Original Article

CARL ADVANCE MULTIDISCIPLINARY
https://cartcarl.com/journal/carl-advance-multidisciplinary

E-ISSN: 3043-6583

Closed-Circuit Television (CCTV) as a Mitigation Measure Against Misappropriation and Fraud in Selected Government Agencies in Rivers State (2013–2018)

Authors
Onyerimma, L. A., Martin I. I., Daisy, C. O.

Department of Sociology, Faculty of Social Science, University of Port Harcourt, Nigeria

Corresponding Author
Onyerimma, L. A.
(onyerimma_leonard@uniport.edu.ng)

Received: 02 October 2025
Accepted: 31 October 2025
Published: 03 November 2025

Citation
Onyerimma, L. A., Martin I. I. & Daisy, C. O. (2025). Closed-Circuit Television (CCTV) as a Mitigation Measure Against Misappropriation and Fraud in Selected Government Agencies in Rivers State (2013–2018). *Carl Advance Multidisciplinary*, 2(1), 54-64. https://doi.org/10.70726/cam.2025.215464

Abstract

This study investigates the effectiveness of Closed-Circuit Television (CCTV) as a mitigation measure against misappropriation and fraud in selected government agencies in Rivers State, Nigeria. Despite increased investments in surveillance systems across public offices, cases of financial mismanagement, asset diversion, and procedural manipulation remain prevalent. The research adopts a descriptive survey design supported by qualitative insights to assess how CCTV installations influence accountability and transparency in public service operations. A total of 400 respondents were selected using stratified random sampling from staff across five government agencies, including finance, procurement, works, and administrative departments. Primary data were collected through structured questionnaires, key informant interviews, and observation checklists, while secondary data were drawn from audit and administrative records. Descriptive statistics such as frequency and percentage distributions were used to summarize the data, while inferential analyses including chi-square and regression tests were applied to determine the relationship between CCTV usage and incidents of misappropriation and fraud. Findings are expected to reveal that effective CCTV deployment, continuous monitoring, and clear data management policies significantly reduce the occurrence and concealment of fraudulent practices within government offices. However, technical challenges, inadequate maintenance, weak enforcement of surveillance policies, and limited staff awareness were identified as major constraints. The study concludes that CCTV systems, when properly implemented and integrated with institutional accountability frameworks, can serve as a vital tool for enhancing transparency and curbing financial malpractice in the public sector. It recommends continuous training of monitoring personnel, periodic evaluation of surveillance coverage, and stricter policy enforcement to ensure sustainable use of CCTV technology in safeguarding public resources.

Keywords: CCTV, Misappropriation, Fraud, Surveillance, Accountability, Government Agencies, Rivers State

Introduction

Fraud within government offices has resulted in massive economic damage particularly in areas that are not well supervised. Fraud may occur in any social system, be it complex or simple should there be no monitoring of institutions. This unregulated state of affairs provides individuals opportunities to abuse the system in order to make money at the expense of development, responsibility, and trust (Owie and Eshemogie, 2023). In the Niger Delta, particularly, Rivers State, fraud in government services channels funds that should be spent in education, health, roads and welfare in the wrong hands in personal accounts and unauthorized projects that shatters service delivery and damages equitable development. The citizens were victims of the poor services, declining infrastructure and reduced social safety (Economic and Financial Crimes Commission [EFCC], 2018).

Government agencies in Rivers State have invested in CCTV and other security technologies, yet reports and audit findings still reveal instances of misappropriation and fraud. It is unclear to what extent CCTV installations deter or detect financial and asset-related wrongdoing, how CCTV data are managed and used for accountability, and what operational or policy gaps limit their effectiveness. Without systematic assessment, funds may be wasted on ineffective CCTV deployments and agencies remain vulnerable to continued financial malpractice.

Misappropriation of funds and fraud remain persistent problems across public sector organizations in many jurisdictions. Surveillance technologies such as CCTV are widely adopted in private and public sectors to deter and detect wrongdoing, improve transparency, and support investigations. However, CCTV effectiveness depends not only on installation but on strategic placement, monitoring practices, data retention policies, staff compliance, and integration with administrative controls. In Rivers State—like many subnational settings—there is limited empirical evidence on whether CCTV systems meaningfully reduce misappropriation and fraud in government agencies, and what institutional factors affect their success.

Literature Review

Close Circuit Television and Fraud Mitigation

Close circuit television (CCTV) refers to the surveillance technology where the behaviour of the people in organisations, homes and the general places are recorded and monitored. It relies on video cameras to record images shown on a small number of screens that are linked to non-broadcast transmission system, like a network of cables (Gilman, 2016). Organisations and governments around the world have greatly embraced CCTV. According to Piza et al. (2019) around the world CCTV is used to capture images or videos to monitor and surveil the world. Ashby (2017) further stated that recorded data have numerous applications such as criminal investigations, traffic monitoring, crime mitigation, etc. According to Ogunleye et al. (2011) CCTV is a surveillance method which tries to reduce crime by making the potential offenders perceive that it is costlier. Even though commercial cable television is technically a type of CCTV, the term closed-circuit television is typically used in reference to systems with few screens that are being observed to provide security.

The authors: Ogunleye et al. (2011) also elaborate that a closed-circuit system has all its parts directly linked unlike in broadcast television where any receiver within the right tuning can receive the signal. Direct links are microwave, infrared beam and so on. The theme of this review to CCTV devices is based on the diversity of models. Other current models, including Dome, Bullet, PTZ (Pan-Tilt-Zoom), Thermal, and 360 -degree cameras, have better performance than older models as they do not consist of many product reviews (Caught on Camera, 2023; BusinessWatch, 2019).

Dome cameras have recently been mentioned in surveys as one of the most desirable and affordable surveillance solutions (Stein & Levi, 2023). They are easily mounted on the walls or the ceilings due to their dome-shaped structure (Lamaazi et al., 2023). Dome cameras are also able to rotate in more than one direction and have a wide angle of coverage. They usually have infrared night view, motion sensor, and remote access (Amazon, n.d.). Another enhanced one is the bullet cameras. A lens is usually long and cylindrically shaped and is located on one side with the other side of the mounting bracket (Caught on Camera, 2023). They are weatherproof and can be spread over a long distance and are ideal outdoors. The new models are higher resolving more zoomed and better performing than older models and better performing than newer dome cameras. PTZ cameras enable operators to remotely control pan, tilt and zoom (Barker, n.d.). This has made them applicable in large outdoor spaces. PTZs can also be programmed to track objects or people that are on the move within its range of vision. Infrared cameras or

thermal cameras use heat to detect any kind of activity instead of light. They are also good at detecting movement even in full darkness, and are often employed in security applications like airport surveillance (Brook, 2020). Thermal cameras can detect the heat impact of living creatures even when there is no light since they do not depend on visible light instead, they combine shots taken with multiple lenses (Workswell, 2023). 360 and cameras provide a panoramic view of the surroundings by stitching together images taken by two or more lenses (Avatour, 2022). They are used in shopping malls, airports, or train stations that have large indoor areas, and these cameras are ideal to prevent fraudulent activities.

In the future, MJ Flood Security (2022) acknowledged that, in spite of what people may believe, CCTV may be critical when it comes to mitigating fraud. According to organizations, CCTV is considered to be a deterrent of visual nature, a way to monitor transactions and help in investigations which in turn plays a role in alleviating fraud. Lallupersad (2023) presented the argument that deterring potential perpetrators is one of the ways in which CCTV decreases fraud. People feel observed and monitored as cameras scare them away into trying to commit fraud. This reduces the chances of fraud initially, which conserves organizations time and money. Transactions and suspicious activity that might make it clear that there is fraud are also tracked by CCTV (Ansari, 2023; Staff writer, 2021). The footage provided by CCTV has in many occasions been taken as concrete evidence to probe suspects who are suspected to have committed fraudulent acts.

According to Ashby (2017) and Ratcliffe (2011), CCTV finds numerous uses in the safeguarding of the populace, to curb crime, enhance emergency response, control venues, and alleviate the fear of crime in the minds of the populace. According to Ogunleye et al (2011), CCTV cameras record images of offences in real-time. In most instances, these photographs result in punishment and depriving the perpetrators of future occasions of perpetrating the offense, either by taking them to jail or applying extra monitoring and supervision.

The most publicized mechanism is this one, and there are a handful of cases of bank robbery where CCTV images helped to detect and arrest a criminal (Holland, 2023). Financial fraud is one of the most common applications of CCTV footage as it may be used in court to prosecute an offender (Ansari, 2023). Williams (2019) supported these arguments and added that, to enjoy the significant advantages of CCTV as an IT asset, the latter should be combined with other security solutions. According to the US Department of Homeland Security (2013), CCTV is a fundamental IT device that can be used to improve security in residential homes, enterprises, and even in the community. The CCTV system may be greatly integrated with access control systems, intrusion detection systems, alarm systems, and video analytics.

Access control systems restrict access to certain areas or resources in a facility. The combination of CCTV and access control will allow operators to check the identity of a person trying to enter the premises visually (Lodge Service Group, 2023). Access control may be connected to cameras at the entrance points to take pictures when individuals enter or leave the facility (Bradding, 2021). Unauthorized entry is detected using intrusion detection systems. The combination of CCTV and these systems enables the operators to be able to locate an intrusion and its character within a short period of time (Akos, 2023). GoPro cameras may be fitted in areas of strategic locations, and can be connected to intrusion sensors to show real time video of any intrusion (Singapore Police Force, et al., 2022).

The alarm systems will inform the operators and authorities about the possible threats or incidences. CCTV with alarms allow the operators to determine the reason behind an alarm and act accordingly by visually verifying the cause (Singapore Police Force, et al., 2022). Safes or cash registers can have cameras that can provide visual confirmation of the incidents whenever alarms are

triggered (Ansari, 2023; Staff writer, 2021). Video analytics software involves studying videos and identifying possible threats or incidents with the help of AI algorithms (Zereen, et al., 2023). The combination of CCTV with analytics provides operators with real time alerts when suspicious activity has been detected. Analytics software cameras allow constant observation of the most important areas (Jessurun, 2023; Piza and Moton, 2023).

Concept of Fraud Mitigation

Fraud constitutes when a person takes advantage of flaws and vulnerabilities in an organizational system and uses deceit to profit personally and the core of fraud is intentional deception as noted by Abdullahi and Manor (2018). Moukoro et al (2011) noted that fraud is a tendency and propensity to do what is wrong regardless of the awareness of the harm it may cause to one's neighbour. They further expressed that it is a deliberate attempt of subverting the rules of the game using some logical tricks or anything of such nature to defraud public fund for personal interest. Fraudulent activity is a significant financial threat to world economies, costing billions of dollars annually. They can take a variety of different forms, ranging from bribery to corrupt activities, to falsified financial records.

Authors such as Ar et al (2023), Bellentani (2023), Albanese et al (2019), Kratcoski (2018), Graycar (2015), Dada (2014) and Stein (2012) saw bribery, extortion, graft, pay to play, misappropriation, nepotism and embezzlement as kith and kin of fraud. Moukoro et al admitted that it is a much cost effective and secure way to control fraud than it is to investigating the fraud after it occurs - that is why organizations must be proactive in taking precautions against fraud. This is in line with Chhabra-Roy and Prabhakaran (2023) that one of the greatest challenges for the governments of all types is that most fraud is discovered after a crime has already been committed. Mitigating fraud by not hiring illegitimate businesses in the first place - is sometimes difficult because surface appearances can be (and in fact are meant to be) deceiving. Fraudsters are extremely good at posing as real service providers, as their fraud relies on it (Cole, 2023; Albrecht, et al., 2018). U.S. Attorney's Office (2015) mentioned that in Missouri, an owner of a construction organisation recently pleaded guilty to a scheme whereby he pretended that his organisation was being run by a disabled veteran, which allowed it to receive preferential treatment for $13.8 million in contracts the organisation otherwise would not have qualified for. In El Paso, according to Perez (2016), $3.2 million in funds for a downtown streetcar project were diverted into the bogus bank accounts of a front organisation pretending to be a legitimate vendor.

Fraud according to Ernst and Young (2005) is an intentional act which employs trickery or dishonesty in an attempt to steal someone's legal rights or property. In the same vein, Albrecht's concept paper on fraud from 19 years ago remains true today in 2023. It says using deceitful strategies to gain unfair advantages regardless of the consequences is a fraudulent behaviour. According to Albrecht (2005), fraud is rarely in nature to be seen. Therefore, the signs or symptoms of fraud are usually visible. Sukirman et al (2018) described two major types of fraud. Sukirman et al noted that the first category of fraud encompasses fraudulent financial statements while the second was asset misappropriation. Sukirman et al viewed fraud in financial statements as a misstatement or deletion of the amount or disclosure that is intentionally performed with the aim of deceiving its users. Most cases are misstatement of the amount of what is reported as opposed to disclosure while misuses of assets are embezzlement of assets by employees as well as theft of office items by employees (Sukirman et al, 2018). This is in tandem with Hock (2023) and Patel (2023) that fraud is a criminal activity that has numerous manifestations such as identity theft, embezzlement and false billing.

Implementations of fraud mitigation strategies help detect and mitigate the potential fraudulent transaction.

Al-Taee et al (2023) added that fraud mitigation is essential to minimize and mitigate the risks it presents to financial wellbeing. It is necessary to have the adequate mechanisms and guidelines in place so that fraud does not happen or cause harm when it does occur. In their paper, Ionici and Evans (2023) noted that there are several forms of fraud that organizations need to protect against, such as asset misappropriation, corruption, and financial statement fraud. Misappropriation is a kind of white-collar offense where individuals steal or use the assets of an organization for their own personal benefit (Homer & Byrne, 2023). This can include embezzlement, theft of organizational property and falsification of records to cover the fraudulent activity (Grumbles, 2023; Tracey, 2023).

The syndicate that managed this organised crime was eliminated in an operation titled Operation Elbrus- a collaborative investigative project by the Australian Federal Police (AFP) which had the ATO, with the support of the Serious Financial Crime Taskforce (SFCT), in an operation. OperationElbrus showed a high level of complexity of a tax-fraud and money-laundering scheme that used businesses like Plutus Payroll Australia Pty Ltd and other payroll service providers to divert both PAYG withholding tax and GST liabilities that would otherwise go to the ATO on behalf of plotters. Federal Revenue Service (RFB), in Brazil, has not been spared by fraudulent activities in the collection and remittance of tax, as reported by Clemente et al. (2021).

Privatization is usually the process of handing over ownership and control of those possessions of the people to the possession of those who are privately owned with the alleged aim of improving the effectiveness of management and service delivery to the people. According to Albati (2023), this type of reform has been introduced by many countries to make it more efficient, cost-effective, and increase income. Nevertheless, malefaces are often availed by the same procedure. An example here is the manipulation of the value of assets, where agencies understate the value of assets to sell them at lower prices to preferred buyers, or overstate the value of assets to attract high bids by private investors (Nwabughiogu, 2022; Koutantou and Howley, 2011). The cases in these situations are that the government officials have been accused of taking bribes or kickbacks in favor of the private parties in an attempt to grant special treatment (Sahara Reporters, 2007).

Even insider trading is a known kind of a fraud in a privatization process; officials who have access to and can learn about confidential information are reported to have taken advantage of the knowledge and made a profit selling or buying shares tied to the privatization process (Chan et al., 2023; Zhu and Kong, 2023). The shell organisations also contribute to the ease of conducting illicit activity; shell organisations have no actual assets or operations and they hide the identity of buyers or sellers, which makes it easier to perpetrate corrupt acts (Nuseibeh, 2023).

The detection and mitigation of fraudulent activities also calls for the prompt and effective investigation. This is in the same vein with Statistical Analysis System (2022) that fraud can encompass waste and abuse, improper payments, money laundering, terrorist financing, public insecurity and cybercrime.

In the past, organizations had to take a fragmented approach to fraud mitigation, using business rules and rudimentary analytics to look for anomalies to create alerts from separate data sets. Data could not be cross-referenced through automation, and investigators could not manually monitor transactions and crimes in real time; they had to do so after the fact. For instance, it has been reported by scholars (such as Clemente et al (2018), Stowell et al, (2018), Krause (2011), Morris (2009), and Simborg (2008)) that in health care, fraud mitigation was more like 'pay and chase', owing to the fact that the criminal was long gone by the time fraud was detected. Hence, to combat fraud, organisations need to take advantage of the new technology that has been developed

to predict conventional tactics (Mohan, et al., 2022; Dutta, et al., 2017), uncover new schemes (Liu, et al., 2016; Mukhopadhyay, 2014; Flegel, et al., 2010) and decipher increasingly sophisticated organized fraud rings (Beranek, 2023; Statistical Analysis Systems, 2023). This involves more than standard analytics; it applies predictive and adaptive analytics techniques - including a form of artificial intelligence known as machine learning. By combining big data sources with real-time monitoring and risk profile analysis to score on fraud risk, fraud mitigation has evolved to start turning the tides of losses (Beranek, 2023; Statistical Analysis Systems, 2023).

Ashby (2017) examined the usefulness of CCTV cameras in an investigation. He studied 251,195 cases in which the British Transport Police registered between 2011 and 2015. It was aimed at understanding the frequency of useful evidence provided by CCTV and the things that influence it. He employed a special data set of the police which was provided with information on the role of CCTV in investigations. The research revealed that CCTV existed in 45 percent and was considered to be useful in 29 percent of instances. Most types of crime, except those involving drugs, possession of weapons and fraud were far more likely to have been solved with the aid of useful CCTV. There was a greater probability of the availability of CCTV footage in serious crimes and lesser cases that occurred at unspecified times or in specific places. This research demonstrates the value of CCTV cameras in crime solving. It resembles a recent study on Information technology and fraud mitigation strategies in selected Rivers State government agencies between 2013 and 2018 since both are on how technology is used to mitigate fraud and crime. The study is however by Ashby on CCTV and its usefulness in investigations, whereas the current study examines the role of information technology in preventing fraud in government agencies in Rivers State, Nigeria.

Afriyie and team get into the process of identifying and estimating credit-card fraud using supervised machine learning. They evaluated three models of logistic regression, random forest, and decision trees on a simulated dataset of January 2020 to December 31, 2020. The dataset contained 555,719 transactions, 23 variables and a fairly balanced proportion of legitimate and fraudulent ones. They whitesniffed the data, fixed formatting, dropped missing values, scaled the features and a little undersampling to take the imbalance down. At that point, they trained the models and discovered that the random forest provided the finest accuracy at 96, hence that is what they are shilling as the best fraud-detector. It was also noted that the most frequent victims are people over 60 and most fraud waves occur during 22:00 - 04:00 GMT. The paper aligns with the existing literature on IT and fraud prevention in Rivers State government agencies in 201318 since both are exploring the field of digging into the area of tech-based fraud prevention, but Afriyie examined how credit card fraud can be curted by means of ML, whereas the new study explores how IT can prevent fraud in the state agencies of Nigeria.

Methodology

Research Design

The research was designed using descriptive survey design, which was selected due to its ability to collect data systematically using questionnaires or interviews or observations to describe the characteristics of a population or a phenomenon.

Population

The study population was 40,667 employees who were working in 27 government agencies distributed in 21 ministries. There were 9,479 senior staff and 31,188 junior staff amongst them (Source: Directors and Registrar of the Agencies). It is also interesting to note that Rivers State Bureau on Public Procurement (RSBOPP) was the only agency out of the 27 that was not allocated to a ministry, as it reports to the state Governor.

Sample Size and Sampling Technique

The multistage sampling was employed in the study to ensure that data gathered were not only statistically viable, but also relevant in relation to preventing fraud at institutions in the public sector. The researchers first of all surveyed 27 government agencies which are under 21 ministries in Rivers State.

The calculation was given assuming a total workforce of 40,667 staff across the parameters and agency of a 95 confidence level (Z -1.96), a 50% distribution of responses (p = 0.5), and a level of precision (4.88) of 0.04876. Given the following mathematical calculation:

$$\frac{(1.96)^2 \times 0.5 \times (1 - 0.5) \times 40667}{(0.04876)^2 \times (40667 - 1) + (1.96)^2 \times 0.5 \times (1 - 0.5)}$$

$$= 40$$

Therefore, it has been established that 400 respondents was a statistically significant sample size.

Data Collection Instruments

1. Structured questionnaire (closed + Likert-type items) for staff: perceptions of CCTV presence, observed changes in misconduct, awareness of CCTV policy, perceived effectiveness.
2. Key informant interview guide: open-ended questions on CCTV procurement, monitoring practices, case examples, constraints.
3. Document review checklist: number/type of CCTV cameras, maintenance logs, retention policies, incident reports, internal audit findings.
4. Observation checklist: camera coverage, signage, monitoring practice, physical security of DVR/NVR units.

Results and Discussion

Table 1 presents the mean scores and standard deviation on ways in which close-circuit television has mitigated misappropriation fraud in selected government agencies in Rivers state between 2013 and 2018.

Results in Table 1 presented data on the mean scores and standard deviations regarding the ways in which CCTV mitigated misappropriation fraud within the selected nine agencies of government in Rivers State. The dataset captured perceptions from both senior and junior staff regarding CCTV applications in various security-related contexts. Among senior staff, the highest mean score of 2.84 (SD = 0.69) corresponded to the item stating that supplementary security measures were employed, with CCTV systems used alongside access control mechanisms. This was followed by a mean of 2.64 (SD = 0.63) for the installation of CCTV systems in high-risk areas, such as inventory storage rooms, suggesting a clear acknowledgment of surveillance systems in strategic locations.

Meanwhile, monitoring visitor behaviour through CCTV received a mean score of 2.62 (SD = 0.62). Items relating to CCTV integration with alarm systems and oversight of employee conduct recorded slightly lower means of 2.46 (SD = 0.57) and 2.55 (SD = 0.60), respectively. These patterns mirrored, though slightly diminished, in the responses from junior staff, where the cluster mean was 2.45 (SD = 0.57). The collective feedback underscored the instrumental role CCTV played as a tool for fraud mitigation strategies deployed in government agencies across Rivers State between 2013 and 2018. This evidence indicated that, although not universally applied, CCTV integration contributed significantly to institutional mechanisms designed to curb misappropriation fraud.

The research revealed that installation of CCTV cameras in areas with high risks such as inventory storage rooms contributed to decrease misappropriation fraud in the selected government agencies in Rivers State in the year 2013-2018. Nevertheless, the cameras had a number of shortcomings: the blind spots were not entirely covered, and the cameras were poorly maintained, resulting in their malfunction; no skilled personnel were assigned to oversee the footage, and the employees believed that their privacy could be violated, which lowered their morale.

These results are in line with the overall perspective that surveillance technology can prevent fraud, but only under the condition that it is deployed properly. The improper implementation of CCTV may lead to illusion of safety and decrease the responsibility in the employees. Piza et al. (2019) also stress that CCTV has the ability to reduce crime. This positive step enhances security and also encourages a culture of responsibility, which is reminiscent of the social-science idea that an ounce of mitigation is a pound of cure. In addition, visible CCTV gives a sense of integrity in its operations to the various stakeholders, which is a major element in ensuring people maintain their trust in the government facilities. The book by Ugoani (2020) explains the value of good governance in terms of management practices.

Table 1: CCTV/ Misappropriation Fraud Mitigation

S/N	Test Items – CCTV/ Misappropriation Fraud Mitigation	Senior Staff (116)		Junior Staff (207)		Mean Set (2.5)	Decision
		Mean (2.5)	Sd	Mean (2.5)	Sd		
1	There was an installation of CCTV systems in high-risk areas such as inventory storage rooms.	2.64	0.63	2.42	0.56	2.53	Agreed
2	CCTV was installed in your section to oversee employee conduct.	2.55	0.60	2.38	0.54	2.47	Disagreed
3	The provision of CCTV in your section was intended to monitor the behaviour of visitors.	2.62	0.62	2.50	0.58	2.56	Agreed
4	Supplementary security measures were employed with CCTV systems being used in conjunction with access control.	2.84	0.69	2.50	0.58	2.67	Agreed
5	In your section, there was an integration of CCTV systems with other security measures, such as alarm systems.	2.46	0.57	2.47	0.57	2.47	Disagreed
	Cluster Mean and Standard Deviation	2.62	0.62	2.45	0.57	**2.54**	

Conclusion and Recommendations

Thematic analysis of the interview guide revealed that concerns over inadequate training and lack of clarity in digital roles were raised by the junior staff, and partial implementation success was reported by senior staff with policy delays and budgetary constraint being cited as the significant barriers. Regarding the use of CCTV in curbing the misappropriation fraud, the results showed that senior and junior employees had moderate to high ratings with the highest senior mean of 2.84 on use of CCTV and use of access control systems. This implies that as much as there was implementation variance, CCTV was a major deterrent in areas of operation that were sensitive in the year 2013 and 2018.

In the light of the discoveries made in this study, the following recommendations were made:

1. The Rivers State Road Maintenance and Rehabilitation Agency, in collaboration with the ministry of works and tech consultants should seize CCTV equipment to oversee the major road projects. Although the staff may be concerned with privacy, it will deter bad actors and will contribute to creating a crew that does not break the rules.
2. The Rivers State Bureau on Public Procurement, in collaboration with the IT department and the tech-shrewd individuals, is supposed to introduce IoT devices to monitor the procurement in real-time
3. Rivers state university administration must enhance its BBA integration by integrating it with payroll and registration team during the next semester. There are a few hiccups that can be

anticipated in the technology, yet the reduction of fake hires will ensure that the campus operates more efficiently in the long term.

Declaration of Competing Interest

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

Credit Authorship Contribution Statement

Onyerimma, L. A.: Conceptualization, Methodology, Formal analysis, Investigation, Resources, Data curation, Visualization, Project administration, Writing - original draft, Review & Editing. **Martin, I. I.** and **Daisy, C. O.** : Supervision, Methodology, Validation, Formal analysis, Data curation, Visualization.

References

Aarthy, P., & Kumar, S. (2019). *Effectiveness of CCTV surveillance in crime prevention: A review.* Journal of Security Studies, 12(3), 45–61.

Abdullahi, R., & Manor, J. (2018). Fraud triangle theory and fraud diamond theory: Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 8(4), 38–45.

Akos, J. (2023). *Integrating intrusion detection with CCTV surveillance: A review of security automation systems.* Security Technology Review, 15(2), 67–75.

Albati, H. (2023). *Privatization and fraud risks in developing economies.* Journal of Governance and Reform, 11(2), 99–114.

Albanese, J., Morselli, C., & Lyman, M. (2019). *Organized crime and corruption: Concepts and realities.* Routledge.

Albrecht, W. S. (2005). *Identifying fraudulent financial activities.* Journal of Forensic Accounting, 6(2), 1–25.

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2018). *Fraud examination* (6th ed.). Cengage Learning.

Al-Taee, M., Omar, M., & Hassan, K. (2023). *Fraud mitigation strategies in financial institutions.* International Journal of Financial Crime Studies, 9(1), 15–30.

Amazon. (n.d.). *Features of dome security cameras.* Retrieved from https://www.amazon.com

Ansari, S. (2023). *The role of CCTV in fraud detection and prevention in modern organizations.* Journal of Corporate Security, 7(4), 22–33.

Ar, K., Bello, R., & Tan, P. (2023). *Typologies and mechanisms of financial fraud in public institutions.* Fraud Risk Journal, 12(3), 87–104.

Ashby, M. P. J. (2017). The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research*, 23(3), 441–459.

Avatour. (2022). *The power of 360-degree cameras in surveillance and monitoring.* Retrieved from https://www.avatour.com

Barker, L. (n.d.). *PTZ camera technology and its applications in large-scale surveillance.* Security Equipment Digest.

Bellentani, F. (2023). *Global perspectives on corruption and fraud control.* Springer.

Beranek, T. (2023). *AI and machine learning applications in fraud detection.* Analytics & Security Review, 14(2), 31–47.

Bradding, T. (2021). *The role of access control systems in physical security.* Journal of Security Management, 18(1), 55–70.

Brook, J. (2020). *Thermal imaging technologies for night surveillance.* Journal of Applied Security, 10(1), 12–21.

BusinessWatch. (2019). *CCTV camera models and their modern applications.* Business Watch Security Report. Retrieved from https://www.businesswatchgroup.co.uk

Caught on Camera. (2023). *Comparison of dome and bullet cameras for commercial security.* Retrieved from https://www.caughtoncamera.net

Chan, C., Wong, K., & Zhu, T. (2023). *Insider trading and fraudulent privatization practices.* Journal of Business Ethics, 186(4), 883–901.

Chhabra-Roy, S., & Prabhakaran, N. (2023). *Government fraud and prevention strategies in the digital era.* International Journal of Governance Studies, 8(1), 50–67.

Clemente, R., Dos Santos, L., & Pimenta, R. (2021). *Tax fraud and corruption in Latin America: Case study of the Federal Revenue Service in Brazil.* Public Finance and Accountability Review, 14(3), 120–137.

Cole, A. (2023). *Fraud risk management and prevention in public procurement.* Fraud Prevention Journal, 17(2), 42–57.

Dada, J. O. (2014). *Fraud management in the Nigerian public sector: A theoretical review.* International Journal of Business and Management, 9(1), 118–127.

Dutta, S., Roy, S., & Bhattacharjee, D. (2017). *Predictive analytics for fraud detection in banking systems.* Procedia Computer Science, 122, 804–811.

Ernst & Young. (2005). *Global fraud survey: Deception in business.* EY Global Publications.

Flegel, U., Vayssière, J., & Buttyán, L. (2010). *Security and fraud management in electronic environments.* Springer.

Gilman, E. (2016). *Understanding closed-circuit television systems.* Security Engineering Review, 8(2), 55–63.

Graycar, A. (2015). *Corruption: Classification and analysis.* Policy and Society, 34(2), 87–96.

Grumbles, R. (2023). *Asset misappropriation and fraud risk assessment.* Journal of Corporate Compliance, 16(3), 99–115.

Hock, D. (2023). *Types and implications of financial fraud.* Forensic Audit Review, 5(1), 44–57.

Holland, S. (2023). *CCTV and criminal detection: The role of video evidence in modern policing.* Security Studies Quarterly, 14(2), 30–49.

Homer, P., & Byrne, T. (2023). *Financial misconduct and asset misappropriation in the workplace.* International Journal of Forensic Accounting, 7(2), 66–83.

Ionici, C., & Evans, R. (2023). *Mitigation of financial fraud through internal controls.* Journal of Financial Integrity, 12(2), 133–146.

Jessurun, M. (2023). *Artificial intelligence in video analytics for fraud prevention.* Surveillance Technology Review, 9(1), 12–28.

Koutantou, A., & Howley, K. (2011). *Privatization and corruption: A comparative review.* European Economic Policy Review, 5(2), 122–139.

Kratcoski, P. (2018). *Corruption and organized crime: Implications for law enforcement.* CRC Press.

Lallupersad, N. (2023). *CCTV as a deterrent to fraud in the workplace.* International Journal of Corporate Ethics, 10(2), 101–114.

Lamaazi, F., Fekih, A., & Bouzid, M. (2023). *Modern CCTV technologies and their deployment in smart surveillance.* Journal of Information Security Systems, 11(3), 77–89.

Liu, Y., Wu, X., & Li, H. (2016). *Detecting financial fraud using big data analytics.* Expert Systems with Applications, 80, 227–239.

Lodge Service Group. (2023). *The role of access control and CCTV integration in security management.* Retrieved from https://www.lodgeservice.com

MJ Flood Security. (2022). *The importance of CCTV in fraud mitigation.* Retrieved from https://www.mjfloodsecurity.ie

Mohan, A., Kumar, S., & Patel, D. (2022). *Machine learning for fraud risk prediction.* Journal of Intelligent Systems, 31(4), 411–425.

Morris, J. (2009). *Healthcare fraud: Identifying red flags.* Journal of Health Administration, 26(3), 35–49.

Moukoro, J., Tchankam, J. P., & Manga, J. (2011). *Fraud and corruption in African public sectors.* African Journal of Economic and Management Studies, 2(3), 240–257.

Mukhopadhyay, S. (2014). *Fraud analytics: Tools and techniques.* John Wiley & Sons.

Nuseibeh, H. (2023). *Shell companies and illicit financial flows.* Journal of Financial Crime, 30(1), 34–47.

Nwabughiogu, L. (2022). *Nigeria's privatization challenges and corruption concerns.* Vanguard Nigeria. Retrieved from https://www.vanguardngr.com

Ogunleye, O., Ajayi, M., & Bamidele, T. (2011). *CCTV as a surveillance and crime control tool in Nigeria.* Journal of Security and Development Studies, 4(1), 45–59.

Patel, N. (2023). *Contemporary forms of fraud and financial manipulation.* Forensic Accounting Perspectives, 15(2), 88–102.

Perez, J. (2016). *City contractor fraud case reveals systemic vulnerabilities.* El Paso Times, April 12.

Piza, E. L., & Moton, R. (2023). *Evaluating CCTV surveillance effectiveness through AI-based analytics.* Crime Science, 12(1), 19–36.

Piza, E. L., Caplan, J. M., Kennedy, L. W., & Gilchrist, A. M. (2019). CCTV surveillance for crime prevention: A 40-year systematic review. *Criminology & Public Policy*, 18(1), 135–159.

Ratcliffe, J. H. (2011). *Intelligence-led policing and crime reduction strategies.* Willan Publishing.

Sahara Reporters. (2007). *Privatization and corruption in Nigeria.* Retrieved from https://saharareporters.com

Singapore Police Force, et al. (2022). *Security technology integration for public safety.* Singapore Ministry of Home Affairs Report.

Staff Writer. (2021). *How CCTV footage assists in fraud detection and prosecution.* Corporate Security Weekly, 5(2), 11–14.

Statistical Analysis System. (2022). *Fraud detection and mitigation using AI analytics.* SAS Institute.

Statistical Analysis Systems. (2023). *Predictive analytics in fraud prevention.* SAS Global White Paper Series.

Stein, D. (2012). *Corruption, ethics, and public trust.* Palgrave Macmillan.

Stein, P., & Levi, R. (2023). *User preferences for modern CCTV systems.* International Journal of Smart Surveillance, 8(1), 45–59.

Stowell, G., Morris, R., & Patel, R. (2018). *Healthcare fraud management systems.* Journal of Medical Ethics and Administration, 32(3), 61–78.

Sukirman, S., Sari, R., & Abdullah, N. (2018). *Financial statement fraud and asset misappropriation: Evidence from emerging economies.* Journal of Forensic and Investigative Accounting, 10(2), 98–112.

Tracey, J. (2023). *Corporate misappropriation and forensic investigation.* Journal of Business Integrity, 17(2), 71–86.

U.S. Attorney's Office. (2015). *Contractor fraud case summary: Missouri veteran-owned business scheme.* U.S. Department of Justice.

U.S. Department of Homeland Security. (2013). *Guide to CCTV system integration for critical infrastructure security.* DHS Publication.

Williams, G. (2019). *Leveraging CCTV as part of integrated security systems.* International Security Review, 21(1), 55–69.

Workswell. (2023). *Thermal cameras for industrial and security monitoring.* Retrieved from https://www.workswell.eu

Zereen, M., Bashir, T., & Khan, R. (2023). *AI-based video analytics in fraud detection systems.* International Journal of Advanced Computing, 33(2), 201–215.

Zhu, Y., & Kong, L. (2023). *Insider fraud in privatization processes: A comparative legal review.* Journal of Law and Finance, 14(1), 22–38