4th Indian International Conference on Industrial Engineering and Operations Management
Hyderabad, Telangana, India, November 07-09, 2024
Publisher: IEOM Society International, USA DOI: 10.46254/IN04.20240106
Published: November 07, 2024

A Survey on Deep Learning Approaches for Cloud Forensics Analysis

Sheena Mohammed
Assistant Professor, AI&DS Dept
Chaitanya Bharathi Institute of Technology, Hyderabad, India
sheenamd786@gmail.com

Dr. R Sridevi
Professor, CSE Dept, JNTUH, Hyderabad, India
sridevirangu@jntuh.ac.in

Dr. K.S Sadasiva Rao
Professor, CSE Dept and Dean R&D,
Sri Indu College of Engineering and Technology, Hyderabad.
kssadasivarao@gmail.com

Abstract

This paper presents an in-depth review of deep learning methods employed in the field of cloud forensics analysis, highlighting current advancements, challenges, and future directions. With the rapid adoption of cloud computing, forensic investigations face unique challenges, particularly in data collection, evidence analysis, and maintaining chain of custody. This survey explores how deep learning enhances cloud forensic processes, improving accuracy, automation, and scalability. Key areas such as malware detection, anomaly detection, log analysis, and privacy-preserving techniques are discussed. The paper also examines the gaps in existing research and suggests areas for future exploration.

Keywords

Cloud forensics, Deep learning, Cybersecurity, Malware detection, Anomaly detection, Log analysis, Privacy-preserving forensics

1. Introduction

Cloud forensics is a critical field of investigation that focuses on gathering, preserving, and analyzing evidence from cloud computing environments (Cinar et.al 2023). As businesses and individuals increasingly rely on cloud services for data storage and processing, the need for effective forensic methods becomes essential in the event of cybercrime or data breaches . (Malik et.al 2024). Cloud environments present unique challenges for forensic investigations due to their distributed nature, where data is stored across multiple servers and often in different geographic locations. This distributed structure can make it difficult to acquire complete and accurate forensic evidence (Camilleri and Rebecca 2024). Additionally, the multi-tenant architecture of cloud services, where multiple users share the same resources, further complicates evidence collection (Alshabibi et.al 2024). Data volatility is another challenge, as data in the cloud can change rapidly or be deleted without a trace, making it essential for forensic tools and techniques to capture data quickly and accurately before it is lost (Mujahid and Bisma 2023).

Deep learning has become a valuable approach for tackling challenges in cloud forensics (Mohammed Sheena, and Sridevi Rangu 2024). Utilizing sophisticated algorithms, these models can process large datasets to uncover patterns

and anomalies that are often missed by conventional forensic techniques. For example, deep learning can be used to automate the detection of malware in cloud systems by recognizing suspicious behavior patterns or identifying previously unseen threats (Brown et.al 2024). Additionally, it can enhance the efficiency of log analysis, enabling investigators to quickly sift through large volumes of data and focus on key evidence. The application of deep learning in anomaly detection is also significant, as it allows for real-time monitoring of cloud environments to detect unusual activities that may indicate a security breach (Arjunan and Tamilselvan 2024). Overall, deep learning can streamline and improve the accuracy of cloud forensic investigations, making it an indispensable tool in this evolving field (Chan et al 2023)**.**

The purpose of this survey is to offer an in-depth analysis of how deep learning is being applied within the realm of cloud forensics. This examination includes a review of the current methodologies that utilize deep learning to address various challenges associated with forensic investigations in cloud environments. By evaluating these existing approaches, the survey aims to highlight the effectiveness of current techniques and pinpoint the areas where limitations still exist. Furthermore, this review seeks to identify emerging trends and potential future directions that can help overcome the current challenges, providing insights into the development of more advanced and reliable deep learning solutions for cloud forensics in the coming years.

2. Cloud Forensics: Challenges and Requirements

Cloud environments have distinct characteristics that make forensic investigations particularly complex (Egho-Promise et al 2024). One of the primary challenges is the distributed nature of data storage. In cloud computing, data is often spread across multiple physical servers, which may be located in different regions or even different countries. This dispersal of data complicates the retrieval process and makes it difficult to ensure that all relevant data has been collected. Furthermore, cloud customers typically do not have direct control over the infrastructure, which includes servers, networking, and storage devices. This lack of control means investigators must rely on the cooperation of cloud service providers to access the data, which can lead to delays or incomplete evidence retrieval. Additionally, the shared resource model of cloud computing, where multiple users share the same hardware and software resources, poses challenges in isolating data belonging to a specific user or case, making it harder to maintain the integrity of the forensic process.

Forensic investigations in cloud environments face several specific challenges, one of which is the difficulty in acquiring data from multi-tenant systems. In such systems, multiple users' data coexists on the same physical infrastructure, making it hard to extract evidence pertinent to just one individual or organization without infringing on the privacy of others. Another challenge is the scale of log data that needs to be collected and analyzed. Cloud environments generate vast amounts of logs, which are essential for tracking user activity and identifying potential security breaches. However, processing this volume of data in a timely manner is a significant obstacle. Maintaining the integrity and chain of custody of digital evidence is also a critical issue. In a cloud environment, ensuring that the data has not been altered during collection or transmission and that its source is well-documented becomes challenging, particularly when data is stored in multiple locations.

Deep learning offers several advantages in addressing the challenges associated with cloud forensic investigations (Abdallah et.al 2024). One key benefit is the ability to automate complex tasks, such as pattern recognition and anomaly detection, which would otherwise require significant manual effort. Deep learning models can process and analyze large volumes of data in real time, providing quicker insights into potential breaches or malicious activities within the cloud. Furthermore, deep learning algorithms are adaptable, meaning they can be trained to recognize new types of threats as they emerge, which is crucial in the ever-evolving landscape of cyber threats. This flexibility, combined with the capability to handle large-scale data efficiently, makes deep learning an invaluable tool in modern cloud forensic investigations.

3. Deep Learning Techniques in Cloud Forensics

Deep learning techniques have become increasingly valuable in cloud forensics due to their ability to handle large, complex datasets and identify patterns that may be missed by traditional methods. Several models are particularly relevant for forensic investigations. Convolutional Neural Networks (CNNs) (Rahim et.al 2023) are widely used for image and pattern recognition tasks, making them useful for analyzing malware signatures in cloud environments. Recurrent Neural Networks (RNNs) (Dhumane e.al 2024), and specifically their more advanced form, Long Short-

Term Memory (LSTM) (Thirupathi et.al 2024) networks, are designed to handle sequential data, making them effective for analyzing time-based events such as network traffic logs or user activity in the cloud. Autoencoders, another important deep learning model, are frequently used for anomaly detection and data compression, which can help in detecting irregular patterns or behaviors in vast cloud datasets.

In the context of cloud forensics, deep learning has shown significant promise in several key applications:

i. ***Malware detection:*** Malware detection is one area where CNNs and RNNs have been applied effectively. (Thakur et.al 2024) . CNNs can be used to analyze static features of malware, such as file signatures, while RNNs are suited for dynamic analysis, monitoring how malware behaves over time. Case studies have demonstrated the ability of these models to detect previously unknown malware in cloud environments, offering a high degree of accuracy in identifying both known and emerging threats.

ii. ***Anomaly detection***: Another critical application is anomaly detection, where deep learning models like RNNs and LSTMs play a role in identifying unusual patterns in cloud traffic that could indicate a security breach (Li Gen et.al 2023). By analyzing logs of network activity, these models can detect irregular behaviors that deviate from the norm, providing early warning signs of potential attacks or intrusions.

iii. ***Log analysis:*** Log analysis is another area where deep learning models are making an impact in cloud forensics (Vervaet et.al 2023). Cloud environments generate massive volumes of log data, which are essential for tracking user activity and identifying security incidents. Deep learning techniques, particularly autoencoders and LSTM networks, can automate the process of parsing and analyzing these logs, making it easier to detect patterns that may be relevant for forensic investigations. These models excel at recognizing deviations from normal log activity, which can help investigators focus on critical data points without manually sifting through overwhelming amounts of information.

iv. ***Privacy-preserving techniques:*** These are also becoming an essential consideration in cloud forensics, especially with the growing concern over data privacy regulations. Federated Learning is a deep learning approach that allows models to be trained across multiple cloud environments without sharing raw data, thus protecting user privacy. This technique enables forensic investigations to be carried out without accessing sensitive personal information directly (Mohamed e.al 2023), making it compliant with privacy laws while still allowing for the identification of security incidents or cyberattacks. Federated Learning is particularly useful in multi-tenant cloud environments, where maintaining user confidentiality is critical.

4. Survey of Previous Research Works

This study analyzes various deep learning models and their application to cloud forensics. The table 1 provides a comparative overview of various deep learning techniques used in malware detection across different domains. The Systematic Review of Deep Learning Solutions focuses on IoT malware detection (Amiri e.al 2024) using CNN (Convolution Neural Network), RNN (Recurrent Neural Network), and Autoencoders, with an emphasis on metrics such as accuracy, scalability, and model complexity. The DL-AMDet (Nasser et.al 2024) model leverages CNN-BiLSTM and Autoencoders for Android malware detection, achieving an impressive accuracy of 99.935%. A Hybrid CNN-RNN approach (Hussain et.al 2024) is highlighted in a deep learning-based hybrid analysis study, demonstrating improved malware classification. For cloud malware detection, a Deep Q Network combined with Autoregressive ChOA (Bhingarkar et.al 2024) shows a 94% accuracy and 94.1% sensitivity. Another approach using CNN-LSTM (Karat et.al 2024) achieves 99% accuracy in detecting IoT malware. This comparison underscores the versatility and effectiveness of deep learning models across various malware detection contexts.

5. Analysis of Deep Learning Techniques

5.1 CNN and CNN-Based Models

Convolutional Neural Networks (CNNs) have been widely utilized in the realm of malware detection, particularly for analyzing static characteristics such as file signatures and system calls within cloud environments.These models are highly effective at identifying spatial patterns in data, making them well-suited for detecting malware in system logs and identifying potential anomalies. One of the key advantages of CNNs is their ability to achieve high accuracy, as

demonstrated by several studies, including the DL-AMDet model, which achieved detection rates exceeding 99%. However, one of the primary challenges with CNN-based models is their reliance on large, labeled datasets for training. In cloud forensics, the availability of such datasets can be limited, posing a significant hurdle to the widespread application of CNNs in this field (Table 1).

Table 1. A comparative overview of various deep learning techniques used in malware detection

Sl. No	Title	Deep Learning Techniques	Focus Area	Key Metrics
1	Systematic Review of Deep Learning Solutions	CNN, RNN, Autoencoders	IoT Malware Detection	Accuracy, Scalability, Model Complexity
2	DL-AMDet: Deep Learning-based Malware Detector	CNN-BiLSTM, Autoencoders	Android Malware Detection	99.935% accuracy
3	Deep Learning-based Hybrid Analysis	Hybrid CNN-RNN	Malware Detection and Classification	Improved malware classification with hybrid models
4	Malicious Behavior Detection in Cloud Computing	Deep Q Network, Autoregressive ChOA	Cloud Malware Detection	94% accuracy, 94.1% sensitivity
5	CNN-LSTM for Malware Detection	CNN-LSTM	IoT Malware Detection	99% accuracy

5.2 RNN and LSTM Networks

Long Short-Term Memory (LSTM) models are particularly effective for analyzing time-series and sequential data, making them ideal for tasks like log monitoring and examining behavioral patterns of malware. One of the key advantages of LSTMs is their ability to track user activity or system logs over time, which helps in detecting anomalies that may signal a security breach. Additionally, LSTMs are valuable for dynamic analysis, offering insights into how malware behavior evolves, as seen in CNN-LSTM models(Karat et.al 2024). However, a significant challenge with LSTMs is the complexity of training these models, which can be computationally intensive and require substantial resources, especially in cloud environments**.**

5.3 Hybrid Approaches

Hybrid approaches .(Hussain et.al 2024) that integrate Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), such as CNN-LSTM models (Karat et.al 2024), are designed to capitalize on the strengths of both techniques. These models are particularly effective in real-time malware detection within dynamic environments like the Internet of Things (IoT). By combining spatial and sequential learning, they enhance the ability to detect complex and evolving threats, such as botnets. Hybrid models have consistently demonstrated superior performance over individual models in terms of accuracy and robustness. However, the complexity of this combined architecture presents a challenge, as it increases the difficulty of both training and deploying the models, especially for real-time applications.

5.4 Autoencoders

Autoencoders are frequently applied in cloud forensics for tasks such as anomaly detection and log analysis[19]. These models learn compact representations of normal system behavior, which allows them to effectively identify deviations that may signal suspicious activities. One of the main advantages of autoencoders is their ability to handle unsupervised learning tasks, making them suitable for detecting irregularities even without labeled data. Additionally, autoencoders help improve efficiency by reducing the dimensionality of data, enabling faster and more manageable large-scale log analysis. However, a common challenge with autoencoders is their tendency to produce false positives, particularly in environments where deviations from typical patterns are frequent but not necessarily malicious.

6. Key Challenges Identified:

i. ***Data Availability*:** One of the most commonly noted challenges across all reviewed works is the lack of large, labeled forensic datasets, particularly in cloud and IoT environments. This data scarcity limits the ability to train accurate deep-learning models.

ii. ***Model Interpretability:*** Another significant challenge is the "black box" nature of deep learning models, particularly CNNs and RNNs. In cloud forensics, investigators need to understand and explain model decisions, which is not always possible with these techniques.

iii. ***Scalability:*** Scalability remains a major concern, especially in cloud environments where the volume of data can be immense. While models like CNN-LSTM offer high accuracy, their computational requirements can hinder real-time implementation.

7. Comparative Analysis

The Table 2 gives the comparative analysis of the deep learning models used in cloud forensics: CNN-BiLSTM, Deep Q Network, CNN-LSTM, and Autoencoders. CNN-BiLSTM on performance metrics such as the accuracy, sensitivity, and specificity.

The bar chart visually compares the accuracy, sensitivity, and specificity of four different deep learning models used in cloud forensics: CNN-BiLSTM, Deep Q Network, CNN-LSTM, and Autoencoders. CNN-BiLSTM shows the highest accuracy at 99.935%, followed closely by CNN-LSTM with 99%. The Deep Q Network has lower accuracy (94%) but provides values for both sensitivity (94.1%) and specificity (91.4%), making it effective for dynamic cloud environments. Autoencoders, ranging between 90-95% accuracy, are efficient for log analysis, though they lack sensitivity and specificity data. This chart highlights the strengths and gaps in model performance. Figure 1 is the pictorial representation of comparative analysis.

Table 2. The comparative analysis of the deep learning models

Model	Accuracy	Sensitivity	Specificity	Strengths	Weaknesses
CNN-BiLSTM	99.935%	N/A	N/A	High accuracy in detecting Android malware	High training complexity
Deep Q Network	94%	94.1%	91.4%	Effective in dynamic cloud environments	Limited real-time applicability due to processing
CNN-LSTM	99%	99%	N/A	Combines spatial and sequential learning for IoT	High model complexity
Autoencoders	90-95%	N/A	N/A	Efficient for log analysis and anomaly detection	Prone to false positives

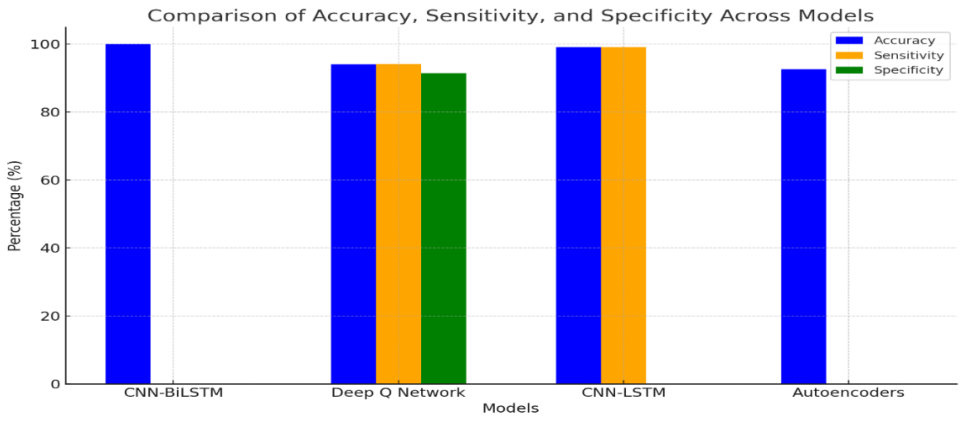

Figure 1. Comparison of Accuracy, Sensitivity and specificity across deep-learning models

8. Challenges in Applying Deep Learning for Cloud Forensics

Deep learning has shown great promise in many fields, including cybersecurity and forensics. However, applying it to cloud forensics presents several unique challenges. Below are some key issues that need to be addressed:

ii ***Data Availability and Quality:*** One of the biggest hurdles in applying deep learning to cloud forensics is the lack of large, labeled forensic datasets. Deep learning models rely heavily on vast amounts of data for training, and in cloud forensics, it is difficult to collect such data. Moreover, forensic data that does exist is often fragmented and incomplete, making it hard to create reliable models. Additionally, cloud providers may not always make forensic evidence readily available due to privacy and legal concerns, further complicating the availability of relevant data.

iii ***Model Interpretability:*** Deep learning models are often referred to as "black boxes" because of their complexity and the difficulty in understanding how they make decisions. This lack of transparency can be a significant issue in cloud forensics, where legal proceedings require clear explanations of how forensic evidence is obtained and analyzed. Without interpretable models, it can be challenging to provide convincing, legally admissible results in court.

iiii ***Adversarial Attacks:*** Another critical challenge is the vulnerability of deep learning models to adversarial attacks. In these attacks, small and subtle changes to the input data can cause the model to produce incorrect results. In the context of cloud forensics, such perturbations can lead to wrong conclusions, potentially causing investigators to miss crucial evidence or, worse, to draw false conclusions. This vulnerability makes it risky to rely on deep learning models without robust defenses against adversarial attacks.

iiv ***Scalability:*** Cloud environments generate vast amounts of data, and for deep learning to be effective in cloud forensics, models must be capable of handling this scale. However, current research in this field often struggles with scaling models to process large datasets efficiently. Training deep learning models on cloud-scale data can be computationally expensive and time-consuming, limiting their practical use in real-world forensic investigations. Scalability remains a significant challenge in making deep learning applicable to cloud forensics on a larger scale.

9. Future Directions and Open Research Areas

Future research in cloud forensics is heading towards several promising areas. One key focus is on transfer learning, where pre-trained models are applied to forensic analysis, helping to overcome the challenge of limited cloud-specific forensic data. Another critical area is explainable AI, which aims to make deep learning models more understandable and transparent for use in legal contexts. Additionally, there is a growing emphasis on adversarial defense mechanisms, which seek to create deep learning models that can withstand adversarial attacks in forensic applications. Researchers are also exploring the integration of quantum-resistant algorithms to ensure the long-term security of forensic processes in a post-quantum world. Lastly, advancements in automated incident response using deep reinforcement learning are being pursued to enhance the speed and efficiency of responses to forensic events**.**

10. Conclusion

In this survey, we explored the application of deep learning techniques in cloud forensics, highlighting both the advancements and challenges in the field. Deep learning has the potential to revolutionize cloud forensic analysis by automating complex tasks such as malware detection, anomaly detection, and log analysis. Its ability to handle large volumes of data and uncover patterns that might be missed by traditional methods makes it a valuable tool for forensic investigators. However, several key challenges, such as the lack of labeled forensic datasets, model interpretability issues, vulnerability to adversarial attacks, and scalability concerns, need to be addressed for its broader application.

The survey also emphasizes the need for more research in areas such as explainable AI, transfer learning, and adversarial defenses to overcome these challenges. As cloud computing continues to grow and become more integrated into various sectors, the importance of effective forensic analysis will only increase. Future research should aim to create more resilient, interpretable, and scalable deep learning models tailored to the unique requirements of cloud forensics. Overcoming these challenges will enable deep learning to significantly enhance forensic capabilities in the constantly evolving cloud landscape.

References

Abdallah, Amira, et al. "Cloud Network Anomaly Detection Using Machine and Deep Learning Techniques-Recent Research Advancements." *IEEE Access,* 2024.

Alshabibi, Munirah Maher, Alanood Khaled Bu dookhi, and M. M. Hafizur Rahman. "Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review." *Computers 13.8,* 213. 2024

Amiri, Zahra, et al. "Adventures in data analysis: A systematic review of Deep Learning techniques for pattern recognition in cyber-physical-social systems." *Multimedia Tools and Applications 83.8* , 22909-22973, 2024.

Arjunan, Tamilselvan. "Real-Time Detection of Network Traffic Anomalies in Big Data Environments Using Deep Learning Models*." International Journal for Research in Applied Science and Engineering Technology 12.9*, 10-22214. 2024

Bhingarkar, Sukhada, et al. "An effective optimization enabled deep learning based Malicious behaviour detection in cloud computing." *International Journal of Intelligent Robotics and Applications 7.3*, 575-588. 2023

Brown, Austin, Maanak Gupta, and Mahmoud Abdelsalam. "Automated machine learning for deep learning based malware detection." *Computers & Security 137*, 103582. 2024

Camilleri, Rebecca. "Data security in cloud-centric multi-tenant databases, 2024.

Chan, Kit Yan, et al. "Deep neural networks in the cloud: Review, applications, challenges and research directions." *Neurocomputing 545*, 126327. 2023

Cinar, Burak, and Jasmin Praful Bharadiya. "Cloud computing forensics; challenges and future perspectives: A review." *Asian Journal of Research in Computer Science 16.1*, 1-14. 2023

Dhumane, Amol, et al. "Design of an Efficient Forensic Layer for IoT Network Traffic Analysis Engine Using Deep Packet Inspection via Recurrent Neural Networks." *International Journal of Safety & Security Engineering 14.3*, 2024.

Egho-Promise, Ehigiator, et al. "Digital Forensic Investigation Standards in Cloud Computing." *Universal Journal of Computer Sciences and Communications*, 23-45. 2024

Hussain, Syed Shuja, Mohd Faizal Ab Razak, and Ahmad Firdaus. "Deep Learning Based Hybrid Analysis of Malware Detection and Classification: A Recent Review." *Journal of Cyber Security and Mobility* , 91-134. 2024

Karat, Gautam, et al. "CNN-LSTM Hybrid Model for Enhanced Malware Analysis and Detection." *Procedia Computer Science 233*, 492-503. 2024

Li, Gen, and Jason J. Jung. "Deep learning for anomaly detection in multivariate time series: Approaches, applications, and challenges." *Information Fusion 91*, 93-102. 2023

Malik, Annas Wasim, et al. "Cloud digital forensics: Beyond tools, techniques, and challenges." *Sensors 24.2*, 433. 2024

Mohamed, Hania, Nickolaos Koroniotis, and Nour Moustafa. "Digital forensics based on federated learning in IoT environment." *Proceedings of the 2023 Australasian Computer Science Week*. 92-101. 2023.

Mohammed Sheena, and Sridevi Rangu. "To secure the cloud application using a novel efficient deep learning-based forensic framework." *Journal of Interconnection Networks 24.01*, 2350008. 2024

Mujahid, Bisma. "Cloud Forensics: Investigating Security Incidents in Cloud Environments., 2023.

Nasser, Ahmed R., Ahmed M. Hasan, and Amjad J. Humaidi. "DL-AMDet: Deep learning-based malware detector for android." *Intelligent Systems with Applications* 21, 200318. 2024

Rahim, Asif, et al. "Hyper-Tuned Convolutional Neural Networks for Authorship Verification in Digital Forensic Investigations." *Computers, Materials & Continua 76.2*, 2023.

Thakur, Preeti, Vineet Kansal, and Vinay Rishiwal. "Hybrid deep learning approach based on lstm and cnn for malware detection." *Wireless Personal Communications 136.3*, 1879-1901, 2024.

Thirupathi, Chaithanyaka Yeddeli, et al. "Malware Classification using LSTM-CF Framework for Disk Forensic Analysis." 2024 *IEEE International Conference on Contemporary Computing and Communications (InC4)*. Vol. 1. IEEE, 2024.

Vervaet, Arthur. Automated Log-Based Anomaly Detection within Cloud Computing Infrastructures. Diss. Sorbonne Université, 2023.

Biographies

Ms. Sheena Mohammed is an Assistant Professor at CBIT, with over 14 years of teaching experience. Her academic background includes a B.Tech in Information Technology and an M.Tech in Software Engineering, both earned with distinction. Currently pursuing a Ph.D. in Computer Science and Engineering, her areas of expertise lie in computer networks, information security, and digital forensics. Ms. Mohammed has published several research papers in international journals and has contributed to conferences on topics like cloud forensics and cybersecurity frameworks. She is a certified CCNA instructor and an active member of ISTE, IAENG, and IACSIT.

Dr. R. Sridevi is a Professor of CSE with 23 years of teaching experience. Presently working as Professor, Director, Directorate of Entrepreneurship, Innovation and Start-ups, JNTUH & Co.ordinator, Centre of Excellence in Cyber Security, JNTUH. Lead various roles as Head of the CSE Department for nearly 3 years, Additional Controller of Examinations(EDEP), Additional Controller of Examinations(Result Processing). Worked as Chairman, Board of Studies for Department of CSE, JNTUHUCEH, Hyderabad. During the tenure of Head, organized several Workshops,FDPs, curricular and extra-curricular events and 3 international conferences .Established three Research Labs IoT Lab, Digital Forensics Lab & Big Data Analytics Lab and one smart classroom under TEQIP in the department. Network security and information security are the research domains. Guided 7 Ph.Ds & Published very good number of research papers in various national and international conferences and reputed journals with high indexing factor.

Dr. K S Sadasiva Rao is a Professor in the Department of CSE and also Dean R&D at Sri Indu College of Engineering Technology (A), Ibrahimpatnam, Hyderabad. He has 23 Years of Teaching Experience at the level of Head of the Department, Principal and Dean-Academics. He has rich experience in organizing seminars, workshop in Computer Science Engineering topics. He is Convener for the International Conference ICICSET'24. He also worked as principal for the period of 8 years at Sri Indu PG College. He published 24 papers in several National as well as International Journals with high indexing factor and presented 6 papers in International Conferences. He is a Lifetime Member in the professional societies CSI, IETE, ISTE. He is also serving as a reviewer member for many international journals.