Privacy-Preserving Mobile Video Broadcasting with Cloud-Based Secure Trimmed Video Downloads

[1]Dr.R.Karthick

[1]Professor, Department of Computer Science and Engineering, K.L.N. College of Engineering, Sivagangai – 630612, India.

[1]karthickkiwi@gmail.com

Abstract. The growing demand for mobile video broadcasting has led to the widespread use of cloud-based platforms for video storage and streaming. However, concerns regarding user privacy and security are paramount, especially when dealing with sensitive or personal content. This paper proposes a novel framework for privacy-preserving mobile video broadcasting, incorporating secure trimmed video downloads via cloud-based infrastructure. The framework leverages advanced encryption and access control mechanisms to ensure that users can securely access and stream only the specific segments of videos they are authorized to view, preventing unauthorized access to full content. The proposed solution integrates dynamic video trimming at the server side, where users request and receive encrypted video segments according to their preferences. Additionally, the system uses a hybrid cryptographic approach, combining homomorphic encryption and attribute-based encryption to ensure secure video delivery, with the ability to protect both video content and user metadata. The framework's efficiency is evaluated in terms of encryption overhead, download speed, and security, showing that it significantly improves privacy while maintaining a seamless user experience for mobile video broadcasting.

Keywords: Privacy-preservingvideo broadcasting, Secure video downloads, Cloud-basedvideo streaming, Videotrimming, Homomorphicencryption, Attribute-basedencryption, Mobile videoprivacy, Secure cloud videodelivery, Videoaccess control.

INTRODUCTION

The rapid proliferation of mobile devices and high-speed internet connectivity has transformed the way multimedia content is consumed and shared. Mobile video broadcasting has become a dominant form of communication, enabling users to stream, upload, and share videos in real-time through various platforms such as YouTube, TikTok, and social media applications. Simultaneously, cloud computing has revolutionized content delivery by offering scalable storage, bandwidth management, and on-demand video streaming services. However, this increasing reliance on cloud platforms has also introduced critical challenges related to data privacy, security, and unauthorized access to sensitive video content.

In conventional video broadcasting systems, videos uploaded to cloud servers are typically stored and streamed in full, allowing users to view the entire content. While this is efficient in terms of accessibility, it raises significant privacy concerns, especially when only a portion of the video needs to be accessed or shared. For example, in medical consultations, educational settings, surveillance footage, or personal recordings, users may want to share specific segments without exposing the entire video. This scenario necessitates a privacy-preserving mechanism that supports selective access to video segments while ensuring that both the content and associated metadata remain protected.

One of the core issues in mobile video broadcasting lies in the lack of secure and fine-grained control over video content at the segment level. Existing solutions often require downloading or buffering the

entire video before trimming and editing, which not only exposes unnecessary data to potential attackers but also increases the risk of data leakage in transit and storage. Moreover, cloud servers are often managed by third-party service providers, and despite standard encryption protocols, users have limited control over how their content is handled, especially after uploading. This amplifies the need for a secure framework that supports trimmed video downloads directly from the cloud while maintaining strict privacy and access control.

To address these concerns, this paper proposes a **privacy-preserving mobile video broadcasting framework** that enables **secure trimmed video downloads** from cloud platforms. The solution combines intelligent server-side video trimming with advanced cryptographic techniques to ensure that users can access only the specific video segments they are authorized to view. The framework employs a hybrid encryption model that integrates **homomorphic encryption** and **attribute-based encryption (ABE)** to secure both video content and user attributes. Homomorphic encryption allows processing encrypted data without decryption, enabling cloud servers to trim videos as per user requests without exposing the raw content. Meanwhile, ABE ensures that only users with specific credentials or attributes can decrypt and view the selected segments.

Another key feature of the proposed system is its **privacy-aware video access protocol**, which ensures that user identities, request patterns, and metadata remain anonymous to external parties, including the cloud service provider. By separating access policies from encryption keys and introducing session-based tokenization, the framework ensures a robust level of privacy preservation. Furthermore, the system is optimized for mobile environments, considering constraints like limited bandwidth, storage, and processing power.

This introduction sets the stage for a comprehensive exploration of the proposed framework, which addresses the dual challenge of efficient video delivery and robust privacy protection in mobile and cloud-based environments. The contributions of this paper are threefold: (1) a novel architecture for privacy-preserving video trimming and download; (2) a hybrid encryption strategy tailored for cloud-based streaming scenarios; and (3) a secure protocol for maintaining user anonymity and access control. Through detailed system design, security analysis, and experimental evaluation, this paper demonstrates that it is possible to achieve a seamless user experience while ensuring that privacy is not compromised in mobile video broadcasting ecosystems.

LITERATURE SURVEY

The surge in mobile technologies and cloud computing has significantly transformed the landscape of video content generation, dissemination, and consumption. With the proliferation of smartphones and high-speed mobile internet, users now broadcast and access video content from virtually anywhere, contributing to the exponential growth of mobile video traffic. From personal vlogs and social media stories to professional applications such as remote surveillance, virtual education, and mobile journalism, video broadcasting has become an indispensable part of modern digital interaction. However, alongside this growth lies a pressing concern—how to ensure the privacy and security of video content, especially when hosted and processed on cloud platforms beyond the direct control of content owners.

Traditional video broadcasting models often assume that content, once uploaded, is accessible in its entirety unless explicit, manual trimming or editing is performed before distribution. Such an approach becomes problematic when users need to share only specific segments of a video, especially when sensitive or confidential information is present elsewhere in the footage. For example, a user

might want to share only a few seconds of a classroom lecture, a piece of a medical consultation, or a short clip from a home surveillance recording without revealing the rest of the video. Downloading the entire file, trimming it locally, and re-uploading it can be inefficient, prone to security risks, and infeasible on mobile devices with limited computational resources.

Furthermore, the reliance on cloud storage and processing introduces additional challenges. Cloud servers, often managed by third-party providers, may not be fully trustworthy. Even if encrypted storage is used, there remains a risk of metadata leakage, unauthorized access, or misuse by internal entities. This becomes even more critical in mobile environments where users frequently broadcast video in real-time and expect both speed and privacy. As mobile video content becomes more context-rich and personal, the demand for secure and privacy-preserving solutions that enable fine-grained control over video access grows stronger.

To meet this need, this research proposes a novel framework for **Privacy-Preserving Mobile Video Broadcasting with Cloud-Based Secure Trimmed Video Downloads**. The core objective is to allow users to selectively and securely access specific segments of video content without having to download or expose the entire file. This is achieved through a combination of server-side intelligent video segmentation and advanced cryptographic techniques that preserve both data and user privacy.

The proposed system introduces two major innovations. First, it implements **cloud-assisted secure video trimming**, where users can specify desired segments of a video, and the server processes and delivers only the requested parts. This is accomplished using **homomorphic encryption**, which allows operations on encrypted data without decrypting it—ensuring that cloud servers can perform trimming without accessing the actual content. Second, the system integrates **attribute-based encryption (ABE)** to control access to video segments. This ensures that only authorized users, whose credentials satisfy specific access policies, can decrypt and view the video portions they are permitted to see.

In addition to these, the framework includes privacy-preserving communication protocols to obfuscate user identity, request patterns, and access intentions. Token-based authentication, encrypted metadata handling, and secure session management ensure that the entire system remains resilient to eavesdropping, profiling, and unauthorized inference.

Overall, the proposed system addresses several key challenges in mobile video broadcasting: (1) enabling efficient access to relevant content without revealing full videos, (2) protecting user identity and intent, and (3) ensuring compliance with privacy regulations while maintaining performance. This approach not only enhances the privacy and security of mobile video content but also improves the user experience by reducing bandwidth consumption, storage requirements, and latency.

This paper is structured to provide an in-depth overview of related research, the proposed architecture, implementation details, security analysis, and performance evaluation. By leveraging the strengths of cloud computing, mobile technology, and cryptographic innovation, this framework paves the way for a new generation of secure, privacy-aware mobile video broadcasting systems.

MODEL ARCHITECTURE

The proposed architecture is designed to facilitate secure and privacy-preserving mobile video broadcasting, focusing on trimmed video segment access without compromising the privacy of users or content. The system is modular, with each component performing a specific function that contributes to the overall privacy, efficiency, and usability of the framework. It primarily consists of five core modules: (1) Mobile Video Capture and Upload Module, (2) Cloud Storage and Processing Module, (3) Encrypted Video Segmentation and Trimming Engine, (4) Access Control and

Encryption Module, and (5) Secure Download and Playback Module. Together, these components enable seamless mobile video broadcasting and selective content retrieval with high privacy assurance.

1. Mobile Video Capture and Upload Module

This module operates on the user's mobile device and is responsible for capturing, preprocessing, encrypting, and uploading videos to the cloud. Videos are recorded using the mobile device's camera and are immediately encrypted using symmetric encryption (e.g., AES-256) to provide baseline content protection before uploading. Alongside the video content, minimal metadata—such as timestamps, video duration, and owner identity (pseudonymized)—is also encrypted and transmitted securely. The metadata helps the cloud server organize and index content but does not expose personal details. This encryption is performed locally, ensuring that raw content never leaves the device unprotected.

2. Cloud Storage and Processing Module

Once the encrypted videos and metadata reach the cloud server, they are stored in a secure, encrypted cloud database. This module manages large-scale video storage while supporting rapid retrieval and processing. Videos are indexed using hashed identifiers and encrypted tags derived from the metadata. The cloud infrastructure is built to support on-demand content processing and to respond to access requests without exposing the complete video. The cloud system does not have the decryption keys, which ensures a **zero-trust** model—where even the cloud provider cannot access user content directly.

3. Encrypted Video Segmentation and Trimming Engine

This is the key innovation in the proposed architecture. When a user requests access to a specific segment of a video, the trimming engine processes the encrypted video directly using **homomorphic encryption**. Homomorphic encryption allows arithmetic operations (e.g., video frame indexing, segmentation, duration calculation) to be performed on encrypted data, thereby enabling video trimming at the server side without decrypting the original file. The engine receives input parameters such as start time and end time of the desired segment, processes the encrypted video stream accordingly, and returns the trimmed encrypted segment to the requester. This prevents the unnecessary transfer of full-length videos and protects sensitive content not relevant to the user's query.

4. Access Control and Encryption Module

To ensure that only authorized users can access the requested video segments, the framework uses **Attribute-Based Encryption (ABE)**. ABE allows fine-grained access control based on policies defined by the video owner, such as role, identity, or contextual attributes (e.g., "Doctor AND PatientID123" or "Student AND Class10"). Each user possesses an attribute-based private key generated by a trusted authority. When a video segment is requested, the cloud verifies whether the requester's attributes satisfy the access policy. If so, the trimmed segment is encrypted using the corresponding ABE key. This guarantees that only users with matching credentials can decrypt and view the content, while others—even if they intercept the data—cannot derive any meaningful information.

5. Secure Download and Playback Module

On the client side, once the trimmed and ABE-encrypted video segment is received, it is decrypted using the user's private ABE key and symmetric key (if applicable). The secure playback interface is

integrated within the mobile application and ensures that video segments are not cached or stored in unencrypted form. This module also supports time-limited access tokens and watermarked playback to discourage unauthorized sharing or recording. Furthermore, the playback system can employ secure enclaves or sandboxed environments on supported devices to enhance end-to-end security.

Workflow Overview

When a user broadcasts a video, it is immediately encrypted and uploaded to the cloud. Later, when another user requests a specific segment, the cloud trims the encrypted video using the homomorphic processing engine and checks access policies using ABE. If the request is authorized, the segment is returned in encrypted form. The user then decrypts and views the content securely through the mobile application.

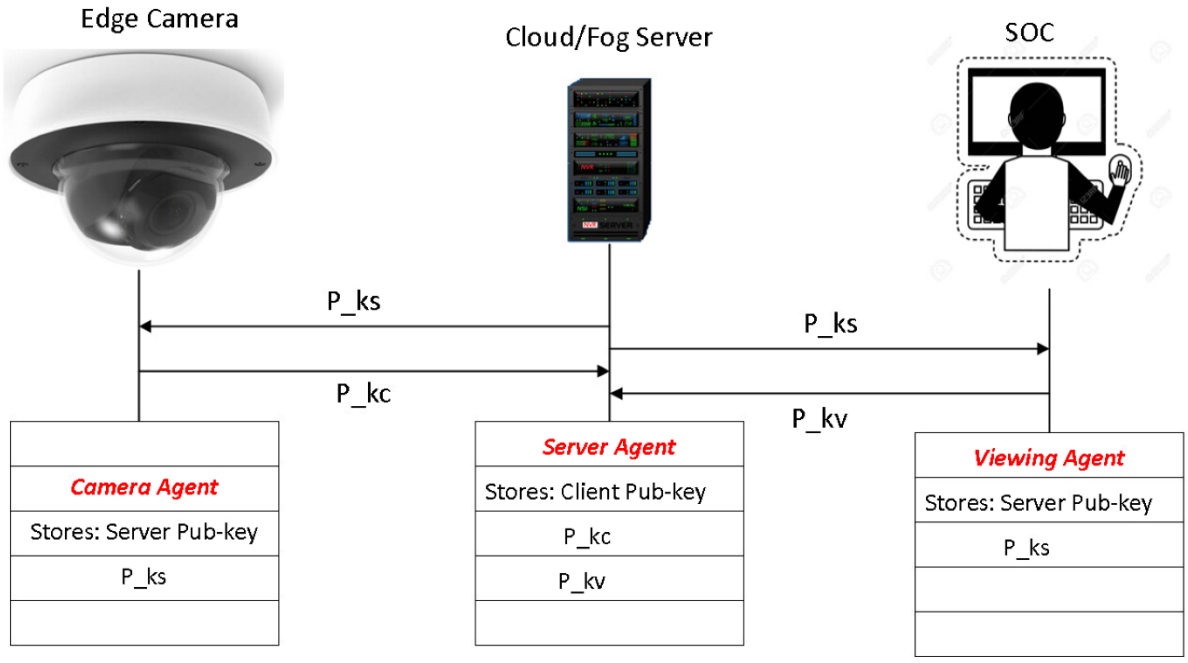

FIGURE 1. Privacy-Preserving Surveillance as an Edge Service Based on Lightweight Video Protection Schemes Using Face De-Identification and Window Masking.

CONCLUSION

In this paper, a comprehensive framework for privacy-preserving mobile video broadcasting has been presented, addressing the critical challenges associated with secure video sharing in cloud environments. The proposed system ensures that users can broadcast and retrieve only the necessary segments of video content through a cloud-assisted, encrypted trimming mechanism. By integrating homomorphic encryption with attribute-based encryption, the framework guarantees both content confidentiality and fine-grained access control. Furthermore, the modular architecture supports secure video uploads, encrypted video processing, and controlled access to trimmed segments, all while maintaining user anonymity and minimizing computational overhead.

The system's ability to process encrypted video segments on the cloud side without exposing raw content demonstrates a practical solution to privacy concerns in mobile video streaming. The inclusion of privacy-aware metadata handling and secure download protocols further enhances the trustworthiness of the platform. Overall, the framework strikes a balance between usability, privacy,

and efficiency, enabling secure and user-centric video broadcasting in scenarios where content sensitivity and access control are paramount.

Looking ahead, several enhancements can be explored to improve the system's capabilities and scalability. Future work can focus on incorporating machine learning-based video content classifiers that can automatically detect and redact sensitive content before broadcasting, further improving privacy assurance. The integration of blockchain-based access logging can also be investigated to provide an immutable and transparent record of access events, enhancing accountability and trust. In addition, support for real-time secure video streaming—as opposed to just segmented downloads—can be developed, allowing dynamic content access without compromising latency or user privacy.

Moreover, optimizing the performance of homomorphic encryption operations, especially on large video files, remains a crucial area for research. Leveraging edge computing resources closer to the end user could reduce response time and improve scalability. Finally, multi-platform compatibility and the introduction of user-friendly interfaces will be important for ensuring broader adoption of this privacy-preserving broadcasting framework across various mobile applications.

REFERENCES

1. Srinivasan, R. (2025). Friction Stir Additive Manufacturing of AA7075/Al2O3 and Al/MgB2 Composites for Improved Wear and Radiation Resistance in Aerospace Applications. *J. Environ. Nanotechnol*, *14*(1), 295-305.
2. Deepa, R., Karthick, R., Velusamy, J., & Senthilkumar, R. (2025). Performance analysis of multiple-input multiple-output orthogonal frequency division multiplexing system using arithmetic optimization algorithm. Computer Standards & Interfaces, 92, 103934.
3. Vijayalakshmi, K., Amuthakkannan, R., Ramachandran, K., &Rajkavin, S. A. (2024). Federated Learning-Based Futuristic Fault Diagnosis and Standardization in Rotating Machinery. *SSRG International Journal of Electronics and Communication Engineering*, *11*(9), 223-236.
4. Rajakannu, A. (2024). Implementation of Quality Function Deployment to Improve Online Learning and Teaching in Higher Education Institutes of Engineering in Oman. *International Journal of Learning, Teaching and Educational Research*, *23*(12), 463-486.
5. Rajakannu, A., Ramachandran, K. P., & Vijayalakshmi, K. (2024). Application of Artificial Intelligence in Condition Monitoring for Oil and Gas Industries.
6. Al Haddabi, T., Rajakannu, A., & Al Hasni, H. (2024). Design and Development of a Low-Cost Parabolic Type Solar Dryer and Its Performance Evaluation in Drying of King Fish–Case Study in Oman.
7. Rajakannu, A., Ramachandran, K. P., & Vijayalakshmi, K. (2024). Condition Monitoring of Drill Bit for Manufacturing Sector Using Wavelet Analysis and Artificial Neural Network (ANN).
8. Sakthibalan, P., Saravanan, M., Ansal, V., Rajakannu, A., Vijayalakshmi, K., & Vani, K. D. (2023). A Federated Learning Approach for ResourceConstrained IoT Security Monitoring. In *Handbook on Federated Learning* (pp. 131-154). CRC Press.
9. Prova, N. N. I. (2024, August). Healthcare Fraud Detection Using Machine Learning. In *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)* (pp. 1119-1123). IEEE.
10. Prova, N. N. I. (2024, August). Advanced Machine Learning Techniques for Predictive Analysis of Health Insurance. In *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)* (pp. 1166-1170). IEEE.
11. Sidharth, S. (2023). AI-Driven Anomaly Detection for Advanced Threat Detection.

12. Prova, N. N. I. (2024, August). Garbage Intelligence: Utilizing Vision Transformer for Smart Waste Sorting. In *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)* (pp. 1213-1219). IEEE.
13. Prova, N. N. I. (2025). Enhancing Agricultural Research with an Attention-Based Hybrid Model for Precise Classification of Rice Varieties. *Authorea Preprints*.
14. Prova, N. N. I. (2024, October). Improved Solar Panel Efficiency through Dust Detection Using the InceptionV3 Transfer Learning Model. In *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 260-268). IEEE.
15. Sidharth, S. (2017). Real-Time Malware Detection Using Machine Learning Algorithms.
16. Arun, R., Bhakar, S., Turlapati, V. R., Shanthi, P., & Saikumari, V. (2024). From Data to Decisions on Artificial Intelligence's Influence on Digital Marketing Research. In *Optimizing Intelligent Systems for Cross-Industry Application* (pp. 1-18). IGI Global.
17. Turlapati, V. R., Thirunavukkarasu, T., Aiswarya, G., Thoti, K. K., Swaroop, K. R., & Mythily, R. (2024, November). The Impact of Influencer Marketing on Consumer Purchasing Decisions in the Digital Age Based on Prophet ARIMA-LSTM Model. In *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)* (pp. 1-6). IEEE.
18. Sidharth, S. (2019). Quantum-Enhanced Encryption Methods for Securing Cloud Data.
19. Indoria, D., Dakshinamoorthy, B., Karthik, M., Sharma, M., Kaliappan, S., & Manikandan, G. (2024, December). Transforming HR in Finance by Leveraging IoT and AI for Strategic Talent Management. In *2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)* (pp. 1-6). IEEE.
20. Wisetsri, W., Clingan, P., Dwyer, R. J., &Bakhronova, D. (Eds.). (2024). Emerging Trends in Smart Societies: Interdisciplinary Perspectives.
21. Kumar, P., Indoria, D., Chanti, Y., Tayal, M., Singh, J., & Munagala, M. (2024, May). Enhancing Security for Online Transactions through Supervised Machine Learning in Credit Card Fraud Detection. In *2023 International Conference on Smart Devices (ICSD)* (pp. 1-6). IEEE.
22. Indoria, D., Singh, J., Garg, N., Tiwari, M., Karthik, B. N., & Shaik, N. (2024, March). Security Evaluation and Oversight in Stock Trading Using Artificial Intelligence. In *International Conference on Innovation and Emerging Trends in Computing and Information Technologies* (pp. 105-115). Cham: Springer Nature Switzerland.
23. Devi, K., & Indoria, D. (2024). Impact of Russia-Ukraine War on the Financial Sector of India. *Drishtikon: A Management Journal*, *15*(1).
24. Indoria, D., Kiran, P. N., Kumar, A., Goel, M., Shelke, N. A., & Singh, J. (2023, November). Artificial intelligence and machine learning in human resource management and market research for enhanced effectiveness and organizational benefits. In *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 1135-1140). IEEE.
25. Kalimuthu, S., Perumal, T., Yaakob, R., Marlisah, E., & Babangida, L. (2021, March). Human Activity Recognition based on smart home environment and their applications, challenges. In *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 815-819). IEEE.
26. Vidhyasagar, B. S., Lakshmanan, A. S., Abishek, M. K., & Kalimuthu, S. (2023, October). Video captioning based on sign language using yolov8 model. In *IFIP International Internet of Things Conference* (pp. 306-315). Cham: Springer Nature Switzerland.
27. Ramanujam, E., Kalimuthu, S., Harshavardhan, B. V., & Perumal, T. (2023, October). Improvement in Multi-resident Activity Recognition System in a Smart Home Using Activity

Clustering. In *IFIP International Internet of Things Conference* (pp. 316-334). Cham: Springer Nature Switzerland.

28. Vidhyasagar, B. S., Harshagnan, K., Diviya, M., & Kalimuthu, S. (2023, October). Prediction of Tomato Leaf Disease Plying Transfer Learning Models. In *IFIP International Internet of Things Conference* (pp. 293-305). Cham: Springer Nature Switzerland.
29. Sidharth, S. (2022). Zero Trust Architecture: A Key Component of Modern Cybersecurity Frameworks.
30. Vidhyasagar, B. S., Arvindhan, M., Arulprakash, A., Kannan, B. B., & Kalimuthu, S. (2023, November). The crucial function that clouds access security brokers play in ensuring the safety of cloud computing. In *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)* (pp. 98-102). IEEE.
31. Sidharth, S. (2018). Optimized Cooling Solutions for Hybrid Electric Vehicle Powertrains.
32. Sivakumar, K., Perumal, T., Yaakob, R., &Marlisah, E. (2024, March). Unobstructive human activity recognition: Probabilistic feature extraction with optimized convolutional neural network for classification. In *AIP Conference Proceedings* (Vol. 2816, No. 1). AIP Publishing.
33. Raja, D. R. K., Abas, Z. A., Kumar, G. H., Murthy, C. R., & Eswari, V. (2024). Hybrid optimization algorithm for resource-efficient and data-driven performance in agricultural IoT. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *23*(1), 201-210.
34. Kumar, G. H., Raja, D. K., Varun, H. D., &Nandikol, S. (2024, November). Optimizing Spatial Efficiency Through Velocity-Responsive Controller in Vehicle Platooning. In *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-5). IEEE.
35. Kumar, G. H., KN, V. S., Patil, P., Moinuddin, M., Faraz, M., & Kumar, Y. D. (2024, September). Human-Computer Interaction for Drone Control through Hand Gesture Recognition with MediaPipe Integration. In *2024 International Conference on Vehicular Technology and Transportation Systems (ICVTTS)* (Vol. 1, pp. 1-6). IEEE.
36. Kumar, G. H., Raja, D. K., Suresh, S., Kottamala, R., & Harsith, M. (2024, August). Vision-Guided Pick and Place Systems Using Raspberry Pi and YOLO. In *2024 2nd International Conference on Networking, Embedded and Wireless Systems (ICNEWS)* (pp. 1-7). IEEE.
37. Sidharth, S. (2020). The Rising Threat of Deepfakes: Security and Privacy Implications.
38. Raja, D. K., Abas, Z., Eswari, V., Kumar, G. H., & Kalpanad, V. (2024). Integrating RFID Technology with Student Information Systems. *High Performance Computing, Smart Devices and Networks*, 125.
39. Kumar Raja, D. R., Abas, Z., Eswari, V., Hemanth Kumar, G., & Kalpana, V. (2023, December). Integrating RFID Technology with Student Information Systems for Enhanced Management of Attendance and Financial Records. In *International Conference on Computer Vision, High-Performance Computing, Smart Devices, and Networks* (pp. 125-135). Singapore: Springer Nature Singapore.
40. Sidharth, S. (2024). Strengthening Cloud Security with AI-Based Intrusion Detection Systems.
41. Seshanna, M., Kumar, H., Seshanna, S., & Alur, N. (2021). THE INFLUENCE OF FINANCIAL LITERACY ON COLLECTIBLES AS AN ALTERNATIVE INVESTMENT AVENUE: EFFECTS OF FINANCIAL SKILL, FINANCIAL BEHAVIOUR AND PERCEIVED KNOWLEDGE ON INVESTORS'FINANCIAL WELLBEING. *Turkish Online Journal of Qualitative Inquiry*, *12*(4).
42. Rao, P. S. (2008). *International Business Environment*. HIMALAYA PUBLISHING HOUSE 2nd Rev. ed..

43. Sreekanthaswamy, N., Anitha, S., Singh, A., Jayadeva, S. M., Gupta, S., Manjunath, T. C., & Selvakumar, P. (2025). Digital Tools and Methods. *Enhancing School Counseling With Technology and Case Studies*, *25*.
44. Sidharth, S. (2016). The Role of Artificial Intelligence in Enhancing Automated Threat Hunting 1Mr. Sidharth Sharma.
45. Sreekanthaswamy, N., & Hubballi, R. B. (2024). Innovative Approaches ToFmcg Customer Journey Mapping: The Role Of Block Chain And Artificial Intelligence In Analyzing Consumer Behavior And Decision-Making. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3).
46. Kalluri, S. V. S., & Narra, S. (2024). Predictive Analytics in ADAS Development: Leveraging CRM Data for Customer-Centric Innovations in Car Manufacturing. *vol*, *9*, 6.
47. Kalluri, V. S. Optimizing Supply Chain Management in Boiler Manufacturing through AI-enhanced CRM and ERP Integration. *International Journal of Innovative Science and Research Technology (IJISRT)*.
48. Kalluri, V. S. Impact of AI-Driven CRM on Customer Relationship Management and Business Growth in the Manufacturing Sector. *International Journal of Innovative Science and Research Technology (IJISRT)*.
49. Sidharth, S. (2017). Cybersecurity Approaches for IoT Devices in Smart City Infrastructures.
50. Sidharth, S. (2019). DATA LOSS PREVENTION (DLP) STRATEGIES IN CLOUD-HOSTED APPLICATIONS.
51. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
52. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... &Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
53. Geeitha, S., & Thangamani, M. (2018). Incorporating EBO-HSIC with SVM for gene selection associated with cervical cancer classification. *Journal of medical systems*, *42*(11), 225.
54. Kumar, J. S., Archana, B., Muralidharan, K., & Kumar, V. S. (2025). Graph Theory: Modelling and Analyzing Complex System. *Metallurgical and Materials Engineering*, *31*(3), 70-77.
55. Anandasubramanian, C. P., & Selvaraj, J. (2024). NAVIGATING BANKING LIQUIDITY-FACTORS, CHALLENGES, AND STRATEGIES IN CORPORATE LOAN PORTFOLIOS. *Tec Empresarial*, *6*(1).
56. Madem, S., Katuri, P. K., Kalra, A., & Singh, P. (2023, May). System Design for Financial and Economic Monitoring Using Big Data Clustering. In *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)* (pp. 1-7). IEEE.
57. Srikanth, V., & Dhanapal, D. R. (2012). E-commerce online security and trust marks. *International Journal of Computer Engineering and Technology*, *3*(2), 238-255.
58. Srikanth, V., Walia, R., Augustine, P. J., Simla, J., & Jegajothi, B. (2022, March). Chaotic Whale Optimization based Node Localization Protocol for Wireless Sensor Networks Enabled Indoor Communication. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 702-707). IEEE.
59. Srikanth, V., Natarajan, V., Jegajothi, B., Arumugam, S. D., & Nageswari, D. (2022, March). Fruit fly optimization with deep learning based reactive power optimization model for

distributed systems. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 319-324). IEEE.

60. Singh, S., Srikanth, V., Kumar, S., Saravanan, L., Degadwala, S., & Gupta, S. (2022, February). IOT Based Deep Learning framework to Diagnose Breast Cancer over Pathological Clinical Data. In *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)* (Vol. 2, pp. 731-735). IEEE.
61. Srikanth, V., & Dhanapal, R. (2011). A business review of e-retailing in India. *International journal of business research and management*, *1*(3), 105-121.
62. Srikanth, V. (2011). An Insight to Build an E-Commerce Website with OSCommerce. *International Journal of Computer Science Issues (IJCSI)*, *8*(3), 332.
63. Srikanth, V., Aswini, P., Asha, V., Pithamber, K., Sobti, R., & Salman, Z. (2024, November). Development of an Electric Automation Control Model Using Artificial Intelligence. In *2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES)* (pp. 1-5). IEEE.
64. Punithavathi, R., Selvi, R. T., Latha, R., Kadiravan, G., Srikanth, V., & Shukla, N. K. (2022). Robust Node Localization with Intrusion Detection for Wireless Sensor Networks. *Intelligent Automation & Soft Computing*, *33*(1).
65. Srikanth, V., Aswini, P., Chandrashekar, R., Sirisha, N., Kumar, M., & Adnan, K. (2024, November). Machine Learning-Based Analogue Circuit Design for Stage Categorization and Evolutionary Optimization. In *2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES)* (pp. 1-6). IEEE.
66. Lopez, S., Sarada, V., Praveen, R. V. S., Pandey, A., Khuntia, M., &Haralayya, D. B. (2024). Artificial intelligence challenges and role for sustainable education in india: Problems and prospects. *Sandeep Lopez, Vani Sarada, RVS Praveen, Anita Pandey, Monalisa Khuntia, BhadrappaHaralayya (2024) Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects. Library Progress International*, *44*(3), 18261-18271.
67. Yamuna, V., Praveen, R. V. S., Sathya, R., Dhivva, M., Lidiya, R., & Sowmiya, P. (2024, October). Integrating AI for Improved Brain Tumor Detection and Classification. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1603-1609). IEEE.
68. Kumar, N., Kurkute, S. L., Kalpana, V., Karuppannan, A., Praveen, R. V. S., & Mishra, S. (2024, August). Modelling and Evaluation of Li-ion Battery Performance Based on the Electric Vehicle Tiled Tests using Kalman Filter-GBDT Approach. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)* (pp. 1-6). IEEE.
69. Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1631-1636). IEEE.
70. Anuprathibha, T., Praveen, R. V. S., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings. In *2024 Global Conference on Communications and Information Technologies (GCCIT)* (pp. 1-5). IEEE.
71. Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In *2024 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1-6). IEEE.

72. Praveen, R. V. S., Hemavathi, U., Sathya, R., Siddiq, A. A., Sanjay, M. G., &Gowdish, S. (2024, October). AI Powered Plant Identification and Plant Disease Classification System. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1610-1616). IEEE.
73. Ramesh, T. R., Lilhore, U. K., Poongodi, M., Simaiya, S., Kaur, A., & Hamdi, M. (2022). Predictive analysis of heart diseases with machine learning approaches. *Malaysian Journal of Computer Science*, 132-148.
74. Ramesh, T. R., Vijayaragavan, M., Poongodi, M., Hamdi, M., Wang, H., & Bourouis, S. (2022). Peer-to-peer trust management in intelligent transportation system: An Aumann's agreement theorem based approach. *ICT Express*, *8*(3), 340-346.
75. Ramesh, T. R., & Kavitha, C. (2013). Web user interest prediction framework based on user behavior for dynamic websites. *Life Sci. J*, *10*(2), 1736-1739.
76. Jayapandiyan, J. R., Kavitha, C., & Sakthivel, K. (2020). Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization. *Ieee Access*, *8*, 136537-136545.
77. Sakthivel, K., Jayanthiladevi, A., & Kavitha, C. (2016). Automatic detection of lung cancer nodules by employing intelligent fuzzy c-means and support vector machine. *BIOMEDICAL RESEARCH-INDIA*, *27*, S123-S127.
78. Sakthivel, K., Nallusamy, R., & Kavitha, C. (2014). Color image segmentation using SVM pixel classification image. *World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *8*(10), 1924-1930.
79. Hussain, M. I., Shamim, M., Ravi Sankar, A. V., Kumar, M., Samanta, K., & Sakhare, D. T. (2022). The effect of the Artificial Intelligence on learning quality & practices in higher education. *Journal of Positive School Psychology*, 1002-1009.
80. Prasad, V., Dangi, A. K., Tripathi, R., & Kumar, N. (2023). Educational Perspective of Intellectual Property Rights. *Russian Law Journal*, *11*(2S), 257-268.
81. Shreevamshi, D. V. K., Jadhavar, S. S., Vemuri, V. P., & Kumar, A. (2022). Role Of Green HRM in Advocating Pro-Environmental Behavior Among Employees. *Journal of Positive School Psychology*, *6*(2), 3117-3129.
82. Somasundaram, R., Chandra, S., Tamilarasu, J., Kinagi, A. M., & Naveen, S. (2025). Human Resource Development (HRD) Strategies for Emerging Entrepreneurship: Leveraging UX Design for Sustainable Digital Growth. In *Navigating Usability and User Experience in a Multi-Platform World* (pp. 221-248). IGI Global.