ACADEMIC JOURNAL OF GLOBAL WHO IS WHO IN ACADEMIA, VOL. 6 NO 1, APRIL 2025. ISSN: 2640 -7370. NEW YORK CITY.

THE POTENCY OF AI IN DETECTION AND CONTROL OF INSECURITY: THE PROSPECT AND STRATEGIES

By

Monday M. Saviour, Ph.D.
University of Illinois at Chicago
Northern Illinois,
United States

And

Bassey UDOM, Ph.D.
Sociology and Anthropology Social Sciences
University of Uyo,
Akwa Ibom State, Nigeria

ABSTRACT

This study examined the potency of artificial intelligence in detection and control of insecurity, assessing its prospect and strategies. In an age marked by rapid technological advancement, artificial intelligence (AI) has emerged as a powerful tool capable of transforming security systems and bolstering efforts to combat insecurity. In the context of carrying out this research, the following subheads were explored among many others: concept of artificial intelligence, concept of insecurity and types of insecurity. The study highlighted on the types of insecurity in our society to include: food insecurity, economic insecurity and physical or personal insecurity among others. Furthermore, the study mentioned the strategies of insecurity detection using artificial intelligence to include: anomaly detection, intrusion detection and prevention systems (IDS/IPS) to mention but a few. Based on this, the study concluded that the potency of artificial intelligence in the detection and control of insecurity lies in its ability to process vast amounts of data swiftly, predict threats with precision, and support real-time decision-making through intelligent surveillance, pattern recognition, and automated response systems. One of the recommendations made was that the governments and security agencies should adopt AI-powered surveillance systems such as facial recognition, behaviour analytics, and drone-based monitoring to preempt criminal activities, while ensuring strong ethical frameworks and human rights protections.

KEYWORDS: Artificial Intelligence, Detection, Control and Insecurity

INTRODUCTION

In an age marked by rapid technological advancement, artificial intelligence (AI) has emerged as a powerful tool capable of transforming security systems and bolstering efforts to combat insecurity. From sophisticated surveillance mechanisms to predictive policing and automated threat detection, AI continues to redefine the boundaries of national and global security frameworks. The growing threats posed by terrorism, cybercrime, organized violence, and internal insurgencies require responsive, intelligent systems that can process vast datasets in real-time—a function AI performs with remarkable precision and speed. As a result, AI is fast becoming indispensable in the toolkit of modern security agencies worldwide.

According to Horowitz (2018), AI technologies such as facial recognition, machine learning, natural language processing, and neural networks are being deployed to detect suspicious behaviour, track criminal activity, and forecast potential security breaches before they escalate. These technologies enable security personnel to move beyond reactive methods to proactive strategies, identifying threats through data analysis, pattern recognition, and anomaly detection. For example, AI-powered surveillance systems can scan thousands of video feeds simultaneously, flagging suspicious activities that would typically go unnoticed by human operators. Such applications are enhancing situational awareness and decision-making in high-risk areas.

The strategic application of AI in national and regional security planning also fosters cross-border collaboration and real-time intelligence sharing. AI systems can process multilingual content and detect misinformation campaigns or online radicalization patterns, thus helping governments stay ahead of emergent security threats. Moreover, the integration of AI with existing defense infrastructures, including drones, robotics, and cybersecurity frameworks, has increased the ability of states to protect critical assets and maintain public order without excessive human intervention. This multidimensional functionality positions AI as a key pillar in future security architectures (Kumar & Mallick, 2018).

Despite its numerous advantages, the use of AI in security comes with ethical, legal, and privacy concerns that must be strategically addressed. The potential for misuse, bias in algorithmic decision-making, and the risk of AI systems being manipulated by hostile actors underscores the need for strict regulatory frameworks and ethical guidelines. Furthermore, ensuring that AI solutions remain transparent, accountable, and aligned with human rights principles is essential to prevent alienation of the public and erosion of trust in security institutions. Strategic governance, training, and inclusivity are crucial to mitigating these challenges. Looking ahead, the prospects of AI in enhancing security are vast, yet contingent upon strategic investment, policy coherence, and international cooperation. With proper deployment and oversight, AI can revolutionize how threats are identified, assessed, and neutralized, ultimately contributing to a more secure and resilient society. As insecurity becomes more sophisticated and decentralized, so must the technologies and strategies employed to contain it. Harnessing the full potential of AI while maintaining ethical safeguards offers a balanced path toward sustained peace and stability.

CONCEPT OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is a technology that allows computers to perform tasks that typically require human intelligence. Udo-Okon and Akpan (2024) defined artificial intelligence as a branch of computer science called artificial intelligence studies how computers learn, comprehend data, recognize characters in images, analyses pictures, and simulate how the eyes work. In addition, artificial intelligence refers to the research and programming of computers to carry out intelligence tasks that require human intervention.

According to Huge and Godwin (2024) artificial intelligence (AI) is the idea and practice of creating computer systems that can do tasks like speech recognition, decision-making, and pattern recognition that traditionally needed human intelligence. Natural language processing, machine learning, deep learning, and other technologies are all included under the broad term artificial intelligence (AI) (NLP).

Moreover, Akpan and Clark (2024) cited in Nathan and Isuaiko (2025) mentioned that artificial intelligence (AI) is the study of how the human brain makes decisions, learns new things, and thinks through difficulties. The goal of artificial intelligence is to enhance computer abilities related to human understanding, including language intelligence, learning, reasoning, and problem-solving. The term artificial intelligence (AI) describes computer programmes that are able to carry out sophisticated operations that were previously limited to human performance, such as problem solving, thinking, and decision-making (Lion and Ekefre, 2024).

Furthermore, Hanson and Okorie (2024) explained that artificial intelligence (AI) is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. Bassey and Owushi (2023) mentioned that artificial intelligence is the collection of technologies that enable machinesto sense, comprehend, act, and perform several functions matching those of humans. Major components of the Artificial Intelligence bucket are machine learning, big data, natural language processing, decision logic, data visualization, and data analytics.

CONCEPT OF INSECURITY

According to Abdullahi (2022), insecurity is the state of fear or anxiety, stemming from a concrete or alleged lack of protection. It refers to lack or inadequate freedom from danger. This definition reflects physical insecurity which is the most visible form of insecurity, and it feeds into many other forms of insecurity such as economic and social security. Insecurity connotes absence of safety, danger, hazard, uncertainty and lack of protection.

Insecurity is a common feeling, often prompted by emotions like sadness, loneliness, jealousy, envy, or self-loathing. Whether you feel like your career is going nowhere, don't believe your partner loves you, struggle to act confidently, or have difficulty believing your worth, insecurity may influence you. If you're living with insecurity, looking at the definition, symptoms, and treatments for this challenge may be advantageous (BetterHelp Editorial Team, 2024).

As defined by Purity (2019), insecurity is the state of being open or subject to danger or threat of danger, where danger is the condition of being susceptible to harm or injury. Secondly, insecurity is the state of being exposed to risk or anxiety, where anxiety is a vague unpleasant emotion that is experienced in anticipation of some misfortune.

TYPES OF INSECURITY IN OUR SOCIETY

- **Food Insecurity**

Food insecurity refers to the lack of consistent access to enough nutritious food for an active and healthy life. It is one of the most pervasive forms of insecurity, especially in low- and middle-income countries. Food insecurity affects physical health, educational attainment, and productivity. During the COVID-19 pandemic, global food systems were disrupted, increasing the prevalence of food insecurity. According to Niles. (2021), food insecurity intensified across several regions due to job losses, inflation, and supply chain breakdowns.

- **Economic Insecurity**

Economic insecurity is the risk of losing one's economic position due to job loss, poverty, inflation, or financial instability. It often manifests in unemployment, underemployment, low wages, and limited access to financial services. Economic insecurity increases vulnerability to other forms of insecurity like homelessness and hunger. Research by Western et al. (2020) shows that economic insecurity negatively affects mental health, leads to societal discontent, and undermines social cohesion.

- **Physical or Personal Insecurity (Violence & Crime)**

This refers to the risk or actual experience of harm through violence, theft, terrorism, kidnapping, or conflict. In societies plagued by armed robbery, gender-based violence, insurgency, or terrorism, individuals often live in fear for their safety. Okoli and Ugwu (2021) argue that in Nigeria, for instance, the rise in kidnapping and terrorism has significantly contributed to societal instability and the displacement of communities.

- **Health Insecurity**

Health insecurity is the lack of access to adequate health services, sanitation, and clean water, exposing people to diseases and early death. It was especially highlighted during the COVID-19 pandemic. Health insecurity leads to poor health outcomes, especially among vulnerable populations. According to Liem. (2021), health insecurity is closely tied to economic status, as those in poverty often suffer the most due to inadequate access to health infrastructure.

- **Political Insecurity**

Political insecurity involves the risk of instability in governance, including coups, corruption, authoritarianism, and civil unrest. When citizens lose trust in leadership or experience frequent changes in governance, there is a high risk of instability, protests, and violence. According to Oshewolo and Durojaye (2020), political insecurity undermines development and causes social fragmentation.

- **Environmental Insecurity**

Environmental insecurity arises when people are at risk due to environmental degradation, climate change, pollution, or natural disasters. It leads to loss of livelihoods, migration, and conflict over resources like water and arable land. Researchers like Mach et al. (2020) have identified climate-related security risks in regions with fragile political systems, where environmental issues can fuel conflict.

- **Educational Insecurity**

This refers to a lack of access to quality education, infrastructure, teachers, or learning materials. Educational insecurity can create generational poverty, widen inequality, and increase social unrest. During the COVID-19 pandemic, school closures exposed millions of students globally to long-term educational disruptions. A study by Brossard et al. (2021) highlights that many children in low-income countries were unable to access online learning, deepening educational gaps.

THE STRATEGIES OF INSECURITY DETECTION USING ARTIFICIAL INTELLIGENCE

- **Anomaly Detection:**

Endpoint security refers to the process of protecting individual devices often called "endpoints" such as desktops, laptops, smartphones, tablets and servers that connect to a network. The goal of endpoint security is to ensure that these devices do not become entry points for cyber threats, such as malware, ransomware, phishing attacks or unauthorized access.

- **Intrusion Detection and Prevention Systems (IDS/IPS):**

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are network security tools that monitor system or network activity for malicious behavior. As NIST notes, intrusion detection is "the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. (Scarfone & Mell, P, 2010).

- **Automated Threat Hunting:**

Automated Threat Hunting is the use of advanced technologies such as artificial intelligence (AI), machine learning (ML) and behavioral analytics to proactively search for signs of cyber threats within an organization's network without requiring constant human input. Unlike traditional threat detection, which waits for alerts from known signatures or rules, threat hunting actively investigates patterns or anomalies that may indicate hidden threats such as advanced persistent threats (APTs) or zero-day exploits. (CrowdStrike. 2025)

- **AI-Powered Incident Response:**

AI-powered incident response refers to the use of artificial intelligence (AI) and machine learning (ML) technologies to enhance and automate the process of detecting, analyzing and responding to cyber security incidents. Traditional incident response can be manual, time-consuming and reactive. AI transforms this process by enabling faster threat detection, real-time analysis and intelligent decision-making.

- **Endpoint Security**

Endpoint security is a cyber-security methodology aimed at protecting the endpoints (such as computers, mobile devices, and servers) that connect to an enterprise network. It involves securing these devices through local protections (e.g., antivirus, firewalls) and centralized monitoring systems. As threats evolve, endpoint security has transitioned from traditional antivirus solutions to more advanced models incorporating machine learning, behavioral analysis, and endpoint detection and response (EDR). (Zhang, Y., & Liu, L, 2021)

The Strategies of Insecurity Control using Artificial Intelligence

Artificial Intelligence (AI) is revolutionizing security management by providing advanced tools for preventing and mitigating insecurity through surveillance, predictive analysis, and decision support systems. One of the most common AI strategies is facial recognition, which aids law enforcement in identifying suspects and tracking criminal activity in real time. Okwor (2022) emphasizes that biometric technologies, particularly AI-powered face detection, are now widely used in urban crime prevention due to their speed, accuracy, and integration with national security

databases. These systems allow for the rapid scanning of individuals in public spaces, enhancing the ability of security agencies to identify threats proactively rather than reactively.

AI also plays a significant role in the deployment of Unmanned Aerial Vehicles (UAVs) for border surveillance and reconnaissance operations. Matthew et al. (2021) present a model where AI-equipped drones can patrol insecure regions, offering live data feeds and detecting anomalies that may signal security threats such as armed conflict or illegal smuggling. These systems have proven essential in hard-to-reach areas where human patrolling is dangerous or inefficient. The drones use AI algorithms to distinguish between human activity and environmental changes, ensuring focused alerts and faster incident response.

Another important strategy is predictive policing, where AI analyzes historical crime data to forecast potential hotspots and criminal behavior. Apene. (2024) advocate the use of machine learning models to predict where crimes are likely to occur based on variables such as time, location, and crime type. This approach not only allows for efficient allocation of policing resources but also minimizes the chance of reactive policing failure. Predictive analytics are especially effective in high-crime urban environments, where large datasets are available for algorithm training.

In smart cities, AI is used to automate crime detection and response through integrated technologies such as smart lighting, IoT sensors, and traffic cameras. According to Laufs (2022), smart city initiatives incorporate AI to analyze sensor inputs in real time, triggering automated alarms and enabling rapid response to emergencies. Similarly, Vogiatzaki. (2020) demonstrate how AI-enhanced lighting systems can detect unusual activity in public areas and adapt their brightness or color to deter potential offenders, contributing to a safer urban ecosystem. These strategies exemplify how cities can become proactive actors in crime prevention.

However, while AI technologies offer significant benefits for insecurity control, they also present ethical and privacy challenges. Zeng (2022) warns that the use of AI in authoritarian regimes may lead to mass surveillance and suppression of civil liberties. The integration of AI in national security strategies must therefore be governed by clear ethical frameworks to prevent abuse. Moreover, King. (2020) highlight the importance of interdisciplinary approaches in designing AI tools that are both effective and socially responsible. As such, while AI provides powerful solutions to modern insecurity, its deployment must be carefully balanced with human rights considerations and transparent governance.

AI-based strategies for insecurity detection encompass a range of techniques, including anomaly detection, intrusion detection and prevention systems and automated threat hunting. These methods leverage machine learning to identify unusual patterns and activities that could indicate potential security breaches, automating threat detection and response.

CONCLUSION

The potency of Artificial Intelligence in the detection and control of insecurity lies in its ability to process vast amounts of data swiftly, predict threats with precision, and support real-time decision-making through intelligent surveillance, pattern recognition, and automated response systems. As AI continues to evolve, its strategic integration into security frameworks holds immense prospects for proactive threat management, crime prevention, and national defense enhancement.

However, harnessing its full potential requires robust policy frameworks, ethical guidelines, interdisciplinary collaboration, and continuous technological innovation to ensure both effectiveness and accountability in safeguarding lives and property.

RECOMMENDATIONS

- Governments and security agencies should adopt AI-powered surveillance systems such as facial recognition, behaviour analytics, and drone-based monitoring to preempt criminal activities, while ensuring strong ethical frameworks and human rights protections.
- Nations should develop and implement dedicated AI policies focused on national security applications, supported by investment in research, infrastructure, and local talent development.
- Security agencies should integrate AI-based predictive analytics tools to assess crime trends, detect cyber threats, and identify potential hotspots for violence or unrest.
- There should be implementation of mandatory training programs for military, police, and intelligence personnel to use AI tools effectively in the detection and control of insecurity

REFERENCES

Abdullahi, H. I. (2022). Insecurity as an Impediment to Development in Nigeria. Available at: https://www.researchgate.net/publication/357836225_Insecurity_as_an_Impediment_to_Development_in_Nigeria.

Apene, O. Z., Blamah, N. V., & Aimufua, G. I. O. (2024). Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions. *European Journal of Applied Sciences and Engineering.*

Bassey, M. M. and Owushi, E. (2023). Adoption of Artificial Intelligence in Library and Information Science in the 21st Century: Assessing the Perceived Impacts and Challenges by Librarians in AkwaIbom and Rivers States. *International Journal of Current Innovations in Education*, 6 (1), 75-85.

BetterHelp Editorial Team, (2024). What Is Insecurity? Exploring the Definition, Symptoms, and Treatments. Available at: https://www.betterhelp.com/advice/self-esteem/insecure-define-and-manage-it/.

Brossard, M., Cardoso, M., & Kamei, A. (2021). Learning losses due to COVID-19 school closures: A review of the evidence. UNESCO Research Briefs. https://unesdoc.unesco.org/ark:/48223/pf0000379107

Cisco (2025). "What Is Endpoint Security?" https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-security.html

CrowdStrike. (2025) "Automated Threat Hunting: How It Works and why it's Essential." CrowdStrike Cybersecurity 101.

Hanson, E. D. and Okorie, U. U. (2024). The Roles of Artificial Intelligence in Library Automation: The Prospects and Challenges. *Erudite Compendiums in Education*, 13-23.

Horowitz, M. C. (2018). *The promise and peril of military applications of artificial intelligence*. Bulletin of the Atomic Scientists, 74(6), 316–321. https://doi.org/10.1080/00963402.2018.1539173

Huge, K. C. and Godwin, O. E. (2024). Adoption of Artificial Intelligence in Curbing Fraud in Public Organization: Assessing Fraud Detection and Control. *GASPRO International Journal of Eminent Scholars,* 11(1), 44-54.

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics*, 26(1), 89–120. Springer.

Kumar, S., & Mallick, P. K. (2018). The role of Big Data and Artificial Intelligence in cyber security. *Computer Science Review*, 30, 70–83. https://doi.org/10.1016/j.cosrev.2018.10.002

Laufs, J. (2022). Crime Prevention and Detection Technologies in Smart Cities. UCL.

Liem, A., Wang, C., Wariyanti, Y., Latkin, C. A., & Hall, B. J. (2021). The neglected health of international migrant workers in the COVID-19 epidemic. *The Lancet Psychiatry*, 8(4), e20. https://doi.org/10.1016/S2215-0366(20)30076-6

Lion, C. J. and Ekefre, A. E. (2024). Risk Control and Management in Banking Sector: Investigating the Work of Artificial Intelligence in Mitigating Risks. *International Journal of Advancement in Education, Management, Science and Technology*, 7(1), 82-92

Mach, K. J., Kraan, C. M., Adger, W. N., Buhaug, H., (2020). Climate as a risk factor for armed conflict. *Nature*, 571, 193–197. https://doi.org/10.1038/s41586-019-1300-6

Matthew, U.O., Kazaure, J.S., Onyebuchi, A. (2021). Artificial Intelligence Autonomous UAV System for Remote Security Surveillance. IEEE.

Niles, M. T., Bertmann, F., Belarmino, E. H., Wentworth, T., Biehl, E., & Neff, R. (2021). The Early Food Insecurity Impacts of COVID-19. *Nutrients*, 13(2), 496. https://doi.org/10.3390/nu13020496

Okoli, A. C., & Ugwu, A. C. (2021). Kidnapping for ransom in Nigeria: Issues and implications. *African Security Review*, 30(1), 72–88. https://doi.org/10.1080/10246029.2020.186763

Okwor, U. D. (2022). Artificial Intelligence as a Tool for Combating Insecurity in Nigeria. ResearchGate

Oshewolo, S., & Durojaye, E. (2020). Governance and insecurity in Nigeria: A critical appraisal. *African Journal of Democracy and Governance*, 7(3), 121–139. https://doi.org/10.4314/ajdg.v7i3.6

Purity, N. O. (2019). Insecurity in Nigeria: the Implications for Industrialization and Sustainable Development. https://www.ijrbsm.org/papers/v6-i5/2.pdf.

Scarfone, K., & Mell, P. (2010). Intrusion Detection and Prevention Systems. In P. Stavroulakis & M. Stamp (Eds.), Handbook of Information and Communication Security (pp. 177–192). Springer. DOI: 10.1007/978-3-642-04117-4_9.

Sundar, P. (2024). AI-enhanced cyber security incident response: Streamlining threat mitigation through automation. *International Machine Learning Journal and Computer Engineering*, 7(7).

Udo-Okon, T. N. and Akpan, E. E. (2024).The Challenges of Artificial Intelligence in Library Management System. *Intercontinental Academic Journal of Library and Information Science*,

Vogiatzaki, M., Zerefos, S., & Hoque Tania, M. (2020). Enhancing City Sustainability through Smart Technologies. Sustainability, 12(15), 6142.

Western, B., Bloome, D., Sosnaud, B., & Tach, L. (2020). Economic Insecurity and Social Stratification. *Annual Review of Sociology*, 46, 213–232. https://doi.org/10.1146/annurev-soc-121919-054728

Zeng, J. (2022). Artificial Intelligence with Chinese Characteristics: National Strategy, Security and Authoritarian Governance. Springer.

Zhang, Y., & Liu, L. (2021). Endpoint security: A critical component of cyber security in the age of remote work. *Journal of Information Security and Applications*, 59, 102828.