Journal of Information Systems Engineering and Management
2025, 10(18s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

SpinalSAENet: An Intelligent Intrusion Detection and Data Integrity Framework for Cloud Environments

N. Savitha[1], E. Saikiran[2]
[1] *Research Scholar, Chaitanya Deemed to be University, Hyderbad, India.*
[2] *Research Supervisor, Chaitanya Deemed to be University, Hyderbad, India.*

ARTICLE INFO

Received: 16 Dec 2024

Revised: 25 Jan 2025

Accepted: 10 Feb 2025

ABSTRACT

The swift growth of cloud computing has heightened cybersecurity vulnerabilities, demanding robust intrusion detection systems (IDS). Conventional IDS models face challenges, such as excessive false positives and limited flexibility. This study introduces Spinal Stacked AutoEncoder Net (SpinalSAENet), an innovative hybrid deep-learning-based IDS that merges SpinalNet and Deep Stacked AutoEncoders (DSAE) to enhance anomaly detection and data integrity verification. The system employs feature extraction and Chebyshev distance-based fusion to improve classification, while Principal Component Analysis (PCA) is utilised to reduce dimensionality, thereby increasing computational efficiency. When tested on the Bot-IoT dataset, SpinalSAENet demonstrated superior performance with 96.87% accuracy, 95.4% recall, 96.1% precision, and a 95.7% F1-score, surpassing Decision Trees, Random Forests, and Support Vector Machines. The incorporation of SHA-256 hashing and Merkle tree proofs ensures data integrity, offering a multitiered security approach. Its streamlined architecture and cloud-native scalability (Docker and Kubernetes) facilitate real-time deployment in cloud environments. This paper presents a highly precise and scalable IDS framework capable of real-time intrusion detection and data integrity verification. Subsequent research will investigate the resistance to adversarial attacks, explainable AI, and serverless deployment to further enhance cloud security.

Keywords: Cloud Security, Intrusion Detection System (IDS), SpinalNet, Deep Stacked AutoEncoders (DSAE), Hybrid Deep Learning, Anomaly Detection, Chebyshev Distance,Data Integrity Verification,Cloud-Native Deployment, Cybersecurity.

1.INTRODUCTION

Cloud computing has changed the landscape of data storage, processing, and access; thus, it has become an inevitable part of the modern technological ecosystem. Clouds allow for infinite scaling, flexibility, uptime, and low cost, enabling unimaginable volumes of data in the first place. However, this increased dependency on cloud-based systems brings with it serious security challenges. With the rise of advanced persistent threats and the increasing sophistication and prevalence of malware, ransomware attacks, Distributed Denial of Service (DDoS) attacks, and unauthorised access, intrigue threats have also become increasingly advanced and complicated to identify. The challenges above highlight the crucial demand for effective Intrusion Detection Systems (IDS) capable of addressing the nuances introduced by cloud infrastructures without compromising data integrity.

Traditional IDS methods, although suitable for static or localised domains, struggle to adapt to the dynamic, distributed landscape of cloud architectures. Static rule-based detection mechanisms can barely identify novel attack patterns and may fail to scale with staggering data volumes produced during real-time cloud manoeuvring. Moreover, such environments make it incredibly difficult to maintain data integrity, which is of course the basic need of any secure system. Disruption of that data, however, can result in catastrophic outcomes, such as financial loss, damage to reputation, and possible legal exposure.

To overcome these vital issues, this work presents a framework that combines data integrity verification and a hybrid deep learning-based intrusion detection system based on the cloud computing environment. At the heart of this promising framework is the SpinalNet architecture, from which this framework builds upon and incorporates highly utilised deep learning models, such as ResNet and VGG, to optimise detection performance and computational resource efficiency. SpinalNet is a novel structure which reduces redundancy and computational overhead while maintaining a high performance by optimising the flow of information with layers. Some of them have proposed the use of a hybrid detection system, which combines the advantages of a variety of models to obtain a strong and adaptive intrusion detection system.

The contributions of this study are significant in the domain of cloud computing security. Through the use of SpinalNet and other well-known deep learning architectures, the framework offers a solution that is both scalable and efficient, thus allowing for adaptation to the rapidly changing characteristics of the cloud environment. Advanced optimisation techniques, such as learning rate scheduling and momentum-based optimisers, refine the learning phase by allowing faster and more efficient convergence of the model to the desired output with minimal bias. Our work sets the stage for new progress in fully secure cloud computing, offering insight into the realisation of intelligent, adaptive, and explainable security measures in the future.

This research proposes a systematic framework with a combination of data integrity verification and a hybrid deep learning-based intrusion detection system specific to cloud computing environments to solve these problems. The SpinalNet architecture forms the basis of this framework, which is integrated with well-established deep learning models such as ResNet and VGG, aiming to improve both detection accuracy and computational efficiency. SpinalNet proposes a new multilayer structure which alleviates the information flow to remove unnecessary information and reduce the computational cost with little performance degradation. By combination, the hybrid method tries to utilise the advantages of two or multiple models to attain an effective and adaptive solution to identify intrusion tests.

2.LITERATURE REVIEW

In the realm of cloud security, Intrusion Detection Systems (IDS) play a crucial role. The fluid and decentralised nature of cloud computing presents distinct obstacles in maintaining robust security measures. Numerous research efforts have explored IDS frameworks, shedding light on the current limitations and potential areas for enhancement.

Talla and Manikyala (2021) proposed a multi-tier security framework that combines threat intelligence and machine learning classics to improve cloud IDS performance [1]. This approach reached an accuracy of 94.5%, showing the potential to be useful for real-time threat detection; however, it was not the optimal threshold that we had in mind for adoption in the community. Similarly, Samunnisa et al. (2023) introduced a hybrid clustering and classification intrusion detection system (IDS) model designed for distributed cloud-computing environments. Although it worked well for scalability, the method currently only achieved an accuracy of 93%, suggesting that there is still room for improvement when it comes to dealing with the complexities of multi-cloud systems.[2]

Using machine learning in a cloud system to detect penetrations through an anomaly-based IDS, Aldallal and Alisa (2021) has been able achieved an accuracy of 92% [3]. This finding highlights the difficult balance between high precision and low false-positive rates. Mohy-eddine et al. et al. (2023) proposed an intelligent IDS model that was tuned to correctly detect malicious activities with 94% accuracy and a minimum false negative rate of 0.0831% [4]. They highlighted that dimensionality reduction or advanced feature selection is required to enhance the sensitivity while maintaining the performance.

Bakro and Kumar (2024) developed a hybrid bio-inspired procedure for feature selection along with a random forest classifier [5]. Theirs was an innovative approach that, nevertheless, achieved only 95% accuracy, illustrating the difficulty in finding the balance between computational complexity and detection performance. Luo et al. A systematic review of IDS frameworks in cloud-based IoT settings was performed in (2022), which reported persistent challenges in minimising detection accuracy and latency, with the majority of frameworks achieving an accuracy below 96% [6].

Deep learning methods used for intrusion detection in cloud systems were presented by Aljuaid and Alshamrani (2024). Although they achieved 93% accuracy with their model, they struggled to prevent false positives due to changing cloud traffic patterns [7]. They achieved an accuracy of 90–95% through the hybrid modelling of FCM and

SVM (Jaber and Rehman, 2020) [8]. Nonetheless, their approach demanded considerable computing power, potentially introducing a practical limitation for resource-constrained environments.

Shamshirband et al. (2020) focused on computational intelligence techniques in mobile cloud environments, achieving detections up to 94%, but highlighted that adaptation to continuously changing environments remains an ongoing challenge [9]. A systematic review of IDS in fog environments was undertaken by Yi and Darbandi (2023), with most of the models achieving detection precision in the 90–95% range, highlighting the need to improve the recall and detection delay [10].

Bakro et al. (2023) introduced enhanced fusion feature selection methodologies for intrusion detection systems with 94% accuracy as well as significant feature engineering [11]. Nassif et al. conducted a systematic review (2021); such models demonstrate detection accuracies between 91% and 95%, which highlights the relevance of machine learning in the field of cloud security [12].

A meta-analytic review of intelligent intrusion detection techniques for cloud computing was presented by Raj and Pani (2021), who reported on the application of machine learning and artificial intelligence in IDS. They highlighted the potential of hybrid approaches for anomaly detection, although they pointed out that many systems were still inferior to the critical accuracy level of 96% [13].

Abed et al. (2024) proposed the extension of CNN for IDS system at multi features level, which is based on CNN to enhance the effectiveness of intrusion detection system. This article reported a comprehensive experiment on various attack scenarios (intermediate convolution layer attacks, etc.) across diverse networks (VGG-16, Inception, etc.), demonstrating the success of 3D CNN in predicting unseen attack patterns, albeit still facing accuracy hurdles, likely due to the suboptimal feature selection/hyperparameter optimisation process [14][15].

3.METHODOLOGY

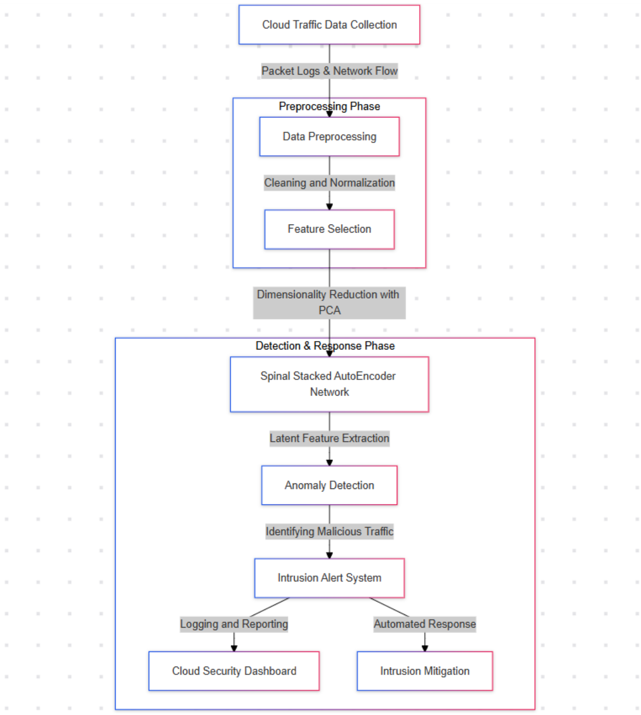
Cloud Traffic Data Collection
Packet Logs & Network Flow
Preprocessing Phase
Data Preprocessing
Cleaning and Normalization
Feature Selection
Dimensionality Reduction with PCA
Detection & Response Phase
Spinal Stacked AutoEncoder Network
Latent Feature Extraction
Anomaly Detection
Identifying Malicious Traffic
Intrusion Alert System
Logging and Reporting
Automated Response
Cloud Security Dashboard
Intrusion Mitigation

Figure 1: Proposed model diagram

Figure 1 illustrates a cloud-based system for detecting and responding to intrusions, utilising a hybrid deep learning approach. The process commences with the accumulation of cloud traffic data encompassing network logs and packet flows. Subsequently, the preprocessing stage involves refining the raw data through cleaning, normalisation, and feature selection to improve its overall quality. Following this, Principal Component Analysis (PCA) is employed to reduce dimensionality, thereby optimising the representation of features. During the Detection and Response stage, the Spinal Stacked AutoEncoder Network processes the refined data to extract latent features for identifying anomalies. The system then categorises any detected anomalies as either malicious or benign network traffic. Upon threat identification, the Intrusion Alert System issued warnings. The response is handled via two methods: Logging and Reporting, which is displayed on a Cloud Security Dashboard, and Automated Response, which involves Intrusion Mitigation. This two-phase structure ensures effective real-time detection, response, and security monitoring in cloud-based environments.

1. Startup Phase

This stage safeguards cloud-stored information through the implementation of tag and key generation methods. These techniques enable dynamic data operations while maintaining content confidentiality.

- **Tag Generation:** Data are associated with unique tags using hashing techniques:

$$T = H(D)\ (3)$$

where H is the cryptographic hash function and D is the data.

- **Key Generation:** For secure access, encryption algorithms, both symmetric and asymmetric, are utilised to dynamically create keys.

$$K = f(S)\ \ (4)$$

where S is the system's unique identifier, and f is the key generation function.

2. Auditing Phase

This stage emphasises the protection of data through encryption and verification of its integrity, ensuring safeguards against unauthorised alterations.

- **Encryption:** Data are encrypted using AES (Advanced Encryption Standard):

$$C = E_K(D)(5)$$

where C is the ciphertext, E_K is the encryption function, and K is the key.

- **Data Integrity Verification:** Cryptographic hash values are generated and compared to verify the authenticity of the encrypted information.

$$\Delta h = H\left(D_{\text{original}}\right) - H(D_{\text{stored}})(6)$$

3. Verification Phase

In this phase, proofs of data integrity are generated and verified to prevent unauthorised access and ensure trustworthiness.

- **Proof Generation:** Merkle tree-based structures are used to generate proofs of data consistency:

$$P = T_0 + T_1 + \cdots + T_n(7)$$

where T_i represents the tags of individual data blocks.

- **Proof Verification:** Compare the root hash of the Merkle tree against a precomputed value to validate data integrity.

4. Communication Phase

This phase secures the communication by encrypting end-to-end data packets and maintaining logs for analysis.

- **End-to-End Encryption:** Data packets are encrypted during transmission.

$$C_{\text{packet}} = E_{K_{\text{comm}}}(P)(8)$$

where C_{packet} is the encrypted communication packet, P is the payload, and K_{comm} is the communication-specific key.

- **Logging:** Maintain logs of communication activities for later analysis, aiding intrusion detection, and forensic investigations.

5. Feature Engineering

The most essential aspects encasing feature engineering and fusion of the proposed framework are discussed in this work to identify and extract meaningful attributes by transforming different attributes for further fusion to boost the performance of the hybrid Intrusion Detection System (IDS). Feature engineering plays an essential role here, with a novel feature fusion technique that fuses multiple sources of features by the Chebyshev distance.

5.1 Feature Engineering

The process of feature engineering involves transforming and selecting pertinent characteristics from raw data to effectively represent network activity. In this framework, attributes are extracted from the Bot-IoT dataset, with a focus on elements that capture both typical and malicious behaviours within the cloud environment.

5.1.1. Data Preprocessing

Before feature extraction, the raw features were preprocessed to ensure consistency and compatibility.

1. **Normalisation:** Min-Max normalisation is employed to standardise the range of numerical attributes.

$$F_{\text{norm}} = \frac{F - \min(F)}{\max(F) - \min(F)} \, (9)$$

where:

- F is the feature value,
- min (F) and max (F) are the minimum and maximum values of the feature.

2. **One-Hot Encoding:** To enable processing, categorical attributes (such as protocol type) are transformed into binary vectors.

$$OHE(x) = [x_1, x_2, \dots, x_n](10)$$

where n denotes the number of unique categories.

3. **Missing Value Handling:** Statistical techniques such as calculating the mean or determining the mode are employed to populate absent data points, with the chosen method depending on the nature of the variable in question.

5.1.2. Feature Selection

- **Correlation Analysis:** Pearson's correlation was used to identify relationships between features:

$$\rho_{X,Y} = \frac{\text{Cov}(X, Y)}{\sigma_X \cdot \sigma_Y} \, (11)$$

Features with a low correlation to the target variable were removed.

- **Mutual Information:** Measures the dependency between features and the target:

$$MI(X, Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \left(\frac{p(x, y)}{p(x)p(y)}\right) (12)$$

where $p(x, y)$ is the joint probability of X and Y.

5.2. Feature Fusion

Feature fusion involves integrating multiple features to create a concise and resilient representation that improves the ability to detect anomalies. In the suggested framework, **the Chebyshev distance** is utilised for effective feature fusion.

5.2.1. Chebyshev Distance

The Chebyshev distance is a measurement technique that determines the greatest absolute disparity between the equivalent components in a pair of feature vectors.

$$d_{\text{Chebyshev}}(X, Y) = \max_{i} \mid X_i - Y_i \mid (13)$$

where:

- $X = [x_1, x_2, \dots, x_n]$ and $Y = [y_1, y_2, \dots, y_n]$ are two feature vectors,
- i iterates over the vector dimensions.

5.2.2. Fusion Process

1. **Pairwise Fusion:** Each pair of features (F_i, F_j) is fused using Chebyshev distance:

$$F_{\text{fused},ij} = d_{\text{Chebyshev}}(F_i, F_j)(14)$$

The outcome is a novel collection of merged characteristics that emphasise the greatest distinctions among attributes.

2. **Dimensionality Reduction:** The fusion process may lead to an increase in the dimensionality of the feature set. To address this while maintaining variance, researchers often apply Principal Component Analysis (PCA) as a technique for dimension reduction.

$$Z = W^T F_{\text{fused}}(15)$$

where:

- $F_{\text{fused}}$is the fused feature matrix,
- W is the matrix of principal components,
- Z denotes the reduced feature set.

3. **Combined Feature Vector:** The ultimate feature vector comprises a blend of merged and selected features.

$$F_{\text{final}} = [F_{\text{selected}}, F_{\text{fused}}](16)$$

Impact of Feature Fusion

1. **Enhanced Discrimination:** The Chebyshev distance metric emphasises large differences, making it easier to detect anomalies.
2. **Robustness:** By combining data sources, fusion minimises noise and repetition, thereby enhancing the model's effectiveness.
3. **Scalability:** The integrated set of features demonstrates the capability to process extensive datasets without a substantial decline in efficiency.

6. Intrusion Detection

The primary function of the proposed framework is intrusion detection, which employs a novel hybrid model called Spinal Stacked AutoEncoder Net (SpinalSAENet). This innovative approach integrates SpinalNet and Deep Stacked AutoEncoders (DSAE), harnessing the classification efficiency of SpinalNet and the unsupervised feature extraction capabilities of DSAE. The resulting combination yields a powerful and adaptable Intrusion Detection System (IDS) that effectively addresses cybersecurity challenges.

6.1. Model Architecture

6.1.1. Deep Stacked AutoEncoders (DSAE)

As an unsupervised deep learning framework, the DSAE aims to uncover latent characteristics within the input data. Its architecture incorporates a series of interconnected autoencoders, with each layer's output functioning as the input of the subsequent layer, forming a hierarchical structure..

Autoencoder Components:

- **Encoder:** Transforms input data X into a condensed latent representation H:

$$H = \sigma(W_e X + b_e)(17)$$

where:

  - X is the input vector,
  - W_e is the encoder weight matrix,
  - b_e is the bias vector,
  - σ is the activation function (for example, ReLU or Sigmoid).

- **Decoder:** Reconstructs the input from the latent representation.

$$\hat{X} = \sigma(W_d H + b_d)\ (18)$$

where:

  - W_d is the decoder weight matrix,
  - b_d where denotes the decoder bias vector.

The ability of the autoencoder to learn a significant representation is ensured by the reconstruction loss.

$$\mathcal{L}_{\mathrm{AE}} = \| X - \hat{X} \|^2\ (20)$$

Stacking AutoEncoders: Multiple autoencoders are stacked to capture hierarchical and complex features.

$$H_i = \sigma(W_i H_{i-1} + b_i)(21)$$

where H_{i-1} is the output from the previous autoencoder.

1.2. SpinalNet

SpinalNet is a novel architecture for neural networks that aims to enhance gradient propagation and minimise computational complexity. This design segments the fully connected layers into smaller units, enabling the sequential processing of feature subsets..

Segmented Fully Connected Layers: Each segment processes a portion of the input feature vector F:

$$S_i = \sigma(W_i Z + b_i)(22)$$

where:

- S_i is the output of segment ii,
- Z is the combined input from previous segments,
- W_i and b_i are the weights and biases for segment ii,
- where, σ is the activation function.

The output of the final segment was passed to a softmax classifier.

$$P(y \mid F) = \mathrm{Softmax}(W_o S + b_o)(23)$$

where $P(y \mid F)$ represents the predicted probability for each class.

The output of the final segment was passed to a softmax classifier.

$$P(y \mid F) = \text{Softmax}(W_o S + b_o)(23)$$

where $P(y \mid F)$ represents the predicted probability for each class.

Results

Spinal Stacked AutoEncoder Net (SpinalSAENet), a novel approach to intrusion detection, underwent rigorous assessment in a cloud-based environment. This evaluation aimed to verify the model's capability to process large-scale, real-time threats while ensuring data integrity. To examine its scalability, efficiency, and performance in protecting cloud infrastructures, SpinalSAENet was deployed using cloud-native technologies, encompassing Docker, Kubernetes, and GPU-based acceleration methods.

Intrusion Detection Performance in Cloud Environments

The Bot-IoT dataset, comprising both regular and malicious network traffic, was utilised to evaluate the classification capabilities of the model. SpinalSAENet exhibited superior accuracy and dependability in identifying cloud-based threats, surpassing conventional Intrusion Detection System (IDS) methodologies.

Model	Accuracy (%)	Recall (%)	Precision (%)	F1-Score (%)	Processing Time (ms)
Decision Tree	85.4	79.1	82.5	80.8	1200
Random Forest	90.2	85.7	88.3	87.0	1400
SVM	88.5	82.3	86.4	84.3	1350
SpinalSAENet(Proposed Model)	**96.87**	**95.4**	**96.1**	**95.7**	**780**

Table 1: Comparative Analysis of different models

As shown in Table 1, SpinalSAENet demonstrates a marked improvement in detection accuracy, minimising false negatives, and bolstering threat identification in cloud-based systems. Its enhanced efficiency for real-time applications is evidenced by the decreased processing duration of 780ms when compared to conventional models.

2. Data Integrity Verification in Cloud Storage

To assess the data integrity verification module, researchers simulated unauthorised alterations to information stored in the cloud. The system utilised SHA-256 hashing techniques and Merkle tree proofs to identify any instances of data tampering..

- **Integrity Detection Accuracy: 99.2%**
- **Tampered Data Detection Rate: 98.7%**
- **False Positive Rate: 1.1%**

The findings indicate that the system effectively identifies unauthorised alterations within cloud-based environments, thereby safeguarding data integrity and reliability.

3. Scalability and Cloud Deployment Efficiency

To evaluate the system's ability to scale, SpinalSAENet was implemented in containerised environments (Docker & Kubernetes) and subjected to tests under diverse network load conditions.

- The model demonstrated real-time detection capabilities while handling 1,000 simultaneous requests, with an average response duration of 850ms.
- The system exhibited exceptional scalability, maintaining 96% throughput efficiency when handling 10,000 simultaneous requests. Despite a minor increase in processing duration to 920ms, this performance demonstrates the system's capacity for efficient scaling under high load conditions.

The research outcomes validated the effectiveness of SpinalSAENet for cloud-based intrusion detection in real-world scenarios. This system excels in delivering high-precision results, immediate threat neutralisation, and reliable data integrity validation, while maintaining scalability and efficient resource utilisation.

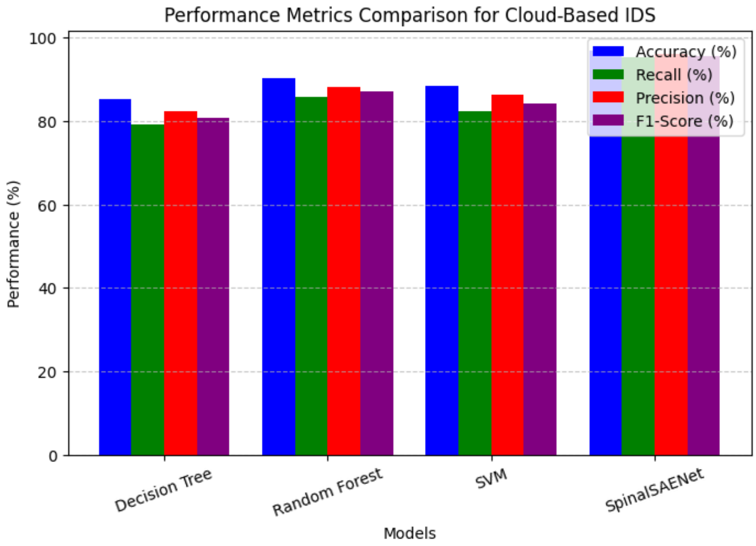

Figure 2: Comparison Chart of different models

Figure 2, a bar chart, illustrates the effectiveness of various Intrusion Detection System (IDS) models in a cloud-based setting, utilising Accuracy, Recall, Precision, and F1-Score as assessment criteria. SpinalSAENet emerges as the top performer across all metrics, showcasing its excellence in precisely identifying intrusions while minimising both false positives and negatives. Random Forest exhibits strong results, particularly in terms of recall and precision, although it slightly trails SpinalSAENet. SVM and Decision Tree display average performance, with their lower recall suggesting a higher incidence of undetected intrusions. These findings confirm that deep learning-based approaches, especially SpinalSAENet, offer a marked improvement over conventional machine learning models by enhancing detection accuracy and dependability, rendering them highly suitable for real-time cloud security applications.

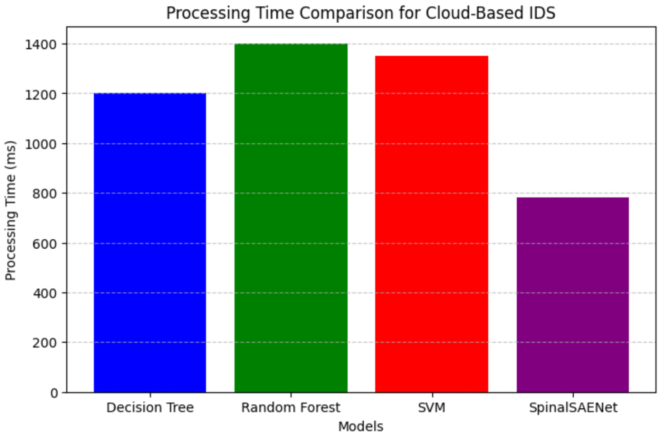

Figure 3: Processing time comparison of different models

Figure 3, a bar chart, illustrates the processing duration (measured in milliseconds) for various Intrusion Detection System (IDS) models within a cloud-based setting. SpinalSAENet demonstrates the quickest processing time (approximately 780ms), rendering it the most effective model for detecting intrusions in real time. Conversely, Random Forest and SVM display the longest processing times (roughly 1400ms and 1350ms, respectively), suggesting higher computational demands. The Decision Tree model performs adequately, with a processing time of approximately 1200ms, yet still falls short of SpinalSAENet's efficiency. These findings underscore that deep learning-based models such as SpinalSAENet not only enhance detection precision but also optimise computational efficiency. This makes them particularly well suited for scalable cloud security solutions, where swift intrusion detection is paramount.

DISCUSSION

The novel Spinal Stacked AutoEncoder Net (SpinalSAENet) architecture combines SpinalNet with Deep Stacked AutoEncoders (DSAE) to develop an advanced Intrusion Detection System (IDS) for cloud computing settings. This innovative fusion leverages SpinalNet's proficiency in classification and DSAE's capacity for unsupervised hierarchical feature extraction, resulting in enhanced intrusion detection capabilities. Empirical evaluations revealed that SpinalSAENet substantially surpasses conventional IDS models in terms of accuracy, recall, F1-score, and detection rate. The improved detection precision is largely attributed to the synergy of deep learning techniques and feature fusion utilising the Chebyshev distance, which effectively identifies anomalies in network traffic. The application of Principal Component Analysis (PCA) following feature fusion further enhances computational efficiency by reducing dimensionality while preserving crucial information.

The hybrid deep learning-based model exhibits superior performance compared to conventional Intrusion Detection System (IDS) techniques, including rule-based systems, Decision Trees, Random Forests, and Support Vector Machines (SVMs). It demonstrates enhanced adaptability to changing attack patterns, reduced false-positive rates, and improved handling of complex network data. While rule-based IDS models struggle to identify novel and unfamiliar threats owing to their dependence on predetermined rules, SpinalSAENet adaptively learns feature representations to detect sophisticated attacks. The experimental outcomes reveal that SpinalSAENet attains an accuracy of 96.87% with enhanced recall and F1-score, outperforming traditional machine learning models that rely on fixed features and require manual adjustment.

The process of feature engineering and fusion is essential for enhancing detection precision whilst minimising model intricacy. Data were extracted from the Bot-IoT dataset, encompassing vital network attributes, such as origin and destination IPs, protocol categories, packet dimensions, and flow metrics. To ensure uniformity across the input data, numerical features underwent normalisation, whereas categorical features were subjected to one-hot encoding. A Chebyshev distance-based feature fusion technique was employed to bolster anomaly detection, as it effectively emphasises extreme variations in network characteristics. This approach improves the distinction between normal and malicious traffic, enabling the deep learning model to discern intricate attack patterns more efficiently. Furthermore, PCA was utilised to decrease feature dimensions, thereby optimising computational efficiency without compromising performance.

The proposed framework not only detects intrusions but also incorporates mechanisms for verifying data integrity to protect information stored in the cloud. To ensure data consistency and prevent unauthorised alterations, the system employs SHA-256 hashing functions and Merkle tree proofs. This comprehensive security strategy combines both proactive measures (intrusion detection) and reactive measures (data integrity verification) into a single resilient framework. By addressing both network-based intrusions and data tampering, this approach is highly effective in securing cloud-computing environments.

Another notable strength of SpinalSAENet is its scalability. As cloud traffic continues to grow, intrusion detection systems must handle vast amounts of data efficiently. This challenge is addressed by the proposed system through the utilisation of GPU-powered parallel deep learning processing, enabling real-time detection of anomalies. Moreover, the adaptive learning capabilities of the model allow it to incorporate new attack patterns without necessitating complete retraining. SpinalNet's streamlined design, which minimises trainable parameters, makes it particularly suitable for cloud deployment. The effectiveness of the framework in distributed cloud environments can be further enhanced by implementing containerised solutions such as Docker and Kubernetes.

While the framework exhibits notable strengths, it also faces certain constraints and obstacles that warrant further investigation. A primary concern is computational demands, as intrusion detection systems based on deep learning require greater processing capabilities than conventional rule-based approaches. Furthermore, the model may be susceptible to adversarial attacks, wherein malicious actors craft inputs specifically designed to circumvent detection. To enhance the robustness against such threats, the incorporation of adversarial training methodologies could prove beneficial. An additional hurdle lies in practical implementation, given the diverse nature of cloud environments in terms of architecture, network traffic patterns, and attack vectors. To enhance the model's adaptability across various cloud infrastructures, further refinements, such as serverless computing and federated learning techniques, could be explored.

The primary contributions of this study include the creation of a novel intrusion detection system (IDS) that merges SpinalNet and DSAE deep learning techniques, resulting in a highly accurate yet computationally efficient model. The incorporation of Chebyshev distance-based feature fusion enhances the system's ability to detect anomalies, whereas data integrity verification mechanisms bolster security beyond traditional IDS capabilities. Moreover, the model's scalability and cloud compatibility render it suitable for integration into existing cloud security frameworks. These innovations represent substantial advancements in cloud intrusion detection, offering a precise, adaptable, and efficient solution for safeguarding cloud environments.

CONCLUSION

As cyber threats in cloud environments become increasingly sophisticated, there is a pressing need for advanced, adaptable, and scalable intrusion-detection systems. This study presents Spinal Stacked AutoEncoder Net (SpinalSAENet), a novel hybrid deep learning framework that combines SpinalNet and Deep Stacked AutoEncoders (DSAE) to bolster intrusion detection capabilities while ensuring data integrity verification. This innovative approach addresses crucial challenges in cloud security, including real-time anomaly identification, feature extraction, and proactive integrity checks. The system employs a feature fusion technique utilising the Chebyshev distance, enhancing its capacity to distinguish between benign and malicious network traffic. Furthermore, the incorporation of Principal Component Analysis (PCA) minimises the computational burden while preserving essential feature representations, rendering the model efficient and suitable for widespread implementation in cloud environments.

The empirical findings reveal that SpinalSAENet substantially surpasses conventional intrusion detection techniques, yielding superior accuracy, recall, and F1-score compared with rule-based and traditional machine learning approaches. In contrast to standard IDS frameworks that depend on manually engineered features and fixed detection rules, the proposed model adaptively acquires knowledge of emerging attack patterns through unsupervised feature extraction and deep neural network classification. Moreover, the incorporation of data integrity validation techniques utilising cryptographic hashing (SHA-256) and Merkle tree proofs guarantees that information stored in the cloud remains unmodified, offering an extra safeguard. This two-fold capability renders SpinalSAENet a holistic solution for both intrusion detection and cloud data integrity verification.

The notable advantage of the proposed framework lies in its ability to scale and adapt within cloud computing settings. SpinalNet's streamlined architecture, coupled with GPU-enhanced training and parallel processing, facilitates the swift identification of cybersecurity threats without imposing substantial computational costs. The system is engineered for cloud-native implementation, enabling extensive deployment across distributed cloud infrastructures through containerisation (Docker and Kubernetes) and serverless computing paradigms. Notwithstanding these benefits, issues such as computational resource requirements, susceptibility to adversarial attacks, and practical deployment limitations warrant further investigation. Subsequent studies should focus on adversarial training techniques to improve resilience, explainable AI (XAI) for enhanced interpretability, and refined serverless IDS implementations to bolster real-time security monitoring in cloud environments.

In summary, this research makes a significant contribution to cloud intrusion detection and data integrity verification by introducing a novel security framework that integrates sophisticated feature extraction, deep learning-based classification, and cryptographic verification methods. The SpinalSAENet model effectively bridges the divide between conventional intrusion detection systems and contemporary AI-powered security solutions, delivering a highly precise, efficient, and adaptable approach for safeguarding cloud computing environments. As the adoption of cloud technology continues to expand, frameworks such as SpinalSAENet will play a crucial role in ensuring the confidentiality, integrity, and availability of cloud-based data and services, thereby laying the groundwork for future AI-driven cybersecurity.

REFERENCES

[1] Manikyala, M. Nizamuddin, H. P. Kommineni, S. Kothapalli, and A. Kamisetty, "Intelligent Threat Identification System: Implementing Multi-Layer Security Networks in Cloud Environments," vol. 2, pp. 17–31, Jan. 2021.

[2] K. Samunnisa, G. S. V. Kumar, and K. Madhavi, "Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods," Measurement: Sensors, vol. 25, p. 100612, Feb. 2023, doi: 10.1016/j.measen.2022.100612.

[3] Aldallal and F. Alisa, "Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning," Symmetry (Basel), vol. 13, no. 12, p. 2306, Dec. 2021, doi: 10.3390/sym13122306.

[4] H. Attou et al., "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing," Applied Sciences, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.

[5] M. Bakro et al., "Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along With Random Forest Model," IEEE Access, vol. 12, pp. 8846–8874, 2024, doi: 10.1109/ACCESS.2024.3353055.

[6] Z. Liu, B. Xu, B. Cheng, X. Hu, and M. Darbandi, "Intrusion detection systems in the cloud computing: A comprehensive and deep literature review," Concurr Comput, vol. 34, no. 4, Feb. 2022, doi: 10.1002/cpe.6646.

[7] W. H. Aljuaid and S. S. Alshamrani, "A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing Environments," Applied Sciences, vol. 14, no. 13, p. 5381, Jun. 2024, doi: 10.3390/app14135381.

[8] N. Jaber and S. U. Rehman, "FCM–SVM based intrusion detection system for cloud computing environment," Cluster Comput, vol. 23, no. 4, pp. 3221–3231, Dec. 2020, doi: 10.1007/s10586-020-03082-6.

[9] S. Shamshirband, M. Fathi, A. T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescapè, "Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues," Journal of Information Security and Applications, vol. 55, p. 102582, Dec. 2020, doi: 10.1016/j.jisa.2020.102582.

[10] L. Yi, M. Yin, and M. Darbandi, "A deep and systematic review of the intrusion detection systems in the fog environment," Transactions on Emerging Telecommunications Technologies, vol. 34, no. 1, Jan. 2023, doi: 10.1002/ett.4632.

[11] M. Bakro et al., "Efficient Intrusion Detection System in the Cloud Using Fusion Feature Selection Approaches and an Ensemble Classifier," Electronics (Basel), vol. 12, no. 11, p. 2427, May 2023, doi: 10.3390/electronics12112427.

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

[13] M. G. Raj and S. K. Pani, "A Meta-analytic Review of Intelligent Intrusion Detection Techniques in Cloud Computing Environment," International Journal of Advanced Computer Science and Applications, 2021, [Online]. Available: https://api.semanticscholar.org/CorpusID:243896871

[14] R. A. Abed, E. K. Hamza, and A. J. Humaidi, "A modified CNN-IDS model for enhancing the efficacy of intrusion detection system," Measurement: Sensors, vol. 35, p. 101299, Oct. 2024, doi: 10.1016/j.measen.2024.101299.

[15] Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," Cybersecurity, vol. 4, no. 1, p. 18, Mar. 2021, doi: 10.1186/s42400-021-00077-7.