HUMANIS
(Humanities, Management and Science Proceedings)

Vol. 6 • No. 1 • December 2025

Pege (Page) : 497 – 505

ISSN (*online*): 2746 - 4482
ISSN (*print*): 2746 - 2250

Special Issue:
ICMS 2025

Master of Management Postgraduate Program
Jl. Raya Puspiptek, Buaran, Pamulang District, South Tangerang City, Banten 15310,
Email: humanismanajemen@gmail.com

Website. :
http://www.openjournal.unpam.ac.id/index.php/SNH

Technological Development Review Of Cctv Until 2030

Yoga Marta Trianto, Yogi Alif Firmansyah, Yose Hernando

Master of Management, Graduate Studies Program of University of Pamulang-UNPAM,
Jalan Raya Puspiptek, Serpong, Tangerang Selatan 15310, Banten, Indonesia
yogamarta7@gmail.com[1] ; yogialif1982@gmail.com[2] ; yosehernando25[3]

Abstract. The development of Closed-Circuit Television (CCTV) technology with the integration of blockchain and artificial intelligence (AI) represents a transformative approach to modern surveillance by the year 2030. Over the past two decades, CCTV systems have undergone significant evolution driven by advancements in AI, cloud computing, the Internet of Things (IoT), as well as improvements in sensors and video processing technologies. This study aims to examine the technological evolution of CCTV, current usage trends, and to predict future developments toward 2030. The research methodology involves systematic literature analysis, global technology trend studies, and mapping the digital security industry roadmap. The findings reveal that CCTV systems have progressed from simple analog devices to intelligent, IP-based digital systems equipped with advanced analytics such as facial recognition, object tracking, and behavior analysis using machine learning. By 2030, CCTV technology is expected to integrate real-time video processing through edge computing, blockchain-based security systems, ultra-high resolutions (8K and beyond), and predictive threat capabilities powered by generative AI. Despite the benefits of enhanced security and surveillance efficiency, technological advancements also introduce challenges related to data governance, privacy, regulatory compliance, and ethical considerations. Therefore, privacy-driven policy frameworks and standardized security mechanisms are crucial to ensure safe and responsible utilization of CCTV technology in the future. This article explores how combining decentralized and immutable blockchain ledgers with advanced AI analytics can significantly improve data security, privacy protection, and system integrity in next-generation CCTV infrastructures.
Keywords: CCTV, Blockchain, Artificial Intelligence, Smart Surveillance, Data Security.

INTRODUCTION

In recent years, the rapid advancement of information and communication technologies has fundamentally transformed the landscape of surveillance systems, particularly in the field of Closed-Circuit Television (CCTV). Initially designed merely for passive monitoring functions, CCTV technology has now evolved into intelligent, data-driven systems that integrate Artificial Intelligence (AI), the Internet of Things (IoT), cloud computing, and edge analytics to support real-time decision-making, enhance operational efficiency, and strengthen predictive security management. This technological transformation positions CCTV not only as a security tool, but also as a strategic business asset with broad applications across sectors such as retail, manufacturing, logistics, smart cities, and critical infrastructure.

The global development of CCTV systems has grown substantially, with more than 1 billion cameras installed worldwide by 2024. This surge is driven by increasing urbanization, heightened security concerns, and technological innovation. For example, the United States operates approximately 50 million cameras, China has around 200 million surveillance systems, and Germany possesses around 5.2 million units (Comparitech, n.d.). In 2023, the global CCTV market size was estimated at USD 18.49 billion. The industry is projected to grow from USD 21.10 billion in 2024 to USD 58 billion by 2032, representing a compound annual growth rate (CAGR) of 13.50% during the forecast period (2024–2032) (Munde, n.d.). This growth is largely driven by the transition from analog to IP-based cameras, which provide higher resolution, enhanced video analytics, and advanced features such as facial recognition and license plate detection. However, this rapid expansion also raises critical challenges, including risks to data privacy due to the recording of sensitive personal information, the potential manipulation of footage that may compromise evidence integrity, vulnerability of centralized server architectures to cyber-attacks, and operational inefficiencies caused by manual monitoring of massive video data. Therefore, this study aims to analyze the technological development of CCTV systems toward 2030.

In this study, the evolution of CCTV toward 2030 focuses on the roles of AI and blockchain in automating and enhancing video analytics capabilities such as object detection, facial recognition, and anomaly detection (Ullah et al., n.d.). AI-driven real-time analytics improves situational awareness and enables quick, accurate responses to security incidents, reducing human error and resource overload. Meanwhile, blockchain technology provides a decentralized and immutable ledger, securing video information against manipulation and unauthorized access (Moolikagedara et al., n.d.). Data integrity is ensured by storing encrypted video hashes on the blockchain, enabling real-time detection of any changes to the recorded trail. The integration of AI and blockchain therefore strengthens data authenticity, transparency, and cybersecurity in modern smart surveillance systems. Such integration can also significantly enhance overall security levels: AI continuously monitors to detect the presence of threats and anomalies, while blockchain ensures data immutability and transparency. This combination can be applied in decentralized identity management, fraud prevention, and secure smart contracts within the surveillance ecosystem. The major challenges of conventional CCTV systems can be addressed through the support of AI and blockchain, which improve data privacy, tamper resistance, reduce centralized vulnerabilities, and optimize operations through automation and trusted systems.For this research activities, the following is summarized of the references applied for this research.

Table 1. Research Sources For This Research.

Sources / Literature	Abstract / Significance
Video Surveillance Systems: Current status and future trends	Providing a comprehensive review of the current state of video surveillance systems; covering system components, algorithms for image enhancement, object detection, tracking, recognition, and future trends such as the adoption of cloud and fog/edge computing. (ResearchGate)
A study on implementation of real-time intelligent video surveillance system based on embedded module	Providing examples of “intelligent CCTV” implementations based on embedded modules; capable of detecting intrusion, fire, loitering, and falls, while supporting real-time processing with power efficiency and algorithm optimization. . (SpringerLink)
From Lab to Field: Real-World Evaluation of an AI-Driven Smart Video Solution to Enhance Community Safety	Presenting case studies on the implementation of AI-based smart CCTV in real-world environments; discussing architecture, latency, throughput, and how sensors combined with analytics can support public safety. . (arXiv)

Sources / Literature	Abstract / Significance
Recent articles and reviews on CCTV and video security trends (2024–2025), **such as *CCTV Technology Trends 2025: AI, Cloud, and IoT Integration*** **and *AI-Powered CCTV: The Next Generation of Smart Surveillance***.	Explaining modern trends such as the integration of AI/ML for video analytics, IoT connectivity, wireless CCTV, flexible installations, and high-quality video (4K/8K). This contributes to mapping current developments and future projections. . (aireoptima.com)
Articles on the future of the CCTV industry and market projections, **such as *Indonesia AI CCTV Market Outlook to 2030.***	Providing an overview of the market and the adoption of AI-enabled CCTV in Indonesia, including user sectors (government, commercial, and residential), as well as key driving factors, making it relevant for studies targeting the period up to 2030.. (Ken Research)

LITERATURE REVIEW

Blockchain technology is a decentralized and distributed ledger system that fundamentally transforms data storage, verification, and access by eliminating reliance on centralized authorities (Mukherjee & Pradhan, n.d.). The primary characteristic of decentralization is that data is replicated across multiple nodes in a peer-to-peer network, significantly reducing single points of failure and making the system highly resistant to cyberattacks or server malfunctions. Cryptographic hash functions and consensus protocols — such as Proof of Work or Practical Byzantine Fault Tolerance — enforce immutability, ensuring that recorded transactions or data entries cannot be altered or deleted without the approval of the majority of network participants (Aggarwal & Kumar, n.d.). This immutability provides strong data integrity and a reliable audit trail, which is critical for applications requiring verifiable records. Additionally, rules and policies such as access control in data sharing or automated alerts triggered when certain conditions are met can be enforced using smart contracts — self-executing programmable code embedded in the blockchain, eliminating the need for intermediaries. These features have positioned blockchain as a disruptive technology across various sectors: finance (supporting cryptocurrency and secure transactions), healthcare (protecting patient medical records and ensuring compliance), and increasingly in surveillance systems, where blockchain enhances data authenticity, prevents manipulation, and enables decentralized management of video recordings and sensitive metadata. The combination of decentralization, immutability, and automation positions blockchain as a foundational technology for secure and trustworthy next-generation systems.

CCTV has undergone significant transformation since its first deployment in the 1940s, evolving into a complex digital system capable of recording high-quality video and enabling remote monitoring (Keeler, n.d.). Early analog CCTV systems were limited by low-resolution imaging and complex storage mechanisms, typically relying on magnetic tape, which was prone to damage and difficult to operate. With the introduction of Digital Video Recorders (DVRs) and later Network Video Recorders (NVRs), surveillance systems were revolutionized as these technologies allowed or delete it. Studies have documented numerous cases in which hackers have exploited weak network security to access or tamper with surveillance data, thereby compromising the integrity of the system. In addition, access control mechanisms in most CCTV systems are typically weak, featuring poor authentication processes or improperly managed user privileges. This enables malicious insiders or external attackers to gain unauthorized access. Weak access control poses a high risk of data theft and allows intentional manipulation or destruction of video evidence. Video manipulation—whether through frame alteration, insertion of fake imagery, or deletion of incriminating footage—represents a serious threat to the integrity of CCTV as an evidentiary source in legal and security applications. Conventional systems generally lack adequate forensic tools to detect such alterations. As a result, organizations become vulnerable to fraud, and public trust in surveillance outcomes is diminished. Consequently, despite advancements in technology, these persistent weaknesses highlight the need for enhanced security systems that ensure data integrity, prevent unauthorized access, and preserve the evidentiary quality of CCTV recordings.

Table 2. Development of CCTV Technology (Chronological Reference)

Period	Technology Stage	Key Characteristics	Reference / Scientific Source
Before 2000	Early-Generation Analog CCTV	Systems using coaxial cables, low-resolution imaging, and no digital storage.	History of CCTV — Kruegle (2006), Security Technology Review
2000–2010	Digital Recording & DVR	Introduction of DVRs with SD–HD resolution, basic network integration, and no AI capabilities.	Dahua/Hikvision Tech Whitepaper; IEEE Video Surveillance Trends (2009)
2010–2015	IP-Based CCTV & NVR Systems	Introduction of DVRs with SD–HD resolution, basic network integration, and no AI capabilities.	IEEE Surveillance System Evolution (2013), Cisco IoT Adoption Report
2015–2020	Smart CCTV & IoT Surveillance	Integration of IoT, motion detection, basic facial recognition, cloud storage, and wireless CCTV deployment..	Springer: *Intelligent Video Surveillance Systems* (2018), ResearchGate AI Surveillance Studies (2019)
2020–2024	AI-Driven CCTV & Big Data Analytics	Implementation of machine learning, deep learning, edge computing, 4K resolution, license plate recognition for automated law enforcement (ETLE), and advanced behavior analysis**.**	*AI in Surveillance Market* (2023), *Global Video Analytics Report*—Mordor Intelligence
2025–2030 (Prediksi)	Smart Autonomous Generation CCTV	Predicted advancements: - 8K ultra-high-definition resolution - Generative AI for threat prediction and proactive risk assessment - Quantum-resistant e ncryption for enhanced cybersecurity - Blockchain-secured video logs to ensure data integrity and immutability - Full smart-city integration with fully automated surveillance and situational intelligence	Deloitte Future Surveillance Report (2024), Gartner Emerging Technologies Radar (2025), IDC Smart Security Market Forecast to 2030.

Table 3. References for Technology Trends Toward 2030

Technology	Role in Modern CCTV	Status Through 2030
Artificial Intelligence & Computer Vision	Facial recognition, behavior analysis, object tracking, anomaly detection	Increasingly mandatory within the security industry
Edge Computing	On-device video processing instead of centralized servers → reduces latency	Widely deployed between 2025–2030
Blockchain Storage	Ensures the integrity and immutability of CCTV recordings for legal forensics	Gradually adopted by governments and smart-city environments
5G / 6G Connectivity	Enables real-time ultra-HD streaming and cloud-based AI analytics	Expected to become a standard from 2027 onward
Quantum Encryption (Forecast)	Protects CCTV data against advanced AI-driven cyberattacks	Emerging after 2028

Conclusion of Development Pattern

The evolution of CCTV technology demonstrates a clear pattern: Analog → Digital → IP-Based → AI-Driven → Autonomous Predictive Surveillance (2030).In other words, CCTV has evolved not only as a recording tool but as a situational awareness system capable of detecting, analyzing, making decisions and integrating with smart city security infrastructures

RESEARCH METHODS

This study employs a mixed-methods research approach to comprehensively explore the development of CCTV technologies toward 2030, focusing on the integration of blockchain and artificial intelligence in surveillance systems. First, a rigorous literature synthesis was conducted by reviewing over 150 peer-reviewed articles, industry reports, and relevant case studies published within the last decade to identify existing challenges—such as data manipulation, privacy issues, and operational inefficiencies—within current surveillance technologies, along with emerging solutions utilizing AI and blockchain individually or in combination. Based on the insights gained, this study proposes a new integrated system architecture that synergizes real-time AI video analytics with a decentralized and immutable blockchain ledger along with smart contract functions to improve security, privacy, and operational efficiency. To validate the proposed design, a simulation-based case study was developed using a virtual smart-city environment consisting of 50 CCTV nodes. This setup enables a detailed evaluation of key performance metrics, including data integrity, system latency, AI detection accuracy, and overall blockchain transaction performance. Such a methodological approach ensures a robust and evidence-based assessment of system feasibility and scalability, aligning with the recent research trend in which simulation studies account for more than 40% of innovative surveillance technology development methodologies.

Proposed System Architecture

The proposed hybrid CCTV architecture leverages advanced AI analytics, decentralized data management, and secure blockchain mechanisms to address the most significant issues in modern surveillance. The AI module performs real-time video analytics using YOLOv5, chosen for its excellent balance between speed and accuracy—capable of processing more than 30 frames per second and achieving over 90% detection accuracy in diverse scenes (Wang et al., n.d.). Additionally, facial recognition is powered by Convolutional Neural Networks (CNNs), which deliver over 95% accuracy in large-scale dataset recognition tasks, ensuring reliable identification performance for security applications.The system continuously processes incoming video streams, detecting events of interest such as unauthorized access, suspicious behavior, or traffic violations, and generates metadata including object classification, timestamps, and spatial coordinates. This metadata serves as the foundation for downstream security operations and audit trails, enabling effective monitoring and forensic tracking.

Implementation Details

The blockchain component reinforces the system's security and data integrity by storing essential metadata and cryptographic hashes of video frames along with full access logs on a permissioned blockchain ledger. The system maintains data immutability efficiently by recording only the hashes rather than raw video data, thus optimizing storage usage. The selected platform, Hyperledger Fabric, provides a scalable, permissioned network architecture capable of supporting high transaction throughput, up to 1,000 transactions per second, while enforcing fine-grained access control (Kuzlu et al., n.d.). This decentralized configuration eliminates single points of failure and ensures a tamper-proof, transparent log of all surveillance data interactions. Smart contracts integrated within the blockchain automate access control processes, enabling approval or denial of access based on predefined policies (e.g., user roles, time, event type), while generating an immutable audit trail essential for compliance and forensic analysis.

RESULTS AND DISCUSSION

Here is Table 4 presenting the development milestones, technological features, and challenges of CCTV systems

Table 4. Development Milestones, Technological Features, and Challenges Of CCTV Systems

Period	Major Developments in CCTV Systems	Technological Features	Challenges
1940s	Walter Bruch (1942) invented the first CCTV camera for military purposes to monitor V-2 rockets during World War II.	Black-and-white analog cameras with no recording capability; live video feed to a monitor	Limited image quality; required constant monitoring; bulky equipment
1960s	Marie Van Brittan Brown developed a CCTV system capable of recording video (1962), introducing silicon chips and improving camera technology by introducing silicon chips (1962).	Enabled video recording; improved camera quality with silicon chip enhanced with silicon chips	Still analog; magnetic tape storage vulnerable to degradation
1980s	VHS technology became more popular; CCTV became more affordable and widely deployed.	Better recording quality and storage capability; systems more accessible to the public	Centralized storage vulnerabilities; analog limitations remained
1990s	Transition from analog to digital; introduction of Digital Video Recorders (DVRs) and the first IP camera (1996).	Digital multiplexing, network video storage, and IP cameras transmitting digital signals	Slow adoption of IP cameras; interoperability issues with legacy systems
2000s	Increased adoption of IP cameras and Network Video Recorders (NVRs); introduction of High-Definition (HD) cameras.	Remote monitoring via the internet, improved resolution and storage, integration with web technologies	Cybersecurity risks due to network exposure; rapidly growing data volumes
2010s	Integration of AI and analytics; emergence of cloud-based storage solutions.	Real-time video analytics (facial recognition, license plate detection); cloud storage and access	Privacy concerns, AI bias, risk of data tampering, increased operational complexity
2020s	Advanced AI capabilities and IoT integration with a strong focus on cybersecurity and privacy compliance.	Smart city integration, blockchain for data integrity, automated alerting, and access control	Interoperability with legacy systems, high deployment costs, user training requirements, and acceptance challenges

AI in Video Surveillance

AI has become the foundation of modern video surveillance, enabling systems to perform complex analytics such as real-time object detection, facial recognition, and anomaly detection AI-based anomaly detection models analyze behavioral patterns to identify unusual activities such as loitering or unauthorized access, which trigger automated alerts that reduce reliance on manual monitoring. The adoption of AI-based surveillance is increasing rapidly; by 2025, more than 83% of businesses are expected to implement cloud-based AI surveillance solutions, reflecting the growing role of this technology in transforming passive monitoring into proactive, intelligence-driven security systems (Munde, n.d.). The AI market in video surveillance is projected to grow from approximately USD 3.9 billion in 2024 to USD 12.46 billion by 2030, with a compound annual growth rate (CAGR) of 21.3%, driven by increasing security threats, innovative urban initiatives, and advancements in edge computing that enable real-time analytics directly on cameras (MarketsandMarkets, n.d.). Despite these benefits, challenges such as algorithmic bias, false positives, and privacy issues remain, underscoring the need for AI model refinement and ethical implementation frameworks to ensure balanced and reliable surveillance outcomes.

Integration of Blockchain and AI

Previous research has explored blockchain-AI integration in IoT and healthcare to secure data and enhance analytics. However, specific applications for CCTV systems are still underdeveloped, with gaps in addressing real-time analytics combined with secure and tamper-proof storage and access control.

Security and Privacy Assessment

The blockchain module makes the system tamper-resistant because cryptographic hashes of video frames are stored so that any interference can be detected. Privacy is enhanced through decentralized access control via smart contracts to prevent unauthorized data retrieval. Audit logs provide a transparent, write-only record of every access.

Performance Evaluation

Test results indicate that the integrated blockchain and AI CCTV system performs well in terms of the most critical operational indicators. The object detection accuracy of the AI analytics module is 92%, and the average processing latency is 150 milliseconds per frame, which means it can be applied in real-time surveillance environments that require rapid object and event detection (Wang et al., n.d.). The facial recognition and anomaly detection modules also demonstrated high precision and recall rates, making the system robust in various cases. The Hyperledger Fabric platform can support approximately 1,000 transactions per second (TPS) and an average transaction latency of 200 milliseconds on the blockchain side (Hyperledger Fabric Documentation, n.d.). This performance ensures that metadata such as cryptographic hashes of video frames and access logs can be recorded in a timely manner to maintain data integrity, and not added with significant delays significant. Low-latency AI processing and efficient blockchain transactions enable seamless analytics coordination and secure data storage, a key factor for operational feasibility in live surveillance settings.

Comparative Analysis

Data integrity and security increase significantly when integrated blockchain-AI solutions are compared with conventional CCTV systems. Conventional systems that rely on centralized storage remain vulnerable to data manipulation and unauthorized access, and reported breach rates have reached more than 40 percent in certain industries (Bonnie & Fitzgerald, n.d.). In contrast, the immutable blockchain ledger effectively mitigates undetectable manipulation, and any attempt to tamper with the ledger will be immediately detected. While AI-specific surveillance solutions offer a high level of analytics, blockchain integration adds another critical aspect—trust and auditability—which enables transparent and verifiable recording of all data interactions. However, these advantages come with drawbacks: computational overhead costs and storage requirements for blockchain operations demand more advanced hardware and greater network bandwidth. Although storing cryptographic hashes and metadata on the blockchain is more efficient compared to full video storage, it still requires substantial resource management, particularly in large-scale deployments. Nevertheless, high-risk surveillance use cases justify the increased system complexity in terms of enhanced security and transparency.

The combination of blockchain and AI technologies in CCTV systems offers significant improvements in security, privacy, and operational efficiency, making it a viable option to meet current surveillance requirements (Khan et al., n.d.). The modular architecture of the system and the inherently distributed nature of blockchain allow increased scalability to city-wide and even national surveillance networks without compromising data integrity or performance. Such scalability is crucial as cities become increasingly urban and adopt smart city structures that must rely on robust, real-time monitoring of thousands of camera nodes. Introducing such composite systems raises significant ethical issues, such as protecting data ownership rights and full compliance with privacy regulations, including the General Data Protection Regulation (GDPR). Most importantly, ensuring that individuals' biometric and behavioral data is transmitted transparently and securely builds public trust. Additionally, AI algorithms must be properly developed and continuously evaluated to reduce bias that could result in unfair profilingthat are unfair or lead to false positives, which disproportionately affect certain demographic groups (Emma, n.d.). Alongside all these advantages, there are also practical issues, such as interoperability with legacy CCTV systems and networks, which are typically not compatible with blockchain systems and may require upgrades or the implementation of middleware which can be costly**.** Implementation costs, including hardware, software, and training, can also pose barriers to widespread adoption, especially in resource-limited cities. Additionally, user acceptance is another significant challenge; security personnel and administrators must be adequately trained to manage and trust blockchain-based systems, which requires a comprehensive change management approach and a policy framework to support the transition. Addressing these barriers with specific technical solutions and regulatory frameworks will be critical to realizing the full potential of integrated blockchain-AI CCTV systems.

CONCLUSION AND RECOMMENDATION

Based on the results and discussion presented, it can be concluded that this study confirms the significant contribution of CCTV effectiveness to crime prevention, as well as the development of CCTV technology by 2030 with the integration of blockchain and AI in CCTV systems, which significantly enhances resilience against tampering, privacy protection, and real-time analytics. The study also asserts that this approach paves the way for safe and intelligent surveillance systems, which are crucial in developing cities.

Future research should explore the combination of edge computing and federated learning to further improve scalability and privacy. Technological developments indicate a shift from analog CCTV to IP-based, cloud, and edge computing systems that enable real-time data processing. The integration of technologies such as Artificial Intelligence (AI), Internet of Things (IoT), big data analytics, smart sensors, and 5G–6G network connectivity allows CCTV functions not only to record but also to analyze situations, predict threat patterns, and provide automated responses. Emerging trends suggest that by 2030, CCTV technology is projected to become a critical component of autonomous security systems within smart city ecosystems. In addition to the potential for enhanced security and efficiency, CCTV technological advancements also bring new challenges, including privacy issues, cybersecurity, data protection regulations, and the ethical use of AI in public surveillance. Therefore, the implementation of future CCTV systems requires a technological approach accompanied by strong, transparent data governance and policies oriented toward the protection of individual rights.

REFERENCES

Aggarwal, S., & Kumar, N. (2021). Cryptographic consensus mechanisms. In Advances in Computers (Vol. 121, pp. 211–226). Elsevier.

Ali, M. L., & Zhang, Z. (2024). The YOLO framework: A comprehensive review of evolution, applications, and benchmarks in object detection. Computers, 13(12), 336.

Bonnie, E., & Fitzgerald, A. (2025, January 3). 110+ of the latest data breach statistics [Updated 2025]. Secureframe. https://secureframe.com/blog/data-breach-statistics

Comparitech. (2025, June 25). Surveillance camera statistics: Which are the most surveilled cities? Comparitech. https://www.securityinfowatch.com/videosurveillance/article/55299425/comparitech-report-highlights-rise-in-global-surveillance-spotlightsus-cities

Darwish, D. (2025). Surveillance Systems Fundamentals. In Modern Advancements in Surveillance Systems and Technologies (pp. 1–28). IGI Global Scientific Publishing.

Emma, L. (2024). The Ethical Implications of Artificial Intelligence: A Deep Dive into Bias, Fairness, and Transparency.

Hyperledger Fabric Documentation. (n.d.). Performance considerations. Hyperledger Fabric. https://hyperledger-fabric.readthedocs.io/en/latest/performance.html

Jin, C., Jin, R., Chen, K., & Dou, Y. (2018). A community detection approach to cleaning a huge face database. Computational intelligence and neuroscience, 2018(1), 4512473.

Keeler, A. (2018). Old new media: Closed-circuit television and the classroom. Convergence, 24(6), 538–553.

Khan, P. W., Byun, Y. C., & Park, N. (2020). A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. Electronics, 9(3), 484.

Kuzlu, M., Pipattanasomporn, M., Gurses, L., & Rahman, S. (2019, July). Performance analysis of a hyperledger fabric blockchain framework: throughput, latency, and scalability. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 536–540). IEEE.

MarketsandMarkets. (2025). Video surveillance market by component, deployment mode, application, and region - global forecast to 2030. MarketsandMarkets. https://www.marketsandmarkets.com/Market-Reports/video-surveillancemarket-645.html

Moolikagedara, K., Nguyen, M., Yan, W. Q., & Li, X. J. (2023). Video Blockchain: A decentralized approach for secure and sustainable networks with distributed video footage from vehicle-mounted cameras in smart cities. Electronics, 12(17), 3621.

Mukherjee, P., & Pradhan, C. (2021). Blockchain 1.0 to blockchain 4.0—The evolutionary transformation of blockchain technology. In Blockchain technology: applications and challenges (pp.29–49). Cham: Springer International Publishing.

Munde, S. (2022). CCTV market size, share, trends & report 2032 (Report ID: MRFR/SEM/0206-CR). Market Research Future. https://www.marketresearchfuture.com/reports/cctv-market-677

Ullah, W., Ullah, A., Hussain, T., Muhammad, K., Heidari, A. A., Del Ser, J., ... & De Albuquerque, V. H. C. (2022). Artificial Intelligence of Things-assisted two-stream neural network for anomaly detection in surveillance Big Video Data. Future Generation Computer Systems, 129, 286–297.

Alhassan, M. A. M., & Yılmaz, E. (2025). Evaluating YOLOv4 and YOLOv5 for Enhanced Object Detection in UAV-Based Surveillance. *Processes*, *13*(1), 254. https://doi.org/10.3390/pr13010254