iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67216

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Cloud-Enabled Deep Learning Framework for Public Security Video Investigation Systems

Varunendra Sharma[1], Unmukh Datta[2]
[1]*M.E Scholar,* [2]*Associate Professor, Department of Computer Science and Engineering, Maharana Pratap College of Technology, Gwalior, MP*

Abstract: ***The incorporation of deep learning methods into public security video investigation systems is investigated in this review article with special attention to their transforming ability in improving real-time surveillance and crime prevention. With the rapid developments in machine learning and computer vision, deep learning models which includes Convolutional Neural Networks, and Recurrent Neural Networks (RNNs) have shown astonishing capacity in automating video surveillance tasks including finding objects, activity recognition, and anomaly detection. These models are highly useful for public safety operations since they enable crowd management, identification of suspicious behaviour, and even specific actions like theft or assault.***

Examining the technical architecture of these systems, the paper emphasises on the part edge computing and cloud computing play in allowing scalability and real-time data processing. While edge computing provides localised processing to lower latency and increase response times, cloud-based solutions guarantee perfect integration and storage of vast video information. Moreover, the study tackles the difficulties in applying deep learning in public security including privacy issues, data security, ethical questions, and the necessity of laws.

Notwithstanding these difficulties, the research underlines how these technologies might help to enhance security operations, lower human error, and raise operational efficiency.

Future research directions—such as improving model robustness, combining multimodal data sources, and creating more ethical and transparent artificial intelligence systems—also come out of the review. In the end, this paper offers a thorough summary of the present situation and future possibilities of deep learning in public security video investigation systems, so illuminating their ability to change the scene of public safety.

Keywords: Deep Learning, Public Security, Video Surveillance, Anomaly Detection, Cloud Computing

I. INTRODUCTION

Often used in law enforcement, security, and forensic applications, advanced technology solutions meant to analyse, process, and extract actionable insights from video data are known as video investigation systems These systems track items of interest in real-time or from archival footage using features such video analytics, object recognition, facial recognition, motion detection, and behavioural analysis.

By Using artificial intelligence (AI) & machine learning (ML), they raise the accuracy and efficiency. of investigations, thereby facilitating the detection of abnormalities, pattern identification, and correlation of events spanning several video sources. Modern video investigation systems preserve data integrity and security while being linked with cloud-based platforms that enable flawless storage, retrieval, and sharing of video evidence over distributed networks [1], [2]. These technologies guarantee safety rule compliance and support several uses including traffic monitoring, incident reconstruction, and crime scene analysis. To raise the quality of low-resolution or hidden footage, they are sometimes furnished with tools for video enhancement like noise reduction, frame rate change, and image sharpening.

Advanced systems might also integrate time-stamping and geo-tagging tools, therefore enabling contextual analysis and offering vital evidence in court procedures. Concerns regarding privacy are growing, hence these systems follow rigorous legal guidelines to guarantee moral use and reduce the exploitation of surveillance data. Modern security ecosystems cannot function without video investigation systems, which provide scalability, accuracy, and flexibility to handle changing issues preserving public safety and order [3]–[5].

Fig. 1 Video Investigation Systems [6]

A Cloud-Enabled Deep Learning Framework for Public Security Video Investigation Systems offers a novel method to improve video analytics for incident response, public safety, and criminal prevention. To evaluate enormous volumes of video footage in real time and enable actionable insights for public security authorities, this system combines cutting-edge deep learning algorithms with the scalability and efficiency of cloud computing. These systems can analyse high-quality video inputs from many sources—including CCTV cameras, drones, and body-worn cameras—including CCTV cameras, drones, and minimum latency by using the computational capability of the cloud. Trained to execute tasks like facial awareness, object identification, anomaly detection, & behaviour analysis Deep learning aspects of the framework—convolutionsal neural networks (CNNs) & recurrent neural networks (RNNs)—are remarkably accurate. These qualities considerably increase the efficiency of security. operations by enabling the system to spot criminals, find missing objects, and track crowds for suspicious activity. The capacity of cloud integration to offer nearly limitless storage and processing resources—which are vital for managing the rising volume and complexity of video footage produced in public areas—is a big benefit. The architecture provides real-time data streaming and processing, therefore allowing security agencies to act fast in crucial events. Furthermore, the centralised design of the cloud enables several stakeholders—law enforcement, forensic professionals, and emergency responders—to access and examine data concurrently from several sites, so facilitating cooperative investigations. Modern encryption and safe access mechanisms provide the protection of private information, therefore addressing issues about data breaches and privacy [7], [8]. Edge computing is also included into the system to augment cloud capabilities and enable local preliminary data processing at the data source. In settings with restricted connectivity, this hybrid method guarantees continuity of operations, lowers bandwidth use, and lessens stress on cloud servers. Trained on large datasets, the deep learning models applied in this framework identify anomalies with great accuracy. CNNs are used, for instance, for image and video categorisation, thereby helping to identify weapons, license plates, and faces. Using their capacity to grasp temporal sequences, RNNs provide behaviour prediction and activity recognition, therefore enabling the system to detect possible hazards in real time. Often used to fit pre-trained models to certain public security situations, transfer learning methods help to save computing resources and time by doing so. Moreover, the system uses unsupervised learning techniques for anomaly detection—that is, for the identification of odd trends or behaviours deviating from the norm even in the lack of labelled training data.

This framework's main characteristic is scalability since it can be used all over areas to track public gatherings and major events throughout cities. By means of cloud-native tools and microservices architecture, the system guarantees dynamic resource allocation depending on demand, thereby preserving good performance under diverse workloads. The framework also links with Internet of Things (IoT) devices including smart cameras and sensors to boost its capacities. IoT integration allows geotagging, environmental monitoring, connecting of video footage with other data streams—including media feeds and emergency notifications conceivable. This whole method provides a complete situational awareness that enhances crisis decision-making. The performance of the framework is maximised using noise reduction, frame interpolation, & resolution enhancement. These techniques improve the quality of video data, thereby supporting the significant feature extraction technique for deep learning models. By combining hours of video footage into short pieces utilising video summarising technologies, the framework additionally emphasises significant events and reduces the time needed for hand inspection. Natural language processing (NLP) integrated for automatic tagging and metadata development helps to simplify data management and retrieval even more. Implementing such systems presents a major difficulty in guaranteeing adherence to ethical and legal standards [9], [10].

Strong privacy-preserving features like anonymising personal data, differentiated privacy approaches, and data governance policy adherence are included into the system. Automated auditing systems track video data use to guarantee responsibility and stop abuse. Public awareness efforts also aim to inform people on the advantages and protections of the system, hence building acceptance and confidence. The great influence of the framework on public security helps to enable faster response times, better investigation accuracy, and more effective resource allocation. The system releases human resources for strategic decision-making by automating routine processes such evidence compiling and video review. Predictive analytics improve its value even more since it helps to understand criminal trends and supports proactive prevention of events. Future-proof the system by means of the cloud-enabled infrastructure, which guarantees that it stays flexible enough to accommodate developing technologies such advanced artificial intelligence models and quantum computers [11], [12].

II. RELATED WORK

Ibrahim 2022 et al. [13] has become a necessary in our life, especially following the epidemic of the era of COVID-19, and with the increase of overlapping data over the Internet and networks with an increasing and great speed, the need of protecting those data and applications, especially as the usage of cloud computing, increases. Objectives: Searching for the best solutions to provide the necessary protection against data risks via cloud computing, thus the demand has become more urgent to access enormous storage resources and applications easily and process them anywhere with flexibility and better security. Methods: This work uses one of the encryption techniques to encode a large collection of images; subsequently, we used the Convolutional Neural Network (CNN) algorithm, a frequently applied deep learning method for picture identification. Deep learning undoubtedly has many models that let to expedite and increase the accuracy in the appearance of the results, including the ResNet50 model, in which we developed the model by training many encrypted photographs. Without decoding the encrypted photos, this model helped them to classify and identify them. Results: It was shown that the deep learning method of the ResNet50 model could be applied to classify encoded images such that the encrypted image could be found without decodes. On the test set, the proposed model scored 99.75%, Recall (94.12%), Precision (94.23%), and F1-score (94.70%). This implies the feasibility of this approach for categorising encoded images in class.

Attaallah 2022 et. al [14] has led to significant improvements and breakthroughs. With the advent of digital healthcare, early disease diagnosis is now within reach, and more people have simpler access to the services they need. Despite these encouraging results, everyone involved is understandably worried about the safety of patient information. The healthcare industry is among the most common targets of cybercrime, according to data breach statistics. Breach rates involving sensitive patient information have increased at an alarming rate in the past few years. Professionals in the healthcare industry are developing new strategies, procedures, and technologies to deal with the problem of healthcare data security. With respect to big organisational conditions, the author has highlighted the crucial measurements and criteria to ensure a vast volume of data in this work. Preventing businesses and programmers from accomplishing their objectives is the purpose of security measures. Using multiple iterations of two historical approaches to big data security analysis, this work seeks to catalogue and rate the security procedures used to detect and resolve issues. The authors are utilising the Fuzzy Analytic Hierarchy Process (Fuzzy AHP) method to examine data security in general and prioritise its importance. Plus, we have done quantitative research on the most important weight-related aspects. Experts can use the findings to strengthen the safety of big data.

Minaee 2022 et al. [15] There are a number of segmentation methods published in academic journals; these methods have several important applications such as scene interpretation, medical image analysis, robotic perception, video surveillance, augmented reality, and picture compression. This is where the new photo segmentation approaches that use DL models came from, motivated by the widespread popularity of DL. A convolutional pixel-labeling network, an encoder-decoder architecture, a multiscale and pyramid-based approach, a recurrent network, a visual attention model, and generative models in adversarial settings are all part of the novel work in semantic and instance segmentation that we survey in detail. We take a look at the connections, advantages, and disadvantages of these DL-based segmentation models, go over the often utilised datasets, compare their performances, and discuss intriguing avenues for further research.

Chen 2022 et al. [16] should prove useful in a variety of settings and has promising future prospects. The development of numerous interdependent technologies is the backbone of the Metaverse. Thus, it is undeniable that the expanding Metaverse poses more complex and consequential security concerns. Along with introducing several technologies that are relevant to the Metaverse, we also discuss some potential privacy and security issues that may arise in the Metaverse. We offer modern privacy and security in the Metaverse as a consequence of these technical advancements. In addition, we raise a number of important concerns regarding the potential Metaverse.

Taking everything into account, this survey provides a comprehensive examination of the privacy and security issues raised by key technologies in Metaverse applications. The results of this poll should point researchers in the direction of promising new directions for Metaverse development, particularly with regard to privacy and security.

Reed 2022 et al. [17] washed over by an era of smartphones and cloud computing, which had far-reaching consequences for the future of contemporary scientific computing. A critical juncture has arrived in the history of high-performance computing (HPC). Over the last 60 years, national labs in the US have commissioned nearly all of the world's fastest supercomputers for scientific research. Transitions are commonplace these days. Expenses are now exceeding the limits of U.S. government funding for advanced computing, even though Japan and China are leaders in the tailored HPC systems backed by government requirements. The political unrest surrounding production sites and the global shortage of semiconductors are affecting everyone. There has been yet another fundamental change, perhaps even more significant. The major cloud providers have put money into global, extremely powerful systems that dwarf current HPC facilities. The increasingly processing-intensive nature of AI is driving the trend towards cloud systems built with custom semiconductors, which is putting pressure on traditional computing vendors financially. By breaking new ground in computer vision and game playing, these cloud systems are presently changing the way we think about scientific computation. Embracing end-to-end co-design, custom hardware configurations and packaging, large-scale prototyping (as was common thirty years ago), and cooperative partnerships with leading computing ecosystem companies, smartphone vendors, and cloud computing vendors will help build the next generation of leading edge HPC systems by reevaluating many fundamentals and historical approaches.

TABLE 1 LITERATURE SUMMARY

Authors/year	Model/method	Research gap	Findings
Gill/2022 [18]	AI-driven autonomy enhances emerging computing paradigms' self-management capabilities.	Scalable AI/ML integration for autonomous, multi-paradigm resource management challenges.	AI/ML integration improves autonomy, but scalability and complexity remain challenges.
Pham/2022 [19]	Aerial computing bridges gaps, enhancing scalability, mobility, and smart applications.	Lack of comprehensive design and systematic review in aerial computing.	Aerial computing enhances mobility, scalability, and supports diverse smart applications.
Liang/2022 [20]	Edge YOLO improves object detection efficiency in autonomous vehicles, reducing energy.	Existing object detection systems lack energy efficiency and timeliness in vehicles.	Edge YOLO enhances efficiency, accuracy, and energy use in autonomous vehicles.
Montasari/2022 [21]	AI's national security uses raise legal, ethical, privacy, and human rights concerns.	Limited research on AI's ethical, legal, and privacy implications in security.	AI in national security poses risks to privacy, rights, and ethics.
Verma/2022 [22]	Smart vision-based surveillance systems detect suspicious activities using machine learning techniques.	Limited integration of advanced techniques for abnormal activity detection in surveillance.	Machine learning enhances surveillance, but challenges in accuracy and complexity persist.

III. CLOUD-ENABLED FOR VIDEO INVESTIGATION SYSTEMS

Using the scale and processing capability of cloud computing, cloud-enabled video investigation systems improve video monitoring and analysis for security and investigative uses. To provide effective data storage, real-time processing, and instant access to vast volumes of video data, these systems combine video feeds from many sources—security cameras, drones, mobile devices—into a central cloud platform. High availability and scalability guaranteed by cloud infrastructure let new devices and users to be smoothly integrated as necessary. Deep learning techniques are increasingly applied in these systems for video analytics uses such as behaviour analysis, object detection, face recognition, and anomaly detection. Executing complex ML models without causing edge hardware to crash is feasible by offloading the computational effort of processing and analysing video data from local devices by using cloud resources. Providing flexibility and efficiency, the cloud platform can dynamically distribute resources to satisfy the needs of massive video analysis [23], [24]. Among the main benefits of cloud-enabled video investigation systems are real-time analysis, centralised management of video data, and agency and location-based collaboration. Law enforcement departments can, for instance, instantly access and examine video material from several crime locations, therefore enhancing reaction times and decision-making. Furthermore, cloud solutions have strong security measures like encryption to guard private video footage from illegal access or manipulation.

Fig. 2 Cloud-enabled video investigation systems [25]

Notwithstanding these benefits, there are drawbacks like data privacy issues, limited network capacity, and the necessity of fast processing of enormous volumes of video data by effective algorithms. Furthermore, including artificial intelligence and machine learning models into video investigation systems calls for careful tuning to minimise false positives and produce accurate and dependable findings. Finally, cloud-enabled video investigation solutions are transforming security agency handling and analysis of video data. These systems provide strong tools for enhancing public safety, security, and operational efficiency by merging cloud computing with AI-driven analytics; yet, some issues still have to be resolved for best performance [26]–[29].

IV. DEEP LEARNING

Deep learning is a subfield of machine learning that focusses on modelling and processing complex data patterns using multi-layered artificial neural networks (ANNs). It excels at tasks that need a lot of data analysis, like picture identification, NLP, and speech synthesis. Automatic feature extraction from raw data is a key component of deep learning models, which reduces the burden of human feature engineers and makes it possible to make incredibly accurate predictions and decisions [30], [31].
Key Deep Learning Models:

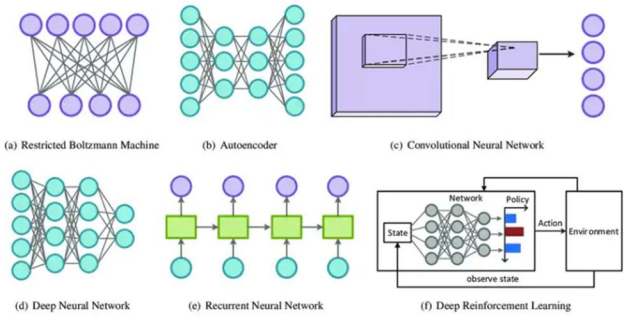


Fig. 3 Deep Learning Models

A. Convolutional Neural Networks (CNNs)

The processing of images and videos is the speciality of convolutional neural networks, or CNNs. Using convolutional layers to efficiently recognise data spatial hierarchies allows them to discover patterns and features: Object identification, face recognition, and medical imaging are just a few examples of the many visual data analytic applications that demonstrate CNNs' efficiency.

B. Recurrent Neural Networks (RNNs)

Apt for textual or time series sequential data,The inclusion of feedback loops allows Recurrent Neural Networks (RNNs) to retain the context of previous inputs. Superior variants, including LSTMs and GRUs, are better able to simulate long-range dependencies. Speech recognition, language translation, and stock market trend prediction are important uses [32]–[34].

C. Transformers

Because they employ self-attention approaches to discover connections between sequences, transformers perform admirably in natural language processing (NLP). Machine translation, text synthesis, and summarisation are just a few of the sophisticated applications made possible by popular technologies like BERT (Bidirectional Encoding Representations from Transformers) and GPT (Generative Pre-trained Transformer).

D. Generative Adversarial Networks (GANs)

In Generative Adversarial Networks (GANs), a generator produces data and a discriminator evaluates its validity; these two components work together to promote performance improvement through competition. Image synthesis, video editing, and style transfer are just a few of the numerous platforms where this framework excels in producing photorealistic results and innovative works of art.

E. Autoencoders

Autoencoders are a type of unsupervised learning neural network that uses encoding and reconstruction of input data to reduce data dimensionality and identify outliers. Jobs requiring minimal storage requirements and data compression (where denoising removes noise from data to improve usability and clarity) make heavy use of them.

F. Deep Belief Networks (DBNs)

Layered generative frameworks learnt hierarchically from unguided information are known as Deep Belief Networks (DBNs). DBNs are great for dimensionality reduction, picture classification, and audio recognition because they stack many layers of Restricted Rab Machines (RBMs), which allow them to identify patterns and extract features [35]–[38].

V. DEEP LEARNING FRAMEWORK FOR PUBLIC SECURITY VIDEO INVESTIGATION SYSTEMS

A Public Safety Framework for Deep Learning Using video analysis in a new and innovative way, Video Investigation Systems can automatically make communities safer. The need for more effective security measures is on the rise, and traditional surveillance systems, which mostly use human operators for video inspection, are finding themselves inadequate in the face of these rising crime rates. One powerful solution to these limitations is deep learning, a branch of AI that automates the real-time processing of massive amounts of surveillance data. In order to process and analyse video streams, the system employs a number of deep learning models, namely RNNs and convolutional neural networks (CNNs). Image recognition tasks are a good fit for convolutional neural networks (CNNs) because of their inherent ability to automatically detect and categorise objects and actions included within visual input. For purposes of public safety, CNNs can identify people, vehicles, and other objects of interest. Additionally, they are able to detect unusual conduct, such as an errant vehicle or a runner in an inappropriate area. On the other hand, RNNs excel at analysing video frames sequentially due to their architecture for sequential data processing. These systems are able to track people's whereabouts and actions, identifying patterns like loitering, unauthorised entry, or interpersonal interactions. Robot neural networks (RNNs) are able to predict potential future actions by processing video frames as a series of temporal data, which includes spotting an individual's intent prior to a crime happens, therefore providing preventative security measures. Deep learning's real-time analysis capability is among its most important benefits for public security video investigation systems. Conventional video surveillance systems depend on human operators to evaluate hours of footage, so prolonged response times and missing occurrences could follow. Deep learning algorithms can instantly identify questionable activity by automating this process, so giving security staff timely warnings. This lowers the possibility of security breaches and enhances general response times, therefore allowing faster intervention when needed [39], [40].

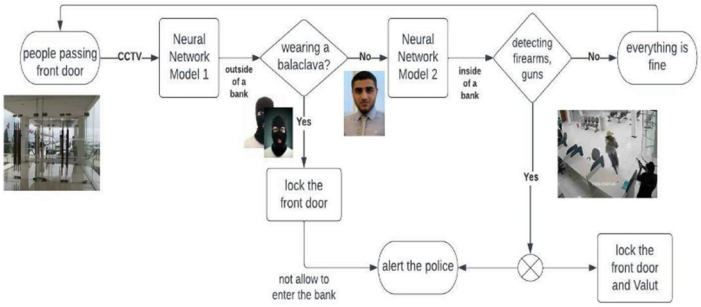


Fig. 4 Video Investigation Systems using deep learning [41]

Moreover, deep learning models help to combine several video sources—fixed cameras, drones, and mobile devices among others. Deep learning models' scalability allows the framework to effectively manage large-scale surveillance activities since it can process data from many cameras concurrently. Edge computing and cloud computing technologies improve this capacity and enable distributed computing.

While edge computing lets for real-time, on-site analysis, hence lowering latency and bandwidth needs, enormous datasets can be kept and examined in the cloud. Deep learning applied in public security improves video analysis's accuracy and dependability as well. Often depending on rule-based systems, which are prone to mistakes and may overlook important events, traditional approaches Trained on enormous volumes of labelled data, deep learning models can find trends that might not be clear to rule-based algorithms or human observers. As more data is exposed to these models, they keep becoming better over time, therefore guaranteeing that the system is more efficient as it is applied. Apart from danger detection, deep learning models can be applied for various chores such crowd surveillance, license plate recognition, and facial identification. In settings like airports, retail centres, and public transit systems—where security is a key concern—these tools are very handy. While license plate recognition helps track vehicle movements in and out of restricted zones, facial recognition systems can help identify known offenders or individuals of interest. Deep learning frameworks in public security video investigation systems present difficulties even if their obvious benefits. Privacy issues are major ones since continuous monitoring begs doubts about the possibility of personal data being used improperly. Legal and ethical requirements must be followed exactly; systems must be built to safeguard personal rights while nevertheless offering efficient security measures [42]–[45].

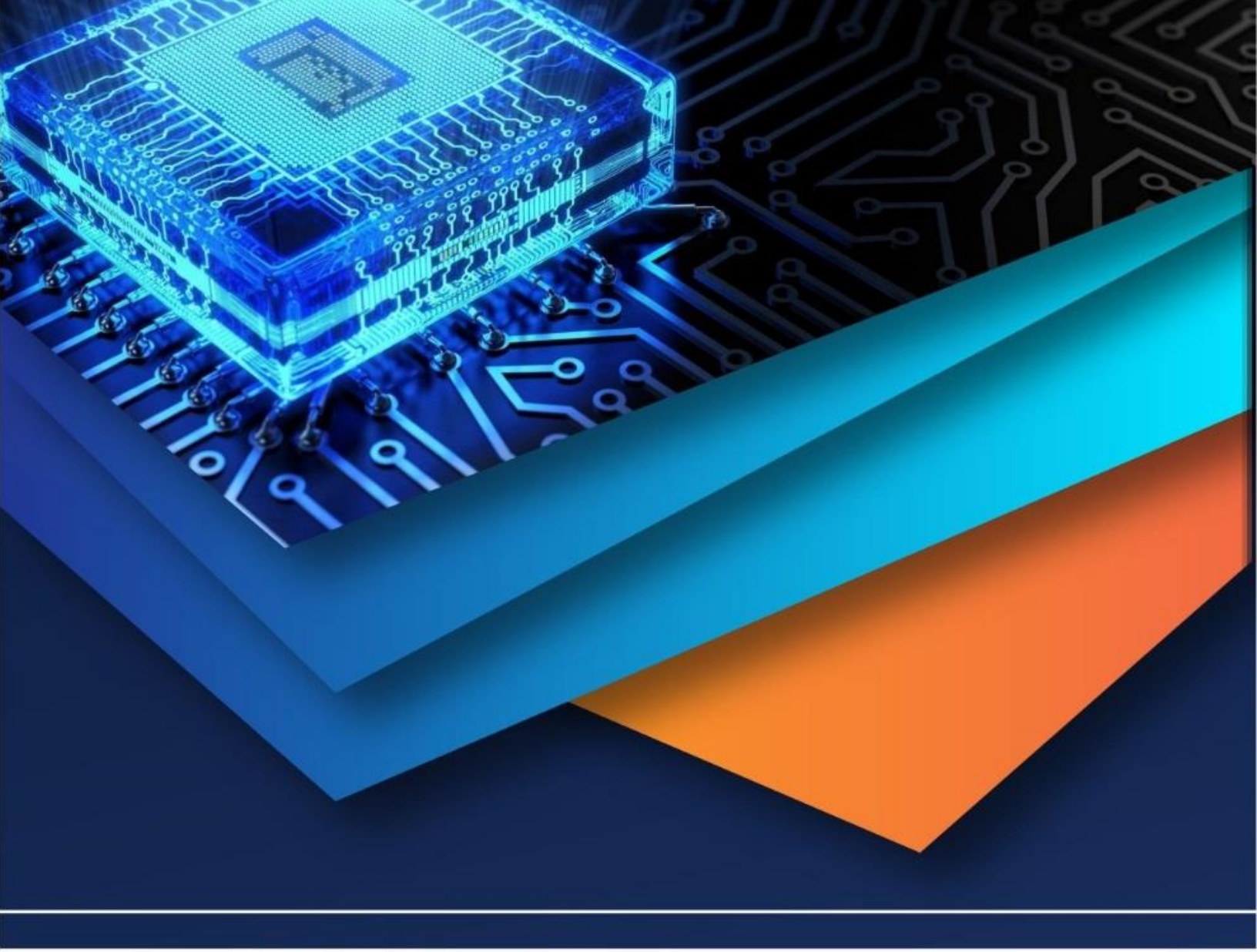
VI. CONCLUSION

Last but not least, this review piece highlights how automated video investigation systems powered by deep learning could change public safety. When coupled with other deep learning methodologies, advanced models such as Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) have significantly improved the accuracy and efficiency of security surveillance systems. By automating tasks like object detection, activity recognition, and anomaly detection, deep learning systems enable real-time, proactive responses to security threats. This reduces reliance on human operators and minimises response times. These systems are scalable, thanks to cloud and edge computing, so they can handle huge datasets from a variety of video sources without any hitches, ensuring complete coverage of public spaces. The ability of deep learning models to ingest massive amounts of data ensures that their accuracy and performance are always improving, making them ideal for environments that are unpredictable. Concerns around data security, privacy, and ethics must be thoroughly investigated in order to ensure the ethical use of new technologies. Open regulations and transparent regulatory frameworks are crucial for balancing security needs with personal privacy rights. Public safety video investigation systems powered by deep learning represent a huge leap forward in security technology since they hold the promise of smarter, more efficient, and safer public environments. Crime prevention, real-time surveillance, and public safety as a whole stand to benefit greatly from their incorporation into many public and private sectors, especially as these systems evolve. In order to enhance their impact on global security initiatives, future research and development should focus on enhancing these systems, resolving ethical concerns, and expanding their applications.

REFERENCES

[1] Y. Liu et al., “Generalized Video Anomaly Event Detection: Systematic Taxonomy and Comparison of Deep Models,” ACM Comput. Surv., vol. 56, no. 7, 2024, doi: 10.1145/3645101.
[2] Y. Abbas and A. Jalal, “Drone-Based Human Action Recognition for Surveillance: A Multi-Feature Approach,” Proc. - 2024 Int. Conf. Eng. Comput. ICECT 2024, no. October, 2024, doi: 10.1109/ICECT61618.2024.10581378.
[3] A. Awasthi et al., “Anomaly Detection in Satellite Videos using Diffusion Models,” 2023, [Online]. Available: http://arxiv.org/abs/2306.05376
[4] X. Chen, Z. Wang, Q. Hua, W. L. Shang, Q. Luo, and K. Yu, “AI-Empowered Speed Extraction via Port-Like Videos for Vehicular Trajectory Analysis,” IEEE Trans. Intell. Transp. Syst., vol. 24, no. 4, pp. 4541–4552, 2023, doi: 10.1109/TITS.2022.3167650.
[5] G. Ramesh, J. Logeshwaran, and V. Aravindarajan, “A Secured Database Monitoring Method to Improve Data Backup and Recovery Operations in Cloud Computing,” BOHR Int. J. Comput. Sci., vol. 2, no. 1, pp. 1–7, 2023, doi: 10.54646/bijcs.019.
[6] Z. S. Ageed, “Cloud computing resources impacts on heavy-load parallel processing approaches,” Researchgate.Net, vol. 22, no. 3, pp. 30–41, 2023, doi: 10.9790/0661-2203043041.
[7] A. Lakhan et al., “Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare,” IEEE J. Biomed. Heal. Informatics, vol. 27, no. 2, pp. 664–672, 2023, doi: 10.1109/JBHI.2022.3165945.
[8] Y. Wang, W. Wang, D. Liu, X. Jin, J. Jiang, and K. Chen, “Enabling Edge-Cloud Video Analytics for Robotics Applications,” IEEE Trans. Cloud Comput., vol. 11, no. 2, pp. 1500–1513, 2023, doi: 10.1109/TCC.2022.3142066.
[9] N. Nasser, Q. Emad-ul-Haq, M. Imran, A. Ali, I. Razzak, and A. Al-Helali, “A smart healthcare framework for detection and monitoring of COVID-19 using IoT and cloud computing,” Neural Comput. Appl., vol. 35, no. 19, pp. 13775–13789, 2023, doi: 10.1007/s00521-021-06396-7.
[10] F. M. Talaat and H. ZainEldin, “An improved fire detection approach based on YOLO-v8 for smart cities,” Neural Comput. Appl., vol. 35, no. 28, pp. 20939–20954, 2023, doi: 10.1007/s00521-023-08809-1.
[11] Y. Huang, Y. J. Li, and Z. Cai, “Security and Privacy in Metaverse: A Comprehensive Survey,” Big Data Min. Anal., vol. 6, no. 2, pp. 234–247, 2023, doi: 10.26599/BDMA.2022.9020047.
[12] B. Bansal et al., Big Data Architecture for Network Security, no. February. 2022. doi: 10.1002/9781119812555.ch11.
[13] J. Y. Ibrahim Alzamily, S. B. Ariffin, and S. S. Abu Naser, “Classification of Encrypted Images Using Deep Learning –Resnet50,” J. Theor. Appl. Inf. Technol., vol. 100, no. 21, pp. 6610–6620, 2022.
[14] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B. K. Gupta, and R. A. Khan, “Analyzing the big data security through a unified decision-making approach,”

Intell. Autom. Soft Comput., vol. 32, no. 2, pp. 1071–1088, 2022, doi: 10.32604/iasc.2022.022569.
[15] S. Minaee, Y. Boykov, F. Porikli, A. Plaza, N. Kehtarnavaz, and D. Terzopoulos, "Image Segmentation Using Deep Learning: A Survey," IEEE Trans. Pattern Anal. Mach. Intell., vol. 44, no. 7, pp. 3523–3542, 2022, doi: 10.1109/TPAMI.2021.3059968.
[16] Z. Chen, J. Wu, W. Gan, and Z. Qi, "Metaverse Security and Privacy: An Overview," Proc. - 2022 IEEE Int. Conf. Big Data, Big Data 2022, pp. 2950–2959, 2022, doi: 10.1109/BigData55660.2022.10021112.
[17] D. Reed, D. Gannon, and J. Dongarra, "Reinventing High Performance Computing: Challenges and Opportunities," pp. 1–22, 2022, [Online]. Available: http://arxiv.org/abs/2203.02544
[18] S. S. Gill et al., "AI for next generation computing: Emerging trends and future directions," Internet of Things (Netherlands), vol. 19, pp. 1–43, 2022, doi: 10.1016/j.iot.2022.100514.
[19] Q. V. Pham et al., "Aerial Computing: A New Computing Paradigm, Applications, and Challenges," IEEE Internet Things J., vol. 9, no. 11, pp. 8339–8363, 2022, doi: 10.1109/JIOT.2022.3160691.
[20] S. Liang et al., "Edge YOLO: Real-Time Intelligent Object Detection System Based on Edge-Cloud Cooperation in Autonomous Vehicles," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 12, pp. 25345–25360, 2022, doi: 10.1109/TITS.2022.3158253.
[21] R. Montasari, "Artificial Intelligence and National Security," Artif. Intell. Natl. Secur., pp. 1–230, 2022, doi: 10.1007/978-3-031-06709-9.
[22] K. K. Verma, B. M. Singh, and A. Dixit, "A review of supervised and unsupervised machine learning techniques for suspicious behavior recognition in intelligent surveillance system," Int. J. Inf. Technol., vol. 14, no. 1, pp. 397–410, 2022, doi: 10.1007/s41870-019-00364-0.
[23] P. McEnroe, S. Wang, and M. Liyanage, "A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges," IEEE Internet Things J., vol. 9, no. 17, pp. 15435–15459, 2022, doi: 10.1109/JIOT.2022.3176400.
[24] A. K. Sandhu, "Big Data with Cloud Computing: Discussions and Challenges," Big Data Min. Anal., vol. 5, no. 1, pp. 32–40, 2022, doi: 10.26599/BDMA.2021.9020016.
[25] J. Hassan et al., "The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges - A Systematic Literature Review (SLR)," Comput. Intell. Neurosci., vol. 2022, 2022, doi: 10.1155/2022/8303504.
[26] A. A. Laghari, H. He, A. Khan, R. A. Laghari, S. Yin, and J. Wang, "Crowdsourcing Platform for QoE Evaluation for Cloud Multimedia Services," Comput. Sci. Inf. Syst., vol. 19, no. 3, pp. 1305–1328, 2022, doi: 10.2298/CSIS220322038L.
[27] J. Li, C. Gu, Y. Xiang, and F. Li, "Edge-cloud Computing Systems for Smart Grid: State-of-the-art, Architecture, and Applications," J. Mod. Power Syst. Clean Energy, vol. 10, no. 4, pp. 805–817, 2022, doi: 10.35833/MPCE.2021.000161.
[28] A. Gohari, A. Bin Ahmad, R. B. A. Rahim, A. S. M. Supa'at, S. A. Razak, and M. S. M. Gismalla, "Involvement of Surveillance Drones in Smart Cities: A Systematic Review," IEEE Access, vol. 10, pp. 56611–56628, 2022, doi: 10.1109/ACCESS.2022.3177904.
[29] B. Omarov, S. Narynov, Z. Zhumanov, A. Gumar, and M. Khassanova, "State-of-the-art violence detection techniques in video surveillance security systems: A systematic review," PeerJ Comput. Sci., vol. 8, pp. 1–41, 2022, doi: 10.7717/PEERJ-CS.920.
[30] M. Smith and S. Miller, "The ethical application of biometric facial recognition technology," AI Soc., vol. 37, no. 1, pp. 167–175, 2022, doi: 10.1007/s00146-021-01199-9.
[31] K. Bayoudh, R. Knani, F. Hamdaoui, and A. Mtibaa, "A survey on deep multimodal learning for computer vision: advances, trends, applications, and datasets," Vis. Comput., vol. 38, no. 8, pp. 2939–2970, 2022, doi: 10.1007/s00371-021-02166-7.
[32] M. Utke, S. Zadtootaghaj, S. Schmidt, S. Bosse, and S. Möller, "NDNetGaming - development of a no-reference deep CNN for gaming video quality prediction," Multimed. Tools Appl., vol. 81, no. 3, pp. 3181–3203, 2022, doi: 10.1007/s11042-020-09144-6.
[33] M. K. Shambour and A. Gutub, "Progress of IoT Research Technologies and Applications Serving Hajj and Umrah," Arab. J. Sci. Eng., vol. 47, no. 2, pp. 1253–1273, 2022, doi: 10.1007/s13369-021-05838-7.
[34] E. M. Onyema, S. Dalal, C. A. T. Romero, B. Seth, P. Young, and M. A. Wajid, "Design of Intrusion Detection System based on Cyborg intelligence for security of Cloud Network Traffic of Smart Cities," J. Cloud Comput., vol. 11, no. 1, 2022, doi: 10.1186/s13677-022-00305-6.
[35] D. R. Patrikar and M. R. Parate, "Anomaly detection using edge computing in video surveillance system: review," Int. J. Multimed. Inf. Retr., vol. 11, no. 2, pp. 85–110, 2022, doi: 10.1007/s13735-022-00227-8.
[36] S. Chaturvedi, P. Khanna, and A. Ojha, "A survey on vision-based outdoor smoke detection techniques for environmental safety," ISPRS J. Photogramm. Remote Sens., vol. 185, no. March, pp. 158–187, 2022, doi: 10.1016/j.isprsjprs.2022.01.013.
[37] T. Hussain, K. Muhammad, W. Ding, J. Lloret, S. W. Baik, and V. H. C. de Albuquerque, "A comprehensive survey of multi-view video summarization," Pattern Recognit., vol. 109, p. 107567, 2021, doi: 10.1016/j.patcog.2020.107567.
[38] S. Paneru and I. Jeelani, "Version of Record: https://www.sciencedirect.com/science/article/pii/S0926580521003915," 2021.
[39] M. Driss, D. Hasan, W. Boulila, and J. Ahmad, "Microservices in IoT security: Current solutions, research challenges, and future directions," Procedia Comput. Sci., vol. 192, pp. 2385–2395, 2021, doi: 10.1016/j.procs.2021.09.007.
[40] Y. Zhai et al., "5G-Network-Enabled Smart Ambulance: Architecture, Application, and Evaluation," IEEE Netw., vol. 35, no. 1, pp. 190–196, 2021, doi: 10.1109/MNET.011.2000014.
[41] A. Galanopoulos, J. A. Ayala-Romero, D. J. Leith, and G. Iosifidis, "AutoML for video analytics with edge computing," Proc. - IEEE INFOCOM, vol. 2021-May, 2021, doi: 10.1109/INFOCOM42981.2021.9488704.
[42] K. K. Santhosh, D. P. Dogra, and P. P. Roy, "Anomaly Detection in Road Traffic Using Visual Surveillance: A Survey," ACM Comput. Surv., vol. 53, no. 6, pp. 1–14, 2021, doi: 10.1145/3417989.
[43] F. Romero, M. Zhao, N. J. Yadwadkar, and C. Kozyrakis, Llama: A heterogeneous & serverless framework for auto-tuning video analytics pipelines, vol. 1, no. 1. Association for Computing Machinery, 2021. doi: 10.1145/3472883.3486972.
[44] D. Wodajo and S. Atnafu, "Deepfake Video Detection Using Convolutional Vision Transformer," 2021, [Online]. Available: http://arxiv.org/abs/2102.11126
[45] M. Dhuheir, A. Albaseer, E. Baccour, A. Erbad, M. Abdallah, and M. Hamdi, "Emotion Recognition for Healthcare Surveillance Systems Using Neural Networks: A Survey," 2021 Int. Wirel. Commun. Mob. Comput. IWCMC 2021, pp. 681–687, 2021, doi: 10.1109/IWCMC51323.2021.9498861.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY