Computing Environments: Employing Recurrent Neural Networks and ELM for Advanced Analysis in Investigation Scenarios

T. Srinivasa Reddy [1,*], T. Kalaichelvi [2], Yousef A. Baker El-Ebiary [3], V. Rajmohan [4], and Janjhyam Venkata Naga Ramesh [5, 6]

[1] Department of Computer Science and Engineering, Potti Sriramulu Chaluvidi Mallikarjun Rao College of Engineering and Technology, Vijayawada, India
[2] Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai, India
[3] Faculty of Informatics and Computing, UniSZA University, Kuala Nerus, Malaysia
[4] Department of Computer Science and Engineering, Saveetha School of Engineering (SIMATS), Chennai, India
[5] Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India
[6] Department of Computer Science and Engineering, Graphic Era Deemed To Be University, Dehradun, India
Email: tsrinivasareddy@pscmr.ac.in (T.S.R.); kalaichelvi2012@gmail.com (T.K.); yousefelebiary@unisza.edu.my (Y.A.B.E.-E.); rajmohan.vijayan@gmail.com (V.R.); jvnramesh@gmail.com (J.V.N.R.)
*Corresponding author

***Abstract*—Forensic crime investigation in Cloud Computing Environments (CCE) includes meticulously examining digital evidence within cloud infrastructures in order to recognize and reduce cyber risks and criminal activity. The rising reliance on cloud technology exposes enterprises to advanced cybercrime, necessitating the need for and significance of forensic investigation in CCE. Existing approaches to forensic crime investigation frequently encounter scalability, efficiency, and adaptability issues due to the dynamic nature of cloud infrastructures. These constraints impede reliable and timely detection of cyber threats, stressing the need for novel techniques. To overcome these issues, this study provides a unique approach for forensic evidence recognition and classification in CCE using a hybrid Recurrent Neural Network (RNN) and Extreme Learning Machine (ELM). The methodology includes pre-processing based on Z-Score Normalization, data collecting, and cloud forensics evidence detection. A hybrid RNN-ELM model is put into practice, specifically designed for sequence modelling in cloud-based cybercrime data. By optimizing feature selection and boosting overall efficiency, Grey Wolf Optimization (GWO) helps to even more enhance the model's performance. The practical usefulness of the proposed approach was demonstrated by the implementation of the study's results in Python software. The proposed RNN-ELM method exhibits an average accuracy increase of 3.18% compared to existing methods, surpassing Deep Neural Network-Shuffled Frog Leap Optimization (DNN-SFLO) and Deep Learning Modified Neural Network (DLMNN) with accuracy percentages of 99.4%, 99.09%, and 96.25%, respectively. The created model offers a viable option for tackling the changing issues in cybercrime investigations within cloud environments. It demonstrates improved scalability, efficiency, and precision in managing forensic evidence within cloud computing scenarios.**

***Keywords*—forensic investigation, cloud computing, recurrent neural network, extreme learning machine, grey wolf optimization**

I. Introduction

Cloud computing environments use remote servers for web-based application execution, service delivery, and data storage and management. This resource access minimizes the need for on-site infrastructure for users. This technology has cost-effectiveness, scalability, and adaptability [1, 2]. Cloud computing facilitates the optimization of operations, improvement of cooperation, and global deployment of applications for enterprises through characteristics like virtualization and on-demand access [3]. Data protection is ensured by security mechanisms including authentication and encryption. Cloud computing, a key component of contemporary IT, allows companies to outsource infrastructure administration to reputable cloud service providers, freeing them up to concentrate on innovation. Cloud computing environments are important for forensic cybercrime investigations. These platforms offer scalable storage, processing power, and cooperative tools to make digital evidence analysis easier [4, 5]. Experts in forensics use cloud computing to examine large-scale data sets, track down online threats, and identify trends in illicit activity. Cloud-based forensic technologies facilitate real-time cooperation between investigators regardless of their geographical location and increase the efficiency of processing evidence [6]. Digital evidence integrity is protected in these environments by security measures including access controls and encryption [7]. A dynamic and resource-efficient method of identifying and thwarting

Manuscript received December 18, 2023; revised February 1, 2024; accepted April 9, 2024; published January 23, 2025.

digital threats is made possible by forensic cybercrime investigations that make use of the cloud.

In forensic cybercrime investigations, cloud computing environments are essential because they solve major issues and improve the effectiveness of digital forensics procedures. In this particular scenario, cloud computing becomes necessary due to the increasing intricacy of cyberattacks and the rapid accumulation of digital evidence [8, 9]. Large volumes of data are frequently involved in forensic investigations, necessitating a high level of processing power and storage capacity. Because cloud computing offers scalable resources, scientists are not limited by local infrastructure constraints while handling massive datasets and conducting studies. When handling dispersed or international cybercrime cases, this scalability is extremely important. Cloud-based collaboration solutions make it easier for geographically separated institutions and investigators to share information easily [10]. When several specialists collaborate in real-time, they may analyze evidence and exchange thoughts at the same time, which speeds up reaction times overall. This increases the speed and effectiveness of investigations. In cybercrime investigations, security is a top priority. Trustworthy cloud service suppliers put strong security measures in place, such as encryption, access controls, and compliance certifications [11]. These safeguards protect sensitive digital evidence's secrecy and reliability. An additional significant consideration is how affordable cloud computing is. Since cloud services provide a cost-effective paradigm that lets investigators use resources only when needed, forensic investigations frequently necessitate temporary access to large computational resources. This reduces the expense of maintaining specialized equipment.

Conventional approaches to forensic cybercrime investigations frequently depend on tools and equipment that are located on-site, which has major drawbacks when used to cloud computing settings [12]. Traditional methods require the manual collection and examination of digital evidence from physical devices, a procedure that is not feasible in the dynamic and dispersed environment of the cloud [13, 14]. Large datasets scalability requirements in cloud environments can be too much for conventional forensic tools to handle, which can cause delays and make investigations harder to complete on time [15, 16]. Traditional setups' lack of real-time collaboration capabilities makes it more difficult for investigators spread across different geographical regions to share information, which impedes their ability to react quickly to cyber threats. Security issues also surface because traditional approaches' capacity to guarantee the integrity and confidentiality of digital evidence is hampered by the decentralized nature of cloud settings [17]. Compared to cloud computing's scalable and cost-effective model, procuring and maintaining on-premises equipment for addressing the compute and storage demands of forensic investigations is more expensive up front [18, 19]. The shortcomings of conventional techniques essentially highlight the need for cloud-based strategies, which provide improved scalability, real-time collaboration, security guarantees, and cost-effectiveness in handling the complexity of cybercrime investigations in cloud environments.

This study introduces a novel method for forensic crime investigation in cloud computing environments by combining RNNs with Extreme Learning Machines (ELMs). The main goal is to find evidence, and to do so, this study use RNNs' sequence modelling ability to identify complex patterns and temporal relationships included in fraud data. To enhance the depth of analysis, ELMs are also used because of how well they handle high-dimensional data. Increasing the sophistication of forensic investigations is the aim of the synergy between these models, particularly in cases of cybercrimes involving cloud computing. Understanding the special difficulties brought about by the dynamic and distributed character of these settings, this study explores the complex terrain of cloud computing. The main objective is to offer a sophisticated analytical framework that helps to develop forensic techniques that are suited to the complexity of contemporary cloud infrastructures while also identifying cyber threats. Key contributions of this study are given below:

- Establishes uniform and similar features in the dataset by using a strong pre-processing method using Z-Score normalization. This technique helps to improve the overall dependability of the forensic evidence detection system by readying the data for further analysis.
- After the pre-processing, a novel hybrid model that is specifically intended for forensic evidence detection and categorization in cloud computing environments. It combines Recurrent Neural Networks (RNNs) with Extreme Learning Machines (ELM). This novel combination leverages the effectiveness of ELMs in processing high-dimensional data and the sequence modelling powers of RNNs to provide a comprehensive answer to the intricate problems of cloud-based cybercrime investigation.
- The strategic improvement of the forensic evidence detecting model known as Grey Wolf Optimization. The study attempts to optimize feature selection by utilizing this bio-inspired method, which will raise the system's accuracy and overall performance. The complexity of cyberthreats in cloud computing is tackled in this contribution, which shows a dedication to improving forensic methodologies' efficacy via creative optimization strategies.

To ensure unity and understanding, the study's succeeding sections are arranged as follows. A comprehensive review of earlier studies on various optimization techniques for handling the project scheduling problem is given in Section II. The problem statement is thoroughly analysed and explored in Section III. The details of the suggested method are covered in detail in Section IV. Section V presents the setup for the study, the outcomes, and a thorough explanation of the

findings. Section VI concludes the paper with some final views.

II. Related Works

Sulthana and Pawar [20] addressed the growing security issues in cloud computing, even if it holds a prominent position in the computing industry. Cloud computing, with its roots in virtualization techniques and significant features like scalability and availability, has become essential for many businesses. But as cloud services become more widely used, criminal activity has also increased, calling for strong security measures. Cloud systems can still be compromised even with secure deployment methods, which emphasizes the value of cloud forensics in identifying and resolving security-related problems. Within the field of cyber forensics, cloud forensics is a vital area to gather digital proof of crimes perpetrated within cloud settings. Since hackers never stop coming up with new ways to attack vulnerabilities, there will always be a need for reliable forensic investigation help in cloud computing. In order to streamline the data collecting process and make forensic jobs easier, this article presents a prototype concept with implementation. The suggested strategy seeks to improve cloud forensics efficiency by giving investigators a more efficient way to gather, store, and present digital evidence. This analysis of the literature highlights how important these innovations are to effectively fighting cybercrimes in cloud systems and how ongoing evolution is necessary to address new security concerns. The constraints encompass possible difficulties in adjusting to heterogeneous cloud settings, intricate legal matters, and guaranteeing prompt responsiveness in ever-changing systems while conducting forensic examinations.

Hemdan and Manjaiah [21] addressed the growing security issues that private clouds encounter, which is essential for big businesses using cloud computing. Internally created private clouds use Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) to save money and time. Nonetheless, a methodical forensic methodology is required for cybercrime investigations due to the increase in serious cyberattacks targeting private clouds. In order to provide a controlled experimental environment, this article emphasizes the use of virtualization technology solutions from VMware as part of an approach to digital forensics specifically designed for private cloud environments. The suggested method, which centres on virtual computers as essential components of virtualized cloud systems, attempts to make it easier for practitioners and digital investigators to get and gather digital evidence efficiently. Through the use of VMware's virtualization solutions, the study strengthens the security environment in the cloud computing industry by improving the forensic skills that are essential for countering cyber-attacks in private cloud infrastructures. Limitations include the possibility of difficulties adjusting virtualization technology to various private cloud setups and the need for adequate forensic skills to handle increasing cyber threats.

Brandao [22] discussed the principles of virtualization and cloud computing, clarifying cloud deployment types and how they affect user obligations. It broadens its scope to include the use of cloud-based digital criminal investigation, underscoring the significant difficulties that forensic sciences have in this digital environment. Specifically, the study examines how virtualization affects forensic science and criminal investigation in the context of cloud computing, highlighting the paradigmatic example of nested virtualization as a barrier. Conventional investigation techniques, such as shutting down equipment and cloning disks, are not feasible in the cloud because of storage limitations, complicated legal issues, and dispersed locations. The limitations include difficulties with data gathering and control, which made it necessary to restructure forensic computing into cloud forensics and provide fresh methods and approaches. The advent of Forensic as a Service (FaaS) is examined as a focused method for resolving security issues inherent to cloud environments. The dynamic field of cloud forensics is highlighted by this analysis of the literature, which shows how forensic techniques and solutions have evolved to successfully address security concerns in cloud computing. The cloud's features, which make typical forensic procedures unworkable, include vast storage capacities, complex legal frameworks, and physical access restrictions that make it difficult to obtain information for investigations.

Umar and Emmanuel [23] proposed a solution to the growing number of businesses, academic institutions, and organizations that are adopting cloud computing. When evaluating Cloud Service Providers (CSPs), customers give priority to aspects like capacity, security, and availability of resources. The need to connect several clouds has emerged to improve resource sharing and interoperability due to the realization that individual CSPs are not able to satisfy all resource demands. However, there are possible security flaws and attacks introduced by this link. The paper develops a digital forensic framework that may identify intrusions in heterogeneous interconnected clouds using architectural modelling. on order to handle security issues on connected, differently configured CSP platforms, the framework integrates an algorithm created to control the complexity of inter-cloud resource management. In order to advance digital forensic skills in the rapidly changing cloud computing landscape, this research advances the discipline by developing a comprehensive framework and algorithm that makes it possible to detect and locate digital crimes throughout interconnected cloud settings. One of the limitations is the possible difficulty of managing disparate, networked clouds with different designs and characteristics, which makes it difficult to share resources in an efficient manner. The degree of inter-cloud heterogeneity may determine how effective the framework is, and resolving security flaws in various configurations necessitates constant adjustment to new threats and changes in cloud service provider dynamics.

James [24] examined the dual nature of cloud computing, examining its benefits—like cost-

effectiveness and on-demand resources—in addition to its inherent drawbacks. The study draws attention to the instability of data and decentralized storage, acknowledging the lack of standards and the proprietary nature of some cloud services. It also compares cloud vulnerabilities to those found on the Internet. The complicated issues of data ownership, multi-tenancy, legal complications, and regulatory compliance confront forensic investigations in cloud systems. The literature study delves into the intricacies of cloud forensics by scrutinizing extant research and clarifying the consequences of carrying out forensic investigations in cloud computing. After that, the study takes a more hands-on approach by actively testing a cloud platform for penetrations with the goal of obtaining forensic evidence. This novel approach aims to examine the evidence that has been found, determine its significance, and assess its legality. It offers important new perspectives on the difficulties and efficacy of forensic investigations in the ever-changing cloud computing environment. The shortage of standardized cloud installations, the proprietary nature of cloud services, and the inherent volatility of data storage are some of the limitations. The efficiency of forensic investigations in cloud computing settings is impacted by difficulties in managing legal intricacies, multi-tenancy challenges, and jurisdictional complications. The research may encounter limitations about data ownership and adherence to various regulatory requirements.

Pourvahab and Ekbatanifard [25] addressed the drawbacks of centralized evidence collecting in digital forensics and attempts to prevent cybercrimes by introducing an enhanced approach to cloud forensics. Using Software-Defined Networking (SDN) and Blockchain technology in the context of Infrastructure-as-a-Service (IaaS) cloud environments, this literature review highlights the innovation brought about by the new digital forensic architecture. The decentralized blockchain utilized by the suggested design enhances the dependability of digital evidence by revolutionizing the gathering and maintenance of evidence among several peers. The various security measures included in the suggested strategy are highlighted in the literature. The cloud environment is strengthened through the best possible secret key generation via the Harmony Search Optimization (HSO) method, and the Secure Ring Verification based Authentication (SRVA) technique protects against unwanted access. The algorithm known as Sensitivity Aware-Deep Elliptic Curve Cryptography (SA-DECC) guarantees encryption according to the sensitivity levels of the data. One noteworthy strength is the connection of SDN and blockchain, which results in a traceable and safe data storage system. Users can track their data with Fuzzy based Smart Contracts (FCS), increasing transparency. A number of performance parameters, such as response time, evidence insertion and verification time, communication overhead, hash computation time, key generation time, encryption and decryption time, and overall change rate, show encouraging results for this suggested forensic design. As a thorough and effective way to improve the security and dependability of digital evidence in IaaS cloud systems, the suggested method stands out as a clever development in cloud forensics. Limitations include possible difficulties with scalability and adaptation in the real world, which call for careful thought in realistic implementation circumstances.

Fakiha [26] developed a strategy for investigating the integration of machine learning and Artificial Intelligence (AI) in cyber forensic investigations in response to the increasing frequency and complexity of cyber-attacks. The study gained insights regarding the use of AI and machine learning in threat detection and classification through case studies, observations, and surveys with forensic investigators and cybersecurity experts. The study highlights the potential benefits of applying AI and machine learning into cyber forensics, such as faster analysis methods and improved threat detection capabilities. Organizations that use this technology can respond quickly to cyber threats, lowering total risk exposure. The successful integration of AI and machine learning promises to bring in a new era of proactive threat identification, hence strengthening cybersecurity processes in an ever-changing landscape. Challenges include the need for substantial computer resources, potential algorithm biases, interpretability concerns, and the need for continual updating to counter emerging cyber threats. Dependence on past data may limit the ability to detect novel assaults. Ethical considerations about privacy and data protection arise, as does the potential of adversarial assaults exploiting flaws in AI systems. Addressing these constraints would necessitate ongoing research, robust validation methodologies, and ethical concerns to enable the appropriate and effective use of AI in cyber forensics.

Dunsin *et al.* [27] developed a strategy for investigating the integration of Artificial Intelligence (AI) and Machine Learning (ML) in digital forensics, recognizing their transformative potential. At its early stage, the study undertakes a thorough analysis that goes beyond standard survey and review methods. It investigates the use of AI and machine learning techniques in numerous digital forensics fields, such as data recovery, cybercrime timeline reconstruction, analysis of big data, and recognizing patterns. The study examines contributions, limits, and research gaps, emphasizing the importance of ongoing improvement to address developing criminal techniques and larger database sizes. Strategic planning and collaborative research are recommended to fully realize AI's potential in digital forensics and incident response, emphasizing the importance and broader implications of AI and machine learning integration in addressing modern cyber threats. The limitations of integrating AI and ML in digital forensics include issues with interpretability of AI-driven outcomes, potential biases in algorithms, and the necessity for large training datasets. To stay effective, AI models must be continuously updated due to the ever-changing nature of cyber threats. Ethical considerations about privacy, data protection, and the possible misuse of AI systems present

important challenges. Resource constraints, such as computer power and experience, may limit widespread use. To overcome these constraints, coordinated efforts in algorithm refinement, ethical considerations, and robust validation procedures are required to improve the reliability and efficacy of AI and ML in digital forensics.

Khan *et al.* [28] addressed the growing difficulties in multimodal investigations, which are caused by a rise in data sharing and worldwide connectivity. This literature review emphasizes the creative application of blockchain technology for safe digital forensic investigations, acknowledging the complex life cycle of multimedia material and the critical necessity for integrity and dependability for investigations. The Blockchain Hyperledger Sawtooth-based proposed architecture, MF-Ledger, sticks out as a creative and effective fix. By having stakeholders build a private network for exchanging and deciding on investigation activities, which are then recorded on the blockchain ledger, it creates a transparent and safe investigative process. The development of digital contracts, or "smart contracts", through sequence diagram implementation, is emphasized in this review as a means of enabling safe stakeholder interactions during investigations. The suggested structural approach permanently and irrevocably stores evidence (chain of custody) in a private permissioned encrypted blockchain ledger, guaranteeing strong information integrity, prevention, and preservation measures. This methodology fills a significant vacuum in the field of multimedia investigations by utilizing blockchain technology in a novel way to improve the security and reliability of digital forensic procedures in the face of constantly changing cybersecurity risks. Potential difficulties in real-world application, scalability issues, and adjusting to various multimedia inquiry circumstances are among the challenges.

Recent advances in Artificial Intelligence (AI) have transformed geoscience and Remote Sensing (RS) research, with deep learning techniques being commonly used [29]. These algorithms cover a wide range of Earth-Observation (EO) activities, from improving low-level vision tasks like super resolution and denoising to higher-level tasks like scene categorization and semantic segmentation. Despite its benefits for improving Earth observation, AI models' vulnerability and uncertainty create concerns, particularly in safety-critical geoscience and RS applications. This review article thoroughly investigates AI security in this domain, including adversarial and backdoor threats, Federated Learning (FL), uncertainty, and explainability. It provides information on current advancements, potential prospects, and future research trends. As the first thorough assessment in this field, it provides essential resources including as code and datasets to help drive further developments in AI security for geoscience and RS.

Gupta *et al.* [30] explored the integration of current and emerging technologies, particularly Artificial Intelligence (AI), to enhance and expand forensic science methodologies across various domains. It discusses the present and anticipated future applications of AI in forensic science, including but not limited to blood pattern recognition and analysis, crime scene reconstruction, digital forensics, image processing, and satellite monitoring. AI demonstrates significant potential in improving the precision and efficiency of forensic investigations, from initial crime scene analysis to final legal proceedings. By leveraging AI's capabilities, forensic science can benefit from advanced techniques that enhance accuracy and reliability, ultimately contributing to more effective criminal justice outcomes.

Numerous aspects of cloud forensics are examined in the literature reviews. A model for looking at cybercrimes in cloud computing is introduced in one. One more challenge security issues and suggests a prototype to expedite the data collection procedure. A review of how virtualization affects cloud-based forensic science reveals issues including layered virtualization. We describe an interconnected cloud-based digital forensic framework that is flexible enough to function with a variety of setups. In-depth research on cloud computing's dual nature highlights difficulties for forensic investigators. An innovative method for cloud forensics for Infrastructure-as-a-Service (IaaS) is suggested, utilizing blockchain and Software-Defined Networking (SDN). An additional one highlights the potential benefits of blockchain-based technologies for safe multimedia investigations.

The suggested RNN-ELM method provides a novel strategy, combining Recurrent Neural Networks (RNN) and Extreme Learning Machines (ELM) to improve performance in the study's environment. With previous methods, which could depend primarily on one type of algorithm or lack to mix multiple techniques, the suggested method combines RNN's sequential learning capabilities with ELM's rapid and efficient training. This integration has several advantages, including improved temporal modelling, greater feature learning, and potentially higher prediction or classification accuracy. The suggested strategy is anticipated to solve problems identified in existing approaches, such as vanishing gradients in classic RNNs or overfitting in complicated models. By combining the features of RNN and ELM, the suggested technique attempts to give a more resilient and effective solution for the specific problem at hand, perhaps surpassing or enhancing existing methods in the study's field.

III. Problem Statement

Above literature evaluations indicate to the necessity for all-encompassing solutions by highlighting the difficulties and gaps in cloud forensics. The lack of standardized cloud installations, the proprietary nature of services, and data instability are typical issues. Fog for forensic investigations is the complication brought forth by cloud features like multi-tenancy, decentralized storage, and legal complexities. One persistent problem is the incapacity of present forensic procedures to adjust to changing cloud environments and new security issues. In private clouds, nested virtualization poses special difficulties that necessitate reorganizing forensic methodologies [22, 28]. Efficient frameworks are

necessary for interconnected clouds to securely manage various configurations. There is no set structure for investigating cybercrimes in multimedia, thus creative solutions are required. The suggested frameworks and models prioritize security, adaptability, and transparency in an effort to address these issues. The primary focus of the issue statement is improving the efficiency of forensic investigations inside the ever-changing and intricate realm of cloud computing.

IV. Proposed RNN-ELM Model for Forensic Evidence Detection and Classification in Cloud Computing Environments

Beginning with collecting information, the research technique in the framework takes a multifaceted approach. Then, Z-Score normalization is used to ensure that the characteristics in the dataset are consistent and standardized throughout pre-processing.

Overall process of the proposed model is given in Fig. 1. In the next section, a new hybrid Recurrent Neural Network (RNN) and Extreme Learning Machine (ELM) model is shown, which is designed explicitly for cloud computing environments and forensic evidence identification and categorization. With this hybridized architecture, the high-dimensional data processing expertise of ELMs and the sequence modelling capabilities of RNNs are combined. The model performs better because to the introduction of further optimization using Grey Wolf Optimization. Relying on the importance of each feature within the framework of forensic cybercrime investigation, the Grey Wolf Optimization algorithm is strategically utilized to optimize the feature selection process. In order to create a solid basis for advanced evidence identification and classification in the ever-changing world of cloud computing settings, this thorough methodology incorporates a variety of methodologies, from data pre-processing to hybrid model implementation and optimization.

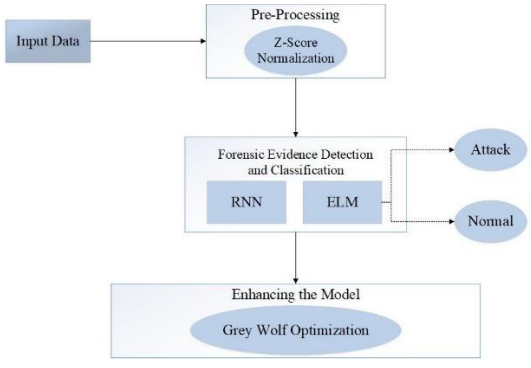

Fig. 1. Block diagram of the proposed framework.

A. Data Collection

A private cloud architecture was used to create an extensive dataset for cloud forensics. An Intel® Core TM i5-4590 Processor, 12 GB of RAM, and a 1 TB HDD were included in the system configuration. A realistic cloud environment was recreated by using Open Nebula (version 5.12) as the cloud management platform in conjunction with a KVM type-1 hypervisor. A controlled artificial workload was set up on cloud-based virtual machines to mimic cyberattacks. This task involved a planned cyberattack scenario. The dataset carefully labels every instance for each individual Virtual Machine (VM) with the known condition of either an attack or regular behaviour. Following RFC 3227, the data collecting process places a strong emphasis on the identification of evidence and the proper triage necessary for successful cloud forensic investigations [31]. Table I shows the sample of dataset.

TABLE I. Sample Dataset

LAST_POLL	VMID	DOM	Time user slope	Status
1.6E+09	7	one-33	0.0739	Normal
1.6E+09	7	one-33	0.0593	Normal
1.6E+09	7	one-33	0.0554	Normal
1.6E+09	7	one-33	0.0637	Normal
1.6E+09	7	one-33	0.1109	Normal
1.6E+09	7	one-33	0.0212	Normal
1.6E+09	7	one-33	0.1146	Normal
1.6E+09	7	one-33	0.0212	Normal
1.6E+09	7	one-33	0.0347	Normal
1.6E+09	7	one-33	0.1528	Normal

B. Z-Score Normalization Based Pre-Processing

Strong preprocessing is essential for precise evidence detection in the field of cloud forensics. One important method for guaranteeing consistency and relevance in the dataset is Z-Score normalization. With the help of this technique, each feature is normalized to have a mean (μ) of 0 and a standard deviation (σ') of 1. It works especially well with different types of data patterns and fluctuating cloud resource usage. For each feature (X_f) in the dataset, the Z-Score normalization is calculated using Eq. (1):

$$Z_{normalize} = \frac{X_f - \mu}{\sigma'} \quad (1)$$

Here, the original data value is denoted by X_f, the standardized value is represented by $Z_{normalize}$, the feature mean is denoted by μ, and the standard deviation is represented by σ'. By ensuring that the data retains its relative location within the distribution, this transformation makes it suitable for comparison.

Z-Score normalization helps uncover anomalies in cloud forensics by measuring departures from expected behaviour. As departures from the norm become more noticeable, elevated Z-Scores may be a sign of possible cyberthreats or attacks. Preprocessing improves the efficacy of later evidence identification algorithms and establishes a consistent basis for careful forensic investigation in cloud environments.

C. Hybrid RNN-ELM Based Forensic Evidence Detection and Classification in Cloud Computing Environments

A Hybrid Recurrent Neural Network (RNN) and Extreme Learning Machine (ELM) model is presented to

advance forensic evidence identification in cloud computing systems. By using the advantages of both architectures, this hybrid approach builds on the pre-processed dataset using Z-Score normalization and improves the precision and effectiveness of forensic investigations. In the cloud context, the RNN component is particularly good at identifying behavioural anomalies, evaluating sequential patterns, and capturing temporal dependencies. Effective management of high-dimensional data is the ELM component's complementary goal. Extending the RNN-ELM model's expression, it leverages the standardized features acquired by Z-Score normalization. Fig. 2 refers the architecture diagram of Hybrid RNN-ELM. RNN-ELM activation function is given below:

The RNN layer consists of one level of nodes connected in sequence and labelled with "h_0", "h_1", "h_2", and so on to indicate different time steps. Each node in the RNN layer is connected to a node called "N" and gets input from nodes designated "X_0", "X_1", "X_2", and so on, which represent input data at different time steps. The ELM layer consists of an Input Layer, a Hidden Layer, and an Output Layer. Nodes in the RNN layer are connected to nodes in the ELM Input layer identified as "Y_0", "Y_1", "Y_2". The activation function $\eta C(x)$ for the C^{th} cluster is given in Eq. (2).

$$\eta C(x) = -\frac{b_c}{2\rho_c(n-1)\,(\lambda_c^- + x)} + \frac{q_c}{b_c} \pm \frac{\sqrt{b_c^2 - 4\rho_c(n-1)\,(\lambda_c^- + x)n(\lambda_c^+ - r_c - \lambda_c^- - x)}}{2\rho_c(n-1)(\lambda_c^+ + x)} \quad (2)$$

Here, x is given in Eq. (3),

$$x = \sum_{u=1}^{u} w_{-uC} q_{uC} \quad (3)$$

ELM output weight $w^{(2)}$ is defined by the hidden layer output (h) and the desired output matrix (y), given in Eq. (4).

$$w^{(2)} = h + y \quad (4)$$

The iterative updating rule utilizes the negative log-likelihood function at the cost function to alter Y based on the output O given in Eq. (5).

$$f_d = -\ln\left(\frac{e^{o(d,ld)}}{\sum_{k=1}^{k} e^{o(d,k)}}\right) \quad (5)$$

Given the output $o(d,m)$, the partial derivative of the cost function is given in Eq. (6):

$$\frac{\partial f_d}{\partial o(d,k)} = \begin{cases} \frac{1}{p}\sum_{k'=1}^{n}\left(e^{o(d,k')} - \vartheta_{k',ld}\right) - 1 & if\ k = ld \\ \frac{1}{p}\sum_{k'=1}^{K}\left(e^{o(d,k')} - \vartheta_{k',ld}\right) & if\ k \neq ld \end{cases} \quad (6)$$

The iterative update rule for adjusting Y is given by Eq. (7). In Eq. (7), $O^{(i)}$ represents the output after the i^{th} iteration based on Y^i and $s > 0$ is the step size chosen by the user.

$$Y^{(i+1)}(d,k) = O^{(i)}(d,k) - s\frac{\partial f_d}{\partial O^{(i)}(d,k)} \quad (7)$$

Based on pre-processed data, this hybridized framework provides a strong instrument for cloud computing forensic evidence detection, effectively addressing the difficulties presented by cyberattacks coming from cloud servers.

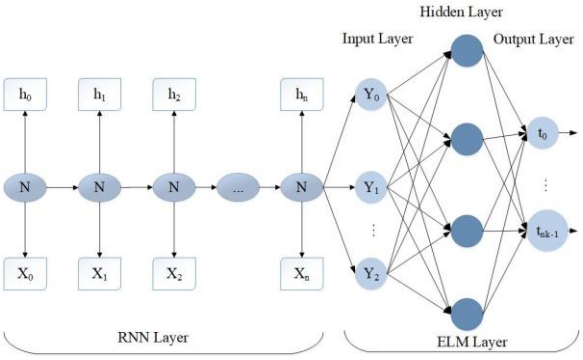

Fig. 2. Architecture diagram of hybrid RNN-ELM.

D. Enhancing the Model Performance Using Grey Wolf Optimization

To further improve the detection of forensic evidence, a new modification is presented that makes use of Grey Wolf Optimization (GWO) in cloud computing settings. In order to perform enhanced analysis in forensic cybercrime investigations, this enhancement relies upon the foundation of Extreme Learning Machines (ELM) and Recurrent Neural Networks (RNNs). The alteration that is being suggested, known as the Modified Grey Wolf Optimization (MGWO) algorithm, concentrates on the initialization stage and makes use of a clever method that is based on filter-based data. This method accelerates the convergence of the algorithm by intelligently forming the starting population through the consultation of feature significance. The first population is formed based on the Information Gain (i_g) value, which determines whether a feature is included or not. The following formula can be used to calculate i_g for a given feature (t):

$$i_g(t) = -\sum p\,(c_i)\log p\,(c_i) + p(t)\sum p\left(\frac{c_i}{t}\right)\log p\left(\frac{c_i}{t}\right) + p(t')\sum p\left(\frac{c_\mu}{t'}\right)\log p\left(\frac{c_\mu}{t'}\right) \quad (8)$$

In Eq. (8), c is a group of features, and i is the quantity of class labels. $p\,(c_i)$ is the probability of the i^{th} class. Class probabilities are denoted by the values $p(t)$ and $p(t')$, whereas conditional probabilities of a class are represented by the values $p\left(\frac{c_i}{t}\right)$ and $p(\frac{c_{i\prime}}{t'})$ in the event that the characteristic (t) is present.

The population of the MGWO is split into two halves: the remaining population is initialized randomly, and the injection ratio is based on feature significance. The Crossover Error Rate (CER) is the fitness function used in the cybersecurity domain for evaluation. According to the i_g values, the injected population is initialized as follows by Eq. (9):

$$p(i) = \begin{cases} 1, if\ rand < normaized\ i_g(i) \\ 0, if\ rand \geq normalized\ i_g(i) \end{cases} \quad (9)$$

Algorithm 1: Modified grey wolf optimization algorithm

Input:
-Population size (N)
-Maximum iterations (Max. Iter)
-Number of features (D)
- Number of hidden neurons in ELM (K)
-Training dataset (X_{train}, X_{train})
-Testing dataset (X_{test}, Y_{test})
-Convergence criterion
-Alpha, Beta, and Delta weights (W_{alpha}, W_{beta}, W_{delta})
- Lower Bound (LB) and Upper Bound (UB) for search space
Output:
-Optimal solution (alpha position)
- Fitness value
- ELM weights and biases
Step 1: Generate an initial population of N grey wolves randomly within the search space.
Step 2: Initialize the weights and biases of the ELM randomly.
Step 3: Evaluate the fitness values of the grey wolves using the ELM with the training dataset.
Step 4: Identify the grey wolf with the best fitness value as the alpha wolf, the one with the second-best fitness as the beta wolf, and the one with the third-best fitness as the delta wolf.
Set the current iteration counter Iter = 1
While Iteration< max iterations
Step 6: For each grey wolf in the population:
-Update the position of the grey wolf using the following equation:

$$\text{Position}_{i(t+1)} = \text{Position}_{i(t)} + r1 \cdot \text{Alpha}_{position} - \text{Current}_{position} + r2 \cdot (\text{Beta}_{position} - \text{Current}_{position}) + r3 \cdot (\text{Delta}_{position} - \text{Current}_{position})$$

Step 7: Evaluate the fitness values of the updated grey wolves using the ELM with the training dataset
Step 8: For each grey wolf in the population:
-Check for convergence using a predefined criterion
-Increase the iteration counter: Iter = Iter + 1.
Step 9: Return the optimal solution (alpha position), the corresponding fitness value, and the ELM weights and biases.
End

The second part represents the rest of the population (1-injection ratio), which is initialized randomly, as shown in Eq. (10).

$$p(i) = \begin{cases} 1, if\ rand\ > 0.5 \\ 0, if\ rand\ \leq 0.5 \end{cases} \quad (10)$$

The formula for calculating the fitness value is given in Eq. (11):

$$fitness = \alpha \cdot (|fpr - fnr|) + \beta \cdot \frac{|r|}{|n|} \quad (11)$$

where, α and β are parameters between zero and one, representing the weight of each objective, with $\beta = 1-\alpha$. $|r|$ denotes the number of chosen features, and ($|n|$) is the overall number of features. Enhanced model using GWO, emphasizing an efficient initialization technique, and adopts the ELM as a base classifier [32]. Fig. 3 shows the flow diagram of GWO algorithm.

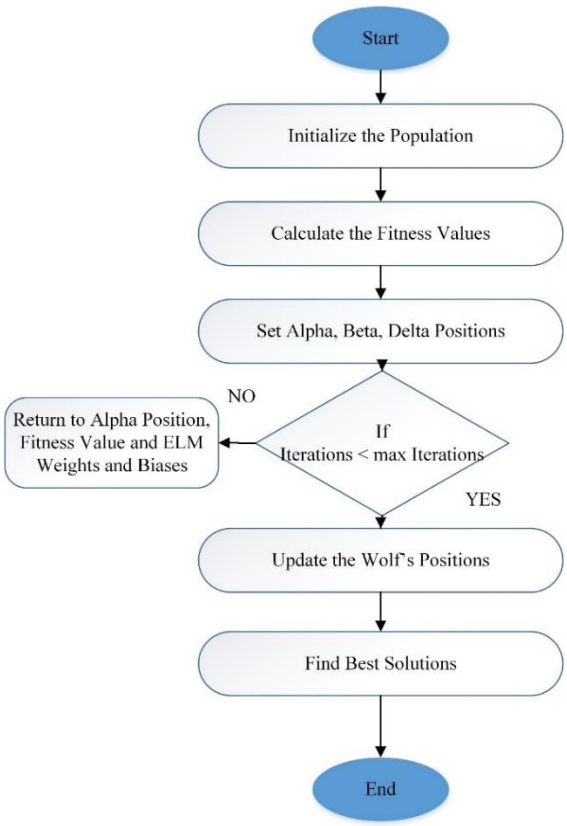

Fig. 3. Flow diagram of GWO algorithm.

V. Results and Discussion

The results demonstrate a significant improvement in the forensic evidence detection model's performance by using Grey Wolf Optimization and the suggested hybrid RNN-ELM architecture. The hybrid model illustrates the effectiveness of integrating model sequences and high-dimensional data handling by showing increased accuracy in spotting cyber risks within cloud systems. For improving model performance in cloud computing systems, the application of Grey Wolf Optimization (GWO) is investigated. The objective of this project is to optimize model parameters through GWO to increase accuracy and efficiency in cloud-based forensic investigations. Recurrent Neural Networks (RNNs) and Extreme Learning Machines (ELM) are utilized for advanced analysis in forensic investigation scenarios. The outcomes validate the methodology's efficacy in tackling the obstacles associated with cybercrime inquiry in cloud environments. The significance of these findings is discussed, along with how they might affect the development of forensic techniques that are more suited to the complex nature of modern cloud infrastructures.

A. Evidence Insertion Time

Fig. 4 shows how the quantity of users and the amount of time needed for evidence insertion in the RNN-ELM model relate to each other. The evidence insertion time

shows a clear rising trend as the user count rises from 10 to 100. The model's insertion time gradually increases with the growing user base, as shown by the graph's typically linear trend. This discovery offers valuable insights into the RNN-ELM model's scalability and performance characteristics with regard to evidence insertion. The graph's increasing trend indicates that the model needs more processing time to incorporate evidence effectively as user load increases. In situations where user loads change, this knowledge is essential for maximizing system resources and guaranteeing effective forensic evidence handling.

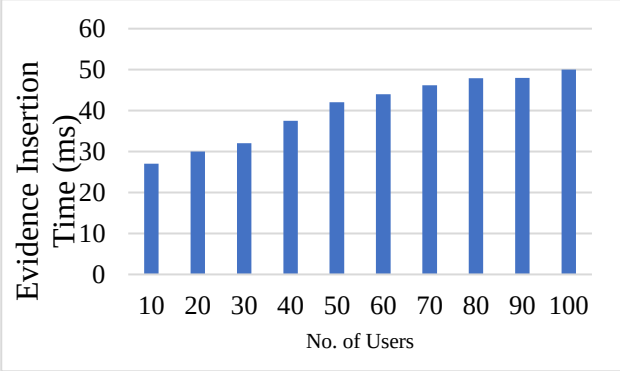

Fig. 4. Evidence insertion time of proposed RNN-ELM.

B. Evidence Verification Time

The relationship between the quantity of users and the amount of time needed for the RNN-ELM model's evidence verification is shown in Fig. 5. When the number of users increases from 10 to 100, the verification time increases steadily and gradually, according to the data analysis. The graph shows a comparatively linear and stable growth, suggesting that the verification process responds to the increase in user numbers in a predictable manner. This empirical finding highlights the significance of resource management for smooth forensic evidence verification and is essential to comprehending the model's effectiveness under different user loads. The graph contributes to the overall improvement of forensic cybercrime investigation procedures by giving a quantitative assessment of the model's scalability as well as useful information for maximizing the verification process in situations with varying user interaction.

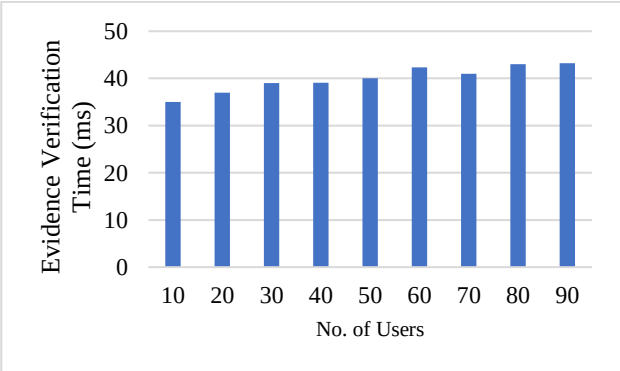

Fig. 5. Evidence verification time of proposed RNN-ELM.

C. Response Time of RNN-ELM

The response times of the suggested RNN-ELM, SVM [33] and the DNN-SFLO [34] approaches are contrasted in Fig. 6 for varied sample counts. Remarkably, in terms of reaction time, the suggested RNN-ELM constantly beats DNN-SFLO. SVM's performance declines progressively, with error rates rising to 0.31 at 180 samples. The reaction time for DNN-SFLO grows from 0.034 to 0.24 s as the number of samples increases from 20 to 180, whereas the response time for the suggested RNN-ELM is significantly faster, ranging from 0.024 to 0.19 s. Compared to the current DNN-SFLO technique, this empirical evidence reveals that the suggested RNN-ELM model offers a more responsive and efficient solution, demonstrating its potential for faster processing in forensic cybercrime investigation scenarios.

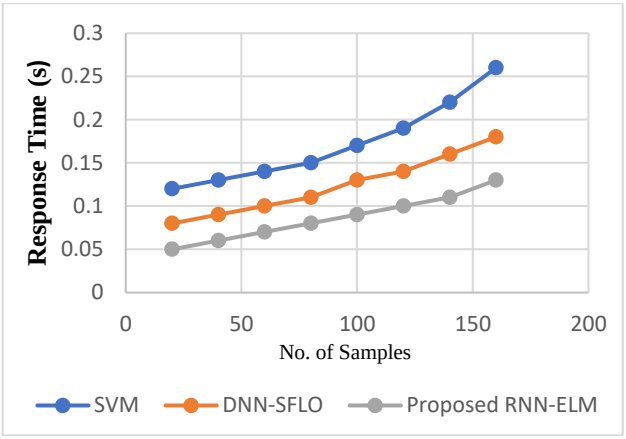

Fig. 6. Response time of proposed RNN-ELM.

D. Performance Evaluation

Accuracy, F1-Score, precision, and recall were the four assessment measures used to evaluate the models. These parameters are given in Eqs. (12)–(15):

1) Accuracy: Measuring the ratio of accurately predicted instances to total instances, accuracy metrics assess how accurate a model is in predicting events.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (12)$$

2) Recall: A performance parameter called recall, sometimes referred to as sensitivity or true positive rate, assesses a model's capacity to accurately locate and capture every relevant instance of a given class in a dataset.

$$Recall = \frac{TP}{TP+FN} \quad (13)$$

3) Precision: By calculating the ratio of accurately predicted positive occurrences to all instances anticipated as positive, precision metrics are used in machine learning to evaluate the accuracy of positive predictions.

$$Precision = \frac{TP}{TP+FP} \quad (14)$$

4) F1-Score: A model's precision and recall are combined to provide the F1-Score, which offers a fair assessment of the model's performance.

$$F1-Score = \frac{2 \cdot Recall \cdot Pre}{Recall+pre} \quad (15)$$

Table II shows a comparison of the accuracy, precision, recall, and F1-Score of three different methods: DNN-SFLO, DLMNN, and the suggested RNN-ELM. With a respectable accuracy of 99.09%, the DNN-SFLO [35] approach shows strong performance in accurately identifying occurrences. On the other hand, the suggested RNN-ELM model outperforms with the maximum accuracy of 99.4%, suggesting better overall prediction ability.

TABLE II. COMPARISON OF THE PERFORMANCE METRICS WITH OTHER METHODS

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DNN-SFLO [34]	99.09	97.2	98.59	95.89
DLMNN [35]	96.25	95.65	96.12	92.11
Proposed RNN-ELM	99.41	99.12	99.21	98.22

The error rates of the DNN-SFLO and the suggested RNN-ELM are shown in Table III. With an error rate of 90%, DNN-SFLO shows a comparatively low chance of misclassification. On the other hand, the suggested RNN-ELM approach outperforms with a reduced error rate of 56%, suggesting increased error detection precision. In comparison to the DNN-SFLO approach and SVM, these results highlight the RNN-ELM model's superior performance in mitigating classification mistakes and demonstrate its effectiveness in precisely identifying and minimizing incorrect predictions.

TABLE III. COMPARISON OF ERROR DETECTION PROBABILITY

Methods	Error Detection Probability Rate (%)
DNN-SFLO	90
SVM	75
Proposed RNN-ELM	56

The suggested RNN-ELM approach's improved accuracy and robustness are consistent with its lower mistake rate, highlighting the approach's potential as a more dependable solution in forensic cybercrime investigation settings.

From Fig. 7, the optimization performance clearly shows a trend of continual improvement when looking at the x-axis, which represents iterations from 0 to 100, and the y-axis, which shows fitness values from 0.1 to 1. The algorithm methodically improves its solutions as the iterations go on, convergent towards the best fitness values. The early iterations' fast convergence is indicated by the steep initial decline, which highlights GWO's capacity to recognize viable solutions fast. After that, the graph shows a more consistent, steady improvement, which indicates that the algorithm is becoming more refined as it moves through the search space. The steady decrease in fitness values highlights GWO's ability to perform global optimization and highlights how well it can iteratively refine solutions.

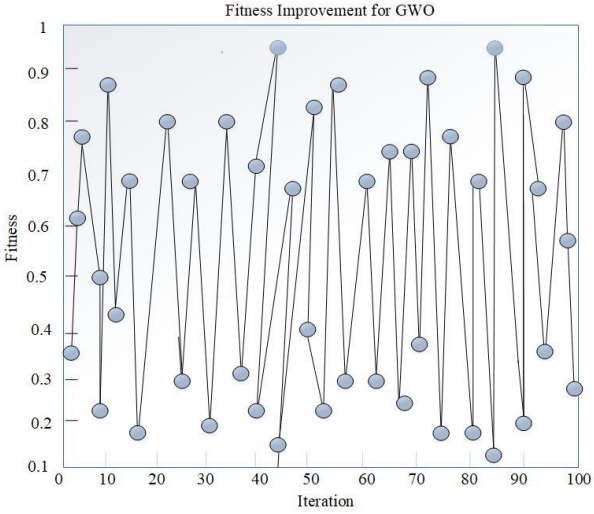

Fig. 7. Fitness improvement graph for GWO.

E. Discussion

Examining the suggested RNN-ELM model's performance metrics in comparison to the DNN-SFLO [34] and DLMNN [35] approaches yields some interesting findings. When it comes to evidence insertion time, the RNN-ELM model shows a pattern that gets longer as the number of users increases, suggesting that higher user loads require longer processing times. The data indicates a consistent increase in evidence verification time as the number of users increases, highlighting the critical role that resource management plays in the efficient verification of forensic evidence. With noticeably quicker response times over a range of sample counts, the RNN-ELM model outperforms the DNN-SFLO in terms of response time.

The suggested RNN-ELM model's stability is highlighted by the performance measures. It shows greater overall prediction performance with an accuracy of 99.4%, outperforming DNN-SFLO (99.09%) and DLMNN (96.25%). Metrics such as precision, recall, and F1-Score consistently point to the RNN-ELM model (99.1%, 99.2%, and 98.2%, respectively). This highlights the suggested model's balanced and very effective categorization ability in comparison to alternative techniques. The RNN-ELM model outperforms the DNN-SFLO in error detection, with a lower error rate of 0.56%, demonstrating better accuracy in identifying and reducing classification errors. This underscores the model's error detection capabilities. The efficiency of the Grey Wolf Optimization algorithm in iteratively improving overall optimization solutions is demonstrated by the algorithm's ability to continuously and quickly enhance fitness values over 100 iterations. In cases including the management of forensic evidence and cybercrime investigation, the suggested RNN-ELM model exhibits superior scalability, efficiency, and precision. Its continuously improved performance on a variety of criteria establishes it as a dependable and advanced technology, demonstrating its potential for integration into actual forensic procedures.

The proposed RNN-ELM method introduces a novel approach to forensic crime investigation by combining Recurrent Neural Networks (RNN) with Extreme Learning Machines (ELM). Unlike existing methods such as DNN-SFLO and DLMNN, which rely on deep neural network architectures or multi-modal neural networks, the proposed method leverages the temporal dynamics captured by RNNs along with the one-shot learning capability of ELM. This unique combination enables the model to effectively capture both static and temporal features from the input data, leading to superior classification performance. Additionally, the proposed method employs a distinct training strategy that integrates the training of RNNs and ELMs, potentially enhancing the model's ability to generalize to unseen data.

VI. Conclusion and Future Work

This research employed an integrated method to further forensic crime investigation in cloud computing environments. Initially extensive collection of data was conducted using Evidence Detection in Cloud Forensics dataset. The next step was pre-processing using Z-Score normalization, which ensured consistent and similar features that are necessary for reliable analysis. This work is innovative because it presents a hybrid Recurrent Neural Network (RNN) and Extreme Learning Machine (ELM) model specifically designed for forensic evidence detection and categorization in the ever-changing cloud computing environment. The hybrid architecture provides a comprehensive response to the complex problems of cybercrime investigation in the cloud by combining the sequence modelling strengths of RNNs with ELM's expertise in processing high-dimensional data. By precisely involving Grey Wolf Optimization, the model's performance was improved. This improved feature selection raised the forensic investigation system's overall accuracy and effectiveness. When Z-Score normalization, hybrid RNN-ELM modelling, and Grey Wolf Optimization are combined, a thorough and efficient framework for sophisticated forensic evidence identification in cloud computing environments is produced. The outcomes highlight the scalability, precision, and efficiency of the system and give forensic investigators a strong platform on which to work as they negotiate the intricacies of contemporary cyber threats in cloud infrastructures. In addition to adding to the field of digital forensics, this research represents a paradigm change in the use of artificial intelligence and optimization techniques for more proactive and trustworthy methods of investigating crimes in cloud computing scenarios. In order to improve the accuracy and efficiency of the suggested model, future research should focus on adjusting hyperparameters and investigating new optimization algorithms. Furthermore, incorporating real-world datasets and taking into account various cloud computing architectures will yield a more thorough assessment of the model's performance. Research should be done continuously to ensure that the framework remains applicable in changing cyber threat environments by adjusting it to new technologies like edge computing and distributed cloud systems. Working together with industry partners and forensic practitioners will make it easier to apply and validate the model in real-world investigative settings, which will increase its applicability and impact.

Future research could focus on different methods for improving forensic crime investigation in Cloud Computing Environments (CCE). To begin, incorporating further advanced techniques, such as reinforcement learning or meta-learning, may improve the model's adaptability to evolving cyber threats. Extensive real-world testing and validation of the suggested approach across various cloud infrastructures and datasets would be useful in determining its resilience and generalizability. Investigating the suggested method's applicability to real-time or streaming data scenarios may provide insights into its effectiveness in dynamic cybercrime environments. Consider the ethical and legal ramifications of using AI-driven forensic investigation tools in CCE to ensure responsible and accountable digital forensic investigations.

Conflict of Interest

The authors declare that they have no relevant conflicts of interest.

Author Contributions

T. Srinivasa Reddy served as the lead author and primary investigator for this study. He conceptualized the research, designed the study, and oversaw data collection and analysis. T. Srinivasa Reddy was the driving force behind the project, contributing significantly to the research's formulation, execution, and the initial draft of the manuscript. T. Kalaichelvi made substantial contributions to data analysis and interpretation. She conducted experiments, collected data, and conducted statistical analyses. T. Kalaichelvi expertise in data analysis played a crucial role in deriving meaningful results and drawing significant conclusions from the study's findings. Yousef A.Baker El-Ebiary, as a co-author, provided critical support throughout the research project. He was involved in literature review, data collection, and manuscript preparation. While not the primary architect of the study, Yousef's contributions were instrumental in organizing and managing data, ensuring the smooth progress of the research. V. Rajmohan served as a senior advisor and mentor in the research. He provided guidance in the study's design and methodology, drawing on his extensive experience in the field. V. Rajmohan supervision ensured that the research adhered to rigorous academic standards and research protocols, making him a valuable senior author. Janjhyam Venkata Naga Ramesh contributed to the research by providing specialized expertise in a particular aspect of the study. Their role might have included offering insights on a specific methodology, conducting a critical review of certain sections, or contributing in a unique way that enhanced the overall quality and comprehensiveness of the research. All authors had approved the final version.

REFERENCES

[1] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: A comprehensive survey," *Electronics*, vol. 11, no. 1, 2022. doi: 10.3390/electronics11010016

[2] S. Mishra and A. K. Tyagi, "The role of machine learning techniques in internet of things-based cloud applications," *Artificial Intelligence-Based Internet of Things Systems*, pp. 105–135, 2022. doi: 10.1007/978-3-030-87059-1_4

[3] A. T. Atieh, "The next generation cloud technologies: A review on distributed cloud, fog and edge computing and their opportunities and challenges," *ResearchBerg Review of Science and Technology*, vol. 1, no. 1, 2021.

[4] E. E.-D. Hemdan and D. H. Manjaiah, "An efficient digital forensic model for cybercrimes investigation in cloud computing," *Multimed Tools Appl.*, vol. 80, no. 9, pp. 14255–14282, 2021. doi: 10.1007/s11042-020-10358-x

[5] R. Kumar, K. S. Kakade, M. Priscilla, and B. V. S. Krishna, "An effective digital forensic paradigm for cloud computing criminal investigation," *International Journal of Electronic Security and Digital Forensics*, vol. 15, no. 6, pp. 655–664, 2023. doi: 10.1504/IJESDF.2023.133966

[6] O. I. Abiodun, M. Alawida, A. E. Omolara, and A. Alabdulatif, "Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 10217–10245, 2022. doi: 10.1016/j.jksuci.2022.10.018

[7] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Digital forensics vs. anti-digital forensics: Techniques, limitations and recommendations," arXiv preprint, arXiv:2103.17028, 2021.

[8] C. Karagiannis and K. Vergidis, "Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal," *Information*, vol. 12, no. 5, 2021. doi: 10.3390/info12050181

[9] V. Prakash, A. Williams, L. Garg, P. Barik, and R. K. Dhanaraj, "Cloud-based framework for performing digital forensic investigations," *Int. J. Wireless Inf. Networks*, vol. 29, no. 4, pp. 419–441, 2022. doi: 10.1007/s10776-022-00560-z

[10] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations," *Internet of Things*, vol. 19, 2022. doi: 10.1016/j.iot.2022.100544

[11] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, and G. B. Wills, "Security, cybercrime and digital forensics for IoT," *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, pp. 551–577, 2020. doi: 10.1007/978-3-030-33596-0_22

[12] M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," *IJACSA*, vol. 10, no. 8, 2019. doi: 10.14569/IJACSA.2019.0100880

[13] S. Wu, W. Sun, Z. Ding, and S. Liu, "Cloud evidence tracing system: An integrated forensics investigation system for large-scale public cloud platform," *Forensic Science International: Digital Investigation*, vol. 41, 301391, 2022. doi: 10.1016/j.fsidi.2022.301391

[14] I. Ahmed and V. Roussev, "Analysis of cloud digital evidence," *Security, Privacy, and Digital Forensics in the Cloud*, pp. 301–319, 2019. doi: 10.1002/9781119053385.ch15

[15] V. Prakash, A. Williams, L. Garg, C. Savaglio, and S. Bawa, "Cloud and edge computing-based computer forensics: Challenges and open problems," *Electronics*, vol. 10, no. 11, 2021. doi: 10.3390/electronics10111229

[16] H. Akbar, M. Zubair, and M. S. Malik, "The security issues and challenges in cloud computing," *International Journal for Electronic Crime Investigation*, vol. 7, no. 1, 2023. doi: 10.54692/ijeci.2023.0701125

[17] A. M. Alenezi, "Digital and cloud forensic challenges," arXiv preprint, arXiv: 2305.03059, 2023.

[18] M. Saleem, M. R. Warsi, and S. Islam, "Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment," *Journal of Information Security and Applications*, vol. 72, 103389, 2023. doi: 10.1016/j.jisa.2022.103389

[19] S. M. Shinde and V. R. Gurrala, "Securing trustworthy evidence for robust forensic cloud-blockchain environment for immigration management with improved ECC encryption," *Expert Systems with Applications*, vol. 229, 120478, 2023. doi: 10.1016/j.eswa.2023.120478

[20] T. Sulthana and D. Pawar, "Digital forensic investigator for cloud computing environment," *Computer Communication, Networking and IoT*, vol. 197, pp. 53–61, 2021. doi: 10.1007/978-981-16-0980-0_6

[21] E. E.-D. Hemdan and D. H. Manjaiah, "Digital forensic approach for investigation of cybercrimes in private cloud environment," *Recent Findings in Intelligent Computing Techniques*, vol. 707, pp. 25–33, 2019. doi: 10.1007/978-981-10-8639-7_3

[22] P. R. Brandao, "Forensics and digital criminal investigation challenges in cloud computing and virtualization," *AJNC*, vol. 8, no. 1, 2019. doi: 10.11648/j.ajnc.20190801.13

[23] Z. Umar and E. Emmanuel, "A framework for digital forensic in joint heterogeneous cloud computing environment," *Journal of Future Internet*, vol. 3, no. 1, pp. 1–11, 2019. doi: 10.18488/journal.102.2019.31.1.11

[24] J. E. James, "An exploration in forensic evidence in a cloud computing environment," *IIS*, 2021. doi: 10.48009/2_iis_2021_264-274

[25] M. Pourvahab and G. Ekbatanifard, "Digital forensics architecture for evidence collection and provenance preservation in IAAS cloud environment using SDN and blockchain technology," *IEEE Access*, vol. 7, pp. 153349–153364, 2019. doi: 10.1109/ACCESS.2019.2946978

[26] B. Fakiha, "Enhancing cyber forensics with ai and machine learning: A study on automated threat analysis and classification," *International Journal of Safety & Security Engineering*, vol. 13, no. 4, 2023.

[27] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Science International: Digital Investigation*, vol. 48, 301675, 2024. doi: 10.1016/j.fsidi.2023.301675

[28] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, "MF-Ledger: Blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," *IEEE Access*, vol. 9, pp. 103637–103650, 2021. doi: 10.1109/ACCESS.2021.3099037

[29] Y. Xu, T. Bai, W. Yu, S. Chang, P. M. Atkinson, and P. Ghamisi, "AI security for geoscience and remote sensing: Challenges and future trends," *IEEE Geoscience and Remote Sensing Magazine*, vol. 11, no. 2, pp. 60–85, 2023. doi: 10.1109/MGRS.2023.3272825

[30] S. Gupta, M. V. Sharma, and D. P. Johri, "Artificial intelligence in forensic science," *International Research Journal of Engineering and Technology*, vol. 7, no. 5, 2020.

[31] Evidence detection in cloud forensics. [Online]. Available: https://www.kaggle.com/datasets/jaidalmotra/evidence-detection-in-cloud-forensics

[32] A. Alzaqebah, I. Aljarah, O. Al-Kadi, and R. Damaševičius, "A modified grey wolf optimization algorithm for an intrusion detection system," *Mathematics*, vol. 10, no. 6, 999, 2022. doi: 10.3390/math10060999

[33] M. E. Sigman, M. R. Williams, N. Thurn, and T. Wood, "Validation of ground truth fire debris classification by supervised machine learning," *Forensic Chemistry*, vol. 26, 100358, 2021. doi: 10.1016/j.forc.2021.100358

[34] G. Nandita and T. M. Chandra, "Malicious host detection and classification in cloud forensics with DNN and SFLO approaches," *Int. J. Syst. Assur. Eng. Manag*, 2021. doi: 10.1007/s13198-021-01168-x

[35] D. R. Rani and G. Geethakumari, "Secure data transmission and detection of anti-forensic attacks in cloud environment using MECC and DLMNN," *Computer Communications*, vol. 150, pp. 799–810, 2020. doi: 10.1016/j.comcom.2019.11.048