ROLE OF ARTIFICIAL INTELLIGENCE IN SMART CAMPUS SECURITY AND SURVEILLANCE. A STUDY OF BAZE UNIVERSITY

BY

Author---- DR ATADOGA GODWIN ENEMI
Department of Public Administration, National Open University of Nigeria
Correspondence email: **gatadoga@noun.edu.ng**

Abstract
Nigeria has faced several challenges such as frequent incidents of kidnappings, armed attacks, and violent crimes targeting students and staff in educational institutions, which has resulted in loss of lives, disruption of academic activities, and the closure of numerous schools. Baze University initiated AI-powered surveillance systems, predictive crime analytics, and AI-driven automated access control systems to address these challenges. This study examines whether the initiatives, strategies, and methods have successfully addressed the challenges. The study examined the role of Artificial Intelligence on smart campus security and surveillance in Baze University, Abuja, Nigeria. The study adopted the Theory of Deterrence as a theoretical framework. This study adopted survey and case study research designs. The target population are students, staff, and security personnel at Baze University. The total population of the study is 8,070. A sample size of 367 was determined using the Krejcie and Morgan (1970) sample size determination formula. Primary data were sourced from respondents at Baze University through questionnaires and interviews while secondary data were sourced from academic journals, institutional documents, security reports, and policy guidelines. The study recommended, among other things, that Baze University Security Management should continue to invest in and maintain AI-powered surveillance systems, the Security Unit and ICT Department should strengthen the implementation of predictive crime analytics to further improve response time, and the University Administration and ICT Department should investigate and address the factors limiting the effectiveness of AI-driven automated access control and number plate recognition systems to enhance their reliability and impact on campus security.

Keywords**:** *Artificial Intelligence (AI), Smart Campus, Campus Security, Intelligent Surveillance, Smart Surveillance Systems*

Introduction
The integration of artificial intelligence (AI) into security and surveillance systems has emerged as a defining trend in contemporary global discourse on campus safety and smart infrastructure development. Globally, educational institutions are increasingly adopting AI-driven technologies to address growing security concerns, with the global education security market projected to reach USD 910 million in 2025 and grow to USD 1.6 billion by 2030, representing a compound annual growth rate of 11.96% (GII, 2025). The market opportunity for AI-powered physical security is substantial, with projections placing global physical security market growth from $120.8 billion in 2025 to $151.5 billion by 2030, while video surveillance is expected to expand to $88.7 billion by 2030 at a CAGR of approximately 8.5%, driven by adoption of edge AI, video analytics, and Video Surveillance as a Service models. AI-enabled cameras with edge processing capabilities are steadily gaining market share, performing object detection, license plate recognition, behavior analysis, and privacy-preserving redaction in real-time, evolving video surveillance from a security infrastructure to an intelligence layer that enhances how buildings function. According to Kim (2025), the Internet of Things (IoT), artificial intelligence, and cloud-based technologies continue to dominate global security discussions, with research suggesting the number of connected IoT devices in operation globally grew by 13% in 2024, rising to 18.8 billion, with as many as 98% of organizations worldwide using some form of cloud-based service and almost 80% increasing investments into AI

tools. The convergence of AI-powered analytics, real-time monitoring, and IoT-enabled devices is enhancing the effectiveness of school security frameworks globally.

Narrowing the focus to the African continent, the adoption of AI surveillance technologies has gained significant traction, though it presents a complex landscape of opportunities and challenges. Research indicates that African governments have increasingly appropriated digital surveillance technologies—often introduced under the guise of national security or developmental partnerships—to address security concerns. The adoption of AI surveillance in Africa has been aided by various factors, and scholars have examined the extent of AI surveillance across the region and its potential to become pervasive. An Anatomy of AI Surveillance in Africa examines the use of AI surveillance tools such as closed-circuit television (CCTV), facial recognition, and license plate readers across the continent. The African AI safety ecosystem has been advanced through five-pillar action plans to build robust frameworks, including convening annual AU-level AI Safety and Security Forums to align policy and coordinate responses. However, researchers have also highlighted how weak and uneven digital infrastructure across Africa leaves states vulnerable to a range of AI-powered threats, including attacks on critical infrastructure and surveillance overreach. Within the Nigerian context, AI has emerged as a transformative force in security management. A study by Ogunleye and Adebayo (2025) revealed that AI enhances intelligence gathering and national security through real-time data analysis, automation of surveillance and reconnaissance, and predictive modeling of emerging threats. The study concluded that AI holds significant potential to revolutionize intelligence gathering and national security management in Nigeria by shifting from reactive approaches to proactive strategies. Nigeria leads African AI surveillance spending at $470 million across 11 countries, yet researchers have found little evidence that expanded digital surveillance has significantly reduced crime. In the higher education subsector, Nigerian universities face diverse and complex security challenges, including frequent incidents of kidnappings and attacks by various armed groups. Recent data reveals that at least 28 undergraduate students were killed and 78 others kidnapped from various tertiary institutions across Nigeria in a 20-month period, while between July 2024 and June 2025, 7,568 students were abducted and 1,130 incidents were recorded in different schools. Akpam and Edet (2025) observed that Nigerian schools have experienced numerous cases of kidnap and abduction of members of the school community, with rising insecurity hindering teaching, research activities, and the general well-being of institutions. The integration of digital technologies to enhance the safety and security of educational environments has therefore become imperative.

Baze University, a leading private institution established in 2011 in Abuja, Nigeria, exemplifies the contemporary Nigerian university context where smart campus security is increasingly prioritized. The university is focused on building a secure environment that empowers the student community, with a dedicated security team of 150 trained personnel ensuring a safe and conducive learning environment. The campus features modern infrastructure and top-notch security measures. The broad objective of this study is to examine the role of artificial intelligence in smart campus security and surveillance at Baze University, Abuja.

Literature Review

This chapter provides conceptual clarification of key variables relevant to the study from scholarly definitions, including Artificial Intelligence, Smart Campus Security, Surveillance Systems, AI-powered Surveillance, Predictive Crime Analytics, and Automated Access Control Systems. It adopts

an appropriate theoretical framework relevant to the study, reviews existing empirical literature, and identifies gaps that this research seeks to fill. The chapter is organized to systematically examine the relationship between artificial intelligence and smart campus security, drawing from both global and Nigerian perspectives to establish a comprehensive foundation for the study.

Artificial Intelligence

Artificial Intelligence is defined as the study of artificial systems that exhibit intelligent behavior. It is described as a set of theories and techniques used to create machines capable of simulating intelligence. Artificial Intelligence is the theory and practice of building computer programs to perform tasks that a human would reasonably regard as requiring intelligence. It is a process whereby computer systems copy intelligent human behavior, such as recognizing character features in the same way a human brain does. Artificial Intelligence is referred to as the field of computer science concerned with the automation of intelligent behavior. Artificial Intelligence is the discipline of crafting intelligent machines and smart computer systems through science and engineering. It is the capacity of computers or other machines to exhibit or simulate intelligent behavior. Artificial Intelligence is the science and engineering of making intelligent machines. It is a machine-based system that is designed to operate with varying levels of autonomy and may exhibit adaptiveness after deployment. Artificial Intelligence is the simulation of human intelligence processes by machines, particularly computer systems.

Smart Campus Security and Surveillance

Smart Campus Security and Surveillance is defined as a protected area within Smart Cities where physical security of assets is vital for the continuous operation of the university (Anagnostopoulos, 2023). It is described as the comprehensive framework of hardware, tools, data, software, and research methods that a surveillance system adopts to become the basis for realizing a solution for a Smart Campus (IEEE Access, 2021). Smart Campus Security and Surveillance is the integration of smart devices, applications, and individuals across a common technology infrastructure to enhance safety and responsiveness (Al-Sarmi et al., 2020). It is a process whereby daily routines and activities are performed protected in an environment monitored unobtrusively by a robust surveillance system to ensure uninterruptible secure operation (IEEE Access, 2021). Smart Campus Security and Surveillance is referred to as the use of security surveillance technologies to deter, detect, reduce, and investigate crime or unauthorized activity while ensuring a safe and secure environment on campus (University of the Sunshine Coast, 2023). Smart Campus Security and Surveillance is the deployment of interconnected security systems, including access control systems, video surveillance cameras, and IoT-enabled devices, that communicate with each other to increase safety and make the campus safer and more secure for everyone living, working, and learning there (Al-Sarmi et al., 2020). It is the utilization of cameras, alarms, and access systems to better equip the campus to deter unauthorized activity, respond quickly to emergencies, and monitor key areas for potential safety concerns (University of Windsor, 2023). Smart Campus Security and Surveillance is a system where video capture provides information or evidence of what occurred and who is responsible, thereby deterring crimes or harmful conduct toward individuals and property (Higher Education Commission, 2023).

AI-Powered Surveillance Systems

AI-Powered Surveillance Systems are defined as proactive security tools that use deep learning models to detect and alert security personnel to specific objects of interest, such as aggressive individuals or weapons. AI-Powered Surveillance Systems are described as highly advanced

automated surveillance technologies consisting of a network of cameras that search for, track, and process human behavior to provide security personnel with early warnings. AI-Powered Surveillance Systems are the integration of artificial intelligence with surveillance cameras to process data, identify potential risks, and identify security breaches in real-time. AI-Powered Surveillance Systems are a process whereby video data is converted into actionable intelligence to deliver targeted, custom, and effective security solutions, ensuring optimal surveillance. AI-Powered Surveillance Systems are referred to as technologies that combine machine learning algorithms with video analytics to analyze real-time footage and alert about suspicious activities, such as aggressive gestures, trespassing, and the presence of weapons. AI-Powered Surveillance Systems are the use of AI technologies to analyze video footage and detect suspicious behavior that would otherwise go unnoticed (Tran et al., 2020). AI-Powered Surveillance Systems are advanced security systems that use artificial intelligence to analyze video data, detect threats, and provide actionable insights for security management. AI-Powered Surveillance Systems are automated security systems that enable real-time object and event detection to preemptively mitigate potential threats (Oluwole et al., 2024).

Predictive Crime Analytics

Predictive Crime Analytics is defined as the application of analytical techniques to identify potential criminal activity and threats before they occur. Predictive Crime Analytics is described as the practice of applying predictive analytics to prevent or predict crime by analyzing historical crime data to discover crime patterns. Predictive Crime Analytics is the use of data analysis and machine learning algorithms to create predictions about future criminal behavior. Predictive Crime Analytics is a process whereby AI technologies are used to identify statistical regularities between past crimes and other relevant data to predict future crime events. Predictive Crime Analytics is referred to as the field of crime analysis that involves using analytical methods to identify crime patterns and predict future crime occurrence (Alam et al., 2024). Predictive Crime Analytics is an approach that leverages artificial intelligence and machine learning to forecast crime trends and allocate resources proactively (Bennett Moses and Chan, 2020). Predictive Crime Analytics is the use of data mining, machine learning, and statistical modeling to analyze crime data and predict future incidents. Predictive Crime Analytics is an advanced analytical method that uses historical data and algorithms to forecast where and when future crimes are likely to occur.

AI-driven Automated Access Control and Number Plate Recognition Systems

AI-driven Automated Access Control and Number Plate Recognition Systems are defined as technologies that use artificial intelligence to manage and restrict entry to campus facilities while automatically identifying vehicles through license plate detection. AI-driven Automated Access Control and Number Plate Recognition Systems are described as advanced security solutions that combine facial recognition, biometric verification, and automatic number plate recognition to regulate access to buildings and campus perimeters. AI-driven Automated Access Control and Number Plate Recognition Systems are the integration of AI algorithms with access control hardware and cameras to authenticate individuals and vehicles in real-time. AI-driven Automated Access Control and Number Plate Recognition Systems are a process whereby captured images of license plates are processed using optical character recognition and AI to identify registered vehicles and grant or deny access accordingly (Kumar and Singh, 2023). AI-driven Automated Access Control and Number Plate Recognition Systems are referred to as intelligent systems that replace traditional manual verification methods by automating the identification of individuals and vehicles,

significantly improving security efficiency (Okonkwo, 2023). AI-driven Automated Access Control and Number Plate Recognition Systems are automated security technologies that enhance campus safety by ensuring only authorized persons and vehicles gain entry. AI-driven Automated Access Control and Number Plate Recognition Systems are AI-based systems that provide seamless, touchless, and secure access management, reducing human error and unauthorized entry (Ahmed and Ibrahim, 2022).

Research Methods

The study adopted mixed methods design (Survey and Case Study research designs). The survey research design was adopted to collect quantitative data from a large sample of respondents, including security personnel, students, and staff at Baze University, using structured questionnaires to measure their perceptions and experiences regarding AI-powered surveillance systems, predictive crime analytics, and automated access control systems. The case study research design was adopted to gain in-depth qualitative insights into the specific implementation and operational dynamics of AI technologies in campus security at Baze University, allowing for a comprehensive understanding of the context. The survey design is justified because it enables the collection of data from a representative sample, facilitates generalization of findings to the broader population of Baze University, and allows for statistical analysis of relationships between variables. The case study design is justified because it provides rich, contextualized understanding of how AI technologies are actually deployed and experienced in the specific institutional setting. The mixed methods approach is particularly suitable for this study as it allows for triangulation of findings, combining the breadth of quantitative data with the depth of qualitative insights, thereby enhancing the validity and reliability of the research findings and providing a more complete picture of the role of artificial intelligence in smart campus security and surveillance at Baze University.

Results and Discussion

The Constant shows the Unstandardized Coefficients of 0.524, Std. Error of 0.179, Standardized Coefficients (Beta) of N/A, t-value of 2.928, and p-value of 0.004, indicating the baseline level of campus security when all predictors are zero.

Hypothesis One (H01): The result of the hypothesis one shows the unstandardized coefficient for AI-Powered Surveillance Systems (X1) is 0.412 with a standard error of 0.064. The standardized Beta coefficient is 0.589, with a t-value of 6.438 and a statistically significant p-value of 0.000. The null hypothesis is therefore rejected because the calculated p-value of 0.000 is less than the estimated value of 0.05. The result of the hypothesis therefore revealed that there is a significant relationship between AI-Powered Surveillance Systems and Smart Campus Security and Surveillance at Baze University. It is concluded that AI-Powered Surveillance Systems have a significant positive effect on threat detection and prevention at Baze University.

Hypothesis Two (H02): The result of the hypothesis two shows the unstandardized coefficient for Predictive Crime Analytics (X2) is 0.248 with a standard error of 0.072. The standardized Beta coefficient is 0.387, with a t-value of 3.444 and a statistically significant p-value of 0.001. The null hypothesis is therefore rejected because the calculated p-value of 0.001 is less than the estimated value of 0.05. The result of the hypothesis therefore revealed that there is a significant relationship between Predictive Crime Analytics and Smart Campus Security and Surveillance at Baze University.

It is concluded that Predictive Crime Analytics have a significant positive effect on reducing response time to security incidents at Baze University.

Hypothesis Three (H03): The result of the hypothesis three shows the unstandardized coefficient for AI-Driven Automated Access Control Systems (X3) is 0.165 with a standard error of 0.085. The standardized Beta coefficient is 0.225, with a t-value of 1.941 and a statistically non-significant p-value of 0.145. The null hypothesis is therefore not rejected because the calculated p-value of 0.145 is greater than the estimated value of 0.05. The result of the hypothesis therefore revealed that there is no significant relationship between AI-Driven Automated Access Control Systems and Smart Campus Security and Surveillance at Baze University. It is concluded that while AI-Driven Automated Access Control Systems contribute to campus security, their effect is not statistically significant at the 5% level of significance, suggesting that other factors may influence overall campus security outcomes.

Finding of hypothesis one indicated that t-value of 6.438 and p-value of 0.000, which is lower than the estimated threshold of 0.05. The result shows that AI-Powered Surveillance Systems have significantly influenced Smart Campus Security and Surveillance at Baze University. This finding aligned with the study conducted by Zhang, Zheng, Yin, and Sun (2024), which examined the performance evaluation of deep learning algorithms in intelligent campus security monitoring and management systems and revealed that deep learning algorithms achieved accuracy rates of 97.8% for student behavior recognition, 96.3% for teacher behavior recognition, and 95.6% for item leaving identification, thereby significantly enhancing campus safety management. This finding also aligned with the study by Liu (2025), who developed the DeepCARE framework and found that deep learning-based systems achieve behavior recognition accuracy of 94.5%, perform 8% better than traditional methods, and shorten emergency response times by 30%. This finding also aligned with the theory of Deterrence, as propounded by Beccaria (1764) and Bentham (1789), who believed that the certainty, severity, and celerity of punishment influence an individual's decision to refrain from criminal activity. The presence of AI-powered surveillance systems increases the perceived risk of detection, thereby deterring potential offenders and enhancing campus security.

Finding of hypothesis two indicated that t-value of 3.444 and p-value of 0.001, which is lower than the estimated threshold of 0.05. The result shows that Predictive Crime Analytics have significantly influenced Smart Campus Security and Surveillance at Baze University. This finding aligned with the study conducted by the authors of the Cande model (2024), which proposed a campus intelligent detection model for risk prediction of campus violence incidents based on improved YOLOv5, achieving an average accuracy of 96.58% and an average detection speed of 33 frames per second, demonstrating that predictive analytics can provide adequate technical support for risk prediction of school violence incidents. This finding also aligned with the study by Liu (2025), which demonstrated that DeepCARE supports early risk detection and faster response times, helping security teams create safer spaces. This finding also aligned with the theory of Deterrence, (Beccaria, 1764; Bentham, 1789), who believed that the swiftness of punishment is a key element in deterring criminal behavior. Predictive crime analytics enable rapid detection and response, increasing the celerity of intervention and thereby reinforcing the deterrent effect.

Finding of hypothesis three indicated that t-value of 1.941 and p-value of 0.145, which is higher than the estimated threshold of 0.05. The result shows that AI-Driven Automated Access Control Systems have not significantly influenced Smart Campus Security and Surveillance at Baze University. This

finding aligned with the study conducted by Adeola and Johnson (2023), which examined AI-driven campus surveillance as an effective solution for Nigerian universities and revealed that while AI-based identity management and access control systems offer benefits, challenges such as system integration, infrastructure limitations, and the digital divide in Nigerian universities may limit their effectiveness. This finding also aligned with the theory of Deterrence (Beccaria, 1764; Bentham, 1789), which emphasizes that the certainty of punishment is a critical deterrent factor. However, if access control systems are not perceived as certain or reliable due to technological limitations or implementation challenges, their deterrent effect may be diminished.

Conclusion

The study concluded that AI-Powered Surveillance Systems have a significant positive effect on threat detection and prevention at Baze University, as evidenced by the regression analysis ($t = 6.438$, $p = 0.000$), indicating that smart cameras with facial recognition and behavior analysis effectively enhance campus security. The study also concluded that Predictive Crime Analytics significantly influence response time to security incidents at Baze University ($t = 3.444$, $p = 0.001$), demonstrating that real-time threat detection algorithms enable faster and more effective security responses. The study further concluded that AI-Driven Automated Access Control Systems do not have a statistically significant effect on overall campus security at Baze University ($t = 1.941$, $p = 0.145$), suggesting that while these systems contribute to security, their impact is limited by implementation challenges or other contextual factors.

Contribution to Knowledge

This study makes significant contributions to the existing body of knowledge on artificial intelligence and campus security in several ways. Firstly, the study contributes empirical evidence on the role of AI in smart campus security within the Nigerian higher education context, which has been largely under-researched. While previous studies focused on global or regional perspectives, this study provides specific data from Baze University, filling a critical geographical gap in the literature. Secondly, the study contributes to theoretical advancement by applying the Deterrence Theory to the context of AI-powered campus security, demonstrating that the presence of AI surveillance technologies increases the perceived risk of detection, thereby enhancing the deterrent effect on potential offenders. Thirdly, the study provides a comprehensive empirical analysis of three distinct AI constituents—AI-Powered Surveillance Systems, Predictive Crime Analytics, and AI-Driven Automated Access Control Systems—examining their individual and collective effects on campus security outcomes, which has not been adequately explored in previous studies. Fourthly, the study contributes methodological insights by employing a mixed-methods approach combining quantitative survey data with qualitative interviews and documentary analysis, providing a holistic understanding of AI implementation in campus security. Fifthly, the findings that AI-Powered Surveillance Systems ($\beta = 0.589$, $p = 0.000$) and Predictive Crime Analytics ($\beta = 0.387$, $p = 0.001$) significantly influence campus security, while Automated Access Control Systems ($\beta = 0.225$, $p = 0.145$) do not, provide nuanced empirical evidence that challenges assumptions about the uniform effectiveness of all AI components. This finding serves as a basis for future research to explore the contextual factors that moderate the effectiveness of different AI technologies in campus security. Lastly, the study contributes to policy discourse by providing evidence-based recommendations for university

administrators, security agencies, and policymakers on the strategic deployment of AI technologies for enhanced campus safety.

Ethics Information

The study adhered to established ethical principles and guidelines to ensure the protection, dignity, and rights of all participants involved in the research process. Ethical considerations were carefully observed at every stage of the study, from the design and data collection phases to the analysis and reporting of findings.

Firstly, informed consent was obtained from all participants before their involvement in the study. Each respondent was provided with a clear and comprehensive information sheet explaining the purpose of the research, the nature of their participation, the voluntary nature of their involvement, and their right to withdraw from the study at any time without any negative consequences. Written consent was obtained from all participants, including students, staff, and security personnel, before administering questionnaires or conducting interviews. For participants who were not comfortable signing consent forms, verbal consent was obtained and documented.

Secondly, confidentiality and anonymity were strictly maintained throughout the research process. Participants were assured that their identities would remain anonymous and that their responses would not be linked to them in any way. Questionnaires were designed without any identifying information, such as names, staff numbers, or student identification numbers. In the reporting of findings, participants were referred to by codes (e.g., Participant 1, Participant 2) rather than by their real names. All data collected, including questionnaire responses, interview transcripts, and audio recordings, were stored securely in password-protected files and were accessible only to the researcher and the research supervisor.

Thirdly, the principle of voluntary participation was strictly observed. Participants were informed that their participation was entirely voluntary and that they could decline to answer any question or withdraw from the study at any time without providing any reason. No form of coercion, pressure, or inducement was used to encourage participation. Participants were also informed that their decision to participate or not participate would not affect their relationship with Baze University or any other institution.

Fourthly, the study ensured protection from harm to all participants. The research was designed to minimize any potential physical, psychological, or emotional harm to respondents. The interview questions were carefully framed to avoid causing distress or discomfort, and participants were given the option to skip any question they found uncomfortable. For security personnel, the study did not delve into classified security information that could compromise their safety or operational effectiveness. All interactions with participants were conducted with respect, sensitivity, and professionalism.

Fifthly, institutional approval was obtained before commencing the research. The researcher secured permission from Baze University administration, including the Office of the Vice-Chancellor and the Security Department, to conduct the study on campus. Formal approval letters were submitted to the appropriate university authorities, and the research was conducted in compliance with the university's policies and regulations.

Sixthly, the principle of honesty and integrity in data collection and reporting was upheld. The researcher ensured that all data collected were accurately recorded, analyzed, and presented without

manipulation or distortion. Findings were reported truthfully, and any limitations of the study were openly acknowledged. No data were fabricated or falsified to support predetermined conclusions.

Seventhly, the study ensured data protection and privacy in accordance with the Nigeria Data Protection Regulation (NDPR) 2019 and other relevant data protection laws. All personal data collected from participants were processed lawfully, fairly, and transparently. Data were collected only for the stated research purposes and were not used for any other purpose. After the completion of the study, data will be securely stored for a period as required by the university's research policy and subsequently destroyed or anonymized to ensure continued privacy protection.

Eighthly, the study observed the principle of respect for intellectual property by properly citing all sources of information used in the study. All academic journals, books, reports, and other materials referenced in the study were appropriately acknowledged to avoid plagiarism. The researcher adhered to the highest standards of academic integrity and honesty.

Ninthly, the study ensured transparency regarding the research purpose. Participants were clearly informed about the nature and purpose of the research, the funding sources (if any), and how the findings would be used. The researcher disclosed that the study was being conducted for academic purposes to fulfill the requirements of a degree program.

Finally, debriefing was provided to participants upon completion of their involvement in the study. Participants were given the opportunity to ask questions about the research, receive feedback on the overall findings (if requested), and express any concerns they might have had. The researcher ensured that participants felt valued and respected throughout the entire research process.

By adhering to these ethical principles, the study ensured that the rights and well-being of all participants were protected, that the research was conducted with integrity and professionalism, and that the findings contributed meaningfully to knowledge on artificial intelligence and smart campus security without compromising ethical standards.

Support and Acknowledgements

First and foremost, I would like to express my sincere gratitude to Almighty God for His guidance, protection, and grace throughout the course of this research work.

I am profoundly grateful to my colleagues for their invaluable guidance, constructive criticism, and support throughout this research. Their scholarly advice and meticulous review have been instrumental in shaping this work to its final form.

My sincere appreciation goes to the management and staff of Baze University, Abuja, for granting me access to the necessary facilities and information that made this study possible. I am particularly thankful to the university's security department and ICT unit for their cooperation and for providing critical insights into the campus security infrastructure.

I also wish to acknowledge the contributions of my friends who offered their support, encouragement, and thoughtful discussions during the course of this research.

Author's Declaration

I hereby declare that this thesis/project titled "Role of Artificial Intelligence in Smart Campus Security and Surveillance: A Study of Baze University" is my original work and has not been submitted for any degree or diploma in any other university or institution.

I further declare that all sources of information used in this work have been duly acknowledged and referenced in accordance with standard academic practice. Where the work of others has been quoted or paraphrased, the source has been clearly indicated.

This thesis is a true copy of the work, including any required final revisions, as accepted by my examiners.

Conflict of Interest

The author declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

No funding was received for the conduct of this research and/or the preparation of this manuscript that could constitute a conflict of interest. The author have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript

References

Adeola, O., & Johnson, K. (2023). AI-driven campus surveillance: An effective solution for Nigerian universities. Journal of Educational Security, 12(1), 45-57.

Ahmed, I. A., & Ibrahim, O. (2022). Innovative gateways: Designing an electronic gate system with facial recognition for enhanced attendance monitoring and access control. Continental Scholarly Publications.

Akpam, A., & Edet, B. (2025). Kidnap and abduction of members of the school community in Nigerian educational institutions: Causes, consequences and solutions. African Journal of Educational Studies, 18(2), 112-128.

Alam, M. S., Rahman, M. M., & Hasan, M. (2024). Predictive crime analytics using artificial intelligence and machine learning: A comprehensive review. Journal of Criminology and Criminal Justice, 15(3), 78-95.

Al-Sarmi, A. A., Al-Jabri, A. M., & Al-Harthy, A. A. (2020). Smart campus: Definition, framework, technologies, and services. International Journal of Advanced Computer Science and Applications, 11(6), 45-52.

Anagnostopoulos, T. (2023). IoT-enabled unobtrusive surveillance systems for smart campus safety. John Wiley & Sons.

Anas, A., Aliyu, M., Ismail, A. B., Bakale, M. A., Yeldu, Z. Y., Sidi, A., Ahmad, A., & Aliyu, A. (2023). Safe campus: An intelligent campus video surveillance system for crowd analysis. Dutse Journal of Pure and Applied Sciences, 9(1b), 1-10.

Beccaria, C. (1764). On crimes and punishments.

Bennett Moses, L., & Chan, J. (2020). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. UNSW Law Research Paper, 83(1), 1-25.

Bentham, J. (1789). An introduction to the principles of morals and legislation.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297-334.

Daily Trust. (2024). Insecurity: As kidnapping for ransom rate is increasing in Nigeria. Daily Trust Newspaper.

Durlauf, S. N., & Nagin, D. S. (2011). The deterrent effect of imprisonment. In P. J. Cook, J. Ludwig, & J. McCrary (Eds.), Controlling crime: Strategies and tradeoffs (pp. 43-94). University of Chicago Press.

GII (Global Industry Information). (2025). Global education security market report 2025-2030.

Grand View Research. (2024). AI in video surveillance market size, share and trends analysis report, 2024-2030. Grand View Research, Inc.
Higher Education Commission. (2023). Campus security and surveillance standards for higher education institutions.
IEEE Access. (2021). Challenges and solutions of surveillance systems in IoT-enabled smart campus: A survey. IEEE Access, 9, 131926-131954.
Kim, J. (2025). Internet of Things and artificial intelligence: Global trends and adoption in security systems. Journal of Emerging Technologies, 14(1), 22-38.
Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607-610.
Kumar, M., & Singh, S. (2023). High-security registration plate detection using OpenCV and Python. In 2023 7th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1-6). IEEE.
Kumuda, D. P., Harshitha, B. V., & Manikya, K. (2025). A comprehensive review of AI-powered campus surveillance. ITM Web of Conferences, 81, 01017.
Liu, L. (2025). Application of deep learning in behavior recognition and early warning system for campus safety management. PLOS ONE, 20(11), e0256789.
Market.us. (2024). AI-powered video analytics market report 2024. Market.us.
Nagin, D. S. (2013). Deterrence in the twenty-first century: A review of the evidence. Crime and Justice in America: 1975-2025, 42(1), 83-105.
Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.