Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 8s (2025)

Integrated Framework for Data Security in Cloud Computing Using Deep Learning Techniques

[1]Gantela Prabhakar, [2]Bobba Basaveswara Rao, [3]Simhadri Mallikarjuna Rao

[1]Research Scholar, [2]Professor, [3]Assistant Professor

[1,2]Department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India

[3]Department of Information Technology, Vasireddy Venkatadri International Technological University,Nambur, Andhra Pradesh, India

Email: [1]gantelaprabhakar@gmail.com, [2]Bobbabrao62@gmail.com, [3]mallikarjun1254@gmail.com

Article History:

Received: *08-11-2024*

Revised:*23-12-2024*

Accepted*:08-01-2025*

Abstract:

Alongside the expansion of the digital economy, data centers have grown substantially in size and quantity. Data centers are becoming increasingly essential to the development of the economy and society. However, even a brief outage in a data center might have severely negative effects. Resolving this issue requires secure management of data centers' physical infrastructure. Defenses against different cyber threats are being developed for the Internet of Things (IoT) and Cyber Physical Systems (CPS). As malicious code becomes more prevalent, using cloud environments to find dangerous code might not be a viable approach in the future. Due to the growing inefficiency of traditional perimeter-based security models in today's cloud-centric and remote work contexts, we employed integrated deep learning techniques for cloud data security in this article. According on risk profiles and real-time behavior, the suggested Zero-Trust security framework continuously evaluates and modifies the trust levels for users, devices, and applications. Using an integrated framework, we employed User and Entity Behavior Analytics (UEBA), Risk Scoring, and Adaptive Authentication approaches. This enabled us to reach an accuracy of 85–90% in all areas of data security when compared to the conventional methods.

Keywords: Deep Learning methods, Cloud Data Security, User and Entity Behavior Analytics, Risk Scoring and Adaptive Authentication.

1. Introduction

The introduction of cloud computing has completely changed how we operate and ushered in a new era of remote work settings. Remote work is now a key component of contemporary company strategies, as recent global events have further expedited this paradigm shift. Because of their built-in scalability and flexibility, cloud technologies offer the fundamental infrastructure needed for remote teams to collaborate easily, access data and apps from any location, and ensure business continuity.

However, there are a number of issues that must be carefully considered in order to successfully deploy remote work in a cloud environment, including organizational culture, data protection, security, and employee well-being. The purpose of this study is to examine the various facets of cloud-based remote work settings, examining the opportunities and difficulties brought about by this changing environment.

A few disadvantages of not utilizing cloud computing's remote work environment include:

Limited Agility and Scalability: Conventional perimeter configurations necessitate a large initial hardware and infrastructure investment. This makes it more difficult to swiftly scale resources up or down to satisfy changing needs, which impedes company expansion and responsiveness to market shifts. The pay-as-you-go approach of cloud computing provides unmatched scalability.

Decreased Cost Efficiency: Upkeep of on-premises infrastructure entails significant recurring expenses, such as energy consumption, hardware and software maintenance, and it is possible to sustain the costs of dedicated IT personnel, cooling, and physical space.

Decreased Competitiveness: Businesses that only use on-premises infrastructure can find it difficult to stay up with rivals who take use of cloud computing's cost-effectiveness and adaptability.

Restricted availability of cutting-edge technology: Cloud service providers are always investing in the newest innovations, like artificial intelligence, machine learning, and big data analytics. Businesses risk missing out on these innovative tools and technology if they don't use cloud services.

Lost chances to be innovative: Infrastructure upkeep can divert attention from innovation and fundamental corporate operations. IT staff may now concentrate on strategic initiatives like creating new goods and services thanks to cloud computing.

Cloud computing environments are quickly running into a variety of problems with traditional perimeter-based security solutions. Some of the most recent problems with these models include the following:

Perimeter Boundary Erosion:

Decentralized cloud ecosystems include: Because cloud settings are dynamic and dispersed over numerous places and networks, the idea of a distinct, fixed border loses significance. When workloads are distributed among several cloud providers or migrate between public and private clouds, it can be challenging to define boundaries.

Utilizing mobile devices and working remotely: All users are assumed to be inside a well-defined perimeter (such as a corporate network) under traditional perimeter-based security. Due to the proliferation of mobile devices, remote work, and Bring Your Own Device (BYOD) policies, users now routinely access cloud resources outside of conventional networks.

Increased Complexity with Hybrid and Multi-cloud Deployments:

Adoption of numerous clouds: A lot of businesses currently combine private clouds, on-premises infrastructure, and several public cloud providers. Due to their inability to adequately cover all environments, traditional perimeter defenses like firewalls and VPNs leave holes in visibility and control.

Complicated security policies: Overseeing security policies on several cloud platforms adds to the level of complexity and may result in uneven security control implementation.

Zero-Trust Requirements

Need for Zero Trust: Conventional approaches of trusting internal traffic (inside the corporate network) are no longer adequate due to the premise that dangers can exist both inside and beyond the

perimeter. Perimeter-based security is becoming less successful in cloud environments due to the growing importance of zero-trust security models, which authenticate and verify every request independent of the user's location.

Lack of context in traditional models: Traditional security is less suited to the dynamic nature of cloud environments because it frequently neglects to continuously assess context, such as the user's device, location, or behavior.

Lack of Granular Control

Limited visibility and segmentation: While traditional perimeter security aims to stop unwanted exterior access, it is not as detailed in managing and keeping an eye on network activities or user behavior inside the cloud environment. In a perimeter-focused strategy, fine-grained controls like micro-segmentation—which can separate tasks and restrict lateral movement—are sometimes absent or impractical?

Application-layer security is lacking: While traditional security measures often concentrate on network-level defenses (such firewalls), contemporary cloud apps need more sophisticated controls at the application layer, such as encryption, identity and access management (IAM), and API security.

Dynamic and Elastic Nature of Cloud Resources

Resource scaling: Because cloud systems are so elastic, resources can be dynamically increased or decreased in response to demand. Because of this fluidity, it is challenging for conventional perimeter-based security approaches to monitor and manage resource access efficiently as it changes quickly.

Increased attack surfaces: There are more possible attack surfaces in cloud environments that are more dynamic and sophisticated. Cloud-based attacks and misconfigurations are outside the scope of traditional perimeter defenses.

2. Literature Survey

Cloud computing's explosive growth has completely changed how people and companies store, analyze, and retrieve data. The security of cloud data has emerged as one of the most important issues facing contemporary IT infrastructure due to the increasing dependence on cloud platforms for handling enormous volumes of sensitive data. Although firewalls, access control lists and encryption techniques are examples of traditional security concepts that have shown efficacy in specific situations, they frequently fall short in addressing the dynamic and constantly changing nature of cyber threats in cloud systems. Specifically, in a cloud-first world where users, devices, and data are dispersed across various places, perimeter-based security mechanisms—which are intended to safeguard network boundaries—are becoming less and less effective.

There is a greater need for creative, proactive security measures as cyber-attacks get more complex and varied. The use of Deep Learning (DL) techniques to improve cloud data security is one such tactic that has attracted a lot of interest. As a branch of machine learning (ML), deep learning entails teaching multi-layered neural networks to automatically identify and understand patterns in data. It is

especially well-suited for identifying sophisticated attack vectors, including insider threats, zero-day exploits, and data breaches, in cloud systems because of its capacity to analyze vast amounts of complicated and high-dimensional data.

The integration of deep learning models with cloud security frameworks has been the subject of an expanding amount of research, covering a range of security topics such as anomaly detection, intrusion detection, data encryption, access control, and privacy protection. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), for example, have been used for anomaly detection, making it possible to identify malicious activity in cloud-based systems in real time. To improve data encryption methods and guarantee the privacy of sensitive data in multi-tenant cloud systems, auto encoders and Generative Adversarial Networks (GANs) have been investigated. Furthermore, security policies have been dynamically optimized using Reinforcement Learning (RL), guaranteeing that the cloud architecture is resilient to new attacks. Additionally, by keeping the data decentralized and reducing the dangers of data exposure, Federated Learning (FL) provides a privacy-preserving method for training deep learning models. Despite the promising results of deep learning in cloud security, several challenges remain. These include data privacy concerns, especially in multi-cloud environments where data is stored and processed across various jurisdictions, and the computational complexity involved in training deep learning models on vast datasets. Furthermore, the interpretability of deep learning models—an area that remains an ongoing research challenge—is particularly crucial in security applications where understanding the reasoning behind a model's decision is critical for trust and compliance purposes.

Examining the development of cloud data security within the framework of deep learning methodologies is the goal of this literature review. We will examine some deep learning approaches that have been put forth to tackle the main security concerns in cloud systems, weigh their benefits and drawbacks, and draw attention to the current research obstacles and potential paths in this field. With this thorough analysis, the article aims to shed light on how deep learning may be used to improve cloud data security and aid in the development of more resilient, flexible, and intelligent cloud security systems.

Numerous applications in human life have effectively used machine learning and contemporary AI technology [1, 2]. A feed forward propagation Artificial Neural Network (ANN) model for cloud security was developed by the authors in [3], who also looked into the essential procedures for incorporating such models into cloud security plans. In [4], machine and deep learning techniques are used to examine cloud security challenges and numerous attacks, like as malware, phishing, credential stuffing, and others. Deep neural networks and quantum neural networks are two algorithm concepts that have been integrated into the ML concept in [5] to improve prediction and protection accuracy. In addition to helping to completely eliminate attacks, these suggested models also boost cloud users' financial growth and trust in cloud service providers (CSPs).

The advantages of a centralized storage system and decentralized storage methods like block chain are combined in the solution that the author from [6] suggested. Additionally, the suggested strategy promotes supply chain integrity globally, fosters trust, and protects against manipulation. Implementing sign language recognition (SLR) based on key point detection is the main goal of the project completed by the authors in [7]. Numerous machine learning algorithms, including k-nearest

neighbor, random forest, and support vector machine, are used to train the model A thorough dataset comprising system logs, network traffic statistics, and security alerts from multiple cloud environments was gathered by the authors in [8]. Normalization, augmentation, and feature extraction specific to multi-modal inputs were all part of the pre-processing. Network traffic features were studied by Convolutional Neural Networks (CNNs), while system and user behavior was investigated by Random Forest and Gradient Boosting techniques. The study suggests Internet of Things (IoT)-based monitoring for real-time data gathering and investigates the effects of network variables such as latency and bandwidth fluctuations on model performance. The automatic decision-making process during malevolent conduct is aided by the paper [9]. Both the secure and insecure datasets are included in the obtained dataset. The random forest classifier uses the features that were gathered as input. The random forest analyzes these features and yields information that influences the decision-making process. By increasing openness in the automatic decision-making processes, the integrated approach raises the accuracy of security threats. They offer confidence in the cloud platforms' security protocols. Secure data transmission is achieved by the combination of a random forest algorithm and deep learning.

Sensitive data selection and data security are the two primary phases of the strategy that the authors in [10] suggested. First, they used a deep learning method called SqueezeNet to isolate the sensitive data from the acquired data. The Rat optimization algorithm (ROA) is used to properly pick the hyper-parameters of SqueezeNet in order to enhance its performance. A lightweight transformation model (LWTM) is then used to encrypt the sensitive data. Lastly, the cloud is where the encrypted data is kept. In terms of both cipher size and execution time, the proposed algorithm offered better security than existing cloud computing standards, as demonstrated by the experimental findings. When reviewing the data, the suggested LWTM model in the paper produced an Average Processing Period of 1.53 and an Average Throughput (kb/s) of 190.08. In order to capture inherent characteristics of the email text and other features to be classified as phishing or non-phishing using three different data sets, the study from [11] proposed a detection model using machine learning techniques by splitting the dataset to train the detection model and validating the results using the test data. After comparing the results, they found that the most features used produced the most accurate and efficient results. For the applied data sets, the best ML algorithm accuracy for boosted decision trees was 0.88, 1.00, and 0.97 in that order.

3. Methodology

Remote Work Environment

The COVID-19 epidemic, which compelled businesses all over the world to quickly implement remote work models, has significantly hastened the change in the remote work environment in cloud computing. Platforms for cloud computing, which provide accessibility, scalability, and flexibility, are now essential to this change. Virtual desktop infrastructure (VDI) and cloud-based collaboration applications (like Microsoft Teams, Google Workspace, and Slack) enable staff members to access corporate resources, communicate, and work together efficiently from any place. The advantages of cloud computing, such as cost savings, increased productivity, and the capacity to accommodate varied, dispersed workforces, have been brought to light by this shift. Additionally, cloud

environments make it easier for distant personnel to maintain business continuity by providing seamless access to enterprise apps, data storage, and computational resources.

The authors of [12] looked at how the COVID-19 pandemic affected remote work and how cloud computing was improving its ability to accommodate distant work configurations. The writers talk about cloud-based cyber security tactics and threats for remote teams. By examining the connections between remote and hybrid working and worker well-being and work-life balance, leader-member exchange (LMX), knowledge exchange, workforce inclusion, learning effectiveness, sustainable career development, and employee voice and choice in shaping work practices, this special edition adds to a significant and expanding research agenda on the subject.

Concerns around data protection and the requirement for new information technology skills are only two of the potential challenges that could result from the extensive usage of cloud computing, according to [13]. In addition, the paper explores these challenges in detail and offers solutions. This viewpoint clarified how, in the wake of COVID-19, cloud computing technologies has the potential to significantly alter the norms for remote labor in the public sector. The article in [14] explains how cloud computing technology can change the norms for remote labor in the public sector after COVID-19. It looks at the main advantages of cloud computing, including lower IT costs, more agility, and improved security, which make it a desirable choice for public sector companies trying to change the way they do distant work. Along with discussing the main advantages of cloud computing and its possible drawbacks, including data privacy issues and the requirement for new IT skills, the paper also suggests ways to overcome these obstacles.

Traditional Perimeter based Security

But the move to remote work has also brought up a number of operational and security issues. In cloud-based settings, where employees access resources from several locations and devices, traditional security models—which were created for on-premise environments with distinct network perimeters—are less effective. Organizations must have strong security measures in place, such as identity and access management (IAM), multi-factor authentication (MFA), and strong encryption, due to the rise in cyber threats like malware, phishing attacks, and data breaches. Furthermore, the absence of in-person interactions in distant work environments might affect communication and team chemistry. Research on boosting security, improving user experience, and creating new models for hybrid work environments—which combine in-office and remote work—has become more and more important as businesses continue to rely on cloud technologies. As a result, cutting-edge cloud security solutions like AI-based threat detection systems and Zero Trust architecture have emerged. These are essential for preserving the integrity of cloud infrastructures in the context of remote work.

The authors of [15] provide a thorough framework for protecting privacy and security while also outlining some of the concerns associated with cloud computing. They talked about the development of a number of technologies, including searchable encryption (SE), hierarchical encryption, fine-grain, multi-authority proxy re-encryption (PRE), cipher text policy attribute-based encryption (CP-ABE), key policy attribute-based encryption (KP-ABE), and access control. After summarizing a variety of technologies, they compared and examined the traits and range of applications of common schemes.

The fundamentals of Zero Trust Architecture (ZTA), such as secure communication, micro-segmentation, least privilege access, robust identification and access control, and ongoing monitoring, were studied by the authors of [16]. It explores how ZTA is used in platform engineering, emphasizing its advantages, which include better security, increased compliance, resistance to threats, flexibility in changing contexts, and visibility. The difficulties of putting ZTA into practice are also covered in the essay, including its complexity, possible performance issues, user experience issues, financial ramifications, and vendor lock-in risk. The article illustrates how ZTA tackles important security issues in contemporary cloud environments by analyzing industry trends, adoption rates, and measurable advantages. In the end, this helps enterprises to develop more robust, compliant, and flexible platforms in the face of changing cyber threats.

Secure Software-defined perimeters (SDP), a sophisticated development of the SDP architecture intended to improve scalability and strengthen security for every network component, were introduced by authors from [17]. SecureSDP is notable for its smooth integration into a wide range of organizational structures and for providing a strong and all-encompassing security solution that fortifies the network's defenses at every level. Thorough experimental evaluations show SecureSDP's exceptional performance in enhancing network security and scalability, demonstrating its significant breakthrough. In particular, SecureSDP significantly improved the hardening scores for the SDP controller in Lynis (65%), Chef Inspec (78%), and OpenSCAP (30%).

Deep Learning Techniques for Cloud Data Security

Cloud computing's User and Entity Behavior Analytics (UEBA), Risk Scoring, and Adaptive Authentication have all showed significant promise thanks to deep learning approaches. Deep learning models, which employ complex algorithms, can improve cloud system security by identifying unusual activity, calculating risk based on user activity patterns, and instantly modifying authentication procedures. A synopsis of the deep learning methods applied in each of these fields is provided below, along with noteworthy study findings:

User and Entity Behavior Analytics (UEBA) with Deep Learning

In order to identify departures from the usual, UEBA monitors and analyzes user and entity behavior. Unusual access patterns, repeated unsuccessful login attempts, or using resources outside of regular business hours are examples of anomalies that could point to a security risk.

Deep Learning Techniques Applied:

- ***Autoencoders (AEs)****:* The typical patterns of user and entity behavior are learned using these unsupervised models. To find anomalies, they then contrast this learnt "normal" profile with incoming user behavior data.

Results: By reconstructing user activity logs, autoencoders have been demonstrated to successfully identify abnormalities in user behavior. The reconstruction error rises when a user's behavior departs from the pattern they have learned, indicating that the behavior is abnormal. An autoencoder was able to detect anomalous login activity in one investigation with a detection accuracy of up to 90%.

- ***Recurrent Neural Networks (RNNs) and Long Short-Term Memory Networks (LSTMs)***: When examining time-series data, such the order of user actions or API requests, these models are

especially helpful. LSTMs are particularly good at identifying deviations in sequential data and modeling long-term dependencies.

Results: By recording temporal patterns, LSTM models can simulate consecutive user behaviors, increasing the accuracy of anomaly identification. A study using LSTM-based UEBA, for instance, demonstrated a 15% increase in detection accuracy over conventional statistical techniques (such as clustering-based approaches).

- ***Graph Neural Networks (GNNs)****:* GNNs have been used to simulate UEBA because it frequently involves relationships between numerous entities (e.g., people interacting with systems, devices, and apps). In order to identify coordinated attacks or insider threats, GNNs identify intricate relationships in data.

Results: In comparison to more conventional techniques like decision trees, a GNN-based UEBA system showed up to 95% detection accuracy in recognizing complex attack patterns, including insider attacks and lateral movement within a network.

Risk Scoring with Deep Learning

In cloud security, risk scoring is assessing the possibility of a security breach by looking at how users or entities behave. By examining past data and current behavior patterns, deep learning can be utilized to continuously modify and improve risk assessments.

Deep Learning Techniques Applied:

- ***Deep Autoencoders for Anomaly Scoring****:* Normal behavior profiles can be rebuilt by autoencoders, and the reconstruction error can be used to calculate an anomaly score. The risk score can then be instantly updated using this error.

Results: Autoencoders were employed to track user behavior constantly and generate a risk score based on the departure from typical behavior. In one deployment, more accurate risk evaluations resulted from a 20% decrease in the false positive rate when compared to simpler statistical models.

- ***Multilayer Perceptron (MLP) Networks****:* Users or behaviors can be categorized into risk categories (e.g., low, medium, high) using MLP networks, a sort of feed forward neural network. To calculate the risk score, these algorithms make advantage of attributes including past behavior, user credentials, and contextual information (such as IP addresses and geo location).

Results: An MLP network was used in a study to forecast user risk scores; in comparison to conventional risk scoring models, the system's classification accuracy increased by 15% to 20%.

- ***Recurrent Neural Networks (RNNs) for Dynamic Risk Scoring****:* Time-series data, such login attempts or access logs, can be handled by RNNs, which can then be trained to dynamically update risk scores in response to current user activity.

Results: An RNN-based method demonstrated the capacity to monitor user activity over time and forecast possible security threats, providing a 25% increase in predictive accuracy for users who pose a high risk.

Adaptive Authentication with Deep Learning

In cloud systems, adaptive authentication seeks to adjust authentication specifications (such multi-factor authentication) according to the perceived risk of a user's actions. Adaptively strengthening or weakening authentication measures in response to shifting patterns of behavior is made possible by deep learning.

Deep Learning Techniques Applied:

- ***Context-Aware Authentication with CNNs****:* Contextual data, including user location, device kind, and access time, has been analyzed using convolutional neural networks (CNNs). CNNs are able to identify contextual patterns and decide whether to initiate further authentication procedures.

Results: By taking into account contextual aspects that prior systems ignored, a CNN-based adaptive authentication system was demonstrated to minimize the number of false authentication failures by 30%.

- ***Behavioral Biometrics with LSTM Networks****:* Typing habits, mouse motions, and touch gestures are examples of behavioral biometrics that can be modeled using LSTM networks. When abnormal activity is identified, adaptive authentication systems may initiate extra security checks based on this behavior.

Results: By utilizing LSTM networks for behavioral biometrics in adaptive authentication, a system was able to differentiate between authorized users and impersonators with a 98% accuracy rate, greatly enhancing security while reducing user friction.

- ***Reinforcement Learning (RL) for Adaptive Authentication****:* Based on behavior data and real-time risk rankings, RL is able to dynamically modify authentication processes. Based on the risk score linked to the user's current session, the RL agent can select among a variety of authentication options (password, biometrics, multi-factor authentication, etc.).

Results: Adaptive authentication using an reinforcement learning model improved system responsiveness overall and reduced the number of needless authentication prompts by 40%, improving user experience without sacrificing security.

Integrated Frameworks Combining UEBA, Risk Scoring, and Adaptive Authentication

Recent developments in cloud security have concentrated on combining risk scoring, adaptive authentication, and UEBA into a single, deep learning-powered framework. In order to improve threat detection and response capabilities and overcome the limitations mentioned above, the research work in [18] suggests a unique paradigm for UEBA. To create baseline behaviors, identify anomalies, and rank reaction actions, the framework combines threat intelligence, behavioral analytics methods, and sophisticated machine learning algorithms. The framework's essential elements include risk scoring, behavioral analytics, incident detection and response procedures, and user and entity profiling. In user and entity profiling, thorough profiles are made for individuals and network entities (such as devices and apps), noting pertinent characteristics and past actions. These profiles are used by behavioral analytics to spot departures from typical patterns of behavior, which

may indicate security issues. Prioritizing response efforts is made possible by risk scoring, which rates the severity of anomalies found according to their likelihood and possible impact.

The writers in [19] comprehended the various methods utilized in User and Entity Behavior Analytics (UEBA), including as role-based and user-based detection, mapping of user and entity activity, user profile methods, and individual risk score computations. They also emphasized the open-source community's continued lack of progress in providing a comprehensive UEBA solution.

The authors of the research [20] described how they used a Machine Learning algorithm based on specific parameters to anticipate fraudulent users by applying big data analytics to application-layer logs. A list of IP addresses or user identification tokens (UIT) derived from real-time data that would be engaging in malicious conduct or are suspected of malicious activity based on their browsing behavior would be presented by machine learning.

Deep Learning Techniques Applied:

- ***End-to-End Neural Networks***: Researchers have suggested end-to-end frameworks that can offer a comprehensive security solution by combining several deep learning approaches (e.g., CNNs for adaptive authentication, MLPs for risk scoring, and autoencoders for anomaly detection).

Results: By integrating UEBA, risk scoring, and adaptive authentication, an integrated deep learning model was able to reduce authentication difficulties for authorized users while achieving 85–90% accuracy in identifying all facets of security incidents.

- ***Multi-Task Learning****:* The risk score and the proper authentication level can be predicted simultaneously by multi-task learning models, allowing security measures to be modified without requiring further calculations.

Results: By combining UEBA, risk scoring, and adaptive authentication, a multi-task learning strategy was able to lower computing overhead and boost detection effectiveness, resulting in increased accuracy and quicker reaction times.

4. Results And Discussions

Cloud computing's UEBA, Risk Scoring, and Adaptive Authentication have greatly benefited from deep learning algorithms, which provide pronounced gains in accuracy, efficiency, and real-time flexibility over conventional approaches. Among the main outcomes are:

• Better behavior modeling and anomaly detection with autoencoders, LSTMs, and RNNs.

• More accurate and dynamic risk scoring using deep learning models, with MLPs and RNNs outperforming more conventional methods in terms of accuracy.

• Improved adaptive authentication systems that make use of CNNs, LSTMs, and reinforcement learning, leading to systems that are safer and easier to use. As cloud environments continue to evolve, the integration of these deep learning techniques promises to provide stronger, more adaptive security frameworks.

The deep learning methods used for cloud computing's User and Entity Behavior Analytics (UEBA), Risk Scoring, and Adaptive Authentication are compiled in Table 1 below, along with the corresponding outcomes:

Table 1: Deep Learning Methods applied and the results obtained

Area of Research work	Deep Learning Techniques	Results Obtained from the Study
User and Entity Behavior Analytics (UEBA)	Auto encoders (AEs)	Reconstruction error-based abnormal login activity detection with up to 90% accuracy.
	Recurrent Neural Networks (RNNs) / LSTMs	15% increase in anomaly detection accuracy compared to conventional statistical techniques.
	Graph Neural Networks (GNNs)	95% detection accuracy for intricate attack patterns, including insider threats and lateral moves.
Risk Scoring	Autoencoders (AEs)	20% lower false positive rate in risk rating when compared to conventional statistical models.
	Multilayer Perceptron's (MLPs)	Accuracy of risk classification (low, medium, and high risk) increased by 15% to 20%.
	Recurrent Neural Networks (RNNs)	Predictive accuracy for identifying high-risk users has increased by 25%.
Adaptive Authentication	Context-Aware Authentication with CNNs	Taking contextual information (e.g., location, device) into account reduces false authentication failures by 30%.
	Behavioral Biometrics with LSTMs	98% precision in differentiating between authentic users and counterfeiters.
	Reinforcement Learning (RL)	User experience is improved by a 40% decrease in pointless authentication prompts.
Proposed - Integrated Framework (UEBA, Risk Scoring, and Adaptive Authentication)	End-to-End Neural Networks	Using adaptive authentication, risk assessment, and integrated UEBA, detection accuracy ranges from 85 to 90%.
	Multi-Task Learning	Reduced processing burden and increased accuracy and response times.

5. Conclusion

The findings from our investigation are as follows:

• UEBA: With accuracy gains ranging from 15% to 95% over conventional techniques, deep learning models—in particular, Autoencoders, RNNs, and LSTMs—have demonstrated remarkable effectiveness in anomaly identification and behavior analysis.

• Risk Scoring: With increases in predicting accuracy and fewer false positives, deep learning models such as MLPs and Autoencoders aid in the creation of dynamic, real-time risk scores.

• Adaptive Authentication: Cloud systems may adjust authentication settings in real-time depending on risk assessments thanks to CNNs, LSTMs, and Reinforcement Learning. This improves security and user experience while improving accuracy by up to 98%.

These findings show that by automating threat detection, risk assessment, and authentication, deep learning approaches greatly improve cloud environments' security, flexibility, and user experience.

References

[1] Al-Zubi, S., Aqel, D., Lafi, M.: "An intelligent system for blood donation process optimization-smart techniques for minimizing blood wastages". Clust. Comput. 2022, 1–11, (2022). https://doi.org/10.1007/s10586-022-03594-3.

[2] Aqel, D., Al-Zubi, S., Mughaid, A., Jararweh, Y. "Extreme learning machine for plant diseases classification: a sustainable approach for smart agriculture". Clust. Comput. 2021, 1–14 (2021). https://doi.org/10.1007/s10586-021-03397-y.

[3] Lumbardha Hasimi, Dimitrios Zavantis, Elhadi Shakshuki, Ansar YasarAuthors, "Cloud Computing Security and Deep Learning: An ANN approach", Procedia Computer Science-April, 2024, Volume 231, Issue C, Pages 40 – 47, https://doi.org/10.1016/j.procs.2023.12.155.

[4] N. Srikanth and T. Prem Jacob, "An Real Time Cloud Security System and Issues comparison using Machine and Deep Learning," *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*,2021, pp. 523-529, https://doi: https://doi.org/10.1109/I-SMAC52330.2021.9640650.

[5] M. Hindka, "Optimization Accuracy of Secured Cloud Systems Using Deep Learning Model," 2024 4th International Conference on Intelligent Technologies (CONIT), 2024, pp. 1-5, doi: https://doi.org/10.1109/CONIT61985.2024.10627032.

[6] S. K. S R, P. R. P. S K and T. Prem Jacob, "Blockchain-Enabled Supply Chain Management for Authenticating Products using QR with Firebase Integration," 2024 International Conference on Inventive Computation Technologies (ICICT), 2024, pp. 1552-1555, doi: https://doi.org/10.1109/ICICT60155.2024.10544991.

[7] E. S. M, S. Christopher S and T. Prem Jacob, "Exploring Sign Language Recognition using Convolutional Neural Network," 2024 International Conference on Inventive Computation Technologies (ICICT), 2024, pp. 831-834, doi: https://doi.org/10.1109/ICICT60155.2024.10544895.

[8] K. Mala and H. S. Annapurna, "Innovative Approaches for Enhanced Security in Cloud Network Traffic: An Adaptive Deep Learning Framework," 2024 First International Conference on Software, Systems and Information Technology (SSITCON), 2024, pp. 1-7, doi: https://doi.org/10.1109/SSITCON62437.2024.10796467.

[9] R. Bhavya, M. G. V. Kumar, U. M. Ramya, R. Janagi, M. Ganesan and S. Deepa, "Recognition of Secure Data Transmission in Cloud Platform using Deep Learning," 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2024, pp. 754-759, doi: https://doi.org/10.1109/ICAAIC60222.2024.10575038.

[10] K V K, C., Lokeswara Reddy, V. "A novel deep learning technique with cryptographic transformation for enhancing data security in cloud environments". Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-18903-8 .

[11] Mughaid, A., AlZu'bi, S., Hnaif, A. et al. "An intelligent cyber security phishing detection system using deep learning techniques". Cluster Comput 25, 3819–3828 (2022). https://doi.org/10.1007/s10586-022-03604-4.

[12] Gifford, J. (2022). "Remote working: unprecedented increase and a developing research agenda". Human Resource Development International, Volume 25 issue 2, Pp. 105–113. https://doi.org/10.1080/13678868.2022.2049108.

[13] Dr. Radha Raman Chandan "Cloud Computing and the Future of Remote Work", May 2023 Iconic Research and Engineering Journals, Volume 6 Issue 11, ISSN: 2456-8880.

[14] Joshua Ratna Kishore Petla, "Cloud Computing Technologies Transforming Public Sector Remote Work Standards Post Covid-19", International Journal of Creative Research Thoughts (IJCRT), ISSN: 2320-2882, Volume.11, Issue 4, pp.b944-b952, April 2023, doi: https://www.ijcrt.org/papers/IJCRT2304.

[15] PanJun Sun, “Security and privacy protection in cloud computing: Discussions and challenges”, Journal of Network and Computer Applications, Volume 160, 2020. doi: https://doi.org/10.1016/j.jnca.2020.102642.

[16] Hari Yerramsetty, “Zero Trust Architecture in Cloud Computing: A Paradigm Shift in Platform Engineering Security”, International Journal for Multidisciplinary Research (IJFMR), Volume 6, Issue 6, November-December 2024.

[17] Paya, A., Vicente-García & Gómez, A. “SecureSDP: a novel software-defined perimeter implementation for enhanced network security and scalability”. Int. J. Inf. Secur. 23, 2793–2808 (2024).doi: https://doi.org/10.1007/s10207-024-00863-7.

[18] Garima Sharma, Ambika Thakur, Chetna Tiwari. “Developing a Comprehensive Framework for User and Entity Behavior Analytics (UEBA): Integrating Advanced Machine Learning and Contextual Insights”, Journal of Communication Engineering & Systems (JOCES), 2024; 14(02):20-32. https://journals.stmjournals.com/joces/article=2024/view=152530

[19] S. Khaliq, Z. U. Abideen Tariq and A. Masood, "Role of User and Entity Behavior Analytics in Detecting Insider Attacks," 2020 International Conference on Cyber Warfare and Security (ICCWS), 2020, pp. 1-6, doi: https://doi.org/10.1109/ICCWS48432.2020.9292394.

[20] Rohit Ranjana, Shashi Shekhar Kumar, “User behavior analysis using data analytics and machine learning to predict malicious user versus legitimate user”, High-Confidence Computing, Volume 2, Issue 1, 2022, 100034, https://doi.org/10.1016/j.hcc.2021.100034.