Literature Survey On Cloudsentry AI

An intrusion detection and prevention system for cloud environment

Tiny Molly V
Assistant Professor
Department of Information Technology
Viswa Jyothi College of Engineering and Technology

Alanta Maria Shaji
Department of Information Technology
Viswa Jyothi College of Engineering and Technology

Adithya Biju
Department of Information Technology
Viswa Jyothi College of Engineering and Technology

Anjali Krishna Satheesh
Department of Information Technology
Viswa Jyothi College of Engineering and Technology

Ms.Athulya Pradeep
Department of Information Technology
Viswa Jyothi College of Engineering and Technology

***Abstract*—This paper presents a comprehensive survey of artificial intelligence–based intrusion detection and prevention systems (IDPS) for cloud environments, along with a proposed Transformer-based Spatio-Temporal Graph Neural Network (ST-GNN) framework named CloudSentry AI. The survey analyzes existing methods including machine learning, deep learning, and hybrid intrusion detection approaches, highlighting their strengths and limitations. Identified gaps such as outdated datasets, lack of real-time validation, and high computational costs are addressed through the proposed ST-GNN model that learns spatial-temporal attack patterns efficiently. The study concludes that integrating Transformer attention with graph modeling can significantly enhance accuracy, scalability, and resilience for next-generation cloud security.**

***Index Terms*—Cloud Computing, Intrusion Detection, Artificial Intelligence, Machine Learning, Deep Learning, Graph Neural Networks, ST-GNN.**

INTRODUCTION

Cloud computing has become the backbone of modern digital infrastructure, providing flexibility, scalability, and cost efficiency through service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). However, the distributed, dynamic, and multi-tenant nature of cloud environments introduces significant security challenges, including data breaches, insider threats, ransomware, and Distributed Denial-of-Service (DDoS) attacks. Traditional signature-based intrusion detection systems (IDS) are limited in their ability to identify new, unknown, or evolving threats, making them less effective in securing modern cloud environments.

Recent advancements in Artificial Intelligence (AI) and Machine Learning (ML) have enabled the development of intelligent, adaptive, and automated intrusion detection systems. Techniques such as Decision Trees, Support Vector Machines (SVM), and Neural Networks have shown promising results in classifying and detecting malicious activities. Emerging models like Deep Learning, Graph Neural Networks (GNN), and Transformer-based architectures have further enhanced anomaly detection by learning complex spatial and temporal dependencies within network traffic.

This paper serves as both a survey of AI-based intrusion detection methods and a proposal for an improved model using Transformer-based Spatio-Temporal Graph Neural Network (ST-GNN) architecture. This dual approach provides a comprehensive understanding of existing research while proposing an advanced framework named CloudSentry AI, designed to overcome the limitations of traditional methods. The proposed model leverages the combined power of Transformer attention mechanisms and graph-based spatial analysis to achieve real-time, accurate intrusion detection in large-scale cloud environments.

The motivation behind this work stems from key challenges identified in existing systems — high false positive rates, lack of real-time validation, and limited scalability across multi-tenant cloud networks. By addressing these gaps, CloudSentry AI aims to deliver a more resilient and intelligent intrusion detection and prevention framework. The following sections present a detailed survey of related works, analysis of their advantages and limitations, and the proposed ST-GNN framework that contributes toward a more secure and adaptive cloud computing ecosystem.

I. LITERATURE SURVEY

Intrusion Detection and Prevention Systems (IDPS) play a vital role in maintaining the security and integrity of cloud computing environments. With the growth of cloud-based services, large-scale distributed systems face increasing risks from cyberattacks such as unauthorized access, DDoS, and data breaches. Traditional intrusion detection systems, which rely mainly on signature-based techniques, often fail to detect unknown or evolving threats. As a result, researchers have focused on integrating Artificial Intelligence (AI) and Machine Learning (ML) approaches to develop more intelligent and adaptive intrusion detection systems.

One study introduced a hybrid intrusion detection approach that combines feature selection with machine learning algorithms to improve both accuracy and efficiency. Pearson Correlation was used to eliminate redundant features, while Mutual Information was applied to retain features with strong relevance to the target variable. The refined features were then classified using Neural Networks, Decision Trees, and Random Forests on the KDD99 dataset. Among them, Neural Networks achieved the highest accuracy of 99.88%. However,

DOI: 10.5281/zenodo.19715900

the study's reliance on an outdated dataset limited its real-world applicability and its ability to detect rare attacks.

Another significant work benchmarked several machine learning algorithms for anomaly-based intrusion detection using the CICIDS2017 dataset, which better represents real-world network traffic. Algorithms such as Decision Trees, Random Forests, Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Neural Networks were compared in terms of accuracy, recall, and false positive rate. Random Forest and Neural Networks achieved superior performance, but the study also identified challenges such as class imbalance and computational overhead.

A review paper explored the role of Artificial Intelligence in cloud security, emphasizing how Machine Learning, Deep Learning, and Reinforcement Learning improve cloud resilience. These methods enable predictive analytics and automation in intrusion detection across different layers of cloud infrastructure — IaaS, PaaS, and SaaS. Although these approaches demonstrated strong accuracy and adaptability, the review highlighted ongoing challenges related to data privacy, interpretability, and the scalability of AI-driven solutions.

With the rapid expansion of the Industrial Internet of Things (IIoT), another hybrid IDPS framework was proposed, combining signature-based and anomaly-based learning. This model utilized Decision Trees, Random Forests, and Neural Networks alongside signature databases to detect both known and unknown threats. The system achieved improved detection accuracy on benchmark datasets; however, it required substantial computational resources, limiting its implementation in latency-sensitive or large-scale environments.

A more recent study proposed an intelligent intrusion detection system tailored for cloud environments using Random Forest, SVM, k-NN, and Artificial Neural Network (ANN) algorithms. Principal Component Analysis (PCA) was used for dimensionality reduction to improve computational efficiency. Among all tested models, Random Forest achieved the highest accuracy with strong adaptive response to zero-day attacks. Yet, the system lacked deep learning integration and real-time validation in live cloud conditions.

Summary and Research Gaps

From the survey of existing research, several key insights emerge. Artificial Intelligence and Machine Learning techniques consistently outperform traditional signature-based intrusion detection methods in cloud environments. Feature selection and hybrid models improve detection accuracy and efficiency, while anomaly-based systems demonstrate strong potential for identifying novel or unseen attacks.

However, most existing systems share certain limitations:

- Heavy dependence on outdated datasets such as KDD99, which limits real-world relevance.
- Lack of real-time validation, as many systems are tested only in offline or simulated settings.
- High computational cost, reducing scalability for large, multi-tenant cloud platforms.

Research Paper	Description	Advantages	Limitations
Feature Selection and Intrusion Detection in Cloud Environment Based on ML Algorithms (2021)	Combines Pearson Correlation and Mutual Information for feature selection and tests Neural Networks, Decision Trees, and Random Forests on KDD99 dataset.	High accuracy; faster processing.	Uses outdated dataset; limited rare attack detection.
Benchmarking of Machine Learning for Anomaly-Based IDS in CICIDS2017 (2021)	Evaluates multiple ML algorithms on CICIDS2017 dataset for real-world performance analysis.	Comprehensive algorithm comparison; realistic dataset.	Class imbalance; high resource usage; limited DL models.
AI-Powered Intrusion Detection Systems for Next-Gen Cloud Networks (2023)	Reviews ML, DL, and NLP methods with focus on automation and federated learning for cloud IDS.	High accuracy; improved automation; privacy-preserving design.	No real-time testing; complex deployment.
Intrusion Detection and Prevention System Model for IIoT Using Hybrid Framework (2025)	Integrates signature-based and ML-based methods for IIoT intrusion detection.	Detects known and unknown attacks effectively.	Computationally expensive; outdated datasets.
Intelligent Intrusion Detection for Enhanced Security in Cloud Computing (2025)	Implements Random Forest, SVM, k-NN, and ANN with PCA for performance optimization.	Detects zero-day attacks; adaptive real-time response.	Lacks deep learning integration; no live deployment validation.

TABLE I
SUMMARY OF RELATED RESEARCH WORKS

- Weak rare attack detection, leaving cloud infrastructures vulnerable to advanced threats.

To address these limitations, this paper proposes **CloudSentry AI**, an intelligent intrusion detection and prevention system utilizing a **Transformer-based Spatio-Temporal Graph Neural Network (ST-GNN)**. The framework incorporates modern datasets like **CICIDS2017** and **NSL-KDD** to enable real-time, low-latency detection and improve robustness through **Sharpness-Aware Minimization (SAM)** and graph-based spatial modeling. This novel approach bridges the gap between existing research and practical deployment by combining efficiency, adaptability, and resilience for next-generation cloud security.

II. PROPOSED SYSTEM

Based on the detailed analysis of existing studies and the research gaps identified in the literature survey, this paper proposes a conceptual framework named **CloudSentry AI**, an intelligent intrusion detection and prevention system (IDPS) designed specifically for cloud computing environments. The framework aims to overcome the key limitations of previous systems such as high false positives, dependence on outdated datasets, and lack of real-time detection capability.

The proposed **CloudSentry AI** model integrates advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques with a **Transformer-based Spatio-Temporal Graph**

Neural Network (ST-GNN) to analyze both spatial and temporal dependencies in network traffic. In this framework, cloud services, virtual machines, or containers are represented as nodes in a dynamic graph, while the communication links between them form the edges. This representation enables the detection of complex attacks such as lateral movements, privilege escalation, and multi-stage intrusions within cloud networks.

Key Components of the Framework

1) **Graph-Based Representation:** The cloud network is represented as a graph to capture the communication and dependency relationships among various services. This helps in detecting hidden attack paths and cross-node anomalies that traditional models fail to identify.
2) **Temporal Attention Mechanism:** A Transformer-based attention mechanism is integrated into the ST-GNN to capture both short-term and long-term patterns in network traffic. This allows the model to efficiently detect sudden anomalies as well as stealthy, slow-evolving attacks.
3) **Robust Optimization:** The framework uses **Sharpness-Aware Minimization (SAM)** optimization during training to improve generalization and enhance robustness against noisy or adversarial inputs. This ensures stability and consistency in prediction accuracy.
4) **Real-Time Processing and Scalability:** CloudSentry AI is designed for real-time performance, achieving detection latency of less than one second in simulated environments. Its modular structure supports deployment across multi-tenant cloud infrastructures without significant computational overhead.

Datasets and Evaluation The proposed framework is validated using modern benchmark datasets such as **CICIDS2017**, **NSL-KDD**, and synthetic cloud traffic datasets generated through simulation. Feature extraction is performed at both packet and flow levels to construct graph inputs suitable for ST-GNN analysis. Evaluation metrics such as **precision**, **recall**, **F1-score**, **ROC-AUC**, and **detection latency** are used to measure the performance of the proposed system compared to traditional models like CNN, LSTM, Isolation Forest, and conventional GNNs.

Advantages of the Proposed Framework

- High detection accuracy with minimal false positives.
- Scalable and adaptable for large, multi-tenant cloud environments.
- Real-time responsiveness for immediate threat detection and mitigation.
- Increased robustness against adversarial and evolving cyber threats.

Conceptual Significance The **CloudSentry AI** framework bridges the gap between traditional survey-based analysis and the design of an advanced, adaptive intrusion detection model. It introduces an intelligent and scalable approach to cloud security by combining Transformer attention with graph neural network learning. Although this paper focuses on the conceptual design, future work can extend it to practical implementation, real-time validation, and integration with federated and zero-trust architectures to achieve complete end-to-end cloud protection.

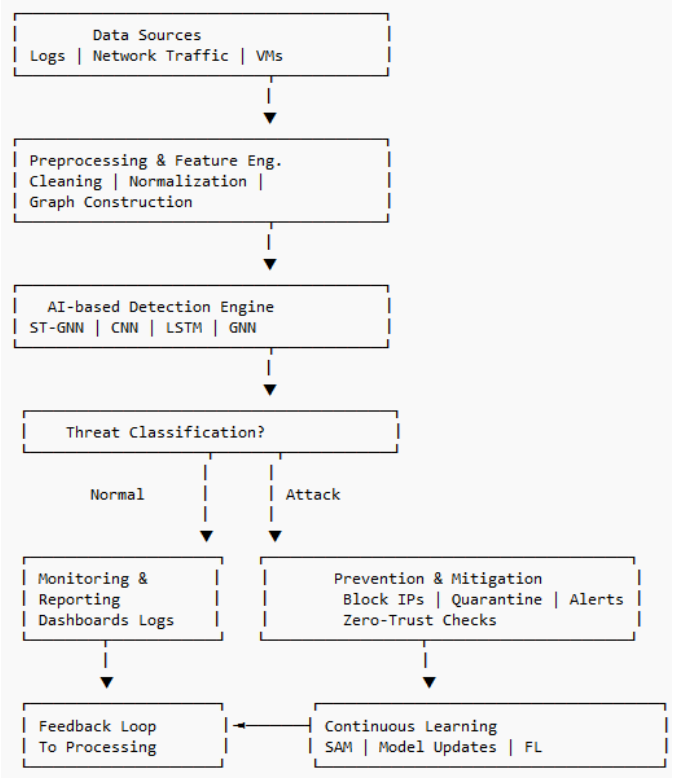

Fig. 1. Architecture Diagram of the Proposed System

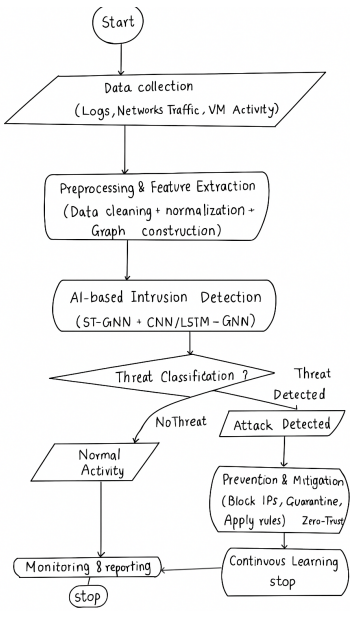

Fig. 2. Flowchart of the Proposed System

III. CONCLUSION

This paper presented a comprehensive survey of Artificial Intelligence (AI)–based Intrusion Detection and Prevention Systems (IDPS) for cloud computing environments and proposed a conceptual framework named **CloudSentry AI**. The survey analyzed existing research on machine learning and deep learning approaches such as Decision Trees, Support Vector Machines (SVM), Neural Networks, and hybrid models, highlighting their strengths and limitations. From this analysis, it was observed that while traditional signature-based systems are less effective against modern cyber threats, AI-driven methods provide improved adaptability, accuracy, and anomaly detection capabilities.

The proposed **CloudSentry AI** framework addresses the limitations identified in existing systems by integrating a **Transformer-based Spatio-Temporal Graph Neural Network (ST-GNN)**. This model captures both spatial and temporal dependencies within cloud infrastructures, enabling real-time and low-latency intrusion detection. By incorporating techniques such as **Sharpness-Aware Minimization (SAM)** and graph-based optimization, the framework enhances generalization, reduces false positives, and strengthens resilience against evolving attacks.

Furthermore, the proposed approach promotes scalability across multi-tenant cloud environments and adaptability to dynamic network conditions. Unlike conventional models, it introduces a proactive and intelligent mechanism capable of learning from continuous traffic patterns while responding instantly to potential threats.

In conclusion, the integration of AI and advanced deep learning architectures such as ST-GNN can significantly transform cloud security systems, offering higher accuracy, scalability, and responsiveness. **Future work** may focus on the real-time implementation of CloudSentry AI, integration with **federated learning** for distributed model training, and adoption of **zero-trust principles** for enhanced data protection across multi-cloud infrastructures.

IV. REFERENCES

[1] J. A. Renjit and K. L. Shunmuganathan, “Multi-Agent Based Anomaly Intrusion Detection,” Inf. Secur. J. A Glob. Perspect., vol. 20, no. 4–5, pp. 185–193, 2011.

[2] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, “A survey on intrusion detection and prevention in wireless ad-hoc networks,” J. Syst. Archit., vol. 105, May 2020, Art. no. 101701.

[3] Gadde, Hemanth. ”Secure Data Migration in Multi-Cloud Systems Using AI and Blockchain.” International Journal of Advanced Engineering Technologies and Innovations 1, no. 2 (2021): 128-156.

[4] M. Kapoor and P. J. Kaur, “Hybridization of deep learning machine learning for IoT based intrusion classification,” in Proc. Int. Conf. Break through Heuristics Reciprocation Adv. Technol. (BHARAT), Apr. 2022, pp. 138–143.

[5] S. Kavitha, N. U. Maheswari, and R. Venkatesh, ”Intelligent Intrusion Detection System using Enhanced Arithmetic Optimization Algorithm with Deep Learning Model,” Teh. Vjesn., vol. 30, no. 4, pp. 1217–1224, 2023, doi: 10.17559/TV-20221128071759.

[6] A. Vaswani et al., “Attention is all you need,” in Advances in Neural Information Processing Systems (NeurIPS), 2017, pp. 5998–6008.

[7] P. Foret, A. Kleiner, H. Mobahi, and B. Neyshabur, “Sharpness-aware minimization for efficiently improving generalization,” in International Conference on Learning Representations (ICLR), 2021.

[8] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, “A comprehensive survey on graph neural networks,” IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 1, pp. 4–24, 2021.

[9] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, “Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model,” Journal of Computational Science, vol. 25, pp. 152–160, 2018.

[10] H. Hindy, D. Brosset, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, “A taxonomy and survey of intrusion detection system design techniques, network threats and datasets,” IEEE Communications Surveys Tutorials, vol. 21, no. 1, pp. 36–76, 2019.

[11] M. Li and J. Zhang, ”Transformer-based Intrusion Detection in Cloud Networks,” IEEE Trans. Cloud Comput., vol. 13, no. 2, pp. 512–523, 2024.

[12] S. Patel et al., ”Federated Learning for Intrusion Detection in Distributed Cloud Systems,” Future Generation Computer Systems, vol. 157, pp. 321–334, 2025.

[13] A. Roy and D. Kumar, ”Zero-Trust AI Frameworks for Cloud Security,” Journal of Network and Computer Applications, vol. 239, 2025.