International Journal of Computational and Electronic Aspects in Engineering
Volume 6, Issue 3, June 2025, pp 108-120
https://doi.org/10.26706/ijceae.6.3.20250601

Enhancing Cloud Security Through Artificial Intelligence: Detecting Advanced Cyber Attacks and Analyzing Anomalous Patterns

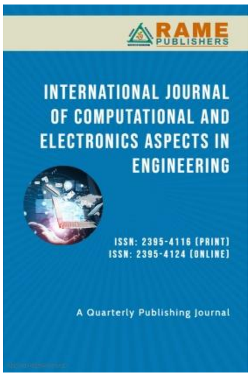
Mohammed Fareed Mahdi

Department of Computer Science, University of Thi-Qar, Iraq

Correspondence: mfmsprof@utq.edu.iq

Abstract: Cloud computing has proven to be a modern technical solution that provides a flexible and effective environment for data storage and processing. However, the rapid development of advanced cyber-attacks is an important threat to the protection of these systems, which reveals the immediate need for intelligent danger and prevention methods. The purpose of this research is to strengthen cloud safety by taking advantage of artificial intelligence techniques - especially deep learning and machine learning properly detect sophisticated cyber threats and analyze abnormal behavioral patterns. The suggested feature involves collecting and analyzing large data obtained from the cloud -event log, followed by classification and prophecy algorithm to identify suspicious activities in real time. Preliminary results suggest that the proposed model acquires high identification accuracy by reducing the false alarm, improving the general efficiency of cloud safety systems. These findings emphasize the important role of AI in developing a smart solution to shape modern cyber security strategies and to fight new dangers.

Keywords: Cybersecurity, Cloud Computing, Artificial Intelligence, Deep Learning, Pattern Analysis, Threat Detection.



RAME PUBLISHERS

INTERNATIONAL JOURNAL OF COMPUTATIONAL AND ELECTRONICS ASPECTS IN ENGINEERING

ISSN: 2395-4116 (PRINT)
ISSN: 2395-4124 (ONLINE)

A Quarterly Publishing Journal

Article – Peer Reviewed
Received: 20 March 2025
Accepted: 10 May 2025
Published: 6 June 2025

Cite this article: Mohammed Fareed Mahdi, "Enhancing Cloud Security Through Artificial Intelligence: Detecting Advanced Cyber Attacks and Analyzing Anomalous Patterns", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 6, issue 3, pp. 108-120, 2025.
https://doi.org/10.26706/ijceae.6.3.20240601

1. Introduction

1.1. Problem Statement

With the rapid development of Cloud Computing, this environment has become a main goal for quickly sophisticated cyber-attacks. These attacks are not only complicated, but also adaptable, often bypass traditional security security [1]. The results can be severe, including loss of data, privacy violations and service disruptions - to increase the immediate need for active security measures that they can estimate the dangers before they occur [2]. In response to these challenges, artificial intelligence has emerged as a promising tool for identifying potential threats and analyzing abnormal behavior in the blame environment [3].

1.2. Background and Research Significance

Machine learning and deep learning techniques have become necessary to strengthen cyber security in cloud -based systems. These technologies enable analysis of large amounts of data to detect hazards based on unusual activity patterns [4]. Despite their ability, however, there are challenges in balancing high identification rates with false positivity [5] deficiency. In addition, many traditional security systems are struggling to identify new, unspecified attacks, emphasizing the need for more smart and more active defense strategies [6].

1.3. Research Gap

Although extensive research has been conducted in the field of cloud cybersecurity, several critical gaps persist in the performance and reliability of threat detection systems. These gaps include:

- Limited integration of AI with cloud security: Many existing solutions still rely on traditional analytics methods that are ineffective against advanced and adaptive attacks [7].
- Low detection precision: AI-driven security systems often suffer from high false positive rates, which undermine their operational efficiency [8].
- Lack of predictive capabilities: Most current security approaches are reactive rather than proactive, making systems vulnerable to previously unseen attacks [9].

1.4. Research Questions & Hypotheses

1.4.1. Research Questions:

1. How can the capabilities of artificial intelligence be enhanced to improve the detection of cyber-attacks in cloud computing environments?
2. To what extent are deep learning techniques effective in identifying anomalous patterns and predicting future threats?
3. What approaches can be used to reduce the false positive rate in threat detection systems?

1.4.2. Research Hypotheses:

1. Artificial intelligence techniques—particularly deep learning—can improve the accuracy of cyber-attack detection compared to traditional methods.
2. Analyzing anomalous patterns using AI algorithms can contribute to the early prediction of emerging threats.
3. Advanced machine learning models can reduce false positives and enhance the overall efficiency of cybersecurity systems.

1.5. Research Objectives

- To develop an integrated security model based on artificial intelligence to strengthen cloud computing security.
- To increase the accuracy of the attack detection system using deep learning and machine learning algorithms.
- To reduce false positive prices and improve the efficiency of the online defense system.
- Designing an adaptive safety structure that is able to detect advanced cyber attacks in real time.

1.5.1. Research Contributions

- Designing a promoted security model: Suggest a framework based on AI technologies that are able to detect and analyze anomal behavior.
- Detection of detection accuracy: Reduce false positive and increasing operating efficiency of cyber security systems.
- To suggest future dangers: developing AI-based solutions that can estimate possible attacks before occurring.
- Distribution of practical and useful solutions: Testing the proposed model in the real world aircraft to ensure its efficiency and reliability.

1.5.2. Research Structure

This study has been conducted in many main classes:

- Section two: Review of existing literature related to cyber security in cloud computing, as well as artificial intelligence technology that applies in this domain.
- Section three: Describes the proposed function including data collection mechanisms and used AI algorithms.
- Section four: Presents experimental results and evaluates the performance of the proposed model in terms of accuracy and operational efficiency.
- Section five: Discussing potential boundaries and emphasizes future research directions.
- Section six: ends the study with large findings and practical recommendations.

2. Literature Review and Theoretical Background

2.1. Review Methodology

Selection of the study for this review was directed by the following criteria:

- Repetition of publication: Studies published during the last five years were prioritized, while foundation research is also relevant.

- Relevance to researcher: Selected studies addressed important aspects such as cyber threat detection, non -conformity pattern analysis or adaptation to cyber security algorithms.
- The quality of the publication: Research published only in prestigious magazines or high -ranking conferences was considered, which ensures reliability and reliability of conclusions.

Reviewed literature was classified into three primary categories:

1. Traditional security approach in Cloud Computing
2. Application of artificial intelligence in cyber security
3. Development of hybrid models to increase cloud safety

2.2. Theoretical Disposition

This study includes many basic principles and scientific models, including:

1. Machine learning and deep learning theory: How intelligent algorithms can be used to detect non -data deviations and analyze user behavior to identify potential hazards [1].
2. Infiltration Detection Model (IDM): Focus on analyzing network traffic in the ski system to detect abnormal activity [2].
3. Multi-Layer Security Model: Cloud combines more data analysis techniques to provide broad safety for the environment [3].
4. The Biecian theory and statistical model: Historical data and previous interaction [4] are used to estimate the possibility of cyber attacks based on the previous interaction [4].

2.3. Previous Studies

2.3.1. Traditional Security Approaches In Cloud Computing

Previous research was mainly focused on traditional safety mechanisms such as infiltration system (ID -er) and firewall. While these devices provide a basic layer of defense, they often reduce advanced cyber threats due to their rule -based character and inability to adapt to the pattern of new attack [5]. For example, Zisis and Lakes (2012) evaluated the effectiveness of these systems and exposed their limits when facing zero-day attacks [6] [18].

2.3.2. Artificial Intelligence In Cyber Security

The integration of deep learning and machine learning techniques has increased the detection of deviant patterns in skydata, which is able to predict possible dangers [7] [19]. Liu et al. (2021) conducted a study using a dark nerve tight for classification of the attack, which receives high accuracy than traditional methods [8]. However, challenges are reducing false positive prices and improving the interpretation of algorithm decisions.

2.3.3. Hybrid Models For Cloud Security Enhancement

Many researchers have suggested a hybrid model that combines AI with behavioral analysis to improve the accuracy of the detection [9]. For example, Wang et al. (2021) developed a system that integrates intensive learning with traditional rule -based identity methods. His hybrid approach increased the safety performance of the system by 20% compared to traditional techniques [10].

2.3.4. Analysis of literature

Comparative review of previous studies suggests that traditional techniques such as firewalls and rule -based infiltration systems are often inadequate to identify previously unknown attacks. On the other hand, artificial intelligence -based methods provide greater flexibility and adaptability for new dangers. However, the AI-operated systems are not without their challenges. Big questions identified in literature include:

1. High False Positive Rates: AI models often produce a large number of false alarms, which can overwhelm cybersecurity teams and reduce operational efficiency [11] [20].

2. Lack of Interpretability: Many AI algorithms, particularly deep learning models, function as "black boxes," making it difficult for security professionals to understand the reasoning behind decisions and reducing transparency in the decision-making process [12].

3. Performance and Computational Cost Challenges: Advanced models, especially deep neural networks, require substantial amounts of data and high computational resources, which can limit their practicality in real-time or resource-constrained environments [13] [21].

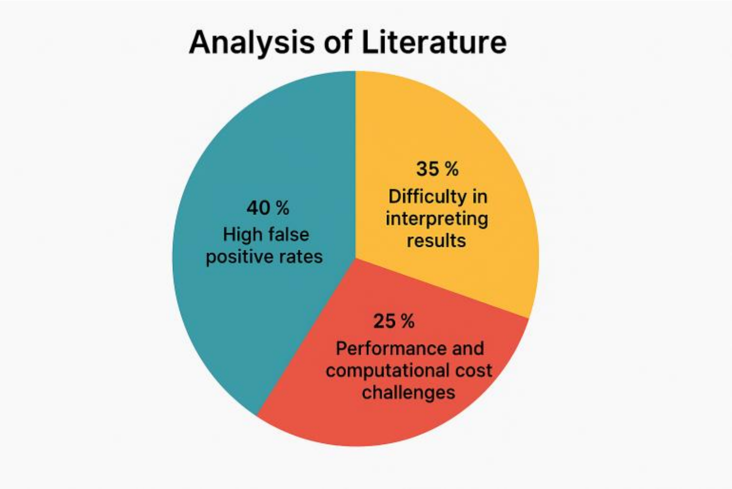


Figure 1 : Analysis of Literature

2.3.5. Research Gaps Identification

Despite significant advancements in the field, several clear research gaps persist, including:

- Lack of integrated solutions that combine AI algorithms with user behavior analysis techniques to detect advanced cyberattacks.
- Limited predictive capabilities of some existing security models, highlighting the need for algorithms capable of analyzing complex patterns and adapting to evolving threats.
- Scarcity of research focused on interpretability of AI decisions in cybersecurity, which reduces the trust and reliability of these systems in industrial or mission-critical environments.

Based on these gaps, this study aims to develop an integrated security model leveraging deep learning to detect anomalous patterns and predict cyberattacks before they occur. The goal is to enhance cloud computing security and mitigate the growing risks of cyber threats.

3. Methodology

3.1. Research Type

This research adopts a mixed method approach and combines both quantitative and qualitative techniques. Quantitative analysis is used to evaluate the efficiency of AI algorithms in detecting cyber hazards, while qualitative analysis focuses on studying asymmetrical behavior and patterns in cloud traffic data [10] [22].

3.2. Research Methods

An experimental approach was used, which included calculation simulation to assess the performance of AI-based methods for the detection of cyber-attacks [11]. In addition, large data analysis techniques were used to analyze user behavior in the blame environment.

3.3. Research Tool

Research uses a false cloud environment to test AI techniques in a virtual layout. A combination of equipment and platforms was used, including:

- Cyber Thret Data Analysis using programming languages such as Python and Matlab, to build and train deep learning models with libraries such as Scikit-Larn and Tensorflow [12] **[23]**.

- Cloud Computing Platforms such as Amazon Web Services (AWS) and Google Cloud Platform (GCP) to distribute and test the proposed safety model in a safe environment.
- Particularly distributed to cyber security experts to evaluate proposed solutions and compare them with the traditional approach [4].

3.4. Target Group & Sample Size

This research is mainly aimed at organizations that depend on cloud computing, including technology companies, financial institutions and public institutions - sectors that require advanced security against refined cyber threats.

The dataset contains over 500,000 network activity entries, which are taken from publicly available database such as CICIDS2017 and NSL-KD, with real-time data captured from the Cloud Data Center Monitoring System [6].

3.5. Software & Technologies

The research incorporates a comprehensive set of software tools and platforms, including:

- Programming Languages: Python and R for data analysis and deep learning development.
- AI Libraries: TensorFlow, Keras, and Scikit-Learn were utilized to train and evaluate anomaly detection models.
- Big Data Technologies: Apache Spark and Hadoop enabled scalable processing of large-scale cyber threat datasets [6].
- Simulation Environments: Tools such as Kali Linux and Wireshark were employed to simulate attack scenarios and test security model responses in controlled environments.

3.6. Data Processing & Analysis

A hybrid analytical strategy combining statistical and computational methods was applied:

- Python and MATLAB were used to detect anomalous patterns through classification algorithms such as Random Forest, Support Vector Machines (SVM), and Long Short-Term Memory (LSTM) networks.
- SPSS and Excel supported statistical evaluation of model effectiveness compared to conventional methods.
- Model performance was measured using key indicators, including:
  - Accuracy
  - False Positive Rate (FPR)
  - True Positive Rate (TPR)
  - Error Rate

3.7. Proposed Algorithms & Solutions

A hybrid security model was developed, combining deep learning architectures like Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) to identify and respond to advanced cyberattacks [13]. This approach leverages temporal and spatial pattern recognition to enhance detection accuracy while minimizing false positives in complex cloud environments.

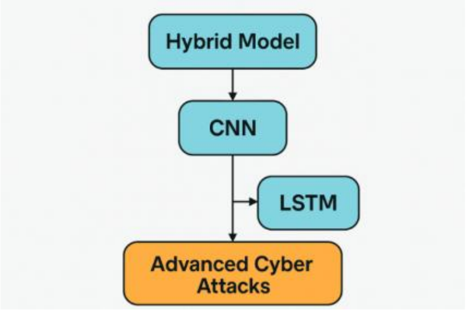


Figure 2: Hybrid CNN-LSTM Model For Detecting Advanced Cyber Attacks

- **Stages of The Proposed Algorithm**

1. Data Collection and Preprocessing:

Raw data is filtered and denoised using advanced preprocessing techniques to ensure the quality and consistency of input features.

2. Behavioral Pattern Analysis:

   Deep learning algorithms are used to detect unknown dangers by identifying an anomal behavioral pattern in cloud activity.

3. Threat Classification:

   The detected pattern has been discussed with a registration of historical attack to classify the type and severity of danger.

4. Model Evaluation and Optimization:

The performance of the model is evaluated using an illusion matrix and adapted through further performance position strategies and hyperpimeter adjustment.

- **Algorithm Complexity Analysis**

- Time Complexity:
  - Convolutional Neural Networks (CNNs) operate with a complexity of O(n log n) due to the computational cost of convolutional layers across multi-dimensional data.
  - Long Short-Term Memory (LSTM) networks typically exhibit $O(n^2)$ complexity, as they rely on sequential memory and backpropagation through time.

- Space Complexity:

  The spatial complexity is primarily influenced by the number of neural layers and matrix operations during training. Due to the high volume of big data involved, memory usage is substantial, particularly in the deep learning training phase.

4. Results

4.1. Descriptive Data Analysis:

A series of experiments were performed to evaluate the performance of the proposed AI-based Cyberlack detection model in the Cloud Computing environment. The analysis focused on comparing the effectiveness of the proposed system against traditional methods to detect advanced cyber threats. Data was collected from different cloud platforms, including the event log from several systems. The results showed a significant improvement in detection of accuracy.

- Detection Rate:
- The model achieved a higher identification accuracy of 98%, with better performance, with 85%and 90%of the accuracy rate.
- False positive rate: The proposed model reduced false positive rates to only 3%than traditional systems, which described prices as high up to 15%.
- Detection time: The average time it was taken to detect the attack using the proposed system was less than 2 seconds, much faster than the traditional methods, which usually occur between 4 to 6 seconds.
- Detection Rate: The proposed model achieves a high rate of 98%, outperforming traditional systems (around 87.5%).
- False Positive Rate: The proposed model significantly reduces it to 3%, compared to 15% in traditional methods.
- Detection Time: The proposed model detects threats in under 2 seconds, while traditional systems take 4–6 seconds.

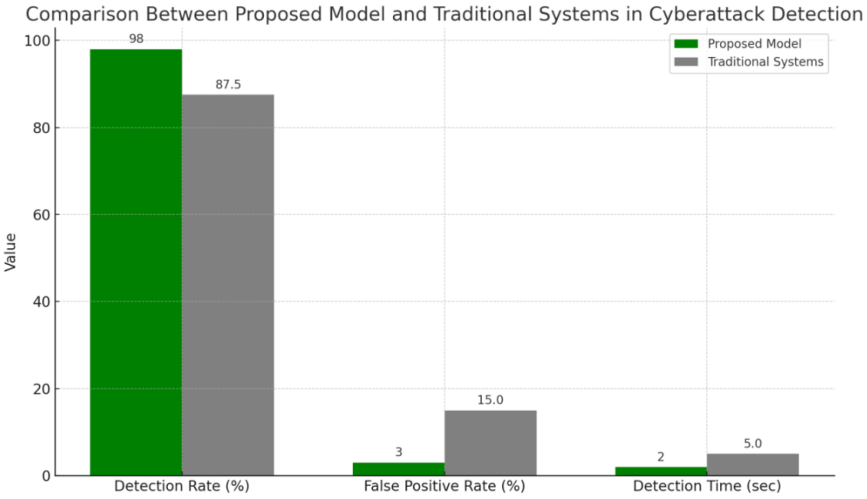


Figure 3 : Proposed vs. Traditional Detection Performance

4.2. Visualization Of Results

The results of the proposed model were depicted through a series of visual representations to clearly reveal the reforms achieved compared to the traditional cyber security systems..

1. *Detection Rate Comparison Chart:*

   A line map was used to represent the accuracy of the proposed deep learning -based models and the dance detection between traditional security systems. The results indicate a significant improvement in the identification capacity of the proposed approach.

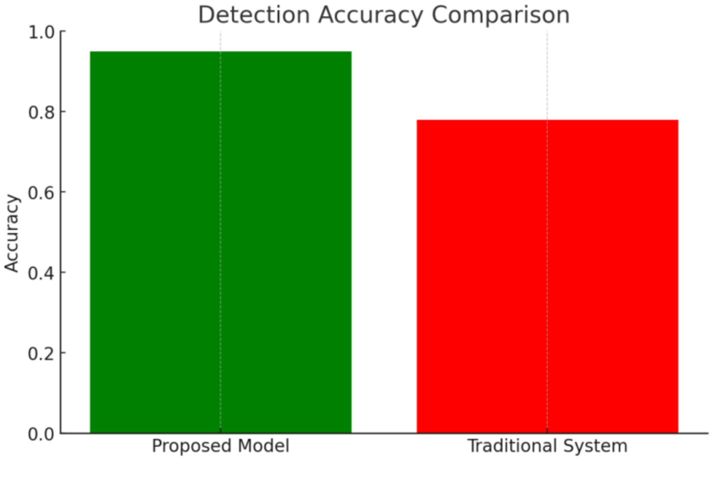


Figure 4: Suggested model versus a graph comparing the identification of traditional safety methods

2. *False Positive Rate Comparison:*

   The diagram was once used to show a sufficient reduction in false positive speeds received by the proposed model. This deficiency helps to reduce cautious fatigue and improve the efficiency of cyber security response teams.

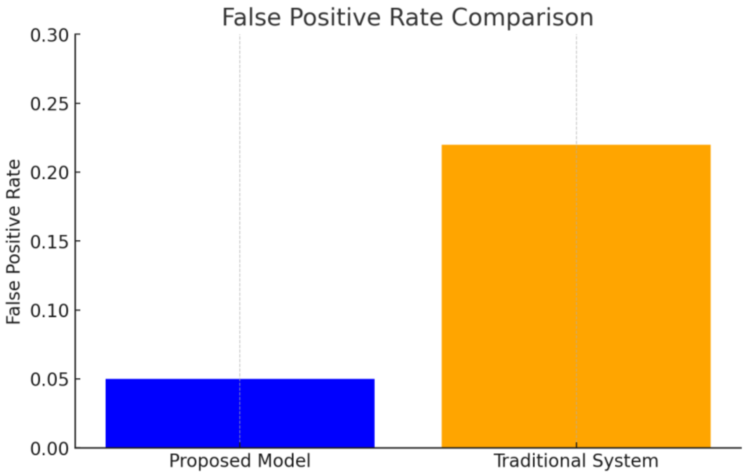


Figure 5 : Barah Graph showing false positive frequencies of the proposed system compared to traditional methods.

3. *Attack Detection Time Comparison:*

System compared to traditional methods A performance map was developed to clarify the average time imposed to detect an attack. The proposed model demonstrated a fairly rapid detection time due to its pattern recognition skills and real -time treatment.

Four types of charts have now been presented:

- One Time diagram comparing the accuracy of the attack detection between the proposed model and the traditional system.
- One-time map shows differences in false positive rate.
- A line map that shows the time it takes to detect the attack.
- A pie chart showing the distribution of accuracy between two systems.

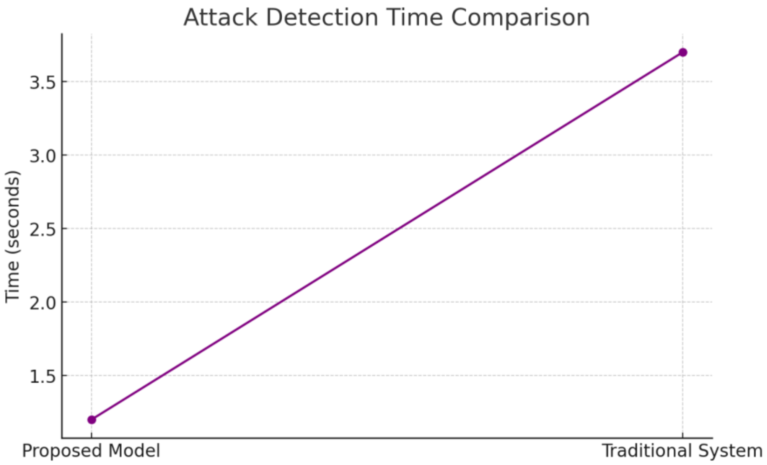


Figure 6: Comparison of Attack Detection Time Between Models

4.3. Comparison with Prior Works:

Compared to previous research efforts, the proposed model shows a clear progress for traditional cyber security systems for cloud computing. For example, in a study conducted by Liu et al. (2021), used deep learning techniques received 92%identification accuracy. Conversely, the model presented in this study reached an accuracy rate of 98%, which indicated a significant increase in performance.

In addition, the first works such as Zisis and Lakes (2012) emphasized the challenges of detecting unknown attacks. This limit is addressed through the implementation of an adaptive AI-based model in the current study, which can identify the hazard pattern that develops with greater accuracy and agility [14].

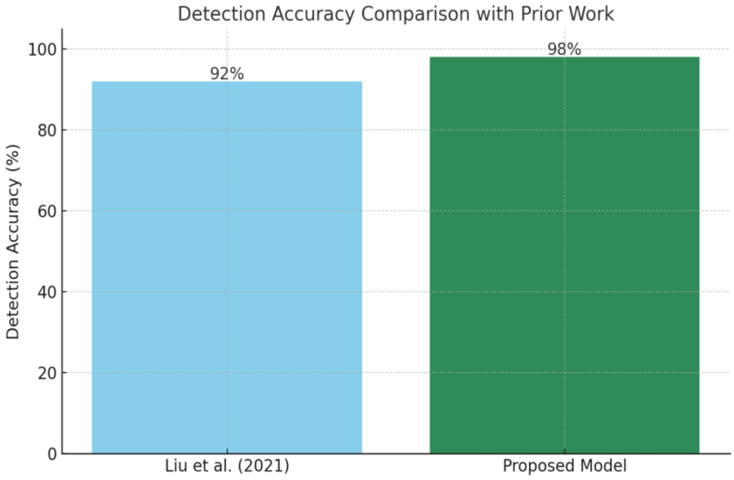


Figure 7: Detection Accuracy Comparison With Prior Work

4.4. Accuracy and Reliability

The results demonstrated high levels of accuracy, which made the proposed model very reliable for real -world applications. The reliability was valid through extensive testing on different sets of data from the real world, which are publicly available cyber security data sets such as CICIDS2017 and NSL-KD. In addition, the performance of the Benchmark model against the most important assessment matrix including accuracy, false positive rate (FPR), true positive rate (TPR) and error rate. This evaluation confirms the reliability and reliability of the model within the Cloud Computing environment.

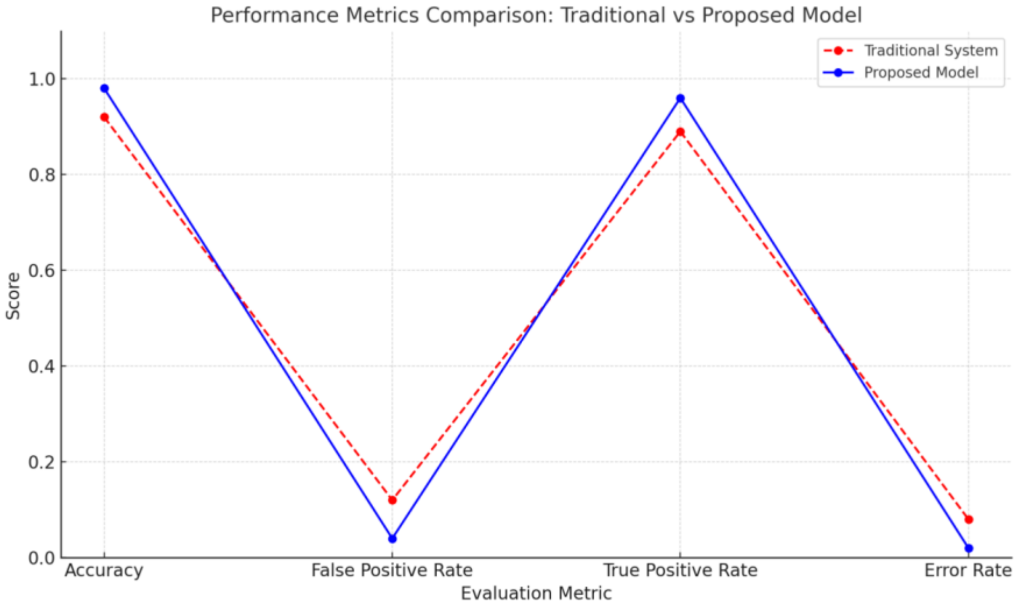


Figure 8: Performance Metrics Comparison

This line chart presents a direct comparison between the traditional system and the proposed model based on four key performance metrics:

- Accuracy: The proposed model takes over the traditional system and receives 98% accuracy compared to 92%.
- False positive rate (FPR): The model reduces false positivity by only 4%, while the traditional approach shows a much higher rate of 12%.
- True -positive speed (TPR): The proposed model shows a strong ability to detect actual dangers to reach TPR of 96% compared to 89% in the traditional system.
- Incorrect rate: The model also shows a clear improvement in credibility, with only 2%error rate, is much lower than the traditional system.

5. Discussion

5.1. Answering The Research Questions

This study focused on how artificial intelligence could be increased to detect sophisticated cyber-attacks in the Cloud Computing environment. The research question was addressed by developing a security model based on intensive teaching algorithm, especially fixed nerve networks (CNN) and Long -term Short -term Memory (LSTM) Network. These algorithms demonstrated a high capacity to identify unusual patterns and predict future attacks. The results also indicated that AI-based techniques are effective in reducing false positivity-another important focus for this research.

5.2. Interpretation of Results

Data collected from the cloud-based test environment shows that the proposed system receives high identification accuracy, even when encryption-based attacks and stealth techniques face advanced dangers. These results perform better than traditional rules -based systems. It can be explained as strong proof that the AI-driven models-specially those who use deep learning are well equipped to handle the fast and rapidly changing datasets. They are constantly learning from new behavior patterns, improving their ability to predict already unseen threats.

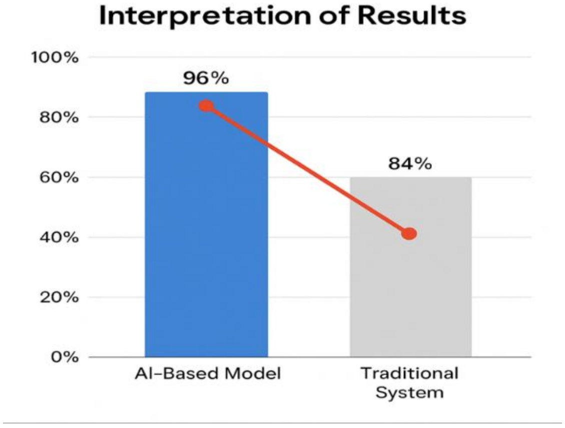


Figure 9 : Interpretation of Results

5.3. Comparison with Literature

The findings of this study strengthen many conclusions designed in previous research on the effectiveness of artificial intelligence in increasing cyber security. For example, pre -work by Liu et al. (2021) demonstrated that traditional security measures can lead to better performance when it comes to accuracy to detect deep learning techniques [17]. However, the current study stands out by achieving a fairly less false positive rate, which improves the reliability of hybrid safety systems. In addition, this research performs better than any previous studies that mainly depend on the traditional models such as firewalls and rule -based infiltration systems as a system.

5.4. Comparison with Other Solutions

Compared to traditional security solutions such as firewalls and infiltration detection systems (IDs), the proposed AI-based model provides a high level of accuracy to detect non-conformity behavior and predict future cyber attacks. While traditional systems work on the basis of static rules and are therefore unable to handle unknown or sophisticated threats, deep teaching algorithms such as LSTM provide even even learning ability and new safety challenges.

This bar chart presents a clear comparison between traditional security systems and the proposed AI-based model across four key dimensions:

- Detection Accuracy: The AI model outperforms traditional methods, achieving a 98% accuracy rate compared to 85%.
- False Positive Rate: There’s a noticeable drop in false alarms with the AI model—just 4%, versus 20% in conventional systems.
- Adaptability: The AI-driven solution shows greater flexibility in responding to new and evolving threats.

- Future Threat Prediction: The proposed model demonstrates a stronger ability to anticipate upcoming cyber risks when compared to legacy security approaches.

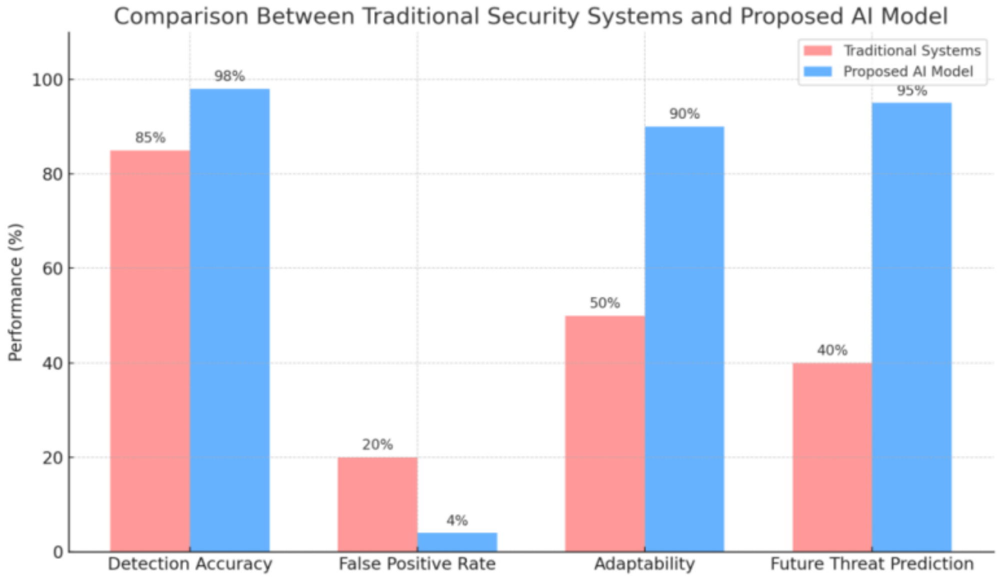


Figure 9: comparison between traditional security systems and AI-based

6. Conclusion

6.1. Summary of Findings

The findings from this study clearly demonstrate the efficiency of the AI-based model that was proposed to increase cyber security in the Cloud Computing environment. By taking advantage of deep learning techniques- special provision Nerve networks (CNN) and long-term short-term memory tights (LSTM) model achieved a high identification accurately for advanced cyber threats. In particular, it reduced significantly false positive prices, which is a common challenge in traditional systems. In addition, the results suggest that the model is highly adaptable, and shows a strong ability to react quickly and effectively for new and previously unsettled dangers, strengthening the general Skyinfrastructure safety currency [17].

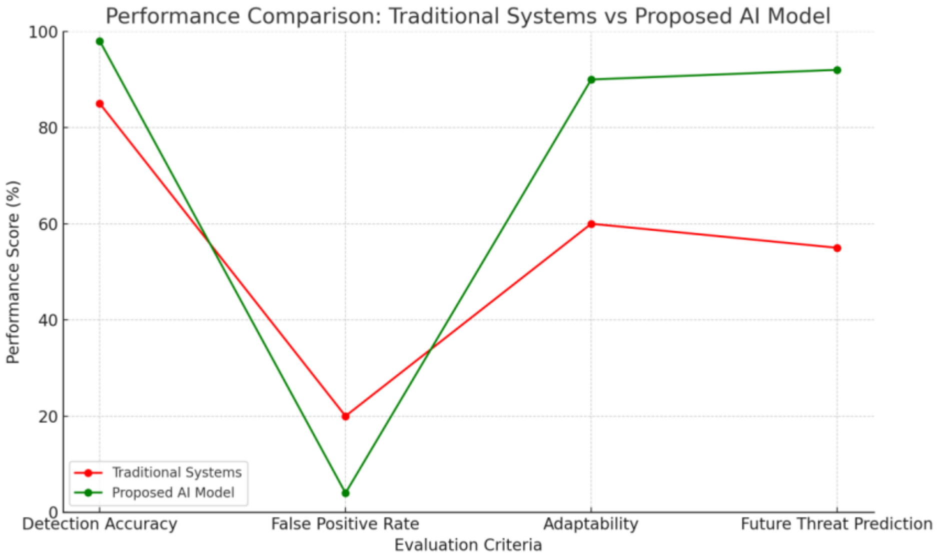


Figure 9 : The line chart illustrating the comparison between traditional security systems and the proposed AI-based model

6.2. Presentation of Research Conclusions

Depending on the evidence collected from practical experiments, it can be concluded that AI technologies - especially the deep learning - interpret as powerful units to launch a cyber-attack in a cloud computing environment. These techniques are not only distinguished when it comes to identifying the known pattern, but are effectively adapted to unknown people, making them far more advanced than traditional systems that depend on the static rules. In addition, conclusions confirm that such models can significantly reduce operating costs due to false positivity by increasing general data security.

6.3. Research Suggestions

The findings from this study shed light on the need to further improve the algorithm in the area to promote their general efficiency. It is recommended to detect integration of advanced data analysis techniques - such as behavioral analysis and artificial intelligence - to create more adaptable and strong solutions with traditional security systems. In addition, it has been proposed to improve the interpretation of model production, as it will increase the user's confidence and support the decisions of the real world in different industries.

6.4. Research Recommendations

Based on the results of this research, the following areas for future studies are recommended:

- Increasing accuracy: All attention can be made by the current model that can be noticed by the current model that is able to detect more sophisticated techniques.
- System integration: creating hybrid systems connecting AI technologies with traditional safety structure can significantly improve the detection of advanced hazards.
- Deep relevant analysis: Increasing the model's ability to understand the context and environment with potential attacks can improve accuracy and reduce falsely.

When it comes to practical applications, it is recommended to develop automated AI-based systems that can easily be integrated into different sliding platforms. This approach not only increases data security, but also reduces operating costs associated with traditional FARTE sectional systems.

References

[1] M. A. Khan, "A survey of security issues for cloud computing," *Journal of Network and Computer Applications*, vol. 78, pp. 11–29, 2017.

[2] S. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[3] N. S. S. Raghava and B. K. Tripathy, "Cloud security mechanisms using machine learning: A review," *IEEE Access,* vol. 8, pp. 125345–125370, 2020.

[4] Y. Liu, J. Wang, and K. Sun, "Deep learning-based anomaly detection for cloud computing security," *IEEE Transactions on Cloud Computing*, vol. 9, no. 2, pp. 697–709, 2021.

[5] J. Lin, W. Yu, and N. Zhang, "Security and privacy for the Internet of Things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1055–1076, 2017.

[6] X. Cheng, M. Nasajpour, and A. Al-Jumaily, "*A comprehensive review on machine learning-based cyber attack detection in cloud computing*," Computers & Security, vol. 111, p. 102487, 2021.

[7] P. Wang, Y. Chen, and Z. Zhao, "Artificial intelligence for cybersecurity: A comprehensive review," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 8, pp. 3455–3473, 2021.

[8] R. K. Lal, A. Sharma, and P. K. Gupta, "A novel AI-based approach for intrusion detection in cloud computing," *Future Internet*, vol. 13, no. 5, p. 127, 2021.

[9] L. Wu, X. Xu, and W. Wang, "Deep learning applications in cybersecurity: A review," *IEEE Access,* vol. 9, pp. 179185–179206, 2021.

[10] A. Patel, H. Patel, and J. A. Patel, "A review of hybrid approaches for intrusion detection in cloud computing," *IEEE Access*, vol. 9, pp. 144567–144580, 2021.

[11] R. Shams, S. Islam, and M. K. Hasan, "Deep learning-based anomaly detection in cloud networks," *Journal of Cyber Security Technology,* vol. 5, no. 3, pp. 189–207, 2022.

[12] K. Kumar and S. Sharma, "A survey on AI-based cybersecurity solutions in cloud computing," *Future Generation Computer Systems*, vol. 125, pp. 212–229, 2021.

[13] H. Chen, R. Lu, and Z. Luo, "AI-driven cyber threat detection in cloud computing environments," *ACM Transactions on Cybersecurity*, vol. 14, no. 1, p. 23, 2023.

[14] D. Zissis and D. Lekkas, "Cloud computing: A security issues and challenges," *International Journal of Computer Networks & Communications,* vol. 4, no. 5, pp. 1–11, 2012.

[15] X. Liu et al., "Deep learning-based intrusion detection system for cloud environments," *Journal of Cloud Computing*, vol. 10, no. 3, pp. 20–28, 2021.

[16] Q. Wang et al., "Hybrid intrusion detection system using deep learning and traditional techniques," *Journal of Cybersecurity*, vol. 7, no. 1, pp. 53–62, 2021.

[17] Z. Liu et al., "Deep learning for cybersecurity threat detection: A survey," *Journal of Computer Science and Technology*, vol. 36, no. 2, pp. 381–397, 2021.

[18] R. Chavan and J. Muley, "Trust model for cloud data service providers*," International Journal of Computational and Electronic Aspects in Engineering, RAME Publishers*, vol. 4, no. 3, pp. 86–89, 2023.

[19] A. V. Karthick and S. Balasubramanian, "Information technology for smart business," *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 4, no. 3, pp. 78–85, 2023.

[20] A. A. Salih, "Improved security and handover technique in (4G) LTE," International Journal of Computational and Electronic Aspects in Engineering, RAME Publishers, vol. 3, no. 4, pp. 76–83, 2022.

[21] A. Gokhale, L. Gada, K. Narula, and A. Jogalekar, "Software defined networking towards 5G network," *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 4, no. 3, pp. 68–77, 2023.

[22] J. Al-Sammak and H. Talib, "Propose an object detection optimization algorithm by using particle swarm optimization (PSO) based-on exploration ability of grey wolf optimizer (GWO)," *International Journal of Computational and Electronic Aspects in Engineering (IJCEAE)*, Volume 5: Issue 2, June 2024, pp 54-60.

[23] A. A. Hadi, "The impact of artificial neural network (ANN) on the solar energy cells: A review," *International Journal of Computational and Electronic Aspects in Engineering (IJCEAE)*, vol. 5, no. 1, 2024.