms race arises from attackers who continuously develop advanced AI-based attacks which force security defenders to develop new strategies. Security systems powered by AI sometimes produce incorrect positive results which creates system interruptions and necessitates human inspection for better detection precision. The main challenge in implementing AI-driven security solutions involves both data privacy concerns and regulatory compliance because these systems need access to extensive datasets that may hold confidential information. Organizations need to verify their AI security systems adhere to privacy regulations including GDPR and CCPA while maintaining robust

cybersecurity standards. The threat landscape driven by AI requires organizations to establish powerful defensive measures based on artificial intelligence. Real-time threat detection through AI and automated incident response with predictive intelligence enable organizations to improve their cybersecurity defenses against complex cyberattacks. The implementation of AI in cybersecurity has become non-negotiable because organizations face ongoing issues with false positives and regulatory problems and the continuous battle between AI defenders and attackers. Organizations need to keep developing their AI security technologies through continuous innovation and investment to defend their digital assets in the AI-powered cyber world.

REFERENCES:

Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *IEEE Access, 10*, 113436-113481.

Sharma, Yashasvi (2025). The Role of AI & Machine Learning in Identity Governance. *SSRG-International Journal of Computer Trends & Technology (IJCTT)*, 2231-2803

Chaithanya, B., & Brahmananda, S. (2022). Ai-enhanced defense against ransomware within the organization's architecture. *Journal of Cyber Security and Mobility*, 621-654.

de Paula, L. C. (2021). *Academic Management Information Interoperability Platform for Higher Education Institutions.* Universidade do Porto (Portugal).

Ghadge, N. (2024). Enhancing threat detection in Identity and Access Management (IAM) systems. *International Journal of Science and Research Archive, 11*(2), 2050-2057.

Giusti Gestri, L. (2019). *Safety vests for jockeys: A case study of primary and dependent-secondary users affecting the evolution of vest design in the Australian horse-racing industry.* Swinburne.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence, 36*(1), 2037254.

Haber, M. J., & Rolls, D. (2024). Identity Threat Detection and Response (ITDR) *Identity Attack Vectors: Strategically Designing and Implementing Identity Security, Second Edition* (pp. 81-86): Springer.

Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews, 2*(1), 074-086.

Kalin, J. (2022). *Defense against the adversarial arts: applying green team evaluations to harden machine learning algorithms from adversarial attacks.* Auburn University.

Kerwin, K. (2017). *Risk Scoring Classification Performance Optimization.* Northwestern University.

Leander, A. D. (2024). *Identification and Implementation of Suitable Decentralized Identifier Methods for Self-Sovereign Identity Wallets in a Data Space.* University of Twente.

Maher, S. K., Bhable, S. G., Lahase, A. R., & Nimbhore, S. S. (2022). *AI and deep learning-driven chatbots: a comprehensive analysis and application trends.* Paper presented at the 2022 6th international conference on intelligent computing and control systems (ICICCS).

Nagarajan, S. M., Devarajan, G. G., Bashir, A. K., & AlZubi, A. A. (2024). Artificial intelligence based zero trust security approach for consumer industry. *IEEE Transactions on Consumer Electronics*.

Rane, N., Choudhary, S., & Rane, J. (2023). Leading-edge wearable technologies in enhancing personalized safety on construction sites: a review. *Available at SSRN 4641480*.

Tiham, F. M., Fahim, A. R., Julcarnine, G. M., & Usman, H. M. (2024). *Decentralized identity verification: a blockchain-based framework for self-sovereign identity (SSI) with issuer trust registry.* Brac University.

Waizel, G. (2024). *Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses.* Paper presented at the International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings.

Zhou, Z., Guo, Y., He, Y., Zhao, X., & Bazzi, W. M. (2019). Access control and resource allocation for M2M communications in industrial automation. *IEEE Transactions on Industrial Informatics, 15*(5), 3093-3103.