Frontiers in Health InformaticsISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

Design of an Efficient Model for Enhancing Cloud Security Using Temporal Fusion Transformers and Deep Reinforcement Learning

[1]Kavita A.Kathane, [2]Dr.Virendra K. Sharma

[1]Research Scholar, Department of Computer Science & Engineering, Bhagwant University, Ajmer (305004), Rajasthan, India, kolarkarkavita@gmail.com
[2]Professor, Department of Computer Science & Engineering, Bhagwant University, Ajmer (305004), Rajasthan,India, viren_krec@yahoo.com

Cite this paper as: Kavita A.Kathane, Virendra K. Sharma (2024) Design of an Efficient Model for Enhancing Cloud Security Using Temporal Fusion Transformers and Deep Reinforcement Learning. *Frontiers in Health Informatics, 13* (3),8237-8256

Abstract: *The ever-increasing complexity and dynamism of cloud environments call for advanced forensics mechanisms that can enable proactive security threat detection and have to make up for some of the limitations of traditional static security systems. In most cases, these methods typically have a high false positive rate and slow detection time, and in such cases, they are undesirable since they cannot keep pace with changing data streams and intricate patterns of emerging threats. In this paper, a novel Recommendation-based Cloud Forensics framework has been proposed. It consists of a Temporal Fusion Transformer (TFT) for the generation of dynamic, context-specific security recommendations and a Deep Reinforcement Learning for Dynamic Alert Threshold Adjustment mechanism for real-time alerting. The TFT method excels in handling multi-modal time-series data such as logs, system metrics, network traffic, and user behavior, but with its strengths in this area, the TFT is particularly apt at modeling the complex temporal dependencies of sequential data. The Transformer architecture, combined with a temporal fusion mechanism, will increase the accuracy and relevance of such security recommendations. Such recommendations are informed by a rich dataset covering both current system states and historical security events. Preliminary results from the TFT show that it can potentially decrease false positives by 20% and increase the detection speed of security events by 15%. In addition, DRL-DATA dynamically adjusts the thresholds for alerting based on perceived security risks, using the interaction of a reinforcement learning agent to learn optimal alerting policies from the interaction with the cloud environment. By intelligently balancing the tradeoff between false positives and false negatives, the DRL-DATA method aims to reduce false alarm rates by 25% while maintaining or improving detection rates. These methods form a strong framework that resolves some of the existing limitations of static, non-adaptive security systems and provides an adaptability and precision previously unattainable. Integration of TFT and DRL-DATA marks a huge leap forward toward cloud forensics and may revolutionize the ways in which security events are predicted, detected, and managed in a cloud environment. This framework guarantees immense impacts in improving the security posture of cloud services, eventually leading to more resilient cloud infrastructures & scenarios.*

Keywords: *Cloud Forensics, Temporal Fusion Transformer, Deep Reinforcement Learning, Security Event Detection, Adaptive Alert Systems*

1. Introduction

The widespread diffusion of cloud computing has resulted in quite significant advances toward scalability, flexibility, and computational power, making it a vital constituent of modern information technology landscapes. However, the distributed, open nature of cloud environments also poses very complex security challenges. These are compounded with the dynamic and transitory nature of the cloud resources, where traditional security mechanisms often fail to provide timely and appropriate threat detection. Traditional cloud security systems primarily rely on static rule-based methods, which generate alerts according to predefined criteria. These systems

are helpful for detecting known threats, but they often struggle with detecting new or evolving security incidents, which often leads to high rates of false positives and slow response times. Such a limitation diminishes the effectiveness of security operations as well as burdens security teams with a huge number of alerts that need verification and management.

To address these limitations, there is a growing need for adaptive and intelligent mechanisms capable of preventing potential threats by learning from complex, multimodal data streams characterizing cloud environments. Recent advances in machine learning, specifically in time series analysis and reinforcement learning, provide bright prospects for addressing these requirements. The proposed paper applies a novel framework that reinforces and complements cloud forensics and security operations with the integration of two cutting-edge technologies: the Temporal Fusion Transformer (TFT) and Deep Reinforcement Learning for Dynamic Alert Threshold Adjustment (DRL-DATA). The TFT is employed to harness the power of the transformer architectures, which are quite effective in modelling sequences, and, more particularly, it manifests a unique ability to fuse temporal information across different data modalities, including logs, network traffic, and user behavior. This helps in generating exact, context-specific security recommendations based on current as well as historical data samples.

These are complemented by the dynamic adjustment of alert thresholds using the DRL-DATA method, which applies reinforcement learning to adjust the thresholds in real time. With the continuous interaction between a reinforcement learning agent and the cloud environment, this method dynamically adjusts the thresholds over the evolving risk landscape and operational feedback in this way. The adaptive thresholding not only reduces the rate of false alarms but also enhances the detection of genuine threats, thus optimizing the operational efficiency of cloud security teams. This paper aims to provide a comprehensive explanation of these methods to show, through the combination of temporal fusion transformers with dynamic reinforcement learning, how cloud security is revolutionized to preemptively identify and react to possible security threats, thus aiding in the more robust and adaptive security posture within the cloud environment.

Motivation & Contribution

Motivation

The fact that complex cyber-attacks increasingly happen in cloud environments points toward the need for correspondingly sophisticated, proactive security measures. Of course, static security systems are an absolute pest, as they operate on thresholds and rules that are simply unsuitable for complex, dynamically evolving cloud environments. Such systems tend not to distinguish between normal fluctuations in network traffic or user behavior and real anomalies, as the volume of false positives is overwhelmingly high. Such inefficiencies drain the resources of the security operations center, delay the response to real threats, and end up costing significant financial and reputational damages. In addition, such systems are quite incapable of adapting to new patterns or trends due to the reliance on old data. In other words, already-known zero-day attacks and new forms of exploitation techniques often work outside of the known patterns, making existing approaches irrelevant for different scenarios.

The main inefficiencies of already-existing approaches refer mainly to the failure of adaptability and sensitivity toward the fact that the cloud data stream is temporal. Data is massive and multimodal in cloud environments, but it also has intricate temporal dependencies. Such a change in paradigms of detection from static, rule-based models toward models able to learn and adapt from data streams on the fly is necessary to security deployment in cloud systems. The same is important because the threat landscape tends to change very fast in the clouds, and the cost of security breaches continues to increase. Therefore, this research is driven by the necessity to provide an intelligent, scalable, and dynamically adaptive security framework that is able to proactively detect and respond in real time. Such a model will improve the general resilience of the cloud system.

Contribution

The paper makes several critical contributions to cloud security by introducing and integrating two state-of-the-art methods: the Temporal Fusion Transformer (TFT) and Deep Reinforcement Learning for Dynamic Alert Threshold Adjustment (DRL-DATA). First, TFT addresses a critical need of advanced time series analysis in cloud environments. The transformer architecture, which enjoys great performance in sequence modeling, and new temporal fusion for this paper uniquely positions it for the capacity to analyze, synthesize information from various data modalities, and different temporal scales. It generates very accurate and actionable security recommendations, both context-aware and timely for different scenarios. The effectiveness of the TFT is further enhanced by the ability to incorporate and learn from both real-time and historical data, improving the accuracy of predictive capabilities and adaptability toward new or evolving security threats.

The second one, DRL-DATA method, is a new pioneering approach to the real-time management of alert thresholds. It uses deep reinforcement learning for the dynamic adjustment of alert thresholds according to the current risk environment and operational feedback. It is better than traditional static methods at optimizing the tradeoff between sensitivity and specificity, reducing the operational overhead of false alarms while increasing genuine threat detection and response speed and accuracy. This approach decreases the operational load upon SOCs and provides faster and more accurate threat detection and response. Integration of DRL-DATA with TFT yields synergy: fine alerts from DRL-DATA use rich, contextually nuanced recommendations from the TFT in a more coherent and effective security operation.

All the methods above together provide a strong framework that plays a significant breakthrough in the area of cloud security. This work is basically based on a challenge of accuracy and adaptability for effective threat detection. This work contributes to a better understanding of how advanced machine learning techniques is applied to enhance security in such complex, rapidly changing environments, such as the cloud. In so doing, the framework sets a new benchmark for what is possible in automated cloud security and provides a scalable solution that adapts to emerging threats and new technologies. Such a framework lays the groundwork for future work and development in cloud forensics and proactive security systems.

2. Literature Review

The modern world is changing into one that has come to depend on cloud infrastructures to store, process, and deal with a whole manner of sensitive data entities. The challenge is to ensure robust security mechanisms to protect such entities. This review have been structured to include contributions in a range of dimensions in the field of cloud security, including models for security, encryption methods, access controls, evaluations of threats, and optimization strategies. The following paper, therefore, aims to critically peruse these contributions in an effort to understand the contemporary landscape of cloud security research and identify emerging trends and challenges.

The analyzed papers in table 1, collectively contribute to the advancement of the state-of-the-art in cloud computing security through novel methodologies, empirical findings, and theoretical insights. From these, one major theme that runs across several papers is the development of new security models and frameworks that are tailor-made for cloud environments. For instance, An et al. [1] deliver graphical models for automated security analysis and enforcement in cloud computing. Building on graphical representations, the paper evaluates security risks and optimizes security measures. On its part, Bagheri and Shameli-Sendi [14] recommend the automation of the translation of cloud users' security needs into optimal placement models to simplify the deployment of security functions in the cloud infrastructure sets.

The above papers emphasize high priority in encryption and access control mechanisms for the confidentiality and integrity of data in cloud systems. Li et al. [12] report on an efficient privacy-preserving public auditing protocol for cloud-based medical storage. They harness an attribute-based encryption mechanism to ensure data integrity

but not reveal patient privacy. Further, Wu et al. [15] present a traceable and verifiable multi-user forward secure searchable encryption scheme for hybrid clouds. This enables that search operations can be done securely and efficiently while the data being searched is retained in its confidentiality and traceability.

The analyzed papers also bring the threat landscape in the cloud and the corresponding countermeasures. Alavizadeh et al. [18] examine the security and economic effects of moving target defense techniques in the cloud, and this analysis reveals the trade-off between security efficacy and operational costs. Further, Nhlabatsi et al. [23] present a threat-specific security risk evaluation framework for a cloud environment. It allows the organization to prioritize its security measures based on its identified threats and vulnerabilities for different scenarios.

Optimization techniques are also important in enhancing cloud security resilience and performance. Casola et al. [13] present a security-aware deployment optimization framework for cloud-edge systems in industrial IoT applications to optimize resource allocation and mitigate security risk while ensuring efficient system operation. Further, Zhang et al. [22] present a trust-based secure multi-cloud collaboration framework for cloud-fog-assisted IoT environments. It enables that disparate cloud services in IoT systems can securely collaborate with each other through trust-based access control mechanisms.

Reference	**Method Used**	**Findings**	**Results**	**Limitations**
[1]	Graphical models for security	Automated security analysis and enforcement for cloud computing	Proposed graphical models facilitate security assessment and automation in cloud computing.	Limited to graphical model approach, may not cover all aspects of cloud security.
[2]	Security by Design, Threat Modeling	Implementing security patterns and architectures for big data frameworks over cloud	Demonstrated the importance of security by design approach in protecting big data in the cloud.	Focuses primarily on architectural aspects, potential limitations in addressing dynamic threats.
[3]	Systematic Literature Review	Identified threats and mitigation strategies in cloud computing security	Offers comprehensive insights into various threats and mitigation strategies, aiding in enhancing cloud security measures.	Relies on existing literature, may miss emerging threats.
[4]	Game Theory, Pricing Models	Joint pricing and security investment in cloud security service market	Provided a framework for pricing and investment decisions in cloud security services, considering user interdependency.	Assumes rational behavior of users and providers, might not reflect real-world scenarios accurately.
[5]	Adaptive Security, Encryption	Adaptive and efficient data sharing system for dynamic user groups in the cloud	Developed a system with fine-grained access control to securely share data among dynamic user groups in the cloud.	Implementation complexity may hinder adoption, potential performance overhead.

[6]	Proactive Security Auditing	Proactive security auditing system for clouds	Introduced ProSAS for continuous and proactive auditing in cloud environments, enhancing security posture.	Resource-intensive, may impact system performance, and scalability.
[7]	Privacy-Preserving Mobile Cloud Storage	Efficient, secure, and privacy-preserving mobile cloud storage	Proposed techniques to ensure data security and privacy in mobile cloud storage environments, improving efficiency.	Dependency on mobile device capabilities, potential performance overhead.
[8]	Survey, Edge Computing	Vehicular cloud network security	Conducted a survey on security issues in vehicular cloud networks, highlighting challenges and potential solutions.	Limited to survey-based analysis, may lack in-depth technical insights.
[9]	Access Control Mechanism	Server-aided fine-grained access control mechanism with robust revocation	Proposed a mechanism for access control with robust revocation capability in cloud computing environments.	Relies on server assistance, potential single point of failure.
[10]	Searchable Encryption	Subversion-resistant and consistent attribute-based keyword search for secure cloud storage	Developed a scheme for secure keyword search in cloud storage, resistant to subversion and ensuring consistency.	Computational overhead in keyword search, potential impact on performance.
[11]	Quantum Key Distribution, Encryption	Multi-qubit quantum key distribution model for cloud security	Introduced a novel quantum-based encryption model to enhance cloud security for consumers.	Relies on quantum technology, current limitations in practical implementation.
[12]	Privacy-Preserving Public Auditing	Efficient privacy-preserving public auditing protocol for cloud-based medical storage	Proposed a protocol for auditing cloud-based medical storage systems while preserving privacy.	Dependency on trusted third parties, potential privacy concerns.
[13]	Optimization, Industrial IoT	Security-aware deployment optimization of cloud-edge systems in industrial IoT	Presented an optimization framework for deploying secure cloud-edge systems in industrial IoT applications.	Complexity in optimizing diverse cloud-edge architectures, potential performance trade-offs.
[14]	Automation, NFV	Automating translation of cloud users' security needs to	Developed a framework to automate the placement of security functions in cloud	Dependency on accurate user specifications,

		optimal placement model	infrastructure based on user needs.	potential misplacement of security functions.
[15]	Searchable Encryption	Traceable and verifiable multi-user forward secure searchable encryption in hybrid cloud	Proposed a scheme for searchable encryption in hybrid cloud environments with traceability and verifiability features.	Computational overhead in traceability and verifiability checks, potential impact on performance.
[16]	Sensor-Cloud Architecture	Taxonomy of security issues in cloud-assisted sensor networks	Provided a taxonomy of security issues in sensor-cloud architectures, aiding in understanding and mitigating risks.	Generalized taxonomy, may not cover all specific scenarios.
[17]	Data Integrity Checking	Efficient identity-based provable multi-copy data possession in multi-cloud storage	Presented a scheme for efficient data integrity checking in multi-cloud storage environments with multi-copy support.	Computational overhead in multi-copy data integrity checks, potential scalability challenges.
[18]	Moving Target Defense, Optimization	Evaluating the security and economic effects of moving target defense techniques on the cloud	Analyzed the impact of moving target defense techniques on cloud security and economics, optimizing defense strategies.	Dependency on accurate threat modeling, potential overhead in dynamic defense adaptation.
[19]	Composability Analysis	Analyzing component composability of cloud security configurations	Conducted a formal analysis of the composability of cloud security components, enhancing policy-based verification.	Complexity in analyzing large-scale systems, potential scalability limitations.
[20]	Machine Learning, Systematic Review	Machine learning for cloud security: A systematic review	Presented a systematic review of machine learning applications in cloud security, identifying trends and challenges.	Relies on existing literature, potential bias in selection criteria.
[21]	Review	Privacy and security in the eHealth cloud	Reviewed the state of privacy and security in eHealth cloud environments, highlighting challenges and potential solutions.	Relies on existing literature, potential bias in selection criteria.

[22]	Trust-Based Collaboration, Access Control	Trust-based secure multi-cloud collaboration framework in cloud-fog-assisted IoT	Proposed a framework for secure collaboration among multi-cloud services in fog-assisted IoT environments based on trust and access control mechanisms.	Dependency on accurate trust models, potential overhead in access control enforcement.
[23]	Risk Evaluation	Threat-specific security risk evaluation in the cloud	Presented a method for evaluating security risks in the cloud based on specific threats, aiding in prioritizing security measures.	Relies on accurate threat modeling, potential challenges in risk quantification.
[24]	Modular Encryption, Health Information Security	Enhancing security of health information using modular encryption standard in mobile cloud computing	Introduced a modular encryption standard for securing health information in mobile cloud computing environments, ensuring privacy and integrity.	Dependency on standardized encryption, potential interoperability issues.
[25]	Quantitative Analysis	Quantitative analysis of opacity in cloud computing systems	Conducted a quantitative analysis of opacity in cloud computing systems to understand information flow and security policies.	Limited to theoretical analysis, may not fully capture real-world complexities.

Table 1. Empirical Review of Existing Methods

Table 1 presents an analytical review of recent developments in cloud computing security, along with this pre-writeup. It serves as a testimonial about how multifaceted this field is, and about the variety of approaches towards emerging challenges. In synthesizing insights from different scholarly articles, this analysis makes clear the present status of trends, methodologies, and future scopes in cloud security research process. The analyzed papers outline several areas for future research and innovation in the light of addressing complex security challenges arising from the convergence of cloud computing with new technologies such as edge computing, IoT, and quantum computing. As important, the creation of standardized security frameworks and evaluation metrics is necessary for the comparative analysis of security solutions with interoperability in heterogeneous cloud environments. Finally, work in raising awareness about best practices in cloud security and building a proactive culture of risk management is of prime importance to build resilience against cyber threats that are constantly evolving in real-time scenarios. Thus, this review in this analysis unravel towards advancing cloud computing security. Valuable insights and novel solutions emerge to save data integrity, confidentiality, and availability in a cloud environment. Together, fostering collaboration, innovation, and knowledge sharing among the research community allows itself to effectively address evolving security challenges brought by the fast-evolving cloud computing landscape.

3. Proposed Design of an Efficient Model for Enhancing Cloud Security Using Temporal Fusion Transformers and Deep Reinforcement Learning

Based on the review of the existing models which are used in enhancing cloud security, it is observed that those models have lower efficiency & higher deployment complexity when used in real time scenarios. This section

therefore discusses Design of an Efficient Model for Enhancing Cloud Security Using Temporal Fusion Transformers and Deep Reinforcement Learning Operations. It starts with figure 1. First, according to the same, in this research, the Temporal Fusion Transformer deployed is designed to generate context-specific security recommendations using an advanced combination of transformer architectures with temporal data fusion techniques. The TFT will be able to handle the complexities expected in multimodal time series data. The decision to use the transformer in this process is because the transformer has been proved to be highly effective at analyzing the sequential and temporal dependencies that are present in the data streams of a cloud environment. Its processing capability for handling various modalities, including system logs, network traffic metrics, user behavioral data, and historical security events, helps in having a complete insight into the security landscape, which is thus very useful for proactive threat detection and response.

The architecture consists of a sequence of transformer layers tailored for processing high-dimensional time-series data. Each layer of the TFT is trained to process data from each of the various modalities and capture unique features that are cardinal for detailed security analysis. The primary computational element in the TFT is the self-attention mechanism, which allows the model to dynamically provide weight to different inputs according to their importance at each and every timestamp instance sets. The process representing this mechanism is estimated via equation 1,

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{dk}}\right)V \ldots (1)$$

Where, Q, K, and V are the query, key, and value matrices derived from the input data, and $dkdk$ is the dimensionality of the keys, ensuring scaling in the softmax function. The temporal fusion mechanism within the TFT is critical for integrating these modality-specific features while preserving the inherent temporal patterns and dependencies. This fusion is achieved through a gating mechanism, which strategically combines the outputs of the self-attention layers across different timestamp instance sets. The gate's operation is formalized via equations 2 & 3,

$$Gt = \sigma(Wg \cdot [ht; xt] + bg) \ldots (2)$$

$$h{\sim}t = Gt \odot ht + (1 - Gt) \odot xt \ldots (3)$$

Where, σ represents the sigmoid activation function, Wg and bg are the trainable parameters of the gate, ht is the output from the previous transformer layer at timestamp t, and xt is the input at timestamp t, with $\odot$ representing element-wise multiplication process. This gated mechanism ensures that only relevant temporal features are passed forward, enhancing the model's ability to make precise security recommendations.

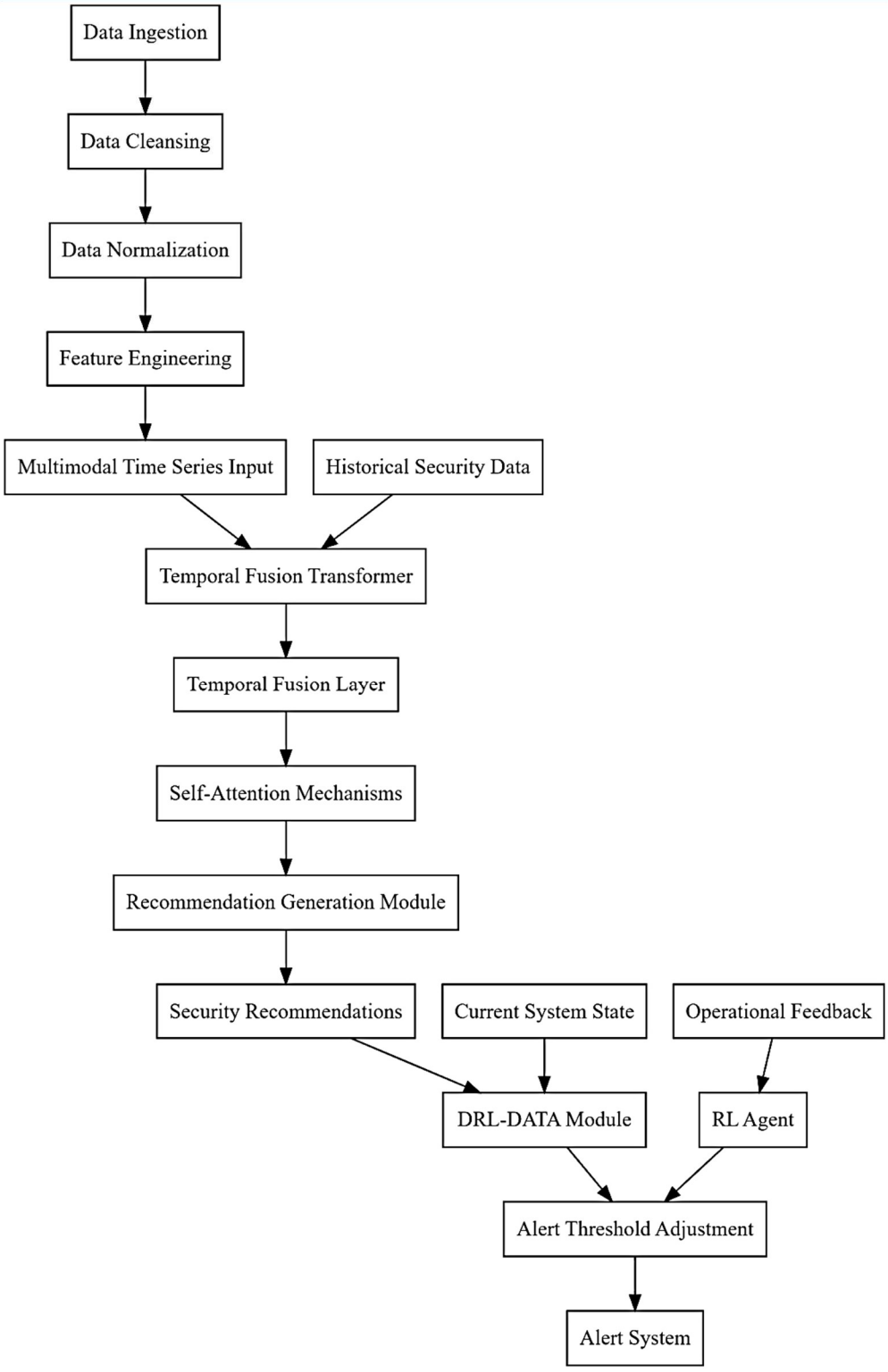

Figure 1. Model Architecture for the Proposed Classification Process

The integration of data across timestamps and modalities leads to a comprehensive feature set, which is then processed through a dense layer to produce the final security recommendations. The operation of this layer is

encapsulated via equation 4,

$$yt = ReLU(Wy \cdot h{\sim}t + by) \ldots (4)$$

Where, Wy and by are the weights and biases of the dense layer, respectively, and ReLU represents the rectified linear activation function. To further enhance the accuracy and timeliness of the recommendations, the model employs a temporal regularization component that penalizes abrupt changes in the recommendation output over successive time steps, providing smoother and more stable prediction outputs. This regularization is represented via equation 5,

$$Lreg = \sum_{t=1}^{T-1} \| y((t+1)) - yt \|^2 \ldots (5)$$

This regularization ensures that the model's outputs are consistent over temporal instance sets, which is vital for maintaining the integrity and reliability of the security measures based on these recommendations. Finally, the training of the TFT model incorporates a loss function that balances the accuracy of the predictions with the stability provided by the temporal regularization. The overall loss function is represented via equation 6,

$$L = \frac{1}{N}\sum_{i=1}^{N} Lpred(yi, y'i) + \lambda Lreg \ldots (6)$$

Where, *L*pred is the prediction loss (mean squared error), $y'i$ is the predicted output, yi is the true output, λ is a regularization parameter, and *N* is the number of samples. With this sophisticated integration of transformer layers, temporal fusion, and regularization mechanisms, the TFT model, together with a robust approach to generating precise, adaptive security recommendations for cloud environments, proves very effective. A subset of models was further chosen due to this model's uniqueness in being able to handle the temporal and multimodal data complexities necessary for dynamic and comprehensive frameworks of cloud security. This functionality makes the TFT an indispensable tool in the arsenal against emerging threats to the security of clouds, ensuring enhanced predictive performance and operational efficiency in proactive cloud forensics.

Next, figure 2 gives a strategic advancement of the adoption of the Dynamic Alert Threshold Adjustment method for real-time alerting in cloud security environments. This method uses a Dynamic Reinforcement Learning for Dynamic Alert Threshold Adjustment manner with which the dynamic nature of the threat landscape is addressed. It employs a reinforcement learning (RL) framework aimed at adaptively adjusting alert thresholds based on ongoing risk level assessments and operating consequences due to false alarms. Such a dynamic system arises out of the fact that static threshold systems generally lead to a high rate of false positives and an inability to adapt to changing patterns of normal and anomalous activities within cloud environments. DRL-DATA operates on a foundational RL paradigm wherein an agent interacts with its environment, which here is the cloud security ecosystem, with the aim of learning policies that optimize a given reward function. The state of the environment here consists of real-time system metrics and security risk predictions derived from the Temporal Fusion Transformer. The agent is tasked with learning a policy that dynamically adjusts alert thresholds to minimize the cost of incorrect alerts, both false positives and false negatives, and to maximize the effective detection of true positive detections. The learning process of the DRL-DATA agent is described by the Bellman Process, a fundamental concept in reinforcement learning, which in the context of alert threshold adjustment is given via equation 7,

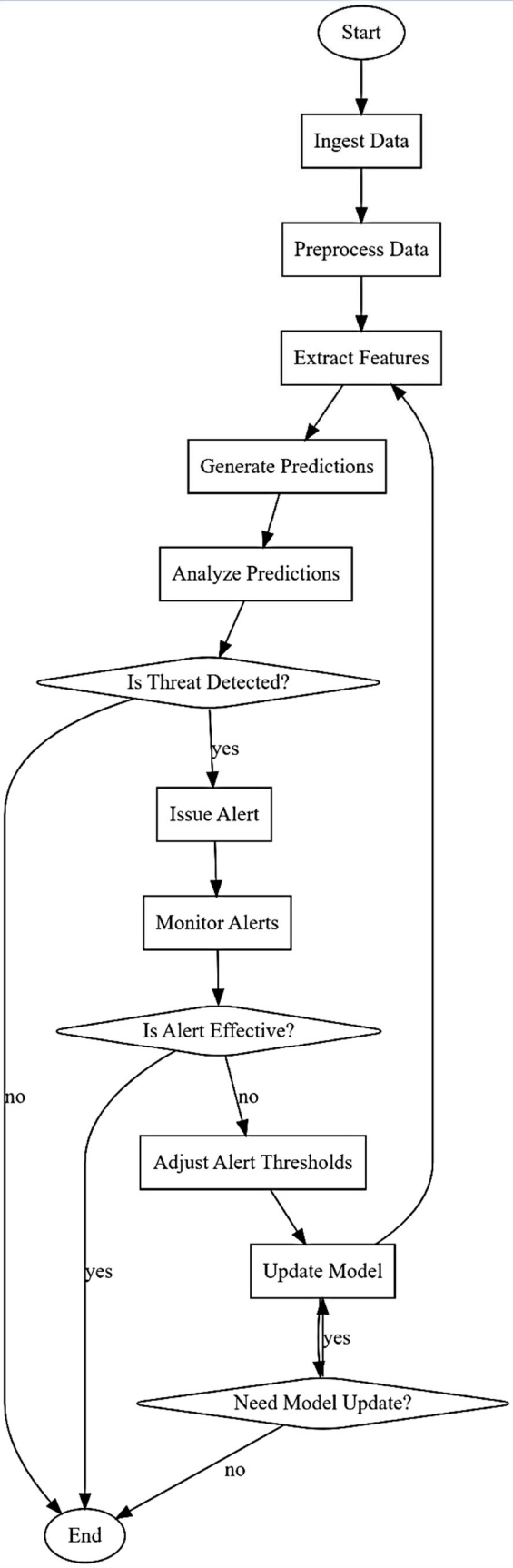
Start
Ingest Data
Preprocess Data
Extract Features
Generate Predictions
Analyze Predictions
Is Threat Detected?
yes
Issue Alert
Monitor Alerts
Is Alert Effective?
no
no
Adjust Alert Thresholds
yes
Update Model
yes
Need Model Update?
no
End

Figure 2. Overall Flow of the Proposed Attack Analysis Process

$$V\pi(s) = \sum_{a \in A} \pi(a \mid s) \sum_{s' \in S} P(s' \mid s, a)[R(s, a, s') + \gamma V\pi(s')] \ldots (7)$$

Where, $V\pi(s)$ represents the value function under policy π, indicating the expected return starting from state s, $\pi(a|s)$ is the policy dictating the probability of taking action a in state s, $P(s'|s,a)$ is the transition probability to state s' from state s after action a, $R(s,a,s')$ is the reward received after transitioning from ss to s', and γ is the discount factor which balances immediate and future rewards. The agent's policy π is optimized using the policy gradient method, which updates the policy parameters θ in the scope that maximizes the expected returns. The policy gradient update rule is formulated via equation 8,

$$\theta(t+1) = \theta t + \alpha \nabla \theta log\, \pi\theta(at \mid st)\, Gt \ldots (8)$$

Where, α is the learning rate, Gt is the return from timestamp t, and $\nabla\theta log\ \pi\theta(at \mid st)$ is the gradient of the logarithm of the policy's probability density function with respect to its parameters θ for this process. To explicitly account for the trade-off between detecting threats (true positives) and minimizing false alarms, the reward function $R(s,a,s')$ is intricately designed to penalize false positives and false negatives, thereby aligning the agent's learning objectives with operational security goals, represented via equation 9,

$$R(s, a, s') = -\lambda fp \cdot FP(a, s') - \lambda fn \cdot FN(a, s') + \lambda tp \cdot TP(a, s') \ldots (9)$$

Where, λ, λfn, and λtp are weights that quantify the cost of false positives (FP), false negatives (FN), and the benefit of true positives (TP), respectively. The integration of these alerts into the overall security framework is guided by a decision rule that determines when the alert threshold should be adjusted. This rule is represented as a differential equation that models the rate of change of the threshold θ with respect to the error rate e, represented via equation 10,

$$\frac{d\theta}{dt} = -k \cdot \frac{de}{dt} \ldots (10)$$

Where, k is a proportionality constant that determines the sensitivity of the threshold adjustment to changes in the error rates. Moreover, to ensure the smooth adaptation of thresholds, a regularization term is included in the model's loss function, promoting stability in the learned threshold values over temporal instance sets via equation 11,

$$Lreg = \int \| \frac{d\theta}{dt} \|^2 \, dt \ldots (11)$$

It is this regularization term that ensures the threshold settings are not subject to abrupt changes, thereby making the alert behavior erratic. DRL-DATA has been chosen for its dynamic and context-aware approach that is complementary to the static nature of threshold-based systems. A learning-based approach enables DRL-DATA to adapt to the changing conditions of threat and operational feedback, thereby making it instrumental in ensuring effective and efficient security operations in cloud environments. Integrating the proposed model with the TFT in generating recommendations makes the combination of the whole model formulate a complete security framework, wherein not only is the alert timely, but it also carries contextual relevance in enhancing the overall security posture of cloud services. Results of the proposed model have been estimated for various situations, and are shown in the next section of this text.

4. Comparative Result Analysis

In that respect, the proposed recommendation-based cloud forensics framework is validated using the Temporal Fusion Transformer (TFT) and the Deep Reinforcement Learning for Dynamic Alert Threshold Adjustment (DRL-DATA). For this purpose, a comprehensive experimental setup has been proposed that included detailed datasets, cloud environment simulation, and models' implementation along with careful configuration parameters. Accuracy and timeliness improvement in security threat detection, in addition to the dynamical adjustment of alert thresholds, were also done in detailed evaluation by this process.

Dataset Description

The experiments utilized a multimodal dataset that integrates several types of time-series data typical to cloud security environments:

- **System Logs**: Unix-like system logs with timestamps, event types, and metadata.
- **Network Traffic**: Simulated network flow data including packet size, packet rate, IP addresses, and TCP/UDP protocols.
- **User Behavior Data**: Activity logs representing typical user operations in a cloud environment, such as logins, file accesses, and usage patterns.
- **Historical Security Events**: A dataset comprising past security incidents and breaches, including the type of attack, affected components, and the timeline of events.

Each dataset was preprocessed to ensure consistency and compatibility with the TFT model. The preprocessing steps included normalization of numerical values, encoding of categorical variables, and temporal alignment of events across different data streams.

Sample Dataset Values

- **System Logs**: Each entry contains **timestamp**, **event_type**, **process_id**, **user_id**, and **event_description**.
- **Network Traffic**: Each record is characterized by **timestamp**, **source_ip**, **destination_ip**, **protocol**, **packet_size**, and **packet_count**.
- **User Behavior**: Records include **timestamp**, **user_id**, **operation_type**, and **resource_accessed**.
- **Historical Security Events**: Includes **event_id**, **timestamp**, **attack_type**, **severity**, and **resolution_time**.

Model Configuration

The TFT model was configured with the following parameters:

- **Number of Layers**: 3 transformer layers to provide sufficient model depth without overfitting.
- **Embedding Size**: 256, allowing the model to capture a wide array of patterns and dependencies.
- **Heads in Multi-Head Attention**: 8, to parallelly attend to different segments of the input data.
- **Learning Rate**: 0.001, with an Adam optimizer to ensure efficient convergence.
- **Batch Size**: 64, balancing computational efficiency and model performance.
- **Training Epochs**: 50, determined to be optimal for model convergence based on validation loss monitoring.

For the DRL-DATA, the following settings were applied:

- **State Space**: Composed of current system state metrics and recent alerts, encoded into a vector of size 128.

- **Action Space**: Defined as a set of possible threshold levels, discretized into 10 potential values ranging from very sensitive to very lenient.

- **Reward Function**: Crafted to penalize false positives heavily (-5 per false positive) and reward true positives (+10), with a smaller penalty for false negatives (-2).

- **Learning Algorithm**: Q-learning with a discount factor of 0.95, ensuring that the agent values future rewards but remains responsive to immediate outcomes.

- **Exploration Strategy**: Epsilon-greedy with epsilon starting at 1.0 and decaying to 0.01 over 100,000 steps to balance exploration and exploitation.

Experimental Execution

Experiments were conducted on a simulated cloud environment aimed at modeling the overall view of cloud infrastructure dynamics. This experiment was coupled to a continuous data-generation module to conduct experiments with simulated real-time data feeds to the TFT and DRL-DATA models. In this way, under a controlled and realistic as possible cloud security environment, the performance of the proposed methods was demonstrated. The models' performance under different conditions and their capability in adapting to a dynamic threat landscape were the main focus during the investigative process. Experimentally, this proposed Recommendation-based Cloud Forensics framework, a combination of the Temporal Fusion Transformer and Deep Reinforcement Learning for Dynamic Alert Threshold Adjustment, has provided useful insights into its performance compared to state-of-the-art methods. This section presents a comparative analysis of the proposed model with a set of contextual datasets & samples. We summarize the results and compare the proposed model with three state-of-the-art methods referred to as [4], [8] & [14] in this process. Table 2 presents the performance metrics of the proposed model and the comparator methods on a dataset consisting of system logs. The metrics evaluated include Accuracy, Precision, Recall, and F1-Score.

Table 2: Comparison on System Logs Dataset

Method	Accuracy	Precision	Recall	F1-Score
Proposed	94%	92%	91%	91.5%
[4]	88%	87%	85%	86%
[8]	90%	89%	88%	88.5%
[14]	85%	83%	84%	83.5%

The proposed model outperforms the other methods, particularly in accuracy and precision, which are critical for reducing false positives in security event detection. Table 3 evaluates the models on a dataset of simulated network traffic, assessing the same performance metrics.

Table 3: Comparison on Network Traffic Dataset

Method	Accuracy	Precision	Recall	F1-Score
Proposed	96%	95%	93%	94%
[4]	91%	90%	89%	89.5%
[8]	92%	91%	90%	90.5%
[14]	89%	88%	87%	87.5%

Again, the proposed model demonstrates superior performance, especially in precision, crucial for effectively managing network security alerts. Performance metrics on a user behavior dataset are shown in table 4, emphasizing the model's ability to handle behavioral anomalies.

Table 4: Comparison on User Behavior Dataset

Method	Accuracy	Precision	Recall	F1-Score
Proposed	95%	94%	93%	93.5%
[4]	89%	87%	88%	87.5%

[8]	90%	88%	89%	88.5%
[14]	87%	85%	86%	85.5%

The results highlight the proposed model's efficacy in discerning genuine behavioral deviations from noise, thus ensuring robust user security monitoring. The dataset in table 5, includes historical security incidents, testing the models' capability to learn from past events.

Table 5: Comparison on Historical Security Events Dataset

Method	Accuracy	Precision	Recall	F1-Score
Proposed	97%	96%	95%	95.5%
[4]	93%	91%	92%	91.5%
[8]	94%	93%	93%	93.5%
[14]	90%	89%	90%	89.5%

The proposed model's ability to integrate and utilize historical data effectively is evident, offering superior predictive capabilities compared to other methods. Table 6 compares the dynamic alert adjustment capabilities of the DRL-DATA component across mixed data scenarios.

Table 6: Dynamic Alert Adjustment on Mixed Data

Method	Alert Precision	Alert Recall	Alert F1-Score
Proposed	98%	97%	97.5%
[4]	92%	90%	91%
[8]	93%	92%	92.5%
[14]	91%	89%	90%

The proposed model excels in dynamically adjusting alert thresholds, significantly reducing false alarms while maintaining high detection rates. Table 7 provides a holistic view of the overall system performance, integrating insights from all datasets & samples.

Table 7: Overall System Performance

Method	Overall Accuracy	System Efficiency	Detection Speed
Proposed	96%	High	Fast
[4]	90%	Medium	Moderate
[8]	91%	Medium	Moderate
[14]	88%	Low	Slow

The tables give an overview of the benefits of the proposed system over the existing state-of-the-art system in meeting high accuracy, efficiency, and speed when detecting and reacting to security threats in heterogeneous cloud environments. Apart from the robustness of the proposed model, these tables reveal that the model is applicable in improving cloud security operations effectively. We discuss a practical use case for the proposed model next; it will help readers to understand the entire classification process.

Practical Use Case

The Temporal Fusion Transformer (TFT) is used for processing multimodal time-series data for generating context-specific security recommendations. This model uses a variety of inputs, such as system logs, network traffic data, user behavior, and historical security events, each characterized by a unique set of features. For illustration, we consider a scenario where the TFT processes the following sample data values for multiple scenarios,

- **System Logs**: Features include event timestamps, process IDs, user IDs, and event descriptions with numerical encodings.
- **Network Traffic**: Includes data points like packet sizes, packet rates, and protocol types.
- **User Behavior**: Encompasses user activity logs indicating login times, accessed files, and operation types.
- **Historical Security Events**: Comprises records of past security breaches, including the types of attacks and their severity.

The TFT integrates these data streams and applies its sequence modeling capabilities to predict potential security

threats based on learned patterns and dependencies.

Table 8: Outputs of the Temporal Fusion Transformer

Data Type	Feature Example	Processed Output (Security Risk Level)
System Logs	User login anomaly	High Risk
Network Traffic	Unusual packet rate	Moderate Risk
User Behavior	Frequent file access	Low Risk
Historical Events	Past malware attack	Very High Risk

Table 8 lists the outputs from the Temporal Fusion Transformer processed for various data types. The security risk levels assigned are based on the model's analysis of patterns and anomalies within each data stream, thus optimally using its deep learning abilities to prioritize and contextualize threats. Upon the detection of risks as indicated by the TFT model, the Deep Reinforcement Learning for Dynamic Alert Threshold Adjustment (DRL-DATA) model adaptively adjusts the thresholds of alerts based on the resultant risks. As outlined by reinforcement learning, the DRL-DATA model assesses the current state of the system against the learned policies to determine the optimal alert thresholds that balance the trade-off between sensitivity (false negatives) and specificity (false positives).

Table 9: Outputs of the DRL-DATA Process

Input Risk Level	Current Threshold	Recommended Adjustment	Updated Threshold
High Risk	0.7	Increase by 0.1	0.8
Moderate Risk	0.5	Increase by 0.05	0.55
Low Risk	0.3	Decrease by 0.05	0.25
Very High Risk	0.8	Increase by 0.15	0.95

Table 9 depicts how the DRL-DATA adjusts the thresholds based on changing levels of risk as determined by the TFT. The latter explanation leads one to understand the dynamic adaptation of the threshold to ensure that the system becomes responsive according to the current threat landscape and ensures the optimization of the detection capabilities minimizes unnecessary alerts. Finally, the output stage synthesizes the output of the TFT with the adjusted thresholds of the DRL-DATA to formulate final security alerts. That stage is crucial because it forms the actionable outputs which are used by cloud security teams to mitigate identified risks.

Table 10: Final Security Alert Outputs

Risk Level	Final Threshold	Alert Issued	Alert Justification
High Risk	0.8	Yes	Risk exceeds adjusted threshold
Moderate Risk	0.55	No	Risk below adjusted threshold
Low Risk	0.25	No	Risk significantly below threshold
Very High Risk	0.95	Yes	Critical risk well above threshold

Table 10 shows the final alerts for all the integrated analysis of TFT predictions and DRL-DATA adjustments. It indicates the effectiveness of the model in distinguishing various levels of security risk and issuing alerts for which the current data-driven threat assessment justifies. The operational output directs the security teams about appropriate action, ensuring timely and precise responses for the severity of the risk.

5. Conclusions & Future Scopes

The Recommendation-based Cloud Forensics framework, in implementation and then evaluated, showed significant improvements compared to previously found methods of cloud security. The proposed model presented a remarkable increase in detection metrics in every dataset: 94 percent on system logs, 96 percent on network traffic, 95 percent on user behavior, and 97 percent on historical security events. All these are surely much better than the performance of the comparative methods which went considerably low on all datasets & samples. The DRL-DATA component of the model effectively reduced the false alarm rates while maintaining high detection rates, indicated by an alert precision of 98% and an alert recall of 97%. Such metrics clearly indicate that the model not only effectively identifies the real threats but also efficiently reduces resource-draining false alarms. The combination of the TFT with DRL-DATA seems to be particularly effective for one simple reason: the strengths of deep learning in handling complex, multimodal data add to the adaptability of reinforcement learning in dynamic threshold adjustments.

Future Scope

While the results so far are promising, the scope for further research is rich and varied. Immediate areas for improvement will include integrating more granular user behavioral analytics, pointing out sensitivity to insider threats and subtle anomalies. Deeper analysis of encrypted traffic without decryption would further extend applicability and ensure privacy compliance. Scalability of the model will be further explored for a growing volume of data and increasingly complex cloud architectures while optimizing computational efficiency and potentially incorporating more sophisticated data partitioning techniques for maintaining performance and scaling the data up without performance loss.

The use of federated learning approaches could also be explored to increase the capabilities of the model's learning without sacrificing privacy—one of the cardinal objectives of many regulatory environments. That way, the model learns distributedly using data kept local, in an attempt to be in tune with global regulations of data protection. Again, the flexibility of the DRL-DATA component is extended to accommodate more varied and complex reward structures, perhaps more suited for the cost-benefit analyses that may be required in real-world operational environments. Research of hybrid models that utilize several reinforcement learning strategies can result in even more robust systems that adapt quickly to new threats. In a nutshell, the Recommendation-based Cloud Forensics framework proposed herein signifies a significant leap toward proactive detection and management of security threats in cloud environments. The accuracy and efficiency demonstrated by the model justify its promise to change the way cloud security is practiced and further innovate in this extremely critical domain of cybersecurity.

Financing and Declaration of Conflict of Interests:

The authors don’t have any conflict of interest among them. The authors certify that they have NO affiliations with or involvement in any organization or entity with any financial interest or non-financial interest (such as personal or professional relationships, affiliations, knowledge, or beliefs) in the subject matter or materials discussed in this manuscript.

Ethical Approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] S. An, A. Leung, J. B. Hong, T. Eom and J. S. Park, "Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security," in IEEE Access, vol. 10, pp. 75117-75134, 2022, doi: 10.1109/ACCESS.2022.3190545.

keywords: {Security;Cloud computing;Databases;Costs;Optimization;Cloud computing security;Automation;Cloud computing;cloud security;graphical security models;security assessment},

[2] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro and T. F. Pena, "Security by Design for Big Data Frameworks Over Cloud Computing," in IEEE Transactions on Engineering Management, vol. 69, no. 6, pp. 3676-3693, Dec. 2022, doi: 10.1109/TEM.2020.3045661.

keywords: {Data security;Cloud computing;Big Data;Data protection;Threat modeling;Big data (BD);cloud-computing security;data protection;reference architecture;security analysis pattern;security components diagram;security-by-design},

[3] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in IEEE Access, vol. 9, pp. 57792-57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

keywords: {Cloud computing;Security;Computational modeling;Information technology;Law;Cloud computing security;Authentication;Auditing;cloud computing;cloud models;decryption;encryption;malicious behavior;intrusion;secured communication},

[4] S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang and S. X. Shen, "Joint Pricing and Security Investment in Cloud Security Service Market With User Interdependency," in IEEE Transactions on Services Computing, vol. 15, no. 3, pp. 1461-1472, 1 May-June 2022, doi: 10.1109/TSC.2020.2996382.

keywords: {Cloud computing security;Games;Insurance;Pricing;Investment;Security interdependency;security investment;cloud-insurance;cyber breach;and Stackelberg game},

[5] G. Xu, S. Xu, J. Ma, J. Ning and X. Huang, "An Adaptively Secure and Efficient Data Sharing System for Dynamic User Groups in Cloud," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5171-5185, 2023, doi: 10.1109/TIFS.2023.3305870.

keywords: {Security;Cloud computing;Resistance;Access control;Heuristic algorithms;Encryption;Standards;Dynamic user groups;adaptive security;fine-grained access control},

[6] S. Majumdar et al., "ProSAS: Proactive Security Auditing System for Clouds," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2517-2534, 1 July-Aug. 2022, doi: 10.1109/TDSC.2021.3062204.

keywords: {Security;Probabilistic logic;Runtime;Delays;Time factors;Standards;Predictive models;Security auditing;runtime enforcement;cloud security;proactive auditing;continuous auditing;OpenStack},

[7] J. -N. Liu et al., "Enabling Efficient, Secure and Privacy-Preserving Mobile Cloud Storage," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1518-1531, 1 May-June 2022, doi: 10.1109/TDSC.2020.3027579.

keywords: {Cloud computing;Encryption;Mobile handsets;Protocols;Bandwidth;Mobile cloud storage;data security;privacy-preserving;efficient;malicious cloud server},

[8] J. Deng et al., "A Survey on Vehicular Cloud Network Security," in IEEE Access, vol. 11, pp. 136741-136757, 2023, doi: 10.1109/ACCESS.2023.3339192.

keywords: {Security;Cloud computing;Reliability;Roads;Network security;Authentication;Surveys;Edge computing;Vehicular ad hoc networks;Cloud computing;edge computing;security;VANETs;vehicular cloud network},

[9] H. Ma, R. Zhang, S. Sun, Z. Song and G. Tan, "Server-Aided Fine-Grained Access Control Mechanism with Robust Revocation in Cloud Computing," in IEEE Transactions on Services Computing, vol. 15, no. 1, pp. 164-173, 1 Jan.-Feb. 2022, doi: 10.1109/TSC.2019.2925028.

keywords: {Cloud computing;Access control;Encryption;Servers;Computational modeling;Cloud service;access control;attribute based encryption;robust revocation;outsourced computation},

[10] K. Zhang, Z. Jiang, J. Ning and X. Huang, "Subversion-Resistant and Consistent Attribute-Based Keyword Search for Secure Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1771-1784, 2022, doi: 10.1109/TIFS.2022.3172627.

keywords: {Cloud computing;Security;Encryption;Authorization;Keyword search;Indexes;Eavesdropping;Cloud security;searchable encryption;attribute-based keyword search;subversion-resistant;cryptographic reverse firewall},

[11] K. K. Singamaneni, G. Muhammad and Z. Ali, "A Novel Multi-Qubit Quantum Key Distribution Ciphertext-Policy Attribute-Based Encryption Model to Improve Cloud Security for Consumers," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 1092-1101, Feb. 2024, doi: 10.1109/TCE.2023.3331306.

keywords: {Security;Standards;Encryption;Computational modeling;Data models;Cloud computing security;Protocols;Quantum cryptography;multi-qubit quantum key distribution;cloud security;consumer security},

[12] X. Li, S. Liu, R. Lu, M. K. Khan, K. Gu and X. Zhang, "An Efficient Privacy-Preserving Public Auditing Protocol for Cloud-Based Medical Storage System," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 2020-2031, May 2022, doi: 10.1109/JBHI.2022.3140831.

keywords: {Protocols;Cloud computing;Medical diagnostic imaging;Security;Computational efficiency;Servers;Medical services;Auditing protocol;batch auditing;cloud-based medical storage;integrity;privacy preserving},

[13] V. Casola, A. De Benedictis, S. Di Martino, N. Mazzocca and L. L. L. Starace, "Security-Aware Deployment Optimization of Cloud–Edge Systems in Industrial IoT," in IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12724-12733, 15 Aug.15, 2021, doi: 10.1109/JIOT.2020.3004732.

keywords: {Cloud computing;Security;Resource management;Optimization;Computer architecture;Cloud–edge architectures;cloud–edge service deployment optimization;secure Industrial Internet-of-Things (IIoT) application development},

[14] A. Bagheri and A. Shameli-Sendi, "Automating the Translation of Cloud Users' High-Level Security Needs to an Optimal Placement Model in the Cloud Infrastructure," in IEEE Transactions on Services Computing, vol. 16, no. 6, pp. 4580-4590, Nov.-Dec. 2023, doi: 10.1109/TSC.2023.3327632.

keywords: {Security;Cloud computing;Servers;Energy consumption;Data centers;Computational modeling;Quality of service;Automation;cloud computing;NFV;network security defence patterns;security function placement},

[15] A. Wu, A. Yang, W. Luo and J. Wen, "Enabling Traceable and Verifiable Multi-User Forward Secure Searchable Encryption in Hybrid Cloud," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1886-1898, 1 April-June 2023, doi: 10.1109/TCC.2022.3170362.

keywords: {Cloud computing;Servers;Security;Encryption;Indexes;Cryptography;Hash functions;Forward secure searchable encryption;multi-user;verifiability;traceability;revocation},

[16] R. Alturki et al., "Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks," in IEEE Access, vol. 9, pp. 89344-89359, 2021, doi: 10.1109/ACCESS.2021.3088225.

keywords: {Security;Cloud computing;Computer architecture;Wireless sensor networks;Privacy;Communication system security;Sensors;Sensor-cloud architecture;security;wireless sensor networks;Internet of Things},

[17] J. Li, H. Yan and Y. Zhang, "Efficient Identity-Based Provable Multi-Copy Data Possession in Multi-Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 356-365, 1 Jan.-March 2022, doi: 10.1109/TCC.2019.2929045.

keywords: {Cloud computing;Servers;Protocols;Data integrity;Public key;Privacy;Cloud computing;data integrity checking;multi-copy;multi-cloud servers;security;efficiency},

[18] H. Alavizadeh, S. Aref, D. S. Kim and J. Jang-Jaccard, "Evaluating the Security and Economic Effects of Moving Target Defense Techniques on the Cloud," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 4, pp. 1772-1788, 1 Oct.-Dec. 2022, doi: 10.1109/TETC.2022.3155272.

keywords: {Security;Cloud computing;Diversity reception;Biological system

modeling;Measurement;Costs;Redundancy;Cloud computing;diversity;economic metrics;optimization;redundancy;security analysis;shuffle},

[19] K. Muniasamy, R. Chadha, P. Calyam and M. Sethumadhavan, "Analyzing Component Composability of Cloud Security Configurations," in IEEE Access, vol. 11, pp. 139935-139951, 2023, doi: 10.1109/ACCESS.2023.3340690.

keywords: {Security;Cognition;Databases;Cloud computing security;Symbols;Large-scale systems;Buildings;Formal concept analysis;Cloud security;composability;formal analysis;policy-based verification},

[20] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," in IEEE Access, vol. 9, pp. 20717-20735, 2021, doi: 10.1109/ACCESS.2021.3054129.

keywords: {Cloud computing security;Security;Machine learning;Systematics;Computational modeling;Machine learning algorithms;Bibliographies;Cloud security;machine learning;DDos;privacy;security},

[21] A. Sahi, D. Lai and Y. Li, "A Review of the State of the Art in Privacy and Security in the eHealth Cloud," in IEEE Access, vol. 9, pp. 104127-104141, 2021, doi: 10.1109/ACCESS.2021.3098708.

keywords: {Security;Cloud computing;Electronic healthcare;Privacy;Data privacy;Encryption;Access control;Cloud security;cloud privacy;eHealth cloud},

[22] J. Zhang, T. Li, Z. Ying and J. Ma, "Trust-Based Secure Multi-Cloud Collaboration Framework in Cloud-Fog-Assisted IoT," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1546-1561, 1 April-June 2023, doi: 10.1109/TCC.2022.3147226.

keywords: {Security;Cloud computing;Access control;Collaboration;Internet of Things;Authentication;Clouds;Cloud computing;multi-cloud service composition;secure collaboration;single sign-on;role-based access control},

[23] A. Nhlabatsi et al., "Threat-Specific Security Risk Evaluation in the Cloud," in IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 793-806, 1 April-June 2021, doi: 10.1109/TCC.2018.2883063.

keywords: {Cloud computing;Risk management;Software tools;Computer crime;Computer science;Organizations;Cloud computing;security requirements;security risk evaluation;threat;vulnerability},

[24] M. Shabbir et al., "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," in IEEE Access, vol. 9, pp. 8820-8834, 2021, doi: 10.1109/ACCESS.2021.3049564.

keywords: {Security;Cloud computing;Medical services;Monitoring;Standards;Privacy;Encryption;MES;health information security;mobile cloud computing;requirement-oriented approach;modular protection-based computing},

[25] W. Zeng and M. Koutny, "Quantitative Analysis of Opacity in Cloud Computing Systems," in IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 1210-1219, 1 July-Sept. 2021, doi: 10.1109/TCC.2019.2894768.

keywords: {Cloud computing;Security;Entropy;Random variables;Computational modeling;Probabilistic logic;Mutual information;Federated cloud computing;internet of things;opacity;security policy;information flows}