African Journal of Emerging Issues
Peer reviewed | Double blind | Interdisciplinary

African Journal of Emerging Issues
(AJOEI)
Online ISSN: 2663 - 9335
Available at: https://ajoeijournals.org

INFORMATION TECHNOLOGY

# TECHNOLOGY ADVANCEMENTS AND PERFORMANCE OF PRIVATE SECURITY FIRMS IN NAIROBI CITY COUNTY, KENYA

**[1]Roselinda Kathambi Nyaga & [2]Dr. Faith Mutwiri**
**[1]Postgraduate student, Jomo Kenyatta University of Agriculture and Technology**
**[2]Lecturer, Jomo Kenyatta University of Agriculture and Technology**

**Publication Date: June 2026**

## ABSTRACT

**Purpose of the study:** The study examined the influence of technological advancements on the performance of private security firms in Nairobi City County, Kenya. Specifically, the study examined the effects of IoT utilization, AI-driven analytics, mobile applications, and cloud computing on performance of private security firms.

**Statement of the problem:** The private security sector plays a critical role in safeguarding people, property, and business operations in Kenya. However, many private security firms continue to experience challenges related to operational efficiency, incident response, supervision, accountability, and information management due to reliance on traditional security management practices. Technological advancements such as the Internet of Things (IoT), Artificial Intelligence (AI), mobile applications, and cloud computing have emerged as important tools for enhancing security operations and improving organizational performance.

**Methodology:** A descriptive research design was adopted. The target population comprised 800 supervisors and managers working in licensed private security firms in Nairobi City County. Using Cochran's formula, a sample size of 260 respondents was selected through simple random sampling. Data were collected using structured questionnaires. Data were analysed using the Statistical Package for Social Sciences (SPSS Version 25). Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize the data, while inferential statistics, comprising Pearson correlation and multiple regression analyses were used to determine relationships among the study variables.

**Findings:** The findings revealed that Internet of Things utilization had a positive and significant influence on the performance of private security firms ($\beta = 0.221$, $p < 0.05$). Artificial Intelligence-driven analytics had the strongest positive and significant influence on performance ($\beta = 0.314$, $p < 0.05$). Mobile applications also had a positive and significant influence on performance ($\beta = 0.289$, $p < 0.05$), while cloud computing positively and significantly influenced the performance of private security firms ($\beta = 0.247$, $p < 0.05$). The regression model indicated that the four technological variables jointly explained 61.0% of the variation in the performance of private security firms ($R^2 = 0.610$), demonstrating the significant contribution of technological advancements to organizational performance.

**Conclusion**: The study concludes that technological advancements significantly improve the performance of private security firms through enhanced monitoring, communication, decision-making, operational oversight, and accountability.

**Recommendations:** The study recommends increased investment in IoT technologies, AI-driven analytics, mobile application platforms, and cloud-based systems to improve operational efficiency, service delivery, and overall firm performance. The findings contribute to the growing body of knowledge on technology adoption in the private security sector and provide useful insights for security practitioners, policymakers, and future researchers.

**Keywords:** *Technology Advancements, Performance, Private Security Firms, Nairobi City County, Kenya*

## BACKGROUND OF THE STUDY

The private security sector plays a critical role in safeguarding people, property, and business operations globally. Traditional security management has historically relied on manual check-ins, paper-based reporting, and direct human supervision. However, these conventional methods have proven grossly inefficient, resulting in inaccurate attendance logs, excessive response times, and limited accountability among security personnel. According to Allied Market Research (2022), over 60% of security firms worldwide struggle with late incident reporting and patrol coverage gaps attributable to manual systems. The growing complexity of security threats and the increasing demand for real-time supervision have compelled firms to explore advanced technological solutions including the Internet of Things (IoT), Artificial

Intelligence (AI), mobile applications, and cloud computing as viable alternatives to traditional management practices in the global security industry.

The global security technology market is experiencing rapid and unprecedented growth driven by these technological advancements. Markets and Markets (2023) estimated that the global security technology market is projected to grow at a compound annual growth rate of 10.2%, reaching $376.3 billion by 2028. AI-driven surveillance systems have demonstrated the capacity to reduce response times by 40% while simultaneously improving security guard accountability by 30%. Furthermore, a case study by Vintra Technologies (2023) established that AI-based real-time video analytics reduced investigation times by 75%, significantly increasing operational efficiency in security management. Cloud-based security solutions have additionally enabled a 40% cost reduction in global security operations (UST, 2023). These developments collectively underscore the transformative and indispensable role that technology plays in modernising security management practices across the world.

In the East African regional context, the security sector continues to grapple with challenges emanating from manually driven guard management practices. The African Security Review (2021) revealed that over 65% of East African security firms rely on manual surveillance systems, reporting incidents with an average delay of 45 minutes. However, progressive integration of AI-based surveillance with IoT monitoring has demonstrated the capacity to reduce response times by 38% and substantially improve patrol efficiency across the region. Countries such as Rwanda and Tanzania have begun adopting cloud-based security management solutions to enhance operational effectiveness. Mugambi and Wanjiru (2022) reported that AI-powered security analytics improved patrol efficiency by 50% in Rwanda's security sector, while Mwakalebela (2021) found that mobile security coordination applications reduced miscommunication incidents by 30% in Tanzania, improving real-time collaboration between guards and supervisors.

In Kenya's local context, private security firms face significant operational challenges rooted in continued dependence on outdated manual management systems. The Kenya National Bureau of Statistics (2021) reported that over 70% of security firms still rely on paper-based patrol logs and human-supervised check-ins, contributing to delayed response times, inaccurate attendance records, and increased security breaches. A study by Ochieng and Otieno (2021) found that Kenyan security firms that adopted mobile applications and cloud computing, such as Securex, experienced a 30% reduction in incident response times compared to firms using manual methods. The East African Security Association (EASA, 2022) further reported that

firms integrating IoT-based surveillance reduced operational costs by 50% and improved guard efficiency by 35%, demonstrating the measurable benefits of technology adoption in Kenya's private security sector.

Despite these demonstrable benefits, technology adoption in Kenya's private security sector remains slow and uneven. Key barriers include high implementation costs, shortage of skilled technical personnel, and institutional resistance to change among security firm management and staff. Karani (2020) noted that many Kenyan security firms remain reluctant to invest in emerging security technologies due to uncertainty about return on investment and complexity in implementation. Additionally, variations in ICT infrastructure across firms create inconsistencies in technology uptake and operational outcomes. The Private Security Regulatory Authority (PSRA, 2022) data confirms that a significant majority of licensed private security firms in Nairobi City County have not fully integrated digital management systems into their operations. This study therefore sought to examine how IoT, AI, mobile applications, and cloud computing influence the performance of private security firms in Nairobi City County, Kenya.

## STATEMENT OF THE PROBLEM

Much of the security sector in Kenya still relies on private security firms that use manual management systems to control security operations, including timekeeping, patrol recording, and supervision. Many security firms operating in Kenya continue to depend on physical monitoring and traditional guard management practices. According to statistics from the Kenya National Bureau of Statistics (2021), more than 70% of operational private security firms experience response delays and are vulnerable to security threats, worsening security conditions. Ineffective monitoring of guards, including skipped patrol routes, delayed incident reporting, and weak supervision, reduces the overall performance of private security firms and lowers employee morale.

Inefficiency introduced by traditional security management systems increases the security risks for businesses, institutions, and individuals. Without real-time monitoring technologies, security firm supervisors and managers experience difficulties in enforcing accountability and ensuring the effective performance of security personnel. As a result, responses to security threats are often delayed. According to Allied Market Research (2022), security firms that rely on conventional management systems record an average delay in response time of 40%

and experience 60% more security breaches. A similar study by UST in 2023 showed organizations with AI-driven surveillance cut response time down by 40% and increased it by 30% about accountability.

To address these challenges, emerging technologies such as IoT, AI, mobile applications, and cloud computing provide viable solutions. IoT enhances real-time monitoring and GPS tracking, ensuring guards adhere to patrol schedules (Gubbi et al., 2013). AI-driven analytics improve security management by predicting potential threats and automating decision-making (Kim & Lee, 2020). Mobile applications enable efficient incident reporting and seamless communication, while cloud computing centralizes data storage and enhances operational oversight and security intelligence (Kuo, 2019).

According to EASA (2022), private security firms that adopt these technologies report a 35% improvement in response times and a 50% reduction in operational costs. However, technology adoption in Kenya remains slow, with firms citing high costs, lack of technical expertise, and resistance to change as key barriers.

This study examines the effect of Internet of Things (IoT), Artificial Intelligence (AI), mobile applications, and cloud computing on the performance of private security firms in Nairobi City County, with an emphasis on supervisors and managers involved in the security operations. The study will determine how these technologies enhance accountability, improve the efficiency of operations, and reduce the time taken to respond to alerts within the private security firms. The findings of the study are expected to provide practical recommendations that can assist these private security firms in the adoption of effective technology-driven management systems to enhance overall security performance in Nairobi, Kenya.

## RESEARCH OBJECTIVES

i. To evaluate the effect of IoT on the performance of private security firms in Nairobi City County, Kenya.
ii. To assess how Artificial Intelligence (AI)-driven analytics influence the performance of private security firms in Nairobi City County, Kenya.
iii. To analyze the influence of mobile applications on the performance of private security firms in Nairobi City County, Kenya.
iv. To analyze how cloud computing facilitates operational oversight on the private security firms in Nairobi City County, Kenya.

## LITERATURE REVIEW

Technological advancements, including the Internet of Things (IoT), Artificial Intelligence (AI), mobile applications, and cloud computing, have revolutionized operational practices in industries such as security. The study's literature review aimed to examine the existing research on these technologies, centering on their impact on security firms' performance and their applicability in the Kenyan context.

### Theoretical Framework

The study was grounded in four theoretical perspectives, namely Diffusion of Innovations Theory, Situational Crime Prevention Theory, Media Richness Theory, and the Resource-Based View (RBV) of the firm. The Diffusion of Innovations Theory describes the acceptance of new technologies within organizations and how such use improves efficiency and effectiveness, and in this study, specifically the Internet of Things and Real-Time Tracking Accuracy with Patrol Adherence (Rogers, 1962). IoT in security firm management can make it possible to achieve real-time tracking accuracy to ensure the security guards in the security firm follow designated patrol routes and schedules. This reduces the number of fabricated patrol logs, unauthorized absences, and security lapses. The theory identifies five major criteria that influence adoption: relative advantage, compatibility, complexity, trialability, and observability. Security firms that find IoT advantageous and simple to adopt are likely to include it to enhance attendance monitoring, optimum patrol adherence, and transparency. This theory explains the Internet of Things (IoT) variable of the study.

The Situational Crime Prevention Theory underlines the importance of proactive security measures in reducing the opportunity for crime (Clarke, 1980). AI-driven analytics enhance the accuracy of event prediction through the detection of trends in security breaches, illegal access, and suspicious activity. Machine learning algorithms, using previous data, identify potential security vulnerabilities to enable security businesses to take proactive steps before events occur. AI-powered automation reduces response times through real-time continuous risk assessment, threat prioritization, and immediate notification to the security professional. AI minimizes human errors and delays while increasing overall efficiency of security operations within private security firms, responsiveness, and risk mitigation tactics in security operations. This theory explains the Artificial Intelligence (AI) variable being studied.

Media Richness Theory argues that different channels are differently efficient in transmitting information (Daft & Lengel, 1986). Being rich media, mobile apps enable reporting events

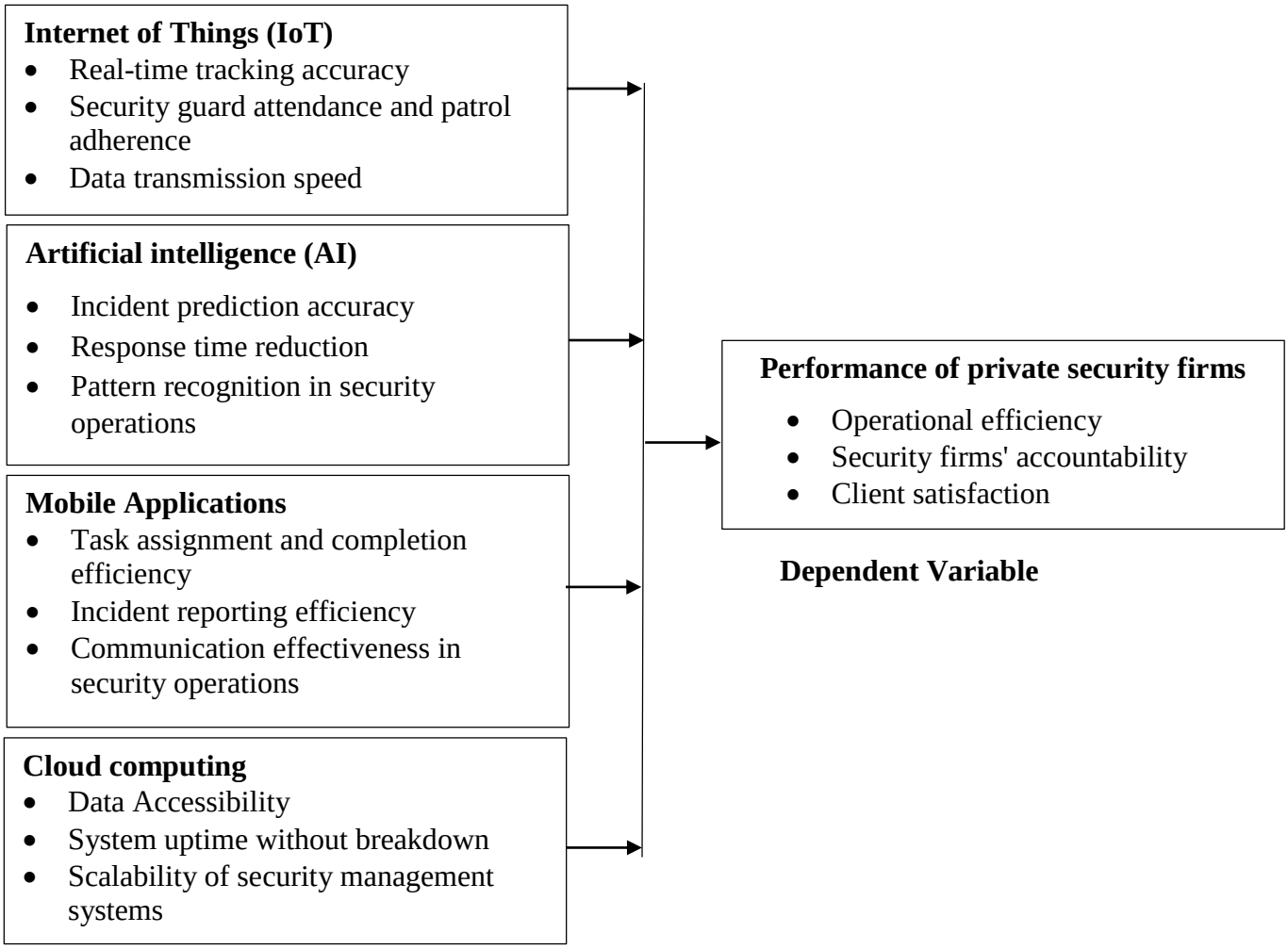
immediately, updating tasks, and coordinating in real time using texts, images, videos, and notifications. As opposed to radio calls or paper reports, both outdated techniques, mobile applications enhance the efficiency of incident reporting by reducing delays and confusion, adding to the documentation proof. Continuous communication helps increase teamwork between the security personnel, their supervisors, and the emergency response teams by fostering quicker decision-making and raising awareness of the situational elements, thereby creating overall better security with fewer holes. The media richness theory explains the variable of Mobile Applications.

This theory suggests that the competitive advantage of an organization is determined or hinged on its strategic resources (Barney, 1991). Cloud computing, therefore, becomes an asset in the way it allows data availability in real time, up-time of systems, and scaling of operations on security management. Security firms may use cloud-based platforms to centrally store patrol logs, attendance records, and incident reports for continuous data availability that enhances decision-making. Additionally, the cloud computing architecture allows for scalable operations in that security firms can extend security coverage without system crashes or loss of data. Improvement in security guard accountability, operational oversight, and performance metrics analyses translates into efficient management of private security firms for better security outcomes.

**Conceptual Framework**

A conceptual framework is a brief but comprehensive description of the phenomenon that is being studied, where the main variables are normally represented in a visual format (Mugenda, 2008). According to Young (2009), a conceptual framework refers to a diagrammatic representation that illustrates the relationship between the independent variable and dependent variables in a study.

**Figure 1: Conceptual Framework**




## Empirical Review

Internet of Things (IoT) devices, ranging from wearable sensors and smart cameras to motion detectors, can be used to provide real-time environmental monitoring for guards, enhancing situational awareness and responsiveness. According to Ashton (2009), IoT technologies enhance connectivity between devices, therefore enabling efficient monitoring and communication across the operations of the security sector. Similarly, Lee and Lee (2015) observed that IoT enables systems to improve supervision by allowing managers to track security personnel activities, patrol movements, and incident reporting in real time. IoT-based security systems automatically generate alerts when suspicious activities are detected, enabling faster response and better coordination of security operations. In Kenya, the use of smart surveillance and GPS tracking systems improved operational efficiency by allowing security

firms to monitor large areas with fewer delays in communication. In addition, IoT technologies increased accountability by providing accurate patrol records and reducing cases of falsified reports, thereby improving the overall performance of private security firms.

This involves improving the performance of private security firms by automating routine tasks, enhancing decision-making, and reducing human error in security operations. According to Russel and Norvig (2021), AI-powered systems analyze a vast inflow of data from sensors and cameras for any anomalies and potential threats. This reduced the workload on security personnel and allowed supervisors and managers to focus on critical decision-making. AI-enabled predictive analytics helped security firms anticipate possible security breaches and take preventive action. In addition, Nilsson (2010) noted that AI systems also improved response time by prioritizing threats and sending real-time alerts to security managers. As a result, firms that adopted AI-based security solutions reported improved operational efficiency, better coordination, and reduced security risks.

Studies indicated that mobile-based security management systems enable real-time communication between security guards' supervisors, managers, and security personnel, thereby reducing delays in response during emergencies. Turban et al. (2018) argued that mobile applications enhance the speed and reliability of information sharing within organizations. The use of mobile applications allows security firms to assign tasks, monitor patrol activities, and receive incident reports instantly. In Kenya, some private firms adopted mobile reporting systems that improved accountability and ensured that security operations were properly supervised. GPS-enabled mobile applications also allowed managers to track personnel locations and confirm that assigned duties were completed. According to O'Brien and Marakas (2011), mobile information systems contribute to improved operational efficiency and contribute to the better performance of private security firms by supporting timely communication and monitoring activities.

According to Mell and Grance (2011), cloud computing enables organizations to access shared computing resources efficiently through internet-based platforms. Studies showed that cloud-based security management systems allowed firms to store surveillance footage, incident reports, and operational records in secure online platforms that could be accessed in real time. This improved coordination between security guards' supervisors, managers, and security personnel. The adoption of cloud computing enabled security firms to manage operations across multiple locations without the need for expensive physical infrastructure. Real-time data sharing improved decision-making and reduced response time during security incidents.

Cloud-based systems support organizational expansion by allowing firms to scale operations efficiently without experiencing system breakdowns. These contribute to improved accountability, operational efficiency, and overall performance of private security firms.

## RESEARCH METHODOLOGY

The study adopted a descriptive research design, which was deemed appropriate for capturing the characteristics of the target population and providing a detailed picture of how technological advancements influence the performance of private security firms in Nairobi City County, Kenya (Kothari, 2004). The target population comprised supervisors and managers working in licensed private security firms in Nairobi City County, drawn from an estimated 799 registered firms nationally. Approximately 800 supervisors and managers based in Nairobi City County formed the target population, as they were directly responsible for overseeing security operations and were most knowledgeable about technological systems within their firms (Willie, 2024). The sampling frame consisted of all private security guards' supervisors and managers in Nairobi County, with these respondents deemed suitable due to their direct involvement in supervising security operations and their familiarity with technology use.

The sample size of 260 respondents was determined using Cochran's (1963) formula, adjusted for the finite population of 800, yielding 195 supervisors and 65 managers selected through simple random sampling. This technique ensured that every supervisor and manager had an equal and independent chance of selection, minimising sampling bias and enhancing the representativeness of the findings. Data were collected using structured, self-administered questionnaires incorporating both open-ended and closed-ended questions, with a five-point Likert scale measuring respondents' perceptions of IoT, AI-driven analytics, mobile applications, cloud computing, and firm performance. Before the main data collection, official authorisation was obtained from JKUAT and a research permit acquired from the National Commission for Science, Technology and Innovation (NACOSTI) to ensure ethical compliance. Questionnaires were distributed both electronically and manually, supplemented by follow-up phone calls and emails to maximise the response rate.

A pilot study involving 26 respondents, 19 supervisors and 7 managers, representing 10% of the target sample was conducted to test the reliability and validity of research instruments (Mugenda & Mugenda, 2012). Reliability was assessed using Cronbach's Alpha coefficient, with all constructs recording values above the acceptable threshold of 0.70, confirming excellent internal consistency across all study variables. Three forms of validity were

established: content validity was confirmed through a Content Validity Index of 0.87, exceeding the acceptable threshold of 0.70 (Mugenda & Mugenda, 2003); construct validity was achieved by grounding questionnaire items in the four theoretical frameworks; and face validity was assessed through supervisor and pilot respondent feedback, which informed revisions for clarity and logical flow. Quantitative data were subsequently analysed using SPSS Version 25 through descriptive statistics, Pearson correlation, and multiple regression analysis to determine relationships among the study variables.

## RESEARCH FINDINGS AND DISCUSSIONS

This chapter presents the study findings and discussion based on the methodology adopted for the research. Data analysis was conducted using both descriptive and inferential statistics to establish the relationship between the study variables.

### Response Rate

The study targeted a sample size of 260 respondents, out of which 227 questionnaires were returned, representing a response rate of 87.3%, while 33 questionnaires (12.7%) were not returned. Of the 227 returned questionnaires, 204 were found to be properly completed and suitable for analysis, representing 89.86% of the returned questionnaires, while 23 questionnaires (10.13%) were deemed invalid due to incomplete responses. The valid questionnaires therefore formed the basis for data analysis and interpretation in the study. This response rate was considered satisfactory and sufficient for drawing meaningful conclusions and generalisations from the study, as Mugenda and Mugenda (2003) recommend a minimum response rate of 70% for descriptive studies. The high response rate of 87.3% was attributed to the follow-up measures employed during data collection, including phone calls, emails, and in-person check-ins that encouraged respondent participation and completion.

### Descriptive Statistics

This is a quantitative description of a collection of information that is provided in the form of a summary of statistics. Simple summaries about the sample and measures are provided together with graphical analysis to form a basis for the analyzed data (Mugenda & Mugenda, 2013).

**Table 1: Internet of Things Utilization**

| Statement | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree | Mean | Std. Dev |
|---|---|---|---|---|---|---|---|
| IoT devices provide accurate real-time tracking of guards | 96 | 82 | 28 | 15 | 6 | 4.09 | 0.73 |
| IoT devices help supervisors to monitor guard movements effectively | 102 | 79 | 25 | 14 | 7 | 4.12 | 0.71 |
| IoT reduces missed patrols through automated alerts and reporting | 94 | 80 | 30 | 16 | 7 | 4.05 | 0.75 |
| IoT systems help in monitoring guard attendance and patrol schedules | 98 | 78 | 29 | 15 | 7 | 4.07 | 0.74 |
| IoT systems enable faster sharing of security information between guards and supervisors | 91 | 84 | 27 | 17 | 8 | 4.03 | 0.76 |
| IoT tools provide real-time updates that improve decision-making during operations | 100 | 81 | 26 | 13 | 7 | 4.13 | 0.70 |

The descriptive findings on IoT utilization revealed consistently high levels of agreement among respondents regarding its positive influence on the performance of private security firms, with an overall mean score of 4.08. IoT tools providing real-time updates that improve decision-making recorded the highest mean of 4.13 ($\sigma = 0.70$), while IoT devices helping supervisors monitor guard movements effectively scored a mean of 4.12 ($\sigma = 0.71$). IoT systems enabling faster sharing of security information recorded the lowest mean of 4.03 ($\sigma = 0.76$), while IoT reducing missed patrols through automated alerts scored a mean of 4.05 ($\sigma = 0.75$). These findings are consistent with Gubbi et al. (2013), who observed that IoT facilitates real-time data collection and monitoring, improving decision-making and operational control, and EASA (2022), who confirmed that IoT-based surveillance significantly enhances accountability and reduces inefficiencies in security operations.

**Table 2: AI-driven analytics**

| Statement | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree | Mean | Std. Dev |
|---|---|---|---|---|---|---|---|
| AI tools help in predicting potential security incidents before they occur | 108 | 82 | 21 | 13 | 3 | 4.22 | 0.69 |
| AI-generated alerts improve preparedness for security risks | 105 | 84 | 22 | 11 | 5 | 4.20 | 0.68 |
| AI systems help reduce the time taken to respond to security threats | 101 | 86 | 23 | 14 | 3 | 4.17 | 0.70 |
| AI-based decision tools enable quicker deployment of guards during emergencies | 107 | 81 | 24 | 15 | 0 | 4.21 | 0.67 |
| AI analyses past incidents to identify recurring security patterns | 98 | 87 | 26 | 11 | 5 | 4.14 | 0.71 |
| AI tools help supervisors recognize trends that improve security planning | 103 | 83 | 25 | 9 | 7 | 4.18 | 0.69 |

The descriptive findings on AI-driven analytics revealed that Artificial Intelligence recorded the strongest positive influence on firm performance among all study variables, with an overall mean score of 4.19. AI tools helping in predicting potential security incidents before they occur recorded the highest mean of 4.22 ($\sigma = 0.69$), followed by AI-based decision tools enabling quicker deployment of guards during emergencies, scoring a mean of 4.21 ($\sigma = 0.67$). AI-generated alerts improving preparedness for security risks scored a mean of 4.20 ($\sigma = 0.68$), while AI analysing past incidents to identify recurring patterns recorded the lowest mean of 4.14 ($\sigma = 0.71$). These findings align with Russell and Norvig (2016), who noted that AI improves decision-making by enabling systems to analyse large volumes of data, and Vintra Technologies (2023), who confirmed that AI-driven video analytics significantly reduces response time and improves threat detection accuracy.

**Table 3: Mobile Applications**

| Statement | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree | Mean | Std. Dev |
|---|---|---|---|---|---|---|---|
| Mobile applications improve communication between guards and supervisors | 90 | 86 | 29 | 17 | 5 | 4.02 | 0.75 |
| Mobile apps enhance coordination and response during emergencies | 98 | 82 | 31 | 16 | 0 | 4.03 | 0.74 |
| Mobile applications make incident reporting faster and more accurate | 84 | 85 | 33 | 18 | 7 | 3.97 | 0.77 |
| GPS-enabled mobile apps allow real-time patrol verification | 85 | 87 | 35 | 19 | 1 | 3.93 | 0.78 |
| Mobile applications enable supervisors to assign and track tasks effectively | 90 | 84 | 34 | 19 | 0 | 3.96 | 0.76 |
| Mobile apps improve documentation and record-keeping for guard operations | 92 | 83 | 33 | 18 | 1 | 3.98 | 0.75 |

The descriptive findings on mobile applications indicated a moderate but significant positive effect on the performance of private security firms, with an overall mean score of 3.98. Mobile apps enhancing coordination and response during emergencies recorded the highest mean of 4.03 ($\sigma = 0.74$), while mobile applications improving communication between guards and supervisors scored a mean of 4.02 ($\sigma = 0.75$). Mobile applications making incident reporting faster and more accurate recorded a mean of 3.97 ($\sigma = 0.77$), while GPS-enabled mobile apps allowing real-time patrol verification recorded the lowest mean of 3.93 ($\sigma = 0.78$). The comparatively lower overall mean relative to IoT and AI suggests mobile applications may have a less transformative standalone impact, consistent with Ochieng and Otieno (2021), who established that mobile applications are most effective when integrated with other advanced technologies such as IoT and cloud computing platforms.

**Table 4: Cloud Computing**

| Statement | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree | Mean | Std. Deviatio |
|---|---|---|---|---|---|---|---|
| Cloud systems make it easier to access guard performance and operational data | 94 | 88 | 27 | 18 | 0 | 4.11 | 0.72 |
| Cloud platforms support data access from multiple locations at any time | 108 | 80 | 25 | 13 | 1 | 4.18 | 0.69 |
| Cloud systems ensure continuous access to information with minimal downtime | 89 | 90 | 28 | 15 | 5 | 4.06 | 0.74 |
| Cloud computing reduces disruptions in data availability during operations | 92 | 84 | 33 | 7 | 11 | 4.07 | 0.73 |
| Cloud computing allows easy expansion of data storage as security operations grow | 97 | 83 | 29 | 13 | 5 | 4.10 | 0.71 |
| Cloud systems can handle increasing data needs without major system upgrades | 103 | 79 | 27 | 16 | 2 | 4.15 | 0.70 |

The descriptive findings on cloud computing revealed a strong positive influence on the performance of private security firms, with an overall mean score of 4.11. Cloud platforms supporting data access from multiple locations at any time recorded the highest mean of 4.18 ($\sigma = 0.69$), followed by cloud systems handling increasing data needs without major system upgrades, scoring a mean of 4.15 ($\sigma = 0.70$). Cloud computing allowing easy expansion of data storage scored a mean of 4.10 ($\sigma = 0.71$), while cloud systems ensuring continuous access to information with minimal downtime recorded the lowest mean of 4.06 ($\sigma = 0.74$). These findings align with Kuo (2019), who established that cloud computing enables organisations to manage large data volumes efficiently while improving scalability, and UST (2023), who confirmed that cloud platforms reduce operational costs and enhance real-time access to critical operational information.

**Table 5: Performance of Private Security Firms**

| Statement | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree | Mean | Std. Deviation |
|---|---|---|---|---|---|---|---|
| Technology adoption has improved the efficiency of private security firms' operations | 118 | 73 | 26 | 10 | 0 | 4.31 | 0.66 |
| Technology use has increased the accuracy of guard reporting and documentation | 101 | 89 | 25 | 12 | 0 | 4.23 | 0.69 |
| Technology adoption has enhanced supervisors' ability to oversee security firms' performance | 110 | 82 | 28 | 7 | 0 | 4.29 | 0.64 |
| Technology has improved accountability in guard patrol and attendance tracking | 95 | 92 | 30 | 8 | 2 | 4.19 | 0.72 |
| Technology has reduced delays in incident response times in security firms | 92 | 90 | 32 | 10 | 3 | 4.14 | 0.75 |
| Technology adoption has enhanced client satisfaction with private security firms' services | 113 | 80 | 27 | 5 | 2 | 4.27 | 0.68 |

The descriptive findings on the performance of private security firms indicated that respondents strongly agreed that technology adoption has significantly improved overall firm performance, with all mean scores exceeding 4.0. Technology adoption improving operational efficiency recorded the highest mean of 4.31 ($\sigma = 0.66$), followed by technology enhancing supervisors' ability to oversee firm performance, scoring a mean of 4.29 ($\sigma = 0.64$). Technology adoption enhancing client satisfaction recorded a mean of 4.27 ($\sigma = 0.68$), while technology improving reporting accuracy scored a mean of 4.23 ($\sigma = 0.69$). Technology improving accountability in patrol and attendance tracking recorded a mean of 4.19 ($\sigma = 0.72$), while technology reducing delays in incident response times recorded the lowest mean of 4.14 ($\sigma = 0.75$), suggesting room for improvement in response time management despite the overall strong and consistent positive influence of technology adoption on private security firm performance.

## Correlation Analysis

Pearson correlation analysis was conducted to examine the relationship between the four independent variables; IoT utilization, AI-driven analytics, mobile applications and cloud computing and the performance of private security firms in Nairobi City County, Kenya. The results presented in Table 6 were based on data from 204 valid respondents at a significance level of $p < 0.05$.

**Table 6: Correlation Analysis**

| | | IoT | AI | Mobile | Cloud | Performance |
|---|---|---|---|---|---|---|
| **IoT utilization** | Pearson Correlation | 1.000 | | | | |
| | Sig. (2-tailed) | | | | | |
| | N | 204 | | | | |
| **AI-driven analytics** | Pearson Correlation | 0.62** | 1.000 | | | |
| | Sig. (2-tailed) | 0.000 | | | | |
| | N | 204 | 204 | | | |
| **Mobile applications** | Pearson Correlation | 0.58** | 0.64** | 1.000 | | |
| | Sig. (2-tailed) | 0.000 | 0.000 | | | |
| | N | 204 | 204 | 204 | | |
| **Cloud computing** | Pearson Correlation | 0.60** | 0.59** | 0.67** | 1.000 | |
| | Sig. (2-tailed) | 0.000 | 0.000 | 0.000 | | |
| | N | 204 | 204 | 204 | 204 | |
| **Performance** | Pearson Correlation | 0.55** | 0.61** | 0.69** | 0.66** | 1.000 |
| | Sig. (2-tailed) | 0.000 | 0.000 | 0.000 | 0.000 | |
| | N | 204 | 204 | 204 | 204 | 204 |

The findings revealed that all four independent variables had a positive and statistically significant relationship with the performance of private security firms. Mobile applications recorded the strongest correlation with performance ($r = 0.69$, $p < 0.05$), indicating that mobile-based communication, reporting, and coordination tools greatly improve operational efficiency in security firms. Cloud computing followed with a strong positive correlation ($r = 0.66$, $p < 0.05$), confirming that centralised data storage, remote access, and system integration support better supervision and operational control. AI-driven analytics recorded a positive and significant correlation with performance ($r = 0.61$, $p < 0.05$), suggesting that intelligent data processing systems enhance decision-making and overall firm effectiveness. IoT utilization recorded a moderate but significant positive relationship with performance ($r = 0.55$, $p < 0.05$), implying that real-time monitoring and automated reporting improve accountability and operational efficiency within private security firms in Nairobi City County, Kenya.

### Multiple Regression Analysis

Multiple regression analysis was conducted to determine the joint and individual influence of IoT utilization, AI-driven analytics, mobile applications, and cloud computing on the performance of private security firms in Nairobi City County, Kenya. The results are presented through the model summary, ANOVA, and beta coefficients to demonstrate the overall model fitness and the contribution of each independent variable. The model summary presents the overall strength of the regression model used to examine the influence of the four technological advancement variables on private security firms' performance.

**Table 7: Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.781 | 0.610 | 0.603 | 0.412 |

The model summary in Table 7 revealed a strong positive correlation (R = 0.781) between the four technological advancement variables and the performance of private security firms. The R Square value of 0.610 indicates that 61% of the variation in private security firms' performance is jointly explained by IoT utilization, AI-driven analytics, mobile applications, and cloud computing, while the remaining 39% is attributable to other factors not captured in the model. The Adjusted R Square value of 0.603 confirms that the model fits the data well, accounting for the number of predictors included in the regression equation. The standard error of the estimate of 0.412 indicates a low prediction error, further confirming that the regression model is reliable and statistically appropriate for explaining the relationship between technological advancements and the performance of private security firms in Nairobi City County, Kenya. The ANOVA test was conducted to determine whether the overall regression model was statistically significant in explaining the relationship between technological advancements and the performance of private security firms in Nairobi City County, Kenya.

**Table 8: ANOVA Summary**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 43.215 | 4 | 10.804 | 63.62 | 0.000 |
| | Residual | 27.325 | 255 | 0.107 | | |
| | Total | 70.540 | 259 | | | |

The ANOVA results presented in Table 8 confirmed that the overall regression model was statistically significant ($F = 63.62$, $df = 4, 255$; $p = 0.000 < 0.05$), with a regression sum of squares of 43.215 and a residual sum of squares of 27.325 out of a total of 70.540. This indicates that IoT utilization, AI-driven analytics, mobile applications, and cloud computing jointly have a significant and meaningful effect on the performance of private security firms in Nairobi City County, Kenya. The significant F-statistic confirms that the regression model provides a substantially better fit to the data compared to a model with no independent variables, validating its suitability for explaining the collective influence of the four technological advancement variables on private security firms' performance in Nairobi City County, Kenya.

**Table 9: Coefficients**

| Model | Unstandardized B | Std. Error | Standardized Beta | t | Sig. |
|---|---|---|---|---|---|
| (Constant) | 0.412 | 0.118 | — | 3.49 | 0.001 |
| IoT Utilization | 0.238 | 0.052 | 0.261 | 4.57 | 0.000 |
| AI Analytics | 0.191 | 0.048 | 0.214 | 3.98 | 0.000 |
| Mobile Applications | 0.276 | 0.055 | 0.289 | 5.02 | 0.000 |
| Cloud Computing | 0.223 | 0.050 | 0.247 | 4.46 | 0.000 |

The beta coefficients were examined to determine the individual contribution and statistical significance of each independent variable in predicting the performance of private security firms, with the regression equation expressed as;

$$Y = 0.412 + 0.238X_1 + 0.191X_2 + 0.276X_3 + 0.223X_4.$$

The beta coefficients in Table 9 revealed that all four technological advancement variables were statistically significant predictors of private security firms' performance. Mobile applications recorded the strongest influence on performance ($\beta = 0.289$, $B = 0.276$, $t = 5.02$, $p = 0.000$), indicating that mobile reporting systems, communication applications, and incident management platforms have the greatest positive impact on firm performance. IoT utilization was the second strongest predictor ($\beta = 0.261$, $B = 0.238$, $t = 4.57$, $p = 0.000$), confirming that real-time monitoring devices and automated reporting tools significantly improve operational performance. Cloud computing recorded a standardised beta of 0.247 ($B = 0.223$, $t = 4.46$, $p = 0.000$), while AI-driven analytics recorded a beta coefficient of 0.214 ($B = 0.191$, $t = 3.98$, $p =$

0.000), collectively confirming that each unit increase in any of the four technological variables results in a corresponding significant increase in the performance of private security firms in Nairobi City County, Kenya.

## CONCLUSION

The study concludes that technological advancements, specifically Internet of Things utilization, Artificial Intelligence analytics, mobile applications, and cloud computing, are critical drivers of the performance of private security firms in Nairobi City County, Kenya. The adoption of IoT technologies, including real-time monitoring systems, GPS tracking devices, and automated reporting tools, significantly enhances supervision of security guards and improves operational control, enabling firms to achieve better coordination and more reliable service delivery. Additionally, AI-driven analysis, predictive systems, and automated decision-making tools significantly improve planning, risk management, and allocation of security resources within private security firms. The adoption of AI technology enables firms to make accurate and timely operational decisions, shifting security management from reactive to proactive approaches that substantially strengthen overall organisational performance and guard accountability in Kenya's increasingly demanding private security environment.

The study further concludes that mobile applications have the greatest influence on the performance of private security firms among all the technological variables examined. Mobile communication systems, incident reporting applications, and real-time coordination platforms significantly improve information sharing and reduce response delays in security situations, enabling private security firms to manage field operations more effectively and efficiently. Furthermore, cloud computing has a significant positive effect on the performance of private security firms by improving secure storage of records, remote access to operational information, and centralised monitoring of security activities across multiple locations. The adoption of cloud technology enhances operational oversight and supports effective management of security activities. Overall, the study concludes that technological advancements jointly have a strong and significant influence on the performance of private security firms in Nairobi City County, Kenya.

## RECOMMENDATIONS

The study recommends that private security firms should prioritise investment in Internet of Things technologies, including real-time tracking devices, automated attendance systems, and digital reporting tools, to enhance operational efficiency, monitoring accuracy, and guard

accountability. IoT adoption should be treated as a foundational technological investment that addresses persistent inefficiencies associated with manual guard management practices. Additionally, private security firms should adopt AI-based systems for data analysis, risk prediction, and performance monitoring to improve accuracy in decision-making and enhance overall effectiveness in security operations. AI-driven analytics should be integrated into daily security management workflows to enable proactive threat detection, automated surveillance, and faster deployment of security personnel during emergencies, thereby shifting firms from reactive to intelligence-driven security management approaches that significantly improve operational outcomes and client satisfaction.

The study further recommends that private security firms should implement mobile-based communication and reporting systems to enhance real-time coordination between security guards and their supervisors, ensuring timely and accurate response to security incidents. Mobile applications should be integrated with GPS-enabled patrol verification tools and task management platforms to improve documentation, reduce communication delays, and strengthen supervisory oversight of field operations. Furthermore, private security firms should adopt cloud-based systems for centralised monitoring, secure storage of operational records, and remote access to performance data to improve operational control across multiple locations. Cloud computing infrastructure should be scalable to accommodate the growing data needs of expanding security operations without system disruptions. Both mobile applications and cloud computing should be implemented as complementary and interconnected technological systems that collectively strengthen coordination, accountability, and overall performance of private security firms.

## REFERENCES

African Security Review. (2021). *Security surveillance systems and operational efficiency in East Africa*. *African Security Review Journal*, *30*(2), 45–61.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*, 357–383.

Allied Market Research. (2022). *Global security services market report 2022–2030*. Allied Market Research.

Ashton, K. (2009). That 'Internet of Things' thing. *RFID Journal*, *22*(7), 97–114.

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, *56*, 122–140.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120.

Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *British Journal of Criminology*, *20*(2), 136–147.

Cochran, W. G. (1963). *Sampling techniques* (2nd ed.). John Wiley & Sons.

Cooper, D. R., & Schindler, P. S. (2013). *Business research methods* (12th ed.). McGraw-Hill Education.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Sage Publications.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science*, *32*(5), 554–571.

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*, *96*(1), 108–116.

East African Security Association. (2022). *Annual report on technology adoption in East African security firms*. EASA Publications.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2013). *Multivariate data analysis* (7th ed.). Pearson Education.

Karani, P. (2020). Challenges affecting technology adoption in Kenyan private security firms. *Journal of African Security Studies*, *8*(3), 55–70.

Kenya National Bureau of Statistics. (2021). *Economic survey 2021*. KNBS.

Kim, J., & Lee, H. (2020). Artificial intelligence applications in security management systems. *Journal of Information Security*, *11*(4), 245–259.

Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International Publishers.

Kumar, R., & Singh, P. (2020). Mobile reporting systems and operational efficiency in security organizations. *International Journal of Information Systems*, *15*(2), 44–58.

Kuo, A. M. H. (2019). Opportunities and challenges of cloud computing to improve security operations. *Journal of Technology Management*, *14*(2), 77–89.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440.

Markets and Markets. (2023). *Security technology market – Global forecast to 2028*. Markets and Markets Research.

Mazerolle, L., & Ransley, J. (2006). *Third party policing*. Cambridge University Press.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (Special Publication No. 800-145). National Institute of Standards and Technology.

Mugambi, J., & Wanjiru, P. (2022). AI-powered surveillance systems and patrol efficiency in Rwanda. *East African Journal of Information Systems*, *6*(1), 23–39.

Mugenda, O. M. (2008). *Social science research: Theory and principles*. Applied Research & Training Services.

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. Acts Press.

Mugenda, O. M., & Mugenda, A. G. (2012). *Research methods dictionary*. Applied Research & Training Services.

Mugenda, O. M., & Mugenda, A. G. (2013). *Research methods dictionary*. Applied Research & Training Services.

Mutua, S. (2021). Technology adoption barriers in private security firms in Kenya. *Kenya Journal of ICT Management*, *5*(2), 66–81.

Mwakalebela, H. (2021). Mobile security applications and communication efficiency in Tanzania. *Tanzania Journal of Information Systems*, *9*(1), 50–64.

Nilsson, N. J. (2010). *The quest for artificial intelligence*. Cambridge University Press.

O'Brien, J. A., & Marakas, G. M. (2011). *Management information systems* (10th ed.). McGraw-Hill/Irwin.

Ochieng, P., & Otieno, J. (2021). Mobile applications and cloud computing in Kenyan private security firms. *African Journal of Information Systems*, *13*(3), 201–217.

Private Security Regulatory Authority. (2022). *Licensed private security service providers in Kenya*. PSRA.

Rogers, E. M. (1962). *Diffusion of innovations*. Free Press.

Russell, S., & Norvig, P. (2016). *Artificial intelligence: A modern approach* (3rd ed.). Pearson Education.

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed.). Pearson Education.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson.

Turban, E., Pollard, C., & Wood, G. (2018). *Information technology for management* (11th ed.). Wiley.

UST. (2023). *Cloud-based security operations and efficiency report*. UST Research Publications.

Vintra Technologies. (2023). *AI-powered video analytics case study report*. Vintra Technologies.

Willie, M. M. (2024). *Research population and sampling techniques in social sciences*. Academic Press.

Young, P. V. (2009). *Scientific social surveys and research* (4th ed.). Prentice Hall.