THE ROLES OF AI IN HOME SECURITY: STUDYING THE INTEGRATION OF AI-DRIVEN SECURITY DEVICES FOR OPTIMUM SECURITY OF HUMAN LIVES & PROPERTY

By

Arc Peter Sunday USANGA
Department of Architecture
University of Uyo

ABSTRACT

The study examined the roles of Artificial Intelligence (AI) in home security, with particular emphasis on the integration of AI-driven security devices for achieving optimum security of human lives and property. The increasing rate of burglary, unauthorized access, vandalism, cybercrime, and other security threats has created the need for more intelligent, proactive, and efficient security systems capable of preventing and responding to threats in real time. The study explored the concepts of artificial intelligence, home security, AI-driven security devices, and optimum security, highlighting how AI technologies such as machine learning, deep learning, computer vision, facial recognition, biometric authentication, predictive analytics, cloud computing, and the Internet of Things (IoT) are transforming conventional home security into intelligent and automated security ecosystems. The study further examined the capacity of AI-powered security devices to provide continuous surveillance, detect suspicious activities, recognize intruders, predict potential security threats, automate emergency alerts, strengthen access control, reduce false alarms, and improve decision-making for enhanced protection of lives and valuable property. It also discussed the significance of AI-driven security systems in promoting crime prevention, improving emergency response, enhancing cybersecurity, increasing operational efficiency, and ensuring effective monitoring of residential environments with minimal human intervention. The study concluded that Artificial Intelligence (AI) has emerged as a transformative technology that is redefining home security through the integration of intelligent security devices capable of monitoring, detecting, analyzing, and responding to security threats in real time. One of the recommendations made was that Governments should establish comprehensive policies and regulatory frameworks to ensure the ethical, secure, and responsible deployment of AI-based home security technologies while safeguarding users' privacy.

KEYWORDS: AI, Home Security, Devices, Human Lives

INTRODUCTION

Artificial Intelligence (AI) has become one of the most transformative technological innovations of the twenty-first century, revolutionizing the way individuals, organizations, and governments address security challenges. AI refers to the capability of computer systems to perform tasks that typically require human intelligence, including learning, reasoning, pattern recognition, decision-making, and problem-solving. Recent advancements in machine learning, deep learning, computer vision, and the Internet of Things (IoT) have enabled AI systems to analyze vast amounts of data in real time, identify suspicious activities, and respond to potential threats with minimal human intervention. As security threats continue to evolve in complexity, conventional security systems are increasingly being replaced by intelligent security solutions capable of predictive analysis, automated surveillance, and rapid emergency response. According

to Swetha et al. (2025), AI-powered security technologies significantly improve threat detection accuracy, reduce false alarms, and enhance real-time monitoring, making them indispensable in modern security management. Similarly, Luke and Akpan (2025) observed that AI has transformed decision-making processes across various sectors by improving efficiency, accuracy, and automation.

The growing concerns over burglary, vandalism, cybercrime, unauthorized access, and other security threats have increased the demand for intelligent home security systems that provide comprehensive protection for human lives and property. Unlike traditional security devices that merely record incidents or trigger alarms after an intrusion has occurred, AI-driven security devices utilize facial recognition, biometric authentication, behavioral analytics, predictive intelligence, and smart surveillance to identify potential threats before they escalate. These technologies continuously learn from environmental data and user behavior, enabling them to distinguish between normal and suspicious activities while minimizing false alerts. Recent studies have demonstrated that integrating AI with smart cameras, sensors, cloud computing, and IoT technologies enhances situational awareness, accelerates emergency response, and strengthens residential security (Hu et al., 2022; Reynaud & Roxin, 2025). Furthermore, Uddin et al. (2025) argued that AI-based predictive analytics enables proactive crime prevention by identifying crime patterns and forecasting potential security risks before incidents occur.

Despite the numerous advantages associated with AI-driven home security systems, their effective deployment requires careful consideration of issues such as data privacy, cybersecurity, algorithmic bias, ethical governance, and system reliability. Nevertheless, continuous improvements in AI algorithms, encryption technologies, and explainable AI have enhanced the reliability, transparency, and resilience of intelligent security systems. The integration of AI-driven security devices into residential environments therefore represents a significant advancement toward achieving optimum security through continuous monitoring, intelligent threat detection, automated response mechanisms, and proactive risk management. Consequently, studying the roles of AI in home security is essential for understanding how intelligent technologies contribute to safeguarding human lives and protecting valuable property against emerging physical and digital security threats in contemporary society (Guembe et al., 2022; Swetha et al., 2025).

Concept of AI

Artificial Intelligence (AI) is the development of computer systems capable of performing tasks that typically require human cognition, such as learning, reasoning, and problem-solving. Instead of following strict, hard-coded rules, modern AI finds patterns in vast amounts of data to make predictions, generate content, or take autonomous actions.

Governments and organizations are creating policies to guarantee that AI is developed and utilized responsibly as AI systems increasingly impact important choices that affect people and society. As noted by Floridi & Chiriatti (2020), establishing ethical principles, transparency, fairness, and human oversight is essential for building trustworthy AI systems that maximize societal benefits while minimizing potential risks.

While deep learning employs artificial neural networks to address challenging issues like image recognition and language translation, machine learning allows computers to learn from data without explicit programming. Applications like chatbots and virtual assistants are made feasible by natural language processing, which enables robots to comprehend and produce human language. Russell & Norvig (2021) describe AI as the science and engineering of creating intelligent agents that perceive their environment and take actions to maximize the likelihood of achieving specific goals. AI possesses unique and powerful characteristics that distinguish it from traditional Information Technology (IT) (Amuzat, 2025).

AI helps with disease diagnosis and medication discovery in the healthcare industry, precision farming and crop monitoring in agriculture, tailored learning in education, and intelligent automation in business to improve customer experience. Despite these advantages, data privacy, algorithmic bias, transparency, cybersecurity, and ethical governance are some of the issues that AI raises. Cao (2021) emphasized that responsible AI development requires fairness, accountability, transparency, and robust regulatory frameworks to ensure that AI technologies benefit society while minimizing potential risks. Artificial Intelligence (AI) has emerged as one of the most transformative technologies in the modern business landscape, reshaping traditional approaches to strategy formulation and decision making (Luke & Akpan, 2025).

Concept of Home Security

Home security is the practice of protecting a house and its people from threats like break-ins, fires, and damage using physical hardware, smart technology, and daily safety habits. Key elements include door locks, security cameras, and alarm systems.

The term "home security" describes the strategies, tools, and procedures used to defend residential buildings, their people, and their priceless possessions against dangers like fire, burglary, vandalism, and illegal entry. As stated by Aldowah, Ghazal, Umar, & Muniandy (2022), smart home security technologies have significantly improved residential safety by enabling continuous monitoring, rapid threat detection, and automated emergency responses. Furthermore, Usanga & Isaac (2024) emphasized that physical architectural interventions—such as strategic boundary elements and half-fences—play a vital role in regulating spatial access and environmental protection alongside active security hardware.

The idea of home security goes beyond deterring theft to guarantee the general security and welfare of family members. Electronic surveillance cameras, biometric access control, intrusion detection systems, smoke detectors, and emergency alerting systems must all be integrated for effective home security. Alqahtani, Alshahrani, Alghamdi, & Alzahrani (2023) emphasized that intelligent home security systems utilizing artificial intelligence and the Internet of Things (IoT) provide enhanced situational awareness, improved response times, and greater convenience for homeowners.

Recent developments in artificial intelligence (AI), cloud computing, and the Internet of Things (IoT) have revolutionized residential security by enabling predictive monitoring and automated decision-making. To reduce false alerts, AI-powered home security systems can

identify faces, spot odd behavior, discern between people and animals, and instantly analyze video material. These features make security systems more dependable and efficient while lowering the requirement for ongoing human oversight. As observed by Albahri, Duhaim, Fadhel, Alnoor, Baqer & Alzubaidi (2021), AI-based surveillance and smart sensing technologies have become essential components of modern home security because they improve threat detection accuracy and support proactive crime prevention.

Concept of AI-Driven Security Devices

Home security is the practice of protecting a house and its people from threats like break-ins, fires, and damage using physical hardware, smart technology, and daily safety habits. Key elements include door locks, security cameras, and alarm systems.

In order to spot unusual activity like unauthorized entrance, strange movement, abandoned objects, or attempted cyber breaches, these devices continuously examine camera feeds, sensor data, and user behavior. By limiting false alarms and adjusting to shifting environmental variables, deep learning algorithms help AI systems become more accurate over time. Naik, Mehta, Yagnik, & Shah (2022) explained that integrating AI techniques into security systems significantly enhances cybersecurity and physical security by providing automated detection, rapid incident response, and continuous monitoring against evolving threats.

AI-powered security cameras are able to identify people by facial recognition, detect weapons, keep an eye on crowd behavior, identify license plates, and instantly alert security staff to any suspicious activity. These capabilities lessen reliance on manual surveillance while enhancing public safety, emergency response, and criminal prevention. Hu, Kuang, Qin, Li, Zhang, Gao, Li, & Li (2022) emphasized that AI-based security technologies have become indispensable in modern intelligent environments because of their ability to provide adaptive protection against increasingly sophisticated physical and cyber threats.

Additionally, AI models may be susceptible to manipulation or hostile attacks, which could lower their dependability in crucial circumstances. In order to guarantee the appropriate application of intelligent security technologies, researchers support secure system architectures, data encryption, explainable AI, and ethical governance. Guembe, Azeta, Misra, Osamor, Fernandez-Sanz, & Pospelova (2022) observed that strengthening AI security through robust defensive mechanisms and continuous system updates is essential for maintaining trustworthy and resilient AI-enabled security systems.

Concept of Optimum Security

Optimum security is the ideal balance where the cost of protection equals the cost of potential losses, maximizing safety without wasting resources. It achieves peak efficiency by weighing risk against expense.

Continuous risk assessment and the implementation of suitable security controls according to the type of threats found are the cornerstones of optimal security. Optimal security necessitates that organizations evaluate risks, spend resources efficiently, and create layered security methods that strike a balance between protection and organizational goals rather than applying the same security measures to every setting. Diéguez, Bustos, & Cares (2020) explained that achieving

optimum security requires systematic selection and implementation of security controls using quantitative decision-making models that optimize security performance under available resource constraints.

Continuous monitoring, frequent security audits, staff awareness, policy revisions, and adherence to international security standards are all necessary for optimal security. In this context, Proske & Schmid (2022) noted that buildings are fundamentally independently usable, covered structures intended to provide physical safety and long-term protection, reinforcing the need to maintain their integrity. This aligns with the findings of Usanga & Usanga (2024), who stressed that neglecting physical building assessment leads to structural decay, posing severe risks to occupants' safety, well-being, and operational performance. Thus, routine inspection and proactive maintenance schedules form an essential component of optimal facility security.

Integrating technology, organizational regulations, and human behavior into a single security management system is a key feature of optimal security. Furthermore, biophilic and environmental architectural principles suggest that integrating nature and well-structured spatial boundaries directly improves human psychological security and spatial awareness (Usanga, 2024). Artificial intelligence, biometric authentication, intelligent surveillance, encryption technologies, ongoing monitoring, staff awareness, and security governance are all combined in contemporary security environments. As noted by Ahmad, Desouza, Maynard, Naseer & Baskerville (2020), organizations achieve stronger security when security management and incident response functions are closely integrated, thereby improving organizational learning, threat intelligence, and proactive defense capabilities.

Potency of AI-Driven Security Devices in Optimum Security of Human Lives and Prosperity

- **Intelligent Surveillance and Real-Time Monitoring**

AI-driven surveillance systems use computer vision, machine learning, and smart cameras to continuously monitor environments without fatigue. Unlike conventional CCTV cameras that only record activities, AI systems can identify suspicious movements, abandoned objects, unauthorized access, crowd congestion, and violent behaviors in real time. Once an unusual event is detected, the system immediately alerts security personnel, enabling rapid intervention before incidents escalate. This capability significantly reduces crime rates, protects human lives, and minimizes damage to property in public places, schools, airports, hospitals, shopping malls, and residential estates (Swetha et al., 2025).

- **Facial Recognition and Biometric Authentication**

Artificial Intelligence enhances access control through facial recognition, fingerprint scanning, iris recognition, and voice recognition. These technologies accurately verify individuals before granting access to restricted areas, thereby preventing impersonation, identity theft, and unauthorized entry. AI-powered biometric systems are widely used in banks, airports, government agencies, educational institutions, and corporate organizations to strengthen security while ensuring only authorized individuals gain access to sensitive facilities (Reynaud & Roxin, 2025).

- **Predictive Crime Analysis**

One of the greatest strengths of AI is its ability to predict criminal activities before they occur. AI algorithms analyze historical crime records, weather conditions, geographical locations, social trends, and behavioral patterns to identify crime hotspots and forecast potential threats. Law enforcement agencies use these predictions to deploy security personnel strategically, allocate resources effectively, and implement preventive measures, thereby reducing criminal activities and safeguarding lives and property (Uddin et al., 2025).

- **Rapid Threat Detection and Response**

AI-powered security systems continuously analyze large volumes of security data to detect threats such as intrusions, gunshots, explosions, fire outbreaks, suspicious packages, and cyberattacks within seconds. Once a threat is identified, automated alerts are immediately sent to security personnel, emergency responders, or relevant authorities. This rapid response capability minimizes casualties, limits property destruction, and enhances emergency preparedness (Swetha et al., 2025).

- **Enhanced Cybersecurity Protection**

Modern security extends beyond physical environments to digital infrastructure. AI-driven cybersecurity systems detect malware, phishing attacks, ransomware, insider threats, and unusual network activities by learning normal user behavior and identifying deviations. These systems provide continuous monitoring and automated responses that protect sensitive information stored in financial institutions, hospitals, government agencies, educational institutions, and cloud computing environments from cybercriminals (Reynaud & Roxin, 2025; Uddin et al., 2025).

Challenges of AI in Home Security

- **Persistent Data Privacy Invasions and Continuous Surveillance**

AI-driven home security solutions continuously process multimodal data streams—including high-definition visual footage, spatial audio, voice recognition samples, and daily household routines—to build predictive behavioral profiles. Storing and transmitting these raw telemetry data to cloud servers exposes households to serious cyber risks, including unauthorized server breaches, insider misuse, and covert data monetization by third-party vendor ecosystems. Unlike dynamic authentication credentials such as passwords, biometric indicators (e.g., facial structural embeddings or unique voice signatures) cannot be reset or changed once intercepted by malicious actors. This continuous data collection creates significant ethical and legal friction under global privacy regulations like GDPR, as non-consenting visitors, domestic workers, and neighbors are regularly captured in automated surveillance nets without explicit consent (Buil-Gil et al., 2023).

- **Susceptibility to Physical and Audio Adversarial Attacks**

Deep learning models integrated into smart surveillance systems remain fundamentally fragile when exposed to adversarial manipulation designed to bypass computer vision and voice recognition filters (Zainuddin et al., 2022). Physical-world evasion techniques—such as custom-patterned apparel, optical light projections, or physical stickers placed in camera fields of view—can render human intruders completely invisible to Convolutional Neural Networks (CNNs). Simultaneously, voice-controlled smart home hubs remain susceptible to physical-layer acoustic vulnerabilities, where near-ultrasound signal injections or concealed audio commands can disarm alarm systems or unlock smart deadbolts without producing sound audible to the home's occupants.

- **Elevated False Alarm Rates from Environmental Noise**

Artificial intelligence models deployed for home intrusion detection regularly encounter out-of-distribution (OOD) ambient conditions in complex, dynamic residential environments. Dynamic factors such as moving vehicle headlights, swaying tree branches, household pets, passing shadows, and weather shifts routinely trigger high volumes of false positive alerts, leading to severe identification failures in practical intrusion detection systems (Santos & Horita, 2023). This recurring noise causes direct "alert fatigue" for homeowners and emergency services, often prompting users to reduce sensor sensitivity—which dangerously elevates false-negative risks—or turn off automated alerting systems entirely.

- **Edge Hardware Bottlenecks and Resource Constraints**

Running complex neural network architectures directly on edge devices (such as smart doorbell cameras or local security hubs) is heavily restricted by microcontrollers with limited processing power, memory capacity, and thermal headroom. While localized processing (e.g., TinyML) is critical for protecting data privacy and ensuring offline functionality, compact edge hardware struggles to process high-throughput, multi-class object recognition in real time without causing significant processing delays. Offloading these operations to cloud servers resolves computational limits, but introduces network latency, consumes residential internet bandwidth, and creates a single point of failure during internet connectivity outages.

- **Algorithmic Bias and the "Black-Box" Interpretability Deficit**

Deep neural networks used in modern access control systems function as uninterpretable "black box" algorithms, making it nearly impossible for non-technical users to inspect why a failure or unexpected lockout occurred. Compounding this interpretability gap, automated recognition systems often reflect underlying dataset biases that degrade algorithmic performance across diverse user populations and ambient lighting setups. Consequently, when a legitimate family member or guest is incorrectly classified as an intruder, the lack of model transparency offers users no clear diagnostic feedback or simple path to manually resolve the misclassification.

Mitigating Strategies to the Challenges of AI in Home Security

- **Privacy-Preserving Federated Learning and Differential Privacy**

To counteract the persistent privacy threats posed by central cloud data collection, security systems are increasingly adopting Federated Learning (FL) coupled with Differential Privacy (DP) mechanisms. Instead of offloading raw security video streams or biometric telemetry to remote vendor servers, local edge hubs train machine learning models locally on-device and only transmit encrypted parameter updates to the cloud. Furthermore, inject noise via differential privacy mathematical techniques ensures that shared parameters cannot be reverse-engineered to reconstruct household routines or biometric features, providing verifiable privacy protection under global regulatory frameworks like GDPR.

- **Adversarial Training and Multimodal Liveness Verification**

Mitigating physical and acoustic evasion attacks requires hardening neural network classifiers during the pre-deployment training phase through Adversarial Training and multi-sensor validation. Security models are intentionally exposed to synthetic adversarial noise—such as corrupted optical patches, physical-world stickers, and near-ultrasound signal perturbations—allowing Convolutional Neural Networks (CNNs) to build robust decision boundaries. (Zainuddin et al., 2022). Complementing this, access controllers deploy multimodal liveness detection (e.g., combining thermal infrared imaging with passive millimeter-wave sensing) to confirm that a target is a genuine physical human rather than an adversarial projection or a spoofed acoustic playback.

- **Context-Aware Adaptive Thresholding and Explainable Dynamic Filtering**

To solve high false-positive notification rates driven by environmental interference, modern AI security architectures use Context-Aware Dynamic Filtering alongside Explainable AI (XAI) techniques. Rather than applying static classification thresholds, these systems ingest external environmental telemetry—such as ambient light metrics, weather forecasts, and known household pet motion patterns—to dynamically recalibrate sensitivity models. Incorporating interpretability frameworks like LIME (Local Interpretable Model-agnostic Explanations) allows the system to isolate environmental noise from actual threats, reducing notification fatigue without compromising true intrusion detection (Yazmyradov & Lee, 2024).

- **TinyML Optimization and Hardware-Aware Quantization**

Engineers address edge compute bottlenecks through advanced software-hardware co-design techniques, specifically TinyML model compression and post-training quantization. By compressing heavy neural network weights from floating-point arithmetic down to 8-bit integers (INT8), state-of-the-art vision and anomaly-detection models can run locally on low-power, constrained microcontrollers without heavy cloud dependency. This localized inference drastically

reduces execution latency, lowers power consumption, preserves local bandwidth, and ensures that critical safety features remain active even during internet connection outages.

- **Explainable AI (XAI) and Demographic Debiasing Pipelines**

Overcoming the "black-box" decision problem and algorithmic bias requires integrating interpretable design principles and demographically balanced training sets into biometrics pipelines. By providing human-readable explanations whenever access is granted or denied (e.g., highlighting specific visual features that failed verification), users gain visibility into lockouts. Simultaneously, implementing rigorous synthetic data augmentation—generating diverse lighting conditions, skin tones, and facial feature angles during training—eliminates demographic performance skew and improves system fairness for all household residents.

CONCLUSION

In conclusion, Artificial Intelligence (AI) has emerged as a transformative technology that is redefining home security through the integration of intelligent security devices capable of monitoring, detecting, analyzing, and responding to security threats in real time. Unlike conventional security systems, AI-driven security devices combine machine learning, computer vision, facial recognition, biometric authentication, predictive analytics, and Internet of Things (IoT) technologies to provide proactive and efficient protection of human lives and property. These intelligent systems not only enhance surveillance and access control but also reduce false alarms, improve emergency response, and strengthen cybersecurity. Despite concerns relating to data privacy, ethical issues, algorithmic bias, and cyber threats, continuous advancements in AI technologies and security governance have significantly improved the reliability and effectiveness of smart home security systems. Therefore, the integration of AI-driven security devices represents a major step toward achieving optimum residential security, ensuring safer homes, protecting valuable assets, and contributing to a more secure and technologically advanced society.

RECOMMENDATION

- Homeowners should adopt AI-driven security devices such as smart surveillance cameras, biometric access control systems, and intelligent alarm systems to improve the protection of lives and property.
- Governments should establish comprehensive policies and regulatory frameworks to ensure the ethical, secure, and responsible deployment of AI-based home security technologies while safeguarding users' privacy.
- Manufacturers of AI security devices should continuously improve system accuracy through regular software updates, advanced machine learning algorithms, and robust cybersecurity measures to minimize false alarms and security vulnerabilities.
- Security agencies and emergency response organizations should integrate AI-powered surveillance and predictive analytics into their operations to enhance crime prevention, rapid threat detection, and emergency response capabilities.

REFERENCES

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71(8), 939–953. https://doi.org/10.1002/asi.24311

Albahri, A. S., Duhaim, A. M., Fadhel, M. A., Alnoor, A., Baqer, N. S., Alzubaidi, L., (2021). Artificial intelligence and Internet of Things for smart home security: A systematic review. *Journal of King Saud University – Computer and Information Sciences*, 33(10), 1211–1228. https://doi.org/10.1016/j.jksuci.2020.11.002.

Aldowah, H., Ghazal, S., Umar, I. N., & Muniandy, B. (2022). Smart home security systems: Technologies, applications, and future directions. *Sensors*, 22(18), 6998. https://doi.org/10.3390/s22186998.

Alqahtani, F., Alshahrani, A., Alghamdi, S., & Alzahrani, N. (2023). Artificial intelligence-enabled Internet of Things for smart home security: *A review. Electronics*, 12(9), 2014. https://doi.org/10.3390/electronics12092014.

Amuzat, O., (2025), How AI will shape up government of alberta and the benefits it can reap and become more competitive globally by the strategic application of AI. Shared Seasoned International Journal of Topical Issues, 12(1), 17.

Buil-Gil, D., Kmep, S., Kuenzel, Coventry, L., Zakhary, S., Tilley, D. & Nicholson, J.(2023). The digital harms of smart home devices: A systematic literature review. Computer in Human beheviour, 145.

Butun, I., Österberg, P., & Song, H. (2020). Security of the Internet of Things: *Vulnerabilities, attacks, and countermeasures. IEEE* Communications Surveys & Tutorials, 22(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364.

Cao, L. (2021). Artificial Intelligence in the Real World: Opportunities and Challenges. Engineering, 7(3), 343–349. https://doi.org/10.1016/j.eng.2020.02.021

Diéguez, M., Bustos, J., & Cares, C. (2020). Mapping the variations for implementing information security controls to their operational research solutions. *Information Systems and e-Business Management*, 18(2), 157–186. https://doi.org/10.1007/s10257-020-00470-8

Eynaud, S., & Roxin, A. (2025). *Review of explainable artificial intelligence for cybersecurity systems. Discover Artificial Intelligence, 5*(78). https://doi.org/10.1007/s44163-025-00318-5

Floridi, L., & Chiriatti, M. (2020). GPT-3: Its nature, scope, limits, and consequences. Minds and Machines, 30(4), 681–694. https://doi.org/10.1007/s11023-020-09548-1

Guembe, B., Azeta, A., Misra, S., Osamor, V., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of AI-Driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, 36(1), 2037254. https://doi.org/10.1080/08839514.2022.2037254.

Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W., & Li, K. (2022). Artificial Intelligence Security: Threats and Countermeasures. *ACM Computing Surveys*, 55(1), 1–36. https://doi.org/10.1145/3487890.

Luke, P.H., & Akpan, E.E., (2025), intelligence and wise decision making in business: the strategies and prospects, Shared Seasoned International Journal of Topical Issues, 12(1), 149.

Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The Impacts of Artificial Intelligence Techniques in Augmentation of Cybersecurity: A Comprehensive Review. *Complex & Intelligent Systems*, 8(2), 1763–1780. https://doi.org/10.1007/s40747-021-00494-8.

Proske, M., & Schmid, T. (2022). Physical boundaries and functional shelter in modern building design. *International Journal of Structural Engineering*, 18(2), 101–115.

Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach and its contemporary applications. AI Magazine, 42(2), 15–28. https://doi.org/10.1609/aimag.v42i2.18136

Santos, R. D., & Horita, F. E. (2023). False positive identification in intrusion detection using eXplainable Artificial Intelligence (XAI). *IEEE Latin America Transactions*, 21(6), 720–728.

Swetha, T., Kumaran, U., Meena, V. P., & Hameed, I. A. (2025). *Leveraging AI for enhanced cybersecurity: A comprehensive review*. *Discover Applied Sciences*, *7*, 584. https://doi.org/10.1007/s42452-025-06773-0

Uddin, M., Irshad, M. S., Kandhro, I. A., Alanazi, F., Ahmed, F., Maaz, M., Hussain, S., & Ullah, S. S. (2025). *Generative AI revolution in cybersecurity: A comprehensive review of threat intelligence and operations*. *Artificial Intelligence Review*, *58*, 236. https://doi.org/10.1007/s10462-025-11219-5

Usanga, A. P. S. (2024). A critical analysis of biophilic design and application of its principles for healthier work environments. *International Journal of Research in Education and Management Science*, 6(1), 71–78.

Usanga, A. P. S., & Isaac, B. E. (2024). Half fence: Evaluating its usefulness and potency in providing thermal comfort and security to occupants. *International Journal of Modern Health Systems and Medical Sciences*, 5(2), 10–19.

Usanga, A. P. S., & Usanga, M. (2024). The menace of dilapidated building: Investigating its effect on students' live and interest in study. *International Journal of Advancement in Education, Management, Science and Technology*, 7(1), 73–84.

Yazmyradov, S. & Lee, H. J. (2024). A Comprehensive Review of AI Security: Threats, Challenges, and Mitigation Strategies. *The Journal of the Institute of Internet Broadcasting and Communication*, 16(4): 375-384.

Zainuddin, A. A., Fathullah, M. Z., Razak, N. A. A., Sidik, N. F. I., Faizul, N. A. A., Roslee, A. M., & Ruzaidi, N. A. A. (2022). Critical analysis of security challenges in Internet of Things smart home system users. *International Journal of Information Security*, 21(3), 611–636.