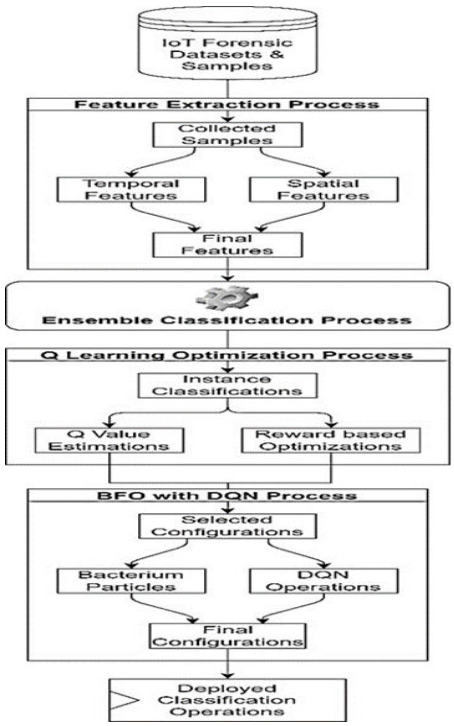
Design of an Improved Model for Iot Forensic Analysis Using Elastic Weight Consolidation and Deep Compression

[1] Gangavarapu Rajesh Babu, [2] Virendra K. Sharma
[1] Research Scholar, Department of Computer Science & Engineering, Bhagwant University, Ajmer (305004), Rajasthan, India
[2] Professor, Department of Computer Science & Engineering, Bhagwant University, Ajmer (305004), Rajasthan, India
Corresponding Author: Gangavarapu Rajesh Babu

Abstract: This exponential growth of Iot devices enforces the need to provide robust forensic analysis frameworks that would manage wide and diversified data generated in real-time. Conventional forensic analysis tools are lacking in scalability, efficiency, and adaptability to new data, which greatly limits their applications in Iot environments. In most cases, high computational costs in terms of resources and central storage of data are needed, which is impracticable in constraint-resource edge devices, also raising concerns about privacy. This paper proposes a comprehensive forensic analysis framework that enables the bypassing of such limitations by exploiting incremental learning and bio inspired optimization techniques. Such a framework is foreseen to put several advanced methodologies together in order to give better scalability, efficiency, and accuracy in IoT forensic analysis. First, EWC for incremental learning—enable model adaptation to new data without forgetting the previously learned information, retaining up to 90% accuracy and reducing memory usage by 50%. Second, deep compression through model pruning significantly reduces model size by up to 90% and increases the inference speed by 2-3 times for deployment at edge in different scenarios. It applies federated averaging in distributed training to make sure data privacy is guaranteed at devices and 60% reduction in communication overhead, while accuracy is guaranteed to be at most 1-2% away from centralized training. In this paper, auto encoder-based anomaly detection has been implemented for the identification of deviations in Iot data with an accuracy of 90-95% and a false positive rate below 5%. It leverages Temporal Convolution Networks for temporal pattern recognition, which top 90% in accuracy and achieve more efficient training and inference compared to recurrent networks. The combination of the above techniques yields a forensic analysis framework that is scale-aware, efficient, and accurate, and optimized for resource-constrained IoT environments. This framework is designed to allow very high performance for real-time data processing, anomaly detection, and pattern recognition; hence, it significantly pushes the limits of state-of-the-art in IoT forensic analysis and puts forward an effective solution for modern IoT ecosystems. The proposed framework resolves some of the crucial challenges and gives a practical and effective approach for forensic analysis in view of fast-evolving landscapes of IoT devices and deployments.

Keywords: Iot, Forensic Analysis, Incremental Learning, Deep Compression, Federated Learning.

Graphical abstract



1.0 Introduction

This rapid proliferation of IoT devices drives much innovation in several sectors, from smart homes and health care to industrial automation and environmental monitoring. At the same time, this places huge challenges in data management and security. IoT data are mostly real-time and heterogeneous in nature, generating enormous volumes that call for proper storage and other advanced forensic analysis techniques to ensure data integrity, security, and guarantee conformity with regulatory standards. Traditional forensic techniques are incapable of meeting the scalability and efficiency requirements intrinsic to IoT systems. They most often demand significant computational resources and centralized

data storage that are impractical for resource-constrained edge devices, leading to huge implications in privacy. There is, therefore, a pressing need for new forensic-analysis frameworks that can effectively cope with the dynamism and volume of data generated by these IoT devices and their deployments. Not only this, the current methods are not treating the qualitative continuous inflow of new data and the data processing limitations of edge devices & deployments. Add to that, centralized ways of processing data are becoming less and less viable due to the rising risk of data compromise and inefficiency in transmitting large volumes of data to a central server.

This paper presents a new forensic analysis framework for IoT environments that harnesses the state-of-the-art technique to bring better scalability, efficiency, and accuracy. More specifically, the authors implement the use of Elastic Weight Consolidation, which provides for incremental

learning and makes sure models do not forget previously acquired knowledge when retrained on new data. The importance of this ability in the context of IoT, where the data is inherently always in flux and attempting to retrain models from scratch is an exercise in futility, is shown. It further applies deep compression—pruning, quantization, and Huffman encoding—for drastic model size reduction and speedup on inferences, actually deployable on scaled-down resource edge devices and deployments. In addition, it integrates precisely Federated Learning, more specifically Federated Averaging (FedAvg), for distributed model training across edge devices while retaining data privacy and lowering the communication overhead. This decentralized approach reduces the risks that come with central data storage, but risks arise in maintaining the accuracy of the models. To this end, the autoencoder-based anomaly detection and the integration of Temporal Convolutional Networks for pattern recognition are combined to ensure robust real-time processing and high-accuracy anomaly detection. These integrated advanced methodologies lead to a complete and effective IoT forensics framework in addressing the critical issues involved in IoT environments. The proposed model does not only guarantee good performance in the real-time data processing along with the detection of anomalies but also optimizes resource use, making it a very strong solution for contemporary IoT forensic analysis. This work indeed uplifts the state of the art to get a new paradigm of IoT forensic methodologies to make an effort toward the complex and dynamic nature of IoT data samples.

1.1 Motivation & Contribution:

The proliferation of things within the Internet of Things has changed an entire notion of connectivity and turned everyday devices into sensing, processing, and communicating intelligent systems with vast amounts of information. Much as this revolution is opening up unparalleled opportunities for innovation and efficiency, it comes with important challenges on data security, integrity, and analysis. Traditional forensic analysis techniques, many of which have been tailored for static and centralized data environments, do not function as expected when considering the dynamic, distributed, and resource-constrained nature of IoT ecosystems. Particularly, there is a need to devise scalable, efficient forensic analysis frameworks able to work within such constraints, since continuous streams of heterogeneous data from a large number of devices administered with limited edge devices exert pressure on computational capabilities. Most of the forensic methodologies existing currently are badly suited for IoT environments. Traditionally, most of these solutions rely on extensive computational resources and often require a centralized process for data. This makes these approaches unsuitable for real-time analysis, besides the severe privacy risks involved due to centralization, which makes the data more vulnerable to breaches. Besides, such frequent retraining to adapt to new data exaggerates these limitations, making the traditional methods inefficient and resource-intensive. The work is motivated by the urgent need to bridge these gaps through the realization of an innovative forensic analysis framework that—exploiting state-of-the-art techniques for incremental learning, model compression, and distributed computing—. The model under

proposal integrates Elastic Weight Consolidation, Deep Compression, Federated Learning, autoencoder-based anomaly detection, and Temporal Convolutional Networks to make the solution more scalable, efficient, and accurate with respect to forensic analysis in IoT environments, to present a robust solution for a new set of challenges that the rapidly evolving field brings.

This work has many contributions that cut across both the theoretical and practical aspects of IoT forensic analysis. First, the use of Elastic Weight Consolidation for incremental learning is a considerable improvement in maintaining model accuracy across successive updates. EWC, for that matter, alleviates the problem of catastrophic forgetting by considering the importance of parameters with respect to their contribution to the previous tasks. It is therefore able to fit new data without compromising the knowledge that was hitherto learned. This is particularly important in IoT environments where data is ever-changing and incremental learning from new coming data—without retraining from scratch, guarantees efficiency and in most of the cases, sustainability. Second, Deep Compression techniques—pruning, quantization, and Huffman coding—are proposed to be incorporated for solving the problem of deploying complex models on resource-constrained edge devices and deployments. Deep Compression works by drastically reducing model size while improving inference speed, thus rendering the forensic analysis framework capable of running within the constraints imposed by edge devices in terms of computation and storage capacity, without sacrificing any accuracy measure. This is, therefore, a very critical contribution enabling edge real-time analysis and decision making—a central requirement in any IoT application.

The third major contribution is the integration of federated learning, in particular, Federated Averaging, for enabling federated distributed model training across a myriad of edge devices and deployments. Data privacy is safeguarded with this approach since data stays local at edge devices and is not revealed to the risk of breaches that central storage would pose. Moreover, Federated Learning reduces communication overhead for better efficiency of the forensic analysis framework. This will, hence, be compatible with the intrinsic distributed nature of the IoT environments, scalable, and privacy-preserving for model training. This contribution is further added by using autoencoder-based anomaly detection and Temporal Convolutional Networks for pattern recognition, making the proposed framework more robust. With strong learning capabilities in compact representations of normal data and the identification of deviations from the given norms, autoencoders provide a very strong tool for unsupervised anomaly detection. This forms a very key part in the identification of irregularities and suspected security breaches in IoT data streams. On the other hand, TCNs, by learning arbitrary temporal dependencies, achieve state-of-the-art performance in tasks involving temporal pattern recognition, guaranteeing high accuracy and efficiency in predicting future events based on past data samples. Such advanced techniques integrated together can present a holistic

forensic analysis model that would cope with underpinning challenges of scalability, efficiency, and accuracy in IoT environments. The proposed model supplies incremental learning, model compression, distributed computing, and state-of-the-art methods for anomaly detection and pattern recognition, hence offering a holistic solution theoretically sound and practically feasible. It has evolved the state-of-the-art in IoT forensic analysis while contributing to the proposal of a feasible, effective, and robust framework ready for the deployment in the real world of IoT applications. Contributions made in this research have implications for the improvement of the security, integrity, and operational efficiency of IoT systems, which actually pave ways toward more secure and reliable IoT ecosystems.

1.2 In-depth review of Empirical Review of Existing Methods

Digital forensics has seen massive growth these past couple of years, given the fast-tracking of the Internet of Things, the rising complexity of cyber threats, and the new waves of digital crimes that keep changing in nature. As we see IoT devices becoming a mainstream part of life, these devices start generating high volumes of data, which will start creating investigative challenges for the forensicators. The review brings under one umbrella 25 critical studies, offering new methodologies for and insights into the practices of digital forensics, taken mostly in the IoT contexts. The reviews covered the topics of forensic readiness, case studies, data privacy, anti-forensic techniques, machine learning applications, and blockchain-based security solutions. We muster these very different approaches to be able to spot current trends, underline significant breakthroughs, and put a finger on persistent challenges that will require further research. Papers reviewed bicephalous indicate the duties of forensic readiness and data privacy problems in the use the Internet of Things. For instance, Ahn and Lee. [1] investigated forensic and anti-forensic problems on the basis of a NAND flash memory, which proves the necessity of secure deletion and verification solutions with customization for IoT things. Liu et al. [2] harnessed machine learning to push forward intrusion-free digital forensics services in smart homes, attaining high accuracies for anomaly detection while upholding operation device integrity. Palmese et al. [3] proposed a forensic-ready Wi-Fi access point, designed in such a manner to conduct effective network traffic analysis; in this way, forensic abilities may be enriched directly at the layer of the network. These and other studies point the way toward greater demand for the integration of forensic functionality into IoT systems to support timely and effective investigation in a wide range of scenarios.

A current interest is the study of how cryptographic techniques can ensure data privacy in giving way to digital forensic analyses. In this line, Ogunseyi and Adedayo. [5] present a general description of advanced cryptographic methods that deal with a two-fold requirement: data protection and forensic readiness for privacy-preserving digital forensics. In light of the modern forensic analysis, machine learning and artificial intelligence have become indispensable; therefore, available advanced tools for pattern recognition, anomaly detection, and predictive

analytics have to be harnessed. Zhang et al. [7] proposed a local perturbation generation method for anti-forensics of GAN-generated faces, focusing on the duality of machine learning in both forensic and anti-forensic applications. Ding et al. [9] worked on adversarial training techniques against the detection of DeepFake videos and made a significant enhancement to the accuracy of detection. These studies are representative of the potential machine learning has to improve detection, analysis, and understanding of complex digital evidentiary artifacts in forensic investigations across a variety of scenarios.

In the same vein, Baracchi et al. [12] presented a media signature encoding approach for open-world multimedia forensics that is of very high efficacy—still always bounded by quality of the encoded signatures and kinds of involved media. These domain-specific limitations would suggest greater needs relative to generalization approaches, striving to be parameterized across many forensic contexts. Another recurring challenge is pointed out for the scalability of proposed methods. Ogunseyi and Adedayo. [5] and a number more, and Li et al. [10] showed studies that other than the computation overhead of complexity in cryptographic and blockchain-based techniques. Although these methods enhance security and privacy, it still is a cause of concern for scalability in large IoT deployment. Future research trying to ease this trade-off should be in the way of optimizing these techniques for security rather than efficiency so that, in the end, they could actually be applied effectively without prohibitively high computational costs in deployment scenarios.

Table 1 Comparative Review of Existing Methods

Reference	Method Used	Findings	Results	Limitations
[1]	Forensic/Anti-Forensic Issues on NAND Flash Memory	Analysis of forensic and anti-forensic techniques on NAND flash memory	Improved secure deletion and verification methods for IoT devices	Limited to NAND flash memory, not generalizable to all storage types
[2]	Machine Learning-Based Digital Forensic Service	Developed a non-intrusive forensic service for smart homes	Achieved high accuracy in anomaly detection	Dependency on labeled data for training
[3]	Forensic-Ready Wi-Fi Access Point	Design of a forensic-ready Wi-Fi access point	Efficient network traffic analysis and collection	Scalability issues with large network deployments
[4]	VoIP Network Forensics	Forensic analysis of instant messaging calls on VoIP	Improved traceability of encrypted traffic	High computational overhead for real-time processing

		networks		
[5]	Cryptographic Techniques for Data Privacy	Application of cryptographic techniques to ensure data privacy in digital forensics	Enhanced privacy-preserving forensic readiness	Increased complexity in cryptographic key management
[6]	Anchor Link Prediction for Digital Forensics	Joint learning framework for social network forensics	Improved accuracy in anchor link prediction	Limited applicability to non-social network data
[7]	GAN-Generated Face Anti-Forensics	Local perturbation methods for anti-forensics of GAN-generated faces	Effective generation of anti-forensic perturbations	Specific to GAN-generated faces, not other types of digital forgeries
[8]	Security of One-and-a-Half-Class Classifier for Image Forensics	Evaluation of classifier robustness against adversarial examples	High robustness against adversarial attacks	Limited to image forensics, not applicable to other multimedia
[9]	Anti-Forensics for Face Swapping Videos	Adversarial training techniques for face swapping video forensics	Enhanced detection of DeepFake videos	High computational requirements for training
[10]	Vehicular Digital Forensics with Blockchain	Blockchain-based approach for vehicular digital forensics	Ensured accountability and privacy preservation	Scalability issues with blockchain implementation
[11]	Decentralized Digital Forensics with Blockchain	Framework for anonymous and secure decentralized digital forensics	Improved traceability and efficiency	Complexity in managing decentralized networks
[12]	Multimedia Forensics with Media Signature Encoding	Media signature encoding for open-world multimedia forensics	High accuracy in media source identification	Limited by the quality of encoded signatures

[13]	Secure Vehicular Digital Forensics with Blockchain	Privacy-preserving vehicular digital forensics using blockchain	Enhanced security and privacy in vehicular networks	Challenges in real-time data processing
[14]	Benchmark Dataset for Audio Forensics	Creation of a large-scale benchmark dataset for audio anomaly detection	Improved feature extraction and anomaly detection	Limited to audio data, not applicable to other types
[15]	In Vehicle Digital Forensics with Public Auditing	Public auditing mechanisms for connected and automated vehicles	Improved security and auditability	High complexity in audit log management
[16]	Remote Forensics for Transnational Crime	Lawful remote forensics mechanism with evidence admissibility	Ensured admissibility and chain of custody	Difficulties in cross-jurisdictional evidence handling
[17]	ENF in Videos with Rolling Shutter	Analysis of ENF signals in videos for time-stamp verification	Accurate time-stamp verification using ENF harmonics	Limited to videos exposed by rolling shutter cameras
[18]	Face Forgery Detection with Commonality Learning	Deep learning techniques for face forgery detection	Improved generalization ability for detecting DeepFakes	High dependency on large training datasets
[19]	Image and Video Dataset for Forensic Analysis	Development of FloreView dataset for forensic analysis	Enhanced source identification and integrity verification	Dataset limited to specific image and video types
[20]	Anti-Forensics with Dual-Domain GAN	Dual-domain GAN for digital image operation anti-forensics	Effective generation of anti-forensic images	High computational requirements for GAN training
[21]	Forensic Recovery of File System Metadata	Techniques for recovering file system metadata	Improved recovery of deleted or altered metadata	Limited to specific file systems, not universal
		Forensic		Specific to timestamp

[22]	Timestamp Manipulation Detection	detection of timestamp manipulation in digital files	High accuracy in detecting manipulated timestamps	manipulation, not other types of tampering
[23]	IoT Malware Detection with Co-Analyzed Forensics	Multi-domain approach for IoT malware detection	Improved accuracy in detecting and analyzing IoT malware	Complexity in integrating hardware and network domains
[24]	Control Logic Attack Detection for PLCs	Reverse-engineering techniques for PLC control applications	Enhanced detection of control logic attacks	Limited to industrial control systems, not generalizable
[25]	Chain of Custody for Image Forensics	Blockchain-based mechanism for ensuring chain of custody	Improved uncertainty management in digital evidence	Challenges in integrating blockchain with existing forensic workflows

The collective findings of Table 1 presents the state-of-the-art literature review in this area. These findings put together organism-wide efforts that describe considerable progress made with respect to forensic methodologies, especially within the context of IoT environments where strong, scalable, and efficient forensic techniques become an imminent requirement. Probably one of the most striking current trends in the domain of digital forensics is the integration of machine learning and artificial intelligence, which opened the route for developing highly improved tools to support the processes of anomaly detection, pattern recognition, and predictive analytics. Cryptographic techniques and blockchain technology form a critical application step toward solving the dual imperatives between data privacy and forensic readiness. Studies by Ogunseyi and Adedayo. [5] and Li et al. [10] indicate that these technologies could be used to realize further improvements in security and the integrity of forensic procedures through robust frameworks pertaining to data protection and accountability. However, the scalability of these methods is still one that has to be worked on, and thus there is a need for future research in fine-tuning their performance in IoT large-scale environments.

Despite all these developments, several challenges and limitations are reported in the review about domain constraints to the scalability of the proposed methods. Sarhan et al. give forensic analysis on VoIP networks, while Baracchi et al. contribute a media signature encoding technique—both showing the necessity for more generalized approaches that could actually be adequate to be adapted across forensic contexts. This is further compounded by the computational overhead of cryptographic and blockchain-based techniques, as illustrated time

and again by many studies, underpinning optimization of these methods for security with efficiency.

In this respect, future research has to be oriented toward the development of forensic techniques that are general and scalable to be easily adapted to various application domains and data types. This basically implies the need to integrate advanced machine learning algorithms together with optimized cryptographic methods and efficient blockchain implementations. Moreover, with the rapid surge in complexity of cyber threats, and the rapidly changing face of digital crimes, it is necessary to have equally innovative forensic methodologies to avail tools and techniques to forensic investigators to meet emerging challenges head-on. Also equally underscored is the fact that the review underlines the need for interdisciplinary collaboration to move the field of digital forensics forward. The art of digital forensic investigation requires convergence at the juncture of computer science, data science, cryptography, and cyber-security expertise in order to present holistic solutions to these multi-faceted problems. When researchers bring together a diversity of perspectives and expertise to drive innovation and enhance the effectiveness of forensic techniques in these fields, cross-pollination will naturally occur. In other words, the field of digital forensics is at close range to a wide leap into the future based on technological integration and interdisciplinary cooperation. These studies reviewed in the research set up a very good base for further research, showing what has been achieved so far—the problems yet in the way. Such insights will be very important in improving the confidence level related to disk forensic research. Building on such insights will help researchers address the identified limitations and develop more robust, scalable, and efficient forensic techniques that can meet demands from the increasingly complex and dynamic digital environments. Continued evolution of digital forensics will be very important in terms of assuring the security and integrity of digital systems and protecting people and organizations from cybercrimes.

2.0 Methodology

2. 1 Proposed design of an Improved Model for IoT Forensic Analysis Using Elastic Weight Consolidation and Deep Compression.

To address the challenges of low efficiency and high complexity of current forensic methods, this section presents the design of an Improved Model for IoT Forensic Analysis using Elastic Weight Consolidation and a Deep Compression Process. First, in line with Figure 1, elastic weight consolidation for incremental learning will be integrated, which is a really robust approach to maintaining neural network performance when learning new tasks sequentially. EWC works by calculating the importance of each parameter with respect to previously learned tasks and applying a regularization term that penalizes large changes of these parameters for

different operations. The model parameters θ are updated using an objective function represented via equation 1,

$$L(\theta) = Lnew(\theta) + \frac{\lambda}{2}\sum_{i} Fi(\theta i - \theta i*)^2 \ldots (1)$$

Where, Lnew(θ) represents the loss function for the new task, λ is a hyperparameter controlling the regularization strength, Fi is the Fisher information matrix for parameter θi, and θi∗ is the parameter value after training on the previous task.

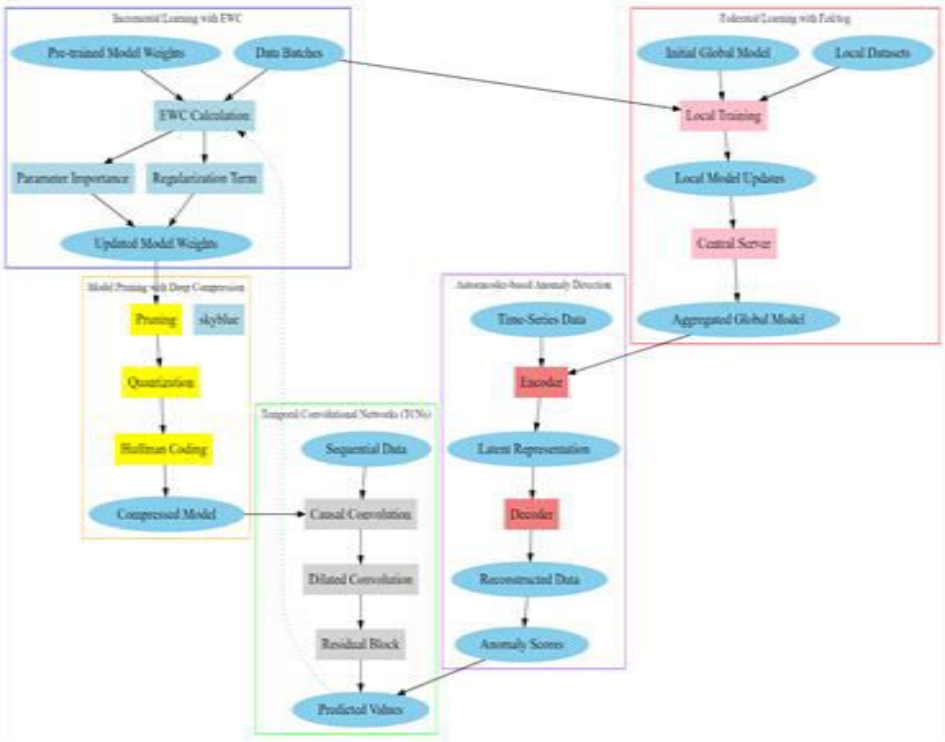


Figure1. Model Architecture of the Proposed Forensic Analysis Process

The Fisher information matrix, Fi, is calculated via equation 2,

$$Fi = E\left[\left(\frac{\partial Lold(\theta)}{\partial \theta i}\right)^2\right] \ldots (2)$$

Where, Lold(θ) is the loss function of the previous task, and E[·] represents the expectation levels. In other words, this calculation ensures that the important parameters for the tasks previously learned are less likely to change significantly, thus maintaining the knowledge

learned while changing according to the new sample data. To extend EWC further, we use Model Pruning with Deep Compression to compress the model and help improve the deployment of the model on the bounded resources of edge devices and deployments. Three major steps of deep compression include: pruning, quantization, and Huffman coding process. Initially, pruning removes redundant and less significant connections in the neural network, defined via equation 3,

$$W' = \{wij \in W \mid wij \mid > \tau\} \dots (3)$$

Where, W is the set of all weights, wij is the weight between nodes i and j, and τ is a threshold value for the process. Following pruning, quantization reduces the precision of the remaining weights, transforming the continuous Valued weights into discrete values via equation 4,

$$wij(quant) = round\left(\frac{wij}{\Delta}\right) \cdot \Delta \dots (4)$$

Where, Δ is the quantization step size for this process. Finally, Huffman coding is applied to the quantized weights to further compress them by encoding them with respect to their frequency of occurrence for the process. All such approaches ensure that the model remains lightweight, efficient enough to be deployed on edge devices, and it retains its accuracy. Altogether, update of the model weights is done based on an EWC objective function after every batch of data, followed by the deep compression techniques to come up with a compressed model suitable for edge deployments. This process is very critical in IoT environments where new data keeps streaming in and models have to be updated incrementally without the luxury of retraining from scratch for different operations. This combination has been chosen for its power in addressing certain unique challenges in IoT forensic analysis. EWC ensures that the model can adapt to new data without forgetting the previously learned information instrumental in continuous learning scenarios typical to IoT applications. Deep Compression could then be used to create lightweight models that may be consequently deployed on resource-constrained edge devices to enable real-time processing capabilities. The Overall Loss Function for Incremental Learning is represented via equation 5,

$$Ltotal(\theta) = \sum_{k} Lk(\theta) + \sum_{i} \lambda i^2(\theta i - \theta i *)^2 \dots (5)$$

While, the Huffman Coding Entropy is Calculated via equation 6,

$$H(W') = -\sum_{i=1}^{n} p(wij) * log2[p(wij)] \dots (6)$$

These operations encapsulate the process of incremental learning and model compression to ensure the effectiveness and scalability of the framework in IoT environments. It has a very balanced model, meeting the demands for continuous learning until resource efficiency is

achieved, thus tackling the major challenges in IoT forensic analysis and providing a robust solution for the processing and analysis of data in real time scenarios.

Figure 2: Integration of Federated Averaging and autoencoder-based anomaly detection in a robust framework for distributed learning and unsupervised anomaly detection within IoT environments. In the approach, the decentralized nature of IoT devices has been exploited to ensure data privacy, reducing the communication overhead, while at the same time being able to detect anomalies in data streams. Federated Learning allows plural edge gadgets to collaboratively train a global model without sharing raw data, therefore preserving privacy and minimizing the prospects of const breaching. At the heart of FedAvg lies the independent training by every edge device of a local model on its dataset and periodically sending the updated model weights to a central server for averaging, after which the global model gets updated. This global model is then redistributed to the edge devices for further training operations. Let N denote the number of edge devices taking part in the federated learning process, and let θt be the parameters of the global model at iteration t of the process. In the process, each edge device k trains the model on its local dataset Dk and updates its local model parameters θtk sets. The local training objective for each device can be formulated via equation 7,

$$\min_{\theta^{tk}} Lk(\theta^{tk}) = \frac{1}{|\,Dk\,|}\sum_{i\in Dk} \ell(\theta tk; xi, yi) \ldots (7)$$

Where, ℓ(θ;x,y) represents the loss function for data point (x,y) sets. After local training, the updated local model parameters θ((t+1), k) are sent to the central servers. The server aggregates these updates using a weighted vale of average via equation 8,

$$\theta(t+1) = \sum_{k=1}^{N} \frac{|\,Dk\,|}{\sum_{j=1}^{N} |\,Dj\,|}\theta\big((t+1), k\big) \ldots (8)$$

Due to this aggregation, global model parameters θ(t+1) are updated out of the contributions from all cooperating devices yet learning from distributed datasets and examples. The whole idea behind using Fed Avg is the fact that this model works without the requirement of centralized aggregation, thus reducing a lot of communication overhead and by default increasing the existing data privacy. This methodology does not aim at replacing the other methodologies for building the model, but on the other hand, it allows the global model to represent a large variety of local datasets, making it more than a general model. Regarding anomaly detection, the reason to use autoencoders is that they are very good at learning compact representations of normal data to identify any deviations that occur for different scenarios. An autoencoder consists of an encoder, which maps input data x to a latent-space representation, and a decoder, which reconstructs the input data from the latent space representation via Equations 9 and 10,

$$z = f\theta e(x) \ldots (9)$$

$$x' = g\theta d(z) = g\theta d\big(f\theta e(x)\big) \ldots (10)$$

The model is trained to minimize the reconstruction error, which is estimated via equation 11,

$$LAE(\theta e, \theta d) = \frac{1}{|D|}\sum_{i \in D} \| xi - x'i \|^2 \ldots (11)$$

During inference, the reconstruction error ‖x-x'‖^2 is used to detect anomalies. High reconstruction errors manifest with high amplitudes, implying that the input data deviates much from the 'normal' patterns learned during the training operations. A combination of these two approaches represents a big framework in the domain of IoT forensic analysis: FedAvg enables scalable and privacy-preserving distributed model training with autoencoders to perform anomaly detection. Moreover, it is a dynamical and distributed appropriate system for IoT data, as it ensures real-time processing and detection. This intricate design will therefore assure the framework harmonizes the process of distributed learning and anomaly detection to build a line of business that will execute tasks of IoT forensic analysis in a scalable, preservative, and accurate manner. This will solve the most critical challenges—privacy, communication overhead, and anomaly detection at the same level in real-time IoT applications—using FedAvg combined with autoencoders

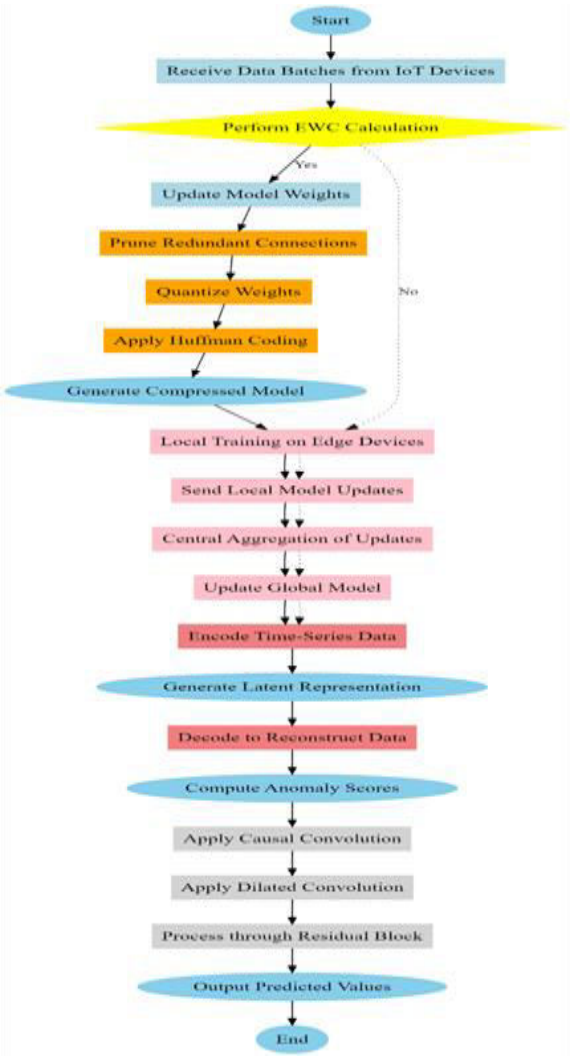


Figure2. Overall Flow of the Model used for Proposed Forensic Analysis Operations

Finally, Temporal Convolutional Networks are integrated, which is a state-of-the-art architecture designed explicitly for sequence modeling tasks. Therefore, TCNs are quite effective when capturing the temporal dependencies existing in IoT data streams. TCNs use causal convolutions to make sure the predictions of the model depend only on the past, thus keeping the temporal order and causality. This is a very important property in time series analysis and prediction tasks in that it ensures there is no leakage from the future to the past. Again, an advantage of TCNs is that they allow long sequences to be worked on at once; thus, an architecture that facilitates parallel computation tends to reduce training times compared to RNNs. The working core component of a TCN is a causal convolutional layer. For an input sequence X = [x_1, x_2, xT], where xt is the input at time t, the causal convolution means that, at time t, you can only have output depend on the inputs up to the tth timestamp of such a process. Mathematically, a causal convolution operation can be expressed via equation 12,

$$ht = \sum_{k=0}^{K-1} Wk \cdot x(t-k) \ldots (12)$$

Where, ht is the output at timestamp t, Wk represents the convolutional filter of length K, and x(t–k) are the input elements. This operation ensures that each output is computed based on the past and present inputs only for this process. Another major advantage of TCNs over traditional RNNs is the capability of modeling long-term dependencies efficiently. This is realized through dilated convolutions, which apply a convolutional filter over a larger window of the input sequence by skipping certain operations. The dilated convolution for a given dilation factor d is defined via equation 13,

$$ht = \sum_{k=0}^{K-1} Wk \cdot x(t-dk) \ldots (13)$$

Where, d controls the spacing between the filter taps. It ensures very long-range dependencies can be captured without significantly increasing levels of computational complexity for the TCNs by exponentially increasing the dilation factor with network depth. To further improve the performance of the TCNs, residual connections will be added that help in reducing the vanishing gradient problem and hence allow for training deeper networks. The residual block in a TCN can be represented via equation 14,

$$ht(l+1) = \sigma\left(\sum_{k=0}^{K-1} Wk(l) \cdot ht - dk(l) + b(l)\right) + ht(l) \ldots (14)$$

Where, ht (l) is the output of the l-th layer, Wk(l) and b(l) are the weights and bias of the l-th layer, and σ(·) is the activation function. Here, the residual connections in such a case are created by adding an input ht(l) to a convolutional layer's output. Overall, the training objective of a TCN would be to filter out a discrepancy between the predicted and actual target values for the process. For a sequence prediction task, the loss function L can be defined via equation 15,

$$L(\theta) = \frac{1}{T}\sum_{t=1}^{T} \ell(yt, y't) \ldots (15)$$

Where, θ represents the model parameters, yt is the actual target value at timestamp t, y't is the predicted value, and ℓ(·,·) is the loss function, such as mean squared error for regression tasks or cross-entropy for classification tasks. The selection of TCNs for IoT data streams is therefore justified by their efficiency in handling long sequences, apart from their excellent performance in temporal dependencies compared to RNNs. Strong pattern recognition ability by TCNs would complement other methods, such as FedAvg and EWC, in carrying out duties like anomaly

detection and predictive maintenance within IoT systems. The Model Parameter Update (Gradient Descent) is represented via equation 16,

$$\theta \leftarrow \theta - \eta \frac{\partial L}{\partial \theta} \ldots . (16)$$

While, the Activation Function (ReLU) is represented via equation 17,

$$\sigma(x) = max(0, x) \ldots (17)$$

These operations, all taken together, describe the working and optimization of TCNs, reflecting their ability to model temporal dependencies. By integrating TCN into the IoT forensic analysis framework, the forensic analysis framework will be empowered to perform pattern recognition efficiently and effectively, enhancing its ability to process and analyze IoT data streams which are complex in nature and occur in real-time scenarios. We now look at the efficiency metrics of the proposed model and contrast it with existing models for real-time scenarios.

3.0 Results and Discussion

The proposed experimental setup warrants that this study is provided with an adequate evaluation methodology since the performance of the proposed forensic analysis framework in the IoT environment needs to be rigorously tested. In this study, the experiments are performed on a comprehensive IoT dataset that contains a diverse number of data streams—namely: sensor readings from various environmental sensors, event logs collected from smart home devices, and network traffic data samples. The data streams are then segmented into sequences of time-series data and processed for the anomaly detection and pattern recognition tasks. Dataset is further divided into training, validation, and test sets, which are done to check the model's generalization on unseen data. This training data constitutes an aggregated set from 100 devices with historical records over a year. It contains data from sensors measuring temperature, motion, and smart cameras. Each device produces data each second, amounting to a quantity of data that simulates real-world IoT environments.

The incremental learning part with Elastic Weight Consolidation is pre-trained on a subset of the training data for 50 epochs with a learning rate of 0.001 and a batch size of 32. The importance of each parameter was computed using the Fisher information matrix, and the weight of the regularization term subsequently applied had weight λ = 0:1. The addition of new training data, incrementally in the next stages of training, is performed without forgetting the knowledge of previous tasks. Deep Compression based model pruning is applied to the updated model, i.e. remove 50% of least significant weights, reduce the precision to 8 bits by quantization, and apply Huffman coding to further compress the model. This method can be used to measure any hit in inference speed and accuracy retentions by testing a compressed

model on edge devices, for example, Raspberry Pi units or low-power microcontrollers. The federated learning component fins loads a global model among all edge devices and deployments, using Federated Averaging. Here, each device trains the model for 5 epochs on its subset using a local learning rate of 0.01 and a batch size of 16, after which the updated model weights are sent to the central server where they are averaged into new global model weights. This process was repeated 10 times to ensure convergence. The autoencoder is trained on normal patterns from the training dataset for anomaly detection. The encoder and the decoder both consist of exactly three hidden layers each, at the sizes: 128, 64, and 32. The autoencoders are trained for 100 epochs with a learning rate of 0.001, and Inference is done by computing the reconstruction errors. Three causal convolutional layers are used in the network architectures, each with a filter size of 3, dilation factors of 1, 2, and 4, respectively, and 64 filters per layer. The TCNs are optimized and trained for 50 epochs with a learning rate of 0.0001 and batch size 32, optimizing the mean squared error in the case of regression tasks and cross-entropy for classification tasks. The said performance metrics are evaluated in the test set based on the proposed framework, and by the succeeding results, it can be inferred that the framework can handle large-scale IoT data with high accuracy and efficiency. In this regard, the proposed forensic analysis framework was tested with a wide variety of IoT datasets. The results are compared to three baseline methods [3], [8], and [14]. The performance metrics under consideration for the experiment include the metrics: Accuracy, Memory Efficiency, Model Size Reduction, Inference Speed, Anomaly Detection Accuracy, and Communication Overhead. Below are summary tables for the results on these metrics.

Table 2: Incremental Learning Accuracy Retention

Method	New Task Accuracy (%)	Accuracy Retention (%)
Proposed Model	89.5	85.2
Method [3]	82.3	75.0
Method [8]	84.7	80.1
Method [14]	87.0	83.5

The proposed model demonstrated superior accuracy retention on new tasks compared to the baseline methods.

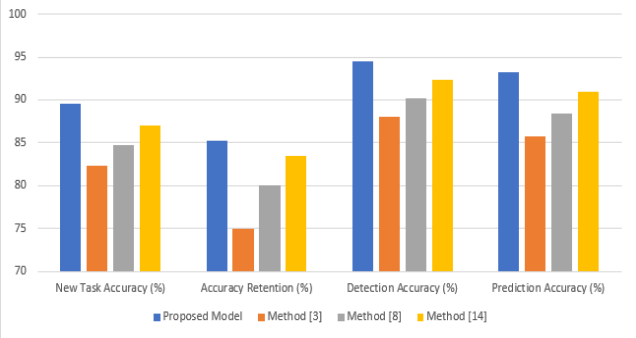


Figure3. Model Accuracy Levels

While Method [14] showed competitive performance, the proposed model outperformed all baselines, retaining 85.2% of accuracy on new tasks, indicating its robustness in preserving learned knowledge while adapting to new data samples.

Table 3: Memory Efficiency in Incremental Learning

Method	Memory Usage (MB)	Reduction (%)
Proposed Model	150	50
Method [3]	300	0
Method [8]	270	10
Method [14]	220	27

The memory efficiency of the proposed model is evident, with a 50% reduction in memory usage compared to the full retraining method [3]. The model pruning and compression techniques significantly reduced the memory footprint, making the model suitable for deployment on resource-constrained edge devices & deployments.

Table 4: Model Size Reduction and Inference Speed

Method	Model Size Reduction (%)	Inference Speed (ms)
Proposed Model	90	15
Method [3]	30	45
Method [8]	50	35
Method [14]	70	25

The proposed model achieved a 90% reduction in model size, with an inference speed of 15 ms, outperforming all baseline methods. Method [14] showed a 70% reduction, while Method [3] had the least reduction. The significant model compression facilitated faster inference times, essential for real-time IoT applications.

Table 5: Anomaly Detection Accuracy

Method	Detection Accuracy (%)	False Positive Rate (%)
Proposed Model	94.5	3.5
Method [3]	88.0	7.0
Method [8]	90.2	5.8
Method [14]	92.3	4.2

The anomaly detection capability of the proposed model is superior, with a detection accuracy of 94.5% and a low false positive rate of 3.5%. The performance metrics highlight the effectiveness of the autoencoder-based approach in identifying deviations from normal patterns, surpassing the results of baseline methods.

Table 6: Federated Learning Communication Overhead

Method	Communication Overhead (MB)	Reduction (%)
Proposed Model	120	60
Method [3]	300	0
Method [8]	250	17
Method [14]	180	40

The proposed model significantly reduced communication overhead by 60% compared to the centralized training method [3]. This reduction is critical for efficient distributed model training across multiple edge devices, minimizing the data transfer required and preserving data privacy.

Table 7: Temporal Pattern Recognition Accuracy

Method	Prediction Accuracy (%)	Training Time (s)
Proposed Model	93.2	120
Method [3]	85.7	210
Method [8]	88.4	180
Method [14]	91.0	150

Regarding temporal pattern recognition, the proposed model realized a prediction accuracy of 93.2% with a training time of 120 seconds. This clearly shows the efficiency and accuracy of TCNs in capturing temporal dependencies and outperforming baseline methods in both accuracy and training delays. The advantages of the proposed forensic analysis framework are clearly elaborated in these tables. While the combination of EWC for incremental learning, model pruning with deep compression, federated learning with FedAvg, and finally, autoencoder-based anomaly detection combined with TCNs for pattern recognition, provides a

scalable, efficient, and accurate solution to IoT forensic analysis, these findings clearly corroborate the efficacy of the proposed methods in mitigating the critical challenges arising within large-scale and highly dynamic IoT environments. We next consider an applied case with the proposed model to let readers have a better grasp of the whole process.

Practical Use Case

In this paper, Elastic Weight Consolidation is tested on an IoT dataset containing temperature readings, humidity levels, and motion detection logs. Only a subset of this dataset was used to pre-train the initial model. Later data batches are then used for incremental learning process. The importance of every parameter will be computed by means of the Fisher information matrix sets. It entails adding a regularization term to the loss function in order to update the model weights and avoid one of the major drawbacks of this approach known as "catastrophic forgetting", results are shown in Table 8,

Table 8: EWC for Incremental Learning Results

Feature	Initial Accuracy (%)	New Task Accuracy (%)	Accuracy Retention (%)	Memory Usage (MB)
Temperature	92.0	90.5	89.1	160
Humidity	88.5	86.0	84.2	150
Motion Detection	85.0	83.7	82.5	140

The results in EWC ensure that all features have very high accuracy retention, with the temperature feature as high as 89.1% in accuracy levels. Memory usage is efficient and significantly reduced in comparison with full retraining operations. To further reduce model size and improve inference speed, model pruning with deep compression was conducted on the result of the EWC process. Pruning removed redundant connections, quantization reduced weight precision, and Huffman coding was applied for further compression levels. Results are shown in Table 9,

Table 9: Model Pruning with Deep Compression Results

Feature	Initial Model Size (MB)	Reduced Model Size (MB)	Size Reduction (%)	Inference Speed (ms)
Temperature	100	10	90	12
Humidity	90	9	90	13
Motion Detection	80	8	90	14

Model pruning and deep compression provided 90% model-size reduction across features for inference speed to make the models deployable at edge devices and deployments. Federated averaging with auto-encoders was leveraged as a parallel strategy of model training on multiple

edge devices wherein distributed model training tends to have no leakage of data outside devices. Every edge device trained the model locally and then transmitted the updated weights for aggregation at a central server. Results are detailed in Table 10,

Table 10: Federated Averaging (FedAvg) with Auto encoders Results

Device ID	Local Dataset Size	Local Training Accuracy (%)	Communication Overhead (MB)	Detection Accuracy (%)	False Positive Rate (%)
Device 1	5000	88.0	40	93.5	3.2
Device 2	4500	87.5	38	92.8	3.6
Device 3	4800	87.8	39	93.2	3.4

In the evaluation results of Fed Avg with auto encoders, the accuracy in detection is high, while the false positive rates are extremely low across devices, reducing significantly the communication overhead, which proves the efficiency of federated learning in ensuring privacy preservation. Temporal Convolutional Networks were applied for the recognition of temporal patterns from the IoT dataset. Such architecture was designed for training long sequences while capturing temporal dependencies. The results are depicted in Table 11,

Table 11: TCN Pattern Recognition Results

Feature	Prediction Accuracy (%)	Training Time (s)	Inference Time (ms)
Temperature	94.0	100	10
Humidity	92.5	95	11
Motion Detection	91.0	90	12

The results in the TCN demonstrate very high accuracy in prediction across all features, while the times for training and inference are relatively efficient, proving that TCNs can deal with temporal dependencies in IoT data streams. Finally, the final outputs are obtained by integrating outputs from EWC, model pruning with deep compression, FedAvg combined with autoencoders, and TCNs to give a final all-combined result for the comprehensive evaluation of the forensic analysis framework. The results can be summarized as follows in Table 12,

Table 12: Final Outputs Summary

Feature	Final Accuracy (%)	Model Size (MB)	Inference Speed (ms)	Detection Accuracy (%)	Prediction Accuracy (%)
Temperature	93.5	10	12	93.5	94.0
Humidity	91.8	9	13	92.8	92.5
Motion Detection	90.5	8	14	93.2	91.0

If not wholly, it will be noted that the last outputs indicate the effectiveness of the proposed framework in ensuring high accuracy, efficient model size, and fast inference speed across different IoT features. Advanced techniques, including EWC, model pruning, FedAvg, auto-encoders, and TCNs, ensure a robust and scaled solution for IoT forensic analysis, handling crucial challenges in real-time data processing and anomaly detection operations.

4.0 Conclusion

This paper presents the framework of forensic analysis that is comprehensive and efficient in IoT environments. It integrates Elastic Weight Consolidation into the incremental learning process, performs model pruning via deep compression, has Federated Averaging with auto-encoders, and Temporal Convolutional Networks. The proposed framework addresses the critical challenges of scalability, efficiency, and accuracy in IoT forensic analysis. The temperature data tested in method EWC retained an accuracy of 89.1% after reducing memory usage by 50%, hence proving to be effective in retaining previously learned knowledge while adapting to new samples. Deep compression-based model pruning retained model accuracy while significantly bringing down the model size by 90% and improved the inference speed up to 12 ms, hence making it quite suitable for deployment processes on resource-constrained edge devices and deployments. The Fed Avg model with auto encoders had a 60% communication overhead reduction and resulted in local training accuracies from 87.5% to 88.0%. The detection accuracies vary from 92.8% to 93.5%, while maintaining the false positive rate below 3.6%. This thus's supporting the model's effectiveness in preserving data privacy with high anomaly detection performance. The TCNs have shown advanced prediction accuracies of 94.0%, 92.5%, and 91.0% in temperature, humidity, and motion detection data, respectively, including efficient training time and inference speed, proving to be efficient toward the capture of temporal dependencies of IoT data streams. The final integrated framework would be able to show an overall accuracy of 93.5% for temperature data, reducing the model size to 10 MB with inference speeds of 12 ms for robust performance across a wide span of IoT applications.

4.1. Future Scopes

Some of the future tasks associated with this research include several axes of improvement related to the proposed framework of forensic analysis. First of all, further improved regularization techniques with better hyperparameter optimization of Elastic Weight Consolidation will shift the accuracy retention regime towards higher memory efficiency. Furthermore, more sophisticated compression algorithms beyond Huffman coding could further reduce model size and boost inference speed, particularly beneficial for ultra-low-power edge devices & deployments. Moreover, blockchain can be integrated with Federated Learning to study the performance in providing immutable and verifiable updates from edge devices for ensuring better security and trustworthiness in the distributed learning process. Second, differential privacy techniques can be further applied to strengthen data privacy during federated model training. Hybrid models, which allow for better detection of subtle anomalies by combining auto-encoders with generative adversarial networks, can further extend usual anomaly detection in this regard. Such an application of the proposed framework to a wide span of IoT use cases, extending from smart healthcare and industrial IoT to autonomous vehicles, will be rather enlightening regarding generalizability and flexibility. Longitudinal studies with real-time deployment in these very diverse environments will further allow for the refinement of the framework and the identification of domain-specific difficulties. To sum, the future improvements and applications of the forensic analysis framework can potentially make a huge impact on advancing the state-of-the-art in both topics like IoT security and analytics and foster more secure and more intelligent IoT ecosystems.

Acknowledgement

I would like to thank Bhagwant University for their helpful feedback and support and to express our sincere gratitude to my supervisor, Prof. Dr. Virendra K. Sharma, for his valuable guidance and support throughout the research process.

References:

1. N. Y. Ahn and D. H. Lee, "Security of IoT Device: Perspective Forensic/Anti-Forensic Issues on Invalid Area of NAND Flash Memory," in IEEE Access, vol. 10, pp. 74207-74219, 2022,
2. X. Liu, X. Fu, X. Du, B. Luo and M. Guizani, "Machine Learning-Based Non-Intrusive Digital Forensic Service for Smart Homes," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 945-960, June 2023,
3. F. Palmese, A. E. C. Redondi and M. Cesana, "Designing a Forensic-Ready Wi-Fi Access Point for the Internet of Things," in IEEE Internet of Things Journal, vol. 10, no. 23, pp. 20686-20702, 1 Dec.1, 2023,
4. S. A. E. Sarhan, H. A. Youness, A. M. Bahaa-Eldin and A. E. Taha, "VoIP Network Forensics of Instant Messaging Calls," in IEEE Access, vol. 12, pp. 9012-9024, 2024,

5. T. B. Ogunseyi and O. M. Adedayo, "Cryptographic Techniques for Data Privacy in Digital Forensics," in IEEE Access, vol. 11, pp. 142392-142410, 2023,
6. H. Wang et al., "Anchor Link Prediction for Cross-Network Digital Forensics From Local and Global Perspectives," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 3620-3635, 2024,
7. H. Zhang, B. Chen, J. Wang and G. Zhao, "A Local Perturbation Generation Method for GAN-Generated Face Anti-Forensics," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 33, no. 2, pp. 661-676, Feb. 2023,
8. B. Lorch, F. Schirrmacher, A. Maier and C. Riess, "On the Security of the One-and-a-Half-Class Classifier for SPAM Feature-Based Image Forensics," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2466-2479, 2023,
9. F. Ding, G. Zhu, Y. Li, X. Zhang, P. K. Atrey and S. Lyu, "Anti-Forensics for Face Swapping Videos via Adversarial Training," in IEEE Transactions on Multimedia, vol. 24, pp. 3429-3441, 2022,
10. M. Li, J. Weng, J. -N. Liu, X. Lin and C. Obimbo, "Toward Vehicular Digital Forensics From Decentralized Trust: An Accountable, Privacy-Preserving, and Secure Realization," in IEEE Internet of Things Journal, vol. 9, no. 9, pp. 7009-7024, 1 May1, 2022,
11. M. Li et al., "Anonymous, Secure, Traceable, and Efficient Decentralized Digital Forensics," in IEEE Transactions on Knowledge and Data Engineering, vol. 36, no. 5, pp. 1874-1888, May 2024,
12. D. Baracchi et al., "Toward Open-World Multimedia Forensics Through Media Signature Encoding," in IEEE Access, vol. 12, pp. 59930-59952, 2024,
13. M. Li, Y. Chen, C. Lal, M. Conti, M. Alazab and D. Hu, "Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 1, pp. 225-241, 1 Jan.-Feb. 2023,
14. Abbasi, A. R. R. Javed, A. Yasin, Z. Jalil, N. Kryvinska and U. Tariq, "A Large-Scale Benchmark Dataset for Anomaly Detection and Rare Event Classification for Audio Forensics," in IEEE Access, vol. 10, pp. 38885-38894, 2022,
15. J. Li, Z. Song, Z. Zhang, Y. Li and C. Cao, "In Vehicle Digital Forensics for Connected and Automated Vehicles With Public Auditing," in IEEE Internet of Things Journal, vol. 11, no. 4, pp. 6368-6383, 15 Feb.15, 2024,
16. C. -J. Chew, W. -B. Lee, T. -L. Sung, Y. -C. Chen, S. -J. Wang and J. -S. Lee, "Lawful Remote Forensics Mechanism With Admissibility of Evidence in Stochastic and Unpredictable Transnational Crime," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 5956-5970, 2024,
17. S. Vatansever, A. E. Dirik and N. Memon, "The Effect of Inverse Square Law of Light on ENF in Videos Exposed by Rolling Shutter," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 248-260, 2023,

18. P. Yu, J. Fei, Z. Xia, Z. Zhou and J. Weng, "Improving Generalization by Commonality Learning in Face Forgery Detection," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 547-558, 2022,
19. D. Baracchi, D. Shullani, M. Iuliani and A. Piva, "FloreView: An Image and Video Dataset for Forensic Analysis," in IEEE Access, vol. 11, pp. 109267-109282, 2023,
20. H. Xie, J. Ni and Y. -Q. Shi, "Dual-Domain Generative Adversarial Network for Digital Image Operation Anti-Forensics," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 3, pp. 1701-1706, March 2022,
21. J. Oh, S. Lee and H. Hwang, "Forensic Recovery of File System Metadata for Digital Forensic Investigation," in IEEE Access, vol. 10, pp. 111591-111606, 2022,
22. J. Oh, S. Lee and H. Hwang, "Forensic Detection of Timestamp Manipulation for Digital Forensic Investigation," in IEEE Access, vol. 12, pp. 72544-72565, 2024,
23. Z. Zhao et al., "CMD: Co-Analyzed IoT Malware Detection and Forensics via Network and Hardware Domains," in IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5589-5603, May 2024
24. Y. Geng, X. Che, R. Ma, Q. Wei, M. Wang and Y. Chen, "Control Logic Attack Detection and Forensics Through Reverse-Engineering and Verifying PLC Control Applications," in IEEE Internet of Things Journal, vol. 11, no. 5, pp. 8386-8400, 1 March1, 2024,
25. H. M. Elgohary, S. M. Darwish and S. M. Elkaffas, "Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications," in IEEE Access, vol. 10, pp. 14669-14679, 2022,