ASSESSMENT OF THE LINK BETWEEN CROWD MONITORING SYSTEM AND FACILITY SECURITY OF COMMERCIAL BANKS IN PORT HARCOURT, RIVERS STATE

BAADOM, Zigalobari[1]**,** Prof. A. E**. Bestmen**[2] and **GBAFAH,** B. L. PhD
Department of Office and Information Management, Faculty of Administration & Management, Rivers State University, Nkpolu- Oroworukwo, PMB, 5080, Port-Harcourt, Nigeria.Email: zigalobari.baadom1@ust.edu.ng Phone no: +2348144049339

ABSTRACT

Crowd monitoring systems have emerged as a critical technological innovation for ensuring facility security in public and semi-public organizations such as banks. This study examined the relationship between crowd monitoring systems and facility security in commercial banks in Rivers State, Nigeria. A structured questionnaire measured respondents' perceptions using a 5-point Likert scale, and data were analyzed through descriptive and inferential statistics. The univariate analysis revealed positive mean scores across all indicators, with the highest support recorded for the statement that facility security is achieved through the adoption of crowd monitoring systems (M = 4.27). Correlation analysis further established strong positive relationships between crowd monitoring systems and three critical dimensions of facility security: access control ($r = 0.910$, $p < 0.05$), threat detection ($r = 0.924$, $p < 0.05$), and confidentiality ($r = 0.889$, $p < 0.05$). These findings confirm that crowd monitoring systems significantly enhance facility security in banking operations by improving access regulation, early detection of threats, and the protection of confidential information. The study recommends that commercial banks adopt advanced crowd monitoring technologies as a strategic tool for safeguarding facilities, ensuring customer safety, and strengthening overall operational resilience.

KEYWORDS: Crowd monitoring systems, facility security, commercial banks, access control and threat detection

INTRODUCTION

The security of banking facilities has become a central concern in the modern financial sector, particularly in developing economies where commercial banks are highly vulnerable to threats ranging from physical breaches to insider attacks. Facility security encompasses the strategies, technologies, and organizational procedures deployed to safeguard physical and digital assets, employees, and customers within the banking environment. As threats to financial institutions evolve, proactive security systems are increasingly required to mitigate risks and guarantee operational continuity (Hassan et al., 2024).

LITERATURE REVIEW

Crowd monitoring systems have emerged as a critical technological innovation for ensuring facility security in public and semi-public organizations such as banks. Crowd monitoring refers to the use of digital tools, including sensors, artificial intelligence, and surveillance systems, to track, analyze, and manage human movement and density within a given space (Ameen and Stone, 2023). In the context of banking operations, such systems assist in detecting unusual gatherings, identifying potential security risks, and enhancing customer safety during peak banking hours. By integrating these technologies into existing facility security frameworks, banks are better positioned to prevent crimes, manage emergencies, and enforce access control measures (Alkhdour et al., 2024).

Crowding is a common phenomenon observed during major events such as concerts, festivals, sports, games, and entertainment. One of the most interesting and active research topics in computer vision is the analysis of crowd behaviour. Crowd is a group of people gathered in a certain location. Crowd differs in different situations like crowd in a temple will be different from the crowd in a shopping area. Crowd is a group of individuals sharing a common physical

location. Now a day's increase in human population tends to increase the crowd in public areas (Bek & Monari, 2015). Thus, it is required to analyze the surveillance system with several closed-circuit Television is used to monitor the crowd. The human eye cannot observe all the cameras semi closed-circuits an automated technique must be used for continuously monitoring the crowd for a long period. Challenging problems in detecting the desired events automatically are that simultaneous occurrence of more than one event, large number of data must be processed, occlusions and real time detection. The proposed method can be applied from small group of objects.

The Internet of Things is a powerful industrial system of radio-frequency identification and wireless devices that have the ability to transfer data over a network without needing human interaction (Hashish & Ahmed, 2015). Analysis of a crowd behaviour using surveillance videos is an important issue for public security, as it allows detection of dangerous crowds and where they are headed. Computer vision-based crowd analysis algorithms can be divided into three groups people counting, people tracking and crowd behaviour analysis. Mainly, IoT consists of three layers, the sensing layer to gather data from real world via existing hardware e.g. sensors, next the network layer to transfer the collected data over wired or wireless network, and the application layer which is responsible for two-way communication between user and systems (Rosario & Massimo, 2017).

The facility security function plays a critical role in enabling smart risk taking by providing risk intelligence and assuring the safety and security of the organization's physical assets, people, and operations in every venture. The facility security function uses people, processes, and technology to protect the organization from negative events and situations. Facility security identifies, monitors, and deters internal and external threats to an organization's personnel, property, and assets and manages physical crises when they occur. It also assesses risks to the organization, communicates them to executives and management, and manages them appropriately (Sarker, 2021).

It is not uncommon for some of the facility security function's responsibilities to be shared with other departments. For instance, while risks to digital information and assets fall under the corporate security umbrella in some organizations, they are frequently managed by separate but related cybersecurity or information security functions within a corporation. Similarly, while business continuity and resilience frequently fall under corporate security, they may exist in some organizations, but in partnership with, the corporate security function (Tagarev, Sharkov, & Lazarov, 2020). In a global economy in which threats have become increasingly multifaceted and complex, corporate security is a critical function of business. Corporate security practitioners are skilled in employing technology, staff, and processes to deter and respond to the manifold hazards that put businesses at risk. Crowd monitoring systems enhances the facility security of commercial banks in Rivers State as it offers real time surveillance as well as keeping track of movement within and outside banking premises. From the above assertion it looks like a relationship exists between crowd monitoring system and facility security.

In Port Harcourt, Rivers State, commercial banks operate in a highly dynamic environment characterized by rapid urbanization, high population density, and security vulnerabilities such as armed robbery and crowd-related disturbances. These contextual realities underscore the need for innovative approaches to facility protection. Crowd monitoring systems can provide real-time insights into human traffic patterns, thereby enabling bank management to anticipate risks and respond swiftly to abnormal security incidents (Abomaye-Nimenibo et al., 2020).

Previous studies have examined the role of surveillance technologies and artificial intelligence in strengthening facility security (Awofala, 2024). However, there remains a paucity of empirical evidence on the direct link between crowd monitoring systems and facility security in the Nigerian banking industry, particularly in Port Harcourt. This study, therefore, seeks to fill this gap by assessing the relationship between crowd monitoring systems and facility security of commercial banks in Port Harcourt, Rivers State. The findings are expected to provide practical insights for bank management, security agencies, and policymakers on how technology-driven monitoring systems can enhance the safety and operational resilience of financial institutions.

METHODOLOGY

Research Design

The purpose of research design is to obtain data to empower the researcher test hypotheses or answer research questions. These hypotheses testing study will adopt explanatory research design and obtain quantitative data from the respondents in a non-contrived environment. More so, the cross-sectional survey research approach was adopted because it offers a wide coverage and also permits the researcher to generalize the research findings to the entire study population.

Population of the Study

The population frame represents a listing of all the elements in the population from which the sample is drawn. Notably, the target population for this study consisted of all registered and functional Commercial Banks in Port Harcourt, Rivers State while the accessible population for the study comprised twenty-three (23) Commercial Banks in Port Harcourt.

Sampling Technique and Sample Size Determination

In this study the researcher adopted the entire population (census) as the sample size considering the fact that the study population is not large. However, four (4) managers were drawn from each of the twenty-three commercial banks in Rivers State that constituted the study population. Preliminary investigation revealed that there are at least four most important managerial positions in these commercial banks. Specifically, the study respondents include: The ICT and Security, Operations Manager, Marketing Manager, and Research and Development Manager. In all, ninety-two (92) managers constituted the respondents for the study. The choice of these categories of people was premised on the fact that they constitute the decision-making body in the organization and as such was armed with the requisite information about the firm relevant to this research. The four (4) top executive managers from each commercial bank belong to the category of persons that are in the right position to provide useful information which the researcher needs in order to enable the researcher to achieve the study objectives.

Method of Data Collection

The study utilized structured and close-end questionnaires as a means of generating primary data from the respondents of the study. The questionnaires were used to enable the researcher to find out the attitude, knowledge and feelings of respondents on questions asked with respect to the study variables in order to enable the researcher to achieve the study objectives. This study adopted primary data through the use of questionnaires. The questionnaire was divided into two parts. The first sections enveloped the demographic details of the respondents while the second contained questions relating to the variables under investigation and the questionnaires were personally administered to the selected respondents.

Instrument for Data Collection

Asika (2004) stated that the questionnaire is an instrument for gathering data beyond the easy physical reach of the researcher. The copies of questionnaires for this study were administered personally as a result of organizational proximity and geographical confinement. The questionnaire will also be designed into two sections; section (A) the demographic section, was used to collect data on the nature and distribution of the target respondents; data such as age, gender, status, and educational qualification, while section (B) elicited respondents' opinions regarding the study variables.

Instrument Validity

Asika (2004) defined validity as the degree to which a measuring instrument measures what it is designed to measure. Every measuring instrument is designed for a specific measurement. Baridam (2001) noted that validity is the extent to which a test measures what it was designed to measure. Validity for measurement seeks to address the issue of researchers measuring what they ought to measure while observing all the set rules. It is concerned with the use of the right measurement instrument, so that conclusion after testing hypothesis can be valid. To assess the validity of the survey instrument, copies of the questionnaires were submitted to my supervisor and other experts in the field of office and information management for verification and modification, before being administered to the respondents. Hence, it was in place to say that the survey instrument had both face and content validity. Content validity focuses on how well the instrument covers the entire construct, whereas face validity deals with the overall superficial appearance of the instrument.

Instrument Reliability

Reliability on the other hand, measures the extent to which a measuring instrument contains variables errors. It is the extent to which the instrument is consistent. To ensure the internal reliability, the survey instrument was assessed by means of Cronbach alpha coefficient, using the statistical package for social sciences (SPSS). Hence, only the items that produced alpha values of 0.7 and above were considered appropriate for the study.

Instrument Administration

A total of ninety-two (92) questionnaires were administered to the respondents by hand with the aid of a research assistant in their respective institutions due to geographical proximity to the researcher and her research assistant. This was done by the researcher through the help of administrative officers and personal assistants to these individuals.

Method of Data Analysis

To empirically evaluate the relationship between the predictor and criterion variable of this study (including their dimensions and measures), the spearman's rank order of correlation coefficient (RHO) was adopted. As a tool, it is considered to be more flexible, and it is not limited or confined to parameters statistical assumption such as applicable in the Pearson's product moment correlation. The multivariate analysis examined the moderating effect of the contextual variable; ICT culture on the relationship between the predictor and criterion variable which was tested using the partial correlation techniques at 95% confidence interval. The analysis was executed using the scientific package for social sciences (SPSS) version 23 software. The formula for the spearman's rank-order correlations is as follows:

$$r_s = 1 - \frac{6\sum d_1^2}{n(n^2-1)}$$

Where r_s= Spearman's rank correlation coefficient

d_1= differences in ranking of a given observation

n= number of observations

By design it is constrained as follows: $-1<r_s<1$ and its interpretation are, the closer r_s is +1 the stronger the monotonic relationship. The sign of a correlation of (+ or -) indicates the direction of relationship between -1.00 and +1.00. Variables may be positively or negatively correlated. A positive correlation indicates a direct, positive relationship between two variables. A negative correlation, on the other hand indicates an inverse, negative relationship between two variables

RESULTS

Univariate analysis

The section highlighted the respondents' rate of response on the dimensions and the measures based on the 5-point Likert's scale as indicated on the table below.

Table 1. Respondents rate on Crowd monitoring systems

	N	Min	Max	Sum	Mean	Std. Deviation
Do you agree that crowd monitoring systems contribute to facility security?	77	1.0	5.0	280.0	3.636	1.1688
Do you subscribe to the idea that crowd monitoring systems cover a wider audience than human security?	77	1.0	5.0	241.0	3.130	1.3214
Do you support the shift from conventional security approaches to the adoption of crowd monitoring systems?	77	1.0	5.0	244.0	3.169	1.3018
Do you subscribe to the notion that crowd monitoring systems enhance facility security?	77	1.0	5.0	236.0	3.065	1.2910
Do you subscribe to the notion that facility security is achieved in your organization as a result of crowd monitoring systems?	77	1.0	5.0	329.0	4.273	1.2422
Valid N (listwise)	77					

Source: Research survey, 2025.

Table 1 showed the respondents' rate on crowd monitoring systems. This table showed that question one on how crowd monitoring system contributes to facility security scored a mean of 3.64. question two on the level of subscription to the idea that crowd monitoring systems cover a wider audience than human security scored a mean of 3.13, question three on how the respondents support the shift from conventional security approaches to the adoption of crowd

monitoring systems scored a mean of 3.17, question four on to the notion that crowd monitoring systems enhance facility security scored 3.07 and lastly question five on the notion that facility security is achieved in your organization as a result of crowd monitoring systems scored 4.27 respectively. All the mean values were above the criterion mean for a 5-point Likert scale, indicated the support and adequate subscription to crowd monitoring system in the organization.

Table 2. Relationship between Crowd Monitoring System and Access Control

			Crowd Monitoring System	Access Control
Spearman's rho	Crowd Monitoring System	Correlation Coefficient	1.000	.910**
		Sig. (2-tailed)	.	.000
		N	77	77
	Access Control	Correlation Coefficient	.910**	1.000
		Sig. (2-tailed)	.000	.
		N	77	77

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Research survey, 2025

Table 2 showed the relationship between Crowd monitoring system and access control. The correlation coefficient shows that there is a strong positive relationship between Crowd monitoring system and access control. The correlation coefficient of 0.910 confirms the magnitude and strength of this relationship which is statistically significant at ($\rho = 0.01<0.05$). Based on this value, the null hypothesis $\mathbf{Ho_1}$ was rejected and the research (Alternate) hypothesis $\mathbf{H_{A1}}$ accepted. Thus, there is a strong positive relationship between Crowd monitoring system and access control of commercial banks in River State, Nigeria.

Table 3. Relationship between Crowd monitoring and Threat detection

			Crowd Monitoring System	Threat Detection
Spearman's rho	Crowd Monitoring System	Correlation Coefficient	1.000	.924**
		Sig. (2-tailed)	.	.000
		N	77	77
	Threat Detection	Correlation Coefficient	.924**	1.000
		Sig. (2-tailed)	.000	.
		N	77	77

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Research survey, 2025.

Table 3 showed the relationship between Crowd monitoring system and threat detection of Commercial Banks in Rivers State, Nigeria. The correlation coefficient shows that there is a strong positive relationship between Crowd monitoring system and Threat detection of Commercial Banks in Rivers State, Nigeria. The correlation coefficient of 0.924 confirms the magnitude and strength of this relationship which is statistically significant at ($\rho = 0.01<0.05$). Based on this value, the null hypothesis $\mathbf{Ho_2}$ was rejected and the research (Alternate)

hypothesis $\mathbf{H_{A2}}$ accepted. Thus, there is a strong positive relationship between Crowd monitoring system and Threat detection of Commercial Banks in Rivers State, Nigeria.

Table 4. Relationship between Crowd monitoring and Confidentiality

			Crowd Monitoring System	Confidentiality
Spearman's rho	Crowd Monitoring System	Correlation Coefficient	1.000	.889**
		Sig. (2-tailed)	.	.000
		N	77	77
	Confidentiality	Correlation Coefficient	.889**	1.000
		Sig. (2-tailed)	.000	.
		N	77	77

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Research survey, 2025.

Table 4 showed the relationship between Crowd monitoring system and confidentiality of commercial Banks in Rivers State, Nigeria. The correlation coefficient shows that there is a strong positive relationship between Crowd monitoring system and Confidentiality of Commercial Banks in Rivers State, Nigeria. The correlation coefficient of 0.889 confirms the magnitude and strength of this relationship which is statistically significant at ($\rho = 0.01<0.05$). Based on this value, the null hypothesis $\mathbf{Ho_3}$ was rejected and the research (Alternate) hypothesis $\mathbf{H_{A3}}$ accepted. Thus, there is a strong positive relationship between Crowd monitoring system and Confidentiality of Commercial Banks in Rivers State, Nigeria.

DISCUSSION

The study shows the critical role of crowd monitoring systems in enhancing facility security among commercial banks in Rivers State. The findings revealed that there is a strong positive relationship between crowd monitoring systems and facility security of commercial banks in Rivers State. The finding agrees with the empirical findings of Shivram and VenkataKrishnan (2021) who investigated crowd monitoring systems using image processing. They stated that organizations have started utilizing sensors enabled smart phones as a tag for large scale human sensing. With the increasing usage of Smart phones, more persons can be tracked without providing any tag in future. Some of the Smartphone based location tracking systems require an application to be installed on the client's Smartphone. The installed application obtains the location using GPS sensor of smart phone and continuously updates the location to the remote server using Internet connection. However, it is rare that users in the large crowd and in remote locations will have the Internet connection all the time. There are many operating systems and versions for Smart phones, which makes the development and distribution of application a difficult task. By embracing the Smart City paradigm, crowd sensing becomes a solution able to cope with air pollution monitoring since this novel paradigm assumes that a significant number of users perform collaborative sensing tasks, thereby collecting data from different populated locations while doing their daily activities. The collected data is periodically transmitted to a central server for data storage and processing. The findings revealed that there is a strong positive relationship between crowd monitoring systems and facility security, thereby mitigating cyber threats and overall safety of organizational assets.

Contemporary literature elaborates on the surge in crowd monitoring system adoption, driven by increasing concerns over public safety and the limitations of traditional security approaches. As Ameen and Stone observe, the effectiveness of crowd monitoring systems is frequently tied to their integration with advanced technologies, such as vision-based and non-vision-based methodologies, and, more recently, artificial intelligence-based automation algorithms (Ameen and Stone, 2023). This technological shift is evident in commercial, sporting, and public environments seeking to anticipate and mitigate incidents proactively. These systems can outperform traditional human security methods in terms of audience coverage and real-time anomaly detection (Rimboux et al., 2019).

A significant finding in the study is the strong positive correlation between crowd monitoring systems and access control ($r = 0.910$). Access control is fundamental to facility and asset protection, and modern security monitoring systems typically integrate with various channels and control points within information communication systems to provide flexible, adaptive management of security threats. The use of automated and interconnected security mechanisms, such as IoT-enabled cameras and sensor networks, increases the granularity and responsiveness of access management in financial institutions, reducing risks associated with unauthorized entry and insider threats (Mackenzie and Njunwamukama, 2024).

Furthermore, the relationship between crowd monitoring systems and threat detection is also robust ($r = 0.924$), reflecting the growing importance of automated surveillance and data-driven security protocols in identifying emerging threats. The inclusion of artificial intelligence and deep learning in surveillance, as validated by simulation and data annotation studies, has enabled more accurate behavioral modeling and anomaly detection, moving beyond the limitations of conventional CCTV or manual surveillance (Rimboux et al., 2019). This is especially critical in banking, where both digital and physical threats must be rapidly identified and contained.

Another notable aspect is the correlation between crowd monitoring systems and confidentiality ($r = 0.889$). In critical sectors such as finance, safeguarding information and maintaining confidentiality are essential not only for regulatory compliance but for the trust and operational continuity of the institution (Lizut, 2019). Security monitoring systems utilizing distributed and integrated components must implement rigorous access controls, encryption, and ongoing risk assessments to prevent breaches and data leaks, as emphasized in research focusing on distributed system reliability (Sosnovsky, 2022). Ensuring confidentiality requires not just technological measures but also strong policy frameworks and continuous evaluation, given the evolving nature of security threats (Khabarani 2024).

From an operational perspective, high mean ratings on support for transitioning from conventional security approaches to automated crowd monitoring indicate a readiness among bank employees to adopt new security technologies. Such readiness aligns with global trends in digital transformation, where facilities increasingly rely on digital and cyber-physical systems to optimize security, surveillance, and resource management (Zou et al., 2025). However, challenges persist, including technological infrastructure constraints and the need for robust data security protocols with any IoT or smart device implementation (Hidayat and Sutabri, 2024).

In summary, the analysis confirms broad support for the integration of crowd monitoring systems within facility security architectures and substantiates their value in enhancing access control, threat detection, and confidentiality. These results reinforce findings from international

studies and demonstrate alignment between empirical user perceptions and the proven efficacy of modern security technologies

CONCLUSION AND RECCOMENDATIONS

This examined the relationship between artificial intelligence dynamics and facility security of commercial banks in Rivers State. The dimensions of artificial intelligence dynamics (predictor variable) as used in this study are crowd monitoring systems. There is a very strong positive relationship between crowd monitoring system and facility security of commercial banks in Rivers State. Crowd monitoring system positively relates to facility security of commercial banks in Rivers State. This implies that the deployment of crowd monitoring systems by commercial banks will optimize safety protocols by monitoring crowd movements, predicting potential risks, and providing real-time data for better decision making. Based on the findings and conclusion, the leadership of commercial banks are encouraged to adopt and implement crowd monitoring systems so as to optimize safety protocols by monitoring crowd movements, predicting potential risks, and providing real-time data for better decision making.

REFERENCES

Abomaye-Nimenibo, P. D., Samuel, W. A., & Abomaye-Nimenibo, S. K. (2020). The Problems of Rapid Urbanisation in Port Harcourt. *Global Journal of Human Social Sciences,* 15

Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024). Assessment of cybersecurity risks and threats on banking and financial services. Journal of Internet Services and Information Security, 14(3), 167-190.

Ameen, M. & Stone, R. (2023). Advancements in Crowd-Monitoring System: A Comprehensive Analysis of Systematic Approaches and Automation Algorithms: State-of-The-Art. International Journal of Network Security & Its Application, 5(3), 95-110

Asika, N. (2004). *Research methodology in the behavioural sciences. Learn Africa Plc*, Felix Iwerebon House, 52 Oba Akran Avenue, Ikeja-Lagos State.

Awofala, T. B. (2024). The role of Artificial Intelligence in Global Health Surveillance. World *Journal of Advanced Research and Reviews*, 24(2), 1772-1778.

Baridam, D., (2001). *Research Methods in Administrative Sciences*. 3rd Edition, Sherbrook Associates, Port Harcourt.

Bek, S. & Monari, E. (2015). The Crowd Congestion Level A New Measure for Risk Assessment In Video Based Crowd Monitoring. *International Journal of Information Technology and Decision Making* 3(4), 2353- 2361.

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, 5(1), 41-59.

Hashish, S. & Ahmed, M. (2015). Efficient wireless sensor network rings overlay for crowd management in Arafat area of Makkah. In 2015 IEEE International

Conference on Signal Processing, Informatics, *Communication and Energy Systems*, 1-6.

Khabarani, K. & K. & Abuanza, A. (2024). Effective Strategies for Risk Management and Mitigation in the Field of Corporate Security in the Kingdom of Saudi Arabia. *International Journal of Financial Administration*, 3(10), 920-962.

Lizut R. A. (2019). Effectiveness of strategic management systems for organizational and economic security of agricultural enterprises. *The journal Actual problems of innovative economy and law.* 15.04.2019. https://doi.org/10.36887/2524-0455-2019-3-14

Mackenzie, D. & S. Njunwamukama, S. (2024). Strengthening Fintech Security in Uganda: An Analysis of Insider Threats and Effective Risk Management Strategies, International journal of technology and systems, 9(2). https://doi.org/10.47604/ijts.2783

Rimboux, A., R. Dupre, T. D. Lagkas, P. G. Sarigiannidis, P. Remagnino, V. Argyriou, Smart IoT Cameras for Crowd Analysis based on augmentation for automatic pedestrian detection, simulation and annotation, International Conference on Distributed Computing in Sensor Systems, 2019. https://doi.org/10.1109/DCOSS.2019.00070

Rosario, F. & Massimo, M. (2017). An IoT System for Social Distancing and Emergency Management in Smart Cities Using Multi-Sensor Data, International Conference on Signal Processing, Informatics, Communication and Energy Systems.

Sarker, I. H. (2021). Cyber Learning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks. Internet of Things, 14, 100393.

Shivram, K. & VenkataKrishnan, R. (2021). Crowd monitoring system using image processing. A research Submitted at Sathyabama Institute of Science and Technology in fulfilment of the requirements for the award of Bachelor of Engineering Degree in Computer Science and Engineering. Sathyabama Institute of Science and Technology,

Sosnovsky, Y.V. (2022). Analysis of the components of information reliability of distributed systems for monitoring a critical agricultural object, None, 2022. https://doi.org/10.29141/2782-4934-2022-1-1-1

Tagarev, T., Sharkov, G., & Lazarov, A. (2020). Cyber Protection of Critical Infrastructures, Novel Big Data and Artificial Intelligence Solutions. Information & Security: An International Journal, 47(1), 7–10

Zou, X., L. Wang, R. Han, Embedded Cyber-Physical Systems for Monitoring and Optimization of Sports Facilities Using Consumer IoT (CIoT) and Edge Computing. IEEE transactions on consumer electronics, 2025. https://doi.org/10.1109/TCE.2025.3535162

Hidayat, A. & T. Sutabri, Optimalisasi Pengelolaan Fasilitas Kampus Menggunakan IoT untuk Monitoring Ketersediaan Ruang dan Peralatan. Jurnal Teknologi dan Sistem Informasi, 2024. https://doi.org/10.61132/saturnus.v3i1.517