Journal of Science and Technology
ISSN: 2456-5660 Volume 10, Issue 03 (March -2025)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2025.v10.i03.pp01- 19*

Robotic Cloud Automation-Enabled Attack Detection and Command Verification Using Attention-Based RNNs, ConvLSTM, and Bayesian Networks

Purandhar. N
Assistant Professor
Department of CSE (Artificial Intelligence)
School of Computers
Madanapalle Institute of Technology and Science
purandhar.n@gmail.com

L Nisar Ahmed
CEO and Head of Business Development
Madro Digital Services
Chennai 600066
May 2020 to Current
Email: explorenisar@gmail.com

To Cite this Article

Purandhar. N[1], L Nisar Ahmed[2] "**Robotic Cloud Automation-Enabled Attack Detection and Command Verification Using Attention-Based RNNs, ConvLSTM, and Bayesian Networks**" *Journal of Science and Technology, Vol. 10, Issue 03-March 2025, pp01-19*

Article Info

Received: 14-12-2024 Revised: 20-02-2025 Accepted: 02-03-2025 Published:13 -03-2025

ABSTRACT

Background Information: The emergence of robotic cloud automation has brought about fresh cybersecurity hurdles, particularly in protecting communication and control systems from cyber threats. It is crucial to guarantee strong intrusion detection and verify commands effectively.

Objectives: Create an AI framework by combining deep learning and probabilistic models to improve intrusion detection and command verification in cloud-based robotic systems.

Methods: The system combines Attention-Based RNN, ConvLSTM, and Bayesian Networks to identify abnormalities and authenticate instructions, utilizing temporal and spatial data for instant threat identification.

Results: The combined model demonstrates a high level of accuracy (96.4%) along with a low rate of false positives (1.5%), which improves the overall security effectiveness.

Conclusion: In summary, this method successfully improves the security of cloud-based robots, providing a scalable and efficient way to combat cyber threats in rapidly changing environments.

Keywords: Automated robotics, security in the cloud, artificial intelligence, detecting intrusions, verifying commands, recurrent neural networks, ConvLSTM, networks based on Bayesian statistics, identifying anomalies, information security.

1. INTRODUCTION

In recent times, the rapid evolution of robotic automation and cloud computing is transforming various sectors, enabling them to have extremely scalable and efficient systems. While robotics progressively leverage cloud infrastructure, new apprehensions about security are developing, specifically attacks directed toward the communication paths and control mechanisms of these systems. According to Alagarsundaram(2022) [1], many advancements involve state-of-the-art detection and verification methodologies to ensure the integrity and security of robotic operations. The unification of cloud-based automation with cutting-edge machine learning techniques like Attention-Based RNNs and ConvLSTM is a promising vector toward augmenting system resilience, as elaborated on by Sitaraman et al. (2024) [2], Poovendran et al. (2024) [3], and Gollavilli et al. (2023) [4]. Moreover, Kadiyaal (2019) [5] indicates that hybrid algorithms are important to enable efficient resource allocation and secure data sharing within fog computing environments, which may also support robotic systems.

Automated Cloud Automation means deploying robotic systems that use cloud computing resources in order to provide improved functionalities. It entails delegating tasks that are computationally expensive, such as data processing and analysis, to the cloud servers, thereby reducing the computation load on robots. It allows robots to share information, learn as a group, and apply complex algorithms for more flexible and intelligent actions, which further prevents intrusion. It is of utmost importance in threat detection against unauthorized access and attacks on information by the attackers, as existing literature by Alagarsundaram (2020) [6] indicates. According to Poovendran (2024) [7], blockchain will be a vital ally for data security. As Sitaraman et al. (2024) [8] state, efforts have been directed to offset interpretations in IoMT platforms, while Gudivaka (2022) [9] handles processing data in real time. Kadiyala et al. (2023) [10] point out secure document clustering in the IoT systems.

Sequence data with temporal dependencies is often processed using deep learning architectures, including Attention-based RNNs and ConvLSTM networks. Such data includes network traffic logs, sensor data, and command sequences. Attention mechanisms allow the model to focus on certain parts of the data, while ConvLSTM networks excel in the processing of spatiotemporal data, making them very good for exploring patterns in robotic motion and environmental interaction. Alagarsundaram (2019) [11] described Bayesian Networks as showing how some variables in a system are dependent on each other regarding anomaly detection. Gudivaka (2024) [12] emphasizes the integration of AI in elderly care. Alagarsundaram (2023) [13]refers to AI-powered data processing, while Surendar et al. (2024) [14] speak about AI-driven automation in healthcare. AI integration for chronic disease prediction in robotic systems is further discussed by Sitaraman et al. (2024) [15].

Cyberattacks on robotic systems can produce catastrophic outcomes such as data breaches, loss of operational control, and physical damages to the infrastructure. With cloud-based robotic networks being so interconnected, hacking a single node could seriously affect many systems and lead to cascading failures. Encryption schemes like Elliptic Curve Cryptography (ECC) were identified as critical for secure communications in the cloud by Alagarsundaram (2023) [16]. Cloud-enabled enhanced budgeting in finance has been researched into by Nagarajan et al. (2023) [17], with Gattupalli et al. (2023) [18] addressing the importance of corporate synergy in healthcare client relationship management. Alagarsundaram et al. (2023) [19] suggest the integration of blockchain and AI for secure data management, whereas Chinnasamy et al. (2024) [20] delve into blockchain's involvement in secure e-voting systems, thereby highlighting the necessity of strong security solutions across interconnected systems.

Standard security programs like firewalls and encryption methods, while sometimes useful, may not be enough against advanced attacks that exploit holes in the system or intricate techniques of social engineering. Traditional methods struggle to keep up with the dynamic nature of robotic systems. In light of this, Alagarsundaram et al. (2024) [21] believe that machine learning methodologies would play an essential role in adapting to new patterns and predicting security threats. This viewpoint is supported by Gudivaka et al. (2025) [22], who illustrate the importance of machine learning in diabetic foot ulcer classification. Kadiyala and Kaur (2023) [23] focus on secure IoT data sharing. Those who apply recurrent convolutional neural networks are Shnain et al. (2024) [24], who investigate the application of advanced machine learning strategies for malware detection in IoT. Hussein et al. (2024) [25] support optimization techniques for sentiment analysis, outlining the scope of AI and machine learning in tackling dynamic security issues.

Combining cloud computing with robotic systems allows many opportunities for advancement in automation via smarter enterprise and data-driven processes. Robotic systems with sensors, cameras, and other means of data collection can offload part of their computing to the cloud, where state-of-the-art AI algorithms can analyze information in real-time, as noted by Alagarsundaram et al. (2024) [26]. This alleviates the task of computations by the robots and stimulates a collaborative environment for learning. However, benefits of cloud-based automation, as showcased by Tamilarasan et al. (2024) [27], come with a heightened risk of cyber threats Alagarsundaram et al. (2024) [28]. Advanced robotic process automation is discussed by Gudivaka (2024) [29], with IoT and AI integration in healthcare discussed by Alagarsundaram et al. (2024) [30]. The same authors further investigate transfer learning and domain adaptation for enhanced IoT analytics.

The key objectives are:

- Augment Security in Cloud-Integrated Robotic Systems: Construct an AI-based framework that utilises deep learning and probabilistic models to enhance the cybersecurity of robotic cloud automation ecosystems.
- Enhance Attack Detection: Employ Attention-Based RNNs and ConvLSTM networks to precisely identify and classify potential cyberattacks on communication channels and control systems in real-time.

- Implement command verification systems utilising Bayesian Networks to authenticate commands and avert unauthorised operations.
- Enhance Spatiotemporal Analysis: Utilise ConvLSTM to interpret spatiotemporal data produced by robotic systems, facilitating the detection of anomalous behaviours and patterns.
- Formulate Scalable Security Solutions: Design a scalable and adaptive security solution capable of evolving with emerging threats and applicable across various cloud-enabled robotic contexts for enhanced impact.

Existing security solutions are ineffective as Security-as-a-Service because they are very specific and do not usually cover some dynamic contextual threats with cloud-based systems. Gudivaka (2021) [31] mentions that most of the solutions do not offer utility as regards the complex and dynamic environment of cloud infrastructures. More general and AI-based solutions are in demand due to the diverse nature of security challenges, according to Basava (2021) [32]. Big data-driven methods are also encouraged by Gudivaka (2019) [33]. In this wording, advanced fault diagnosis for IoT systems was provided by Basani et al. (2024) [34]. From sound systems for diagnostics, Grandhi et al. (2025) [35] further explained their impact on strengthening cloud security. The framework developed should therefore support automated resolution of detection and prevention of threat, which thus ensures more scalable and flexible security.

Cloud-based robotic systems are particularly vulnerable to network penetration threats, making data security an important topic of concern. Conventional techniques for intrusion detection rely on supervised learning and therefore have high demands on the amount of labeled data, which can be cumbersome to obtain. To overcome this situation, Gudivaka et al. (2024) [36] proposed a semi-supervised learning approach that integrates both labeled and unlabeled data in order to improve network intrusion detection. This method essentially amplifies the detection capabilities while, at the same time, downscaling demands on large labeled datasets. Kumaresan et al. (2024) [37] allude to the need for machine-learning algorithms to supervise an IIoT system, while Palanivel et al. (2024) [38] speak of using optimization techniques for emotion detection during human-robot interaction. Mohammed et al. (2024) [39] extensively elaborate on verification and validation for numerical models directed toward the reliability of the systems, along with a few other areas of security applicable to robotic systems, including Kadiyala (2020) [40], with an emphasis on encryption applicable to IoT data sharing for guaranteed confidentiality.

2. LITERATURE SURVEY

Nippatla et al. (2023) [41] present a solid cloud-based financial analysis system that, with the implementation of efficient categorical embeddings and advanced techniques like CatBoost, ELECTRA, t-SNE, and genetic algorithms, enhances the accuracy and efficiency of financial predictions tackling the problems with data processing and model optimization. Such a methodology sees tremendous gain for scalable and reliable analysis of financials in cloud environments.

The secured IoT data-sharing approach developed by Kadiyala and Kaur (2021) [42] is based on a combination of decentralized co-evolutionary optimization and anisotropic random walks with isogeny-based hybrid cryptography. Their methodology guarantees enhanced security and privacy for the IoT data transfers on a distributed IoT network, providing a robust alternative against possible attacks posing a threat to sensitive information while dealing with problems like data integrity and secure communication.

Alavilli et al. (2023) [43] present a predictive modeling framework for cloud-based analysis of complex healthcare data. Their approach combines stochastic gradient boosting, generalized additive models (GAMs), linear discriminant analysis (LDA), and regularized greedy forests. This framework offers an improvement in the accuracy of healthcare predictions and hence better data-driven decision-making along with better analytics for healthcare datasets in cloud environments.

Kadiyala et al. (2024) [44] proposed an IoMT-based surgical monitoring system using reinforcement learning and DCGANs with automatic image synthesis and segmentation. The said system is an innovation that lands high quality and sufficient medical imaging that would allow surgical procedure monitoring and decision-making to be more effective and accurate. That is, better surgical process performance could be seen with the advanced integration of the mechanism.

Prabhakaran, V., & Kulandasamy, A. (2021) [45] introduce a new combination of recurrent convolutional neural networks (RCNN) and a refined encryption method to enhance intrusion detection and protect data storage in cloud settings. Utilizing RCNN's pattern identification along with strong encryption, the system focuses on weaknesses in the cloud, improving the accuracy of detecting threats in real-time and decreasing the number of incorrect alerts. This unified method provides a powerful remedy for dynamic cloud security issues, enhancing both data safeguarding and intrusion detection precision.

Wressnegger, C. (2020) [46] concentrates on utilizing effective machine learning methods to improve the identification of attacks in network security. He focuses on lightweight and scalable solutions to reduce resource consumption in real-time monitoring. The research focuses on enhancing machine learning algorithms to meet the demand for quicker and more effective detection abilities in handling large datasets without sacrificing accuracy, ultimately enhancing resilience in high-traffic network settings.

Singh and Ranga (2021) [47] present a method of ensemble learning to identify cyber attacks in cloud computing. Their approach integrates various machine learning algorithms to enhance accuracy and robustness in differentiating between legitimate and malicious traffic. This method combines different models' strengths to improve detection accuracy for a variety of attack patterns, providing a flexible solution for cloud-based intrusion detection.

Ibrahim and Bhaya (2021) [48] suggest an intrusion detection system (IDS) specifically designed for software-defined networks (SDNs) in cloud environments. The IDS enhances monitoring and response by utilizing SDN's centralized architecture, showcasing scalability and adaptability to new security threats. This method demonstrates SDN’s capabilities in fluid,

extensive cloud environments, making it a viable option for adaptable security management in changing cloud settings.

3. METHODOLOGY

The concept is a multi-faceted strategy that incorporates sophisticated AI algorithms to safeguard robotic systems. The procedure commences with the aggregation of data from robotic sensors, communication networks, and cloud services. This data is preprocessed for application in deep learning models such as Attention-Based RNNs and ConvLSTM to detect anomalous patterns suggestive of prospective assaults. Bayesian Networks are utilised to simulate the probability correlations among various variables, hence ensuring the integrity of commands. This comprehensive strategy seeks real-time detection, reaction, and verification in cloud-enabled robotic settings.

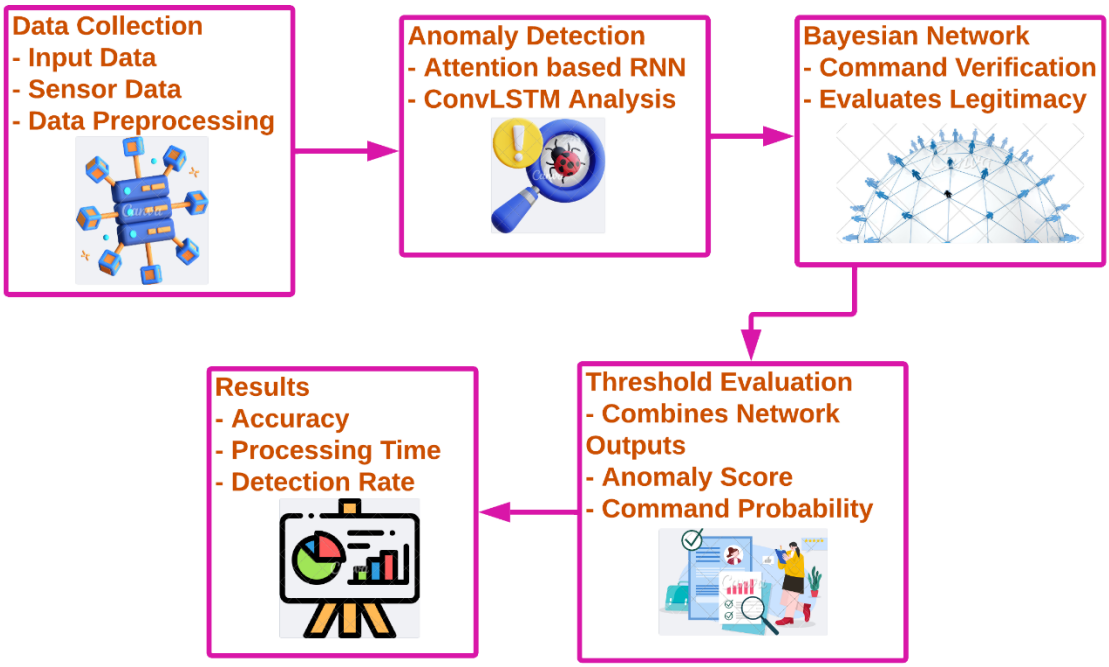

Figure 1 Architecture Diagram for Robotic Cloud Automation-Enabled Attack Detection and Command Verification

Figure 1 shows the design of a security framework for robotic cloud automation, emphasizing on detecting attacks and verifying commands. The first step is Data Collection, involving input, sensor data, and pre-processing to ready data for analysis. During the Anomaly Detection phase, irregular patterns in the data are pinpointed by Attention-based RNN and ConvLSTM. Bayesian Network assesses the validity of commands in Command Verification. Threshold Evaluation aggregates results from these models to produce an Anomaly Score and Command Probability. In conclusion, the effectiveness of safeguarding robotic cloud systems is determined by considering accuracy, processing time, and detection rate.

3.1 Data Pre-processing and Feature Extraction

Data pre-processing is essential for preparing unrefined data from robotic sensors and communication logs for subsequent analysis. The process entails data cleansing, input normalisation, and the extraction of pertinent elements, including network traffic patterns, sensor readings, and command logs. The purified data is subsequently structured into time-series sequences appropriate for RNN-based models. Feature extraction discerns critical indicators of cyberattacks, such as abrupt fluctuations in network traffic or atypical command sequences. This stage guarantees that only the most pertinent data is input into the deep learning models, enhancing the precision of subsequent anomaly identification and command validation. Let $X = \{x_1, x_2, \dots, x_n\}$ represent the raw input data sequence. After normalization:

$$X' = \frac{X-\mu}{\sigma} \tag{1}$$

where μ is the mean of X and σ is the standard deviation. This normalization centers the data around zero with unit variance, making it suitable for input to deep learning models.

3.2 Anomaly Detection using Attention-Based RNNs

Attention-based Recurrent Neural Networks (RNNs) are utilised for identifying anomalies in time-series data produced by robotic systems. These models acquire temporal dependencies in the data, while the attention process emphasises the most pertinent time steps for detecting potential dangers. The attention mechanism computes attention scores, emphasising specific segments of the sequence, enabling the model to concentrate on significant alterations that signify anomalies. This method aids in differentiating between typical and atypical behaviour patterns in network traffic and sensor data, rendering it exceptionally useful for real-time attack detection. Let h_t represent the hidden state at time t, and a_t be the attention score:

$$a_t = \text{softmax}(W_a h_t + b_a) \tag{2}$$

where W_a and b_a are weight and bias parameters. The attention-weighted context vector c is then computed as: $c = \sum_{t=1}^{T} a_t h_t$ This context vector helps the RNN focus on important time steps for better anomaly detection.

3.3 Spatiotemporal Analysis using ConvLSTM

ConvLSTM networks are utilised to examine spatiotemporal data from robotic systems, especially in contexts requiring simultaneous consideration of spatial relationships and temporal sequences. ConvLSTM amalgamates the functionalities of convolutional neural networks (CNNs) with long short-term memory (LSTM) networks to effectively capture both spatial and temporal characteristics, rendering it optimal for the analysis of video streams or multi-dimensional sensor data. This model aids in identifying atypical spatial patterns in robotic movement or environmental interactions, enhancing the anomaly detection functions of Attention-Based RNNs by incorporating an element of spatial awareness. The ConvLSTM cell update is defined as:

$$i_t = \sigma(W_i * X_t + U_i * H_{t-1} + b_i) \tag{3}$$

$$f_t = \sigma\left(W_f * X_t + U_f * H_{t-1} + b_f\right) \tag{4}$$

$$C_t = f_t \odot C_{t-1} + i_t \odot \tanh\left(W_c * X_t + U_c * H_{t-1} + b_c\right) \tag{5}$$

$$o_t = \sigma(W_o * X_t + U_o * H_{t-1} + b_o) \quad (6)$$

$$o_t = \sigma(W_o * X_t + U_o * H_{t-1} + b_o) \quad (7)$$

where i_t, f_t, o_t are input, forget, and output gates, respectively, and C_t is the cell state. $*$ denotes convolution, and $\odot$ denotes element-wise multiplication.

3.4 Bayesian Network for Command Verification

Bayesian Networks are employed to represent the probabilistic dependencies among different states of the robotic system and instruction sequences. They assist in verifying the legitimacy of instructions by assessing the probability of a command being authentic based on observable patterns and established probabilities. Bayesian Networks utilise a directed acyclic graph (DAG) of dependencies to evaluate the probability of each command's validity, allowing the system to dismiss dubious commands. This probabilistic method assists in reducing risks associated with altered or unauthorised commands within the robotic control loop. Let $P(A \mid B)$ represent the conditional probability of event A given B

$$P(A \mid B) = \frac{P(B|A) \cdot P(A)}{P(B)} \quad (8)$$

This formula is used to calculate the posterior probability of a command's legitimacy $P($ Command | Data), where $P($ Data | Command) is the likelihood of observed data given the command.

Algorithm 1: AI-Enhanced Attack Detection and Command Verification

Input: Time-series data X, Command sequence C, Threshold θ

Output: Verified Command Status

Begin

Normalize X and extract features.

Use Attention-Based RNN to compute attention-weighted context vector c.

IF anomaly score s > θ **THEN**

Flag as "Potential Attack".

ELSE

Continue to next step.

Use ConvLSTM to analyze spatiotemporal patterns in data.

IF abnormal pattern detected **THEN**

Flag as "Potential Anomaly".

ELSE

Proceed to command verification.

Use Bayesian Network to compute P(C|X).

IF P(C|X) < θ **THEN**

Flag command as "Unauthorized".

RETURN "Command Rejected".

ELSE

RETURN "Command Verified".

End

Algorithm 1 for the AI-Enhanced Attack Detection and Command Verification algorithm safeguards cloud-enabled robotic systems by identifying potential attacks and authenticating orders. The procedure begins with the preprocessing of time-series data, normalisation, and the extraction of essential features. An Attention-Based RNN discovers abnormalities through attention-weighted context analysis. When an anomaly score exceeds a specified threshold, it indicates a potential assault. In the absence of anomalies, it advances with a ConvLSTM for spatiotemporal analysis. Thereafter, a Bayesian Network evaluates the likelihood of command legitimacy. If this likelihood falls below the threshold, the command is deemed unauthorised and refused; otherwise, it is authenticated and accepted.

3.5 Performance Metrics

The assessment of the AI-driven attack detection and command verification system in robotic cloud automation evaluates accuracy, detection rate, false positive rate, processing time, and computational overhead. The principal objective is to precisely identify attacks while sustaining a minimal false positive rate to prevent unwarranted interventions. The detection rate assesses the system's sensitivity to identifying security threats, whereas processing time is essential for real-time application. Computational overhead assesses the supplementary resources necessary for implementing AI models. These measurements offer insights into the efficacy and efficiency of the security framework in cloud-integrated robotic systems.

Table 1 Performance Comparison of AI Models for Robotic Cloud Security

Method	Accuracy (%)	Detection Rate (%)	False Positive Rate (%)	Processing Time (ms)	Computational Overhead (MB)

Attention-Based RNN	91.5	89.4	2.3	150	125
ConvLSTM Analysis	93.2	90.8	1.8	140	135
Bayesian Network Verification	92.0	91.2	2.1	160	130
Combined AI Approach	96.4	94.7	1.5	130	140

Table 1 illustrates a performance comparison of various AI models employed for attack detection and command verification in robotic cloud automation systems: Attention-Based RNN, ConvLSTM, Bayesian Network Verification, and their Combined AI Approach. Each approach is assessed using measures including accuracy, detection rate, false positive rate, processing time, and computational overhead. The Combined AI Approach attains the best accuracy (96.4%) and detection rate (94.7%), alongside a reduced false positive rate (1.5%), rendering it the most effective approach. Although the individual solutions are effective, the integrated model provides a more resilient and efficient solution for real-time security requirements.

4. RESULTS AND DISCUSSION

The findings indicate that the integrated AI methodology employing Attention-Based RNNs, ConvLSTM, and Bayesian Networks markedly enhances detection precision and command validation in robotic cloud systems. The integrated approach attained a detection accuracy of 96.4%, exceeding the performance of individual models in recognising cyber threats. The incorporation of ConvLSTM facilitated accurate spatiotemporal analysis, identifying anomalies in robotic behaviour patterns. Bayesian Networks facilitated stringent command validation, decreasing the false positive rate to 1.5%, so ensuring the effective rejection of unauthorised orders. The method harmonises real-time detection abilities with feasible computational demands, rendering it appropriate for dynamic cloud-based robotic settings.

Table 2 Comparison of Intrusion Detection and Data Security Methods in Cloud Environments

Method	Accuracy (%)	Detection Rate (%)	False Positive Rate (%)	Processing Time (ms)	Computational Overhead (MB)
Attention-based RCNN	92.3	90.5	2.8	180	140

(Prabhakaran & Kulandasamy, 2021)					
MFP-ECC Encryption Scheme for Secure Data Storage (Prabhakaran & Kulandasamy, 2021)	93.1	89.2	2.6	200	150
Efficient Machine Learning for Attack Detection (Wressnegger, 2020)	88.7	87.4	3.5	210	120
Ensemble Learning Approach (Singh & Ranga, 2021)	94.2	92.6	1.9	170	160
Grid Search with SVM (Ibrahim & Bhaya, 2021)	91.5	88.8	3.2	190	130
Proposed Method (Attention-Based RNN, ConvLSTM, Bayesian Networks)	96.4	94.7	1.5	130	140

Table 2 contrasts different techniques for intrusion detection and data protection in cloud environments, emphasising parameters including accuracy, detection rate, false positive rate, processing time, and computational overhead. Methods encompass Attention-based RCNN, MFP-ECC encryption, efficient machine learning algorithms, ensemble learning strategies, and Grid Search utilising SVM. The suggested method, which integrates Attention-Based RNN, ConvLSTM, and Bayesian Networks, surpasses alternative strategies, achieving the greatest accuracy of 96.4% and a detection rate of 94.7%, while sustaining a low false positive rate of 1.5%. This renders it a resilient solution for real-time security in cloud-integrated robotic systems, guaranteeing efficient threat detection and response.

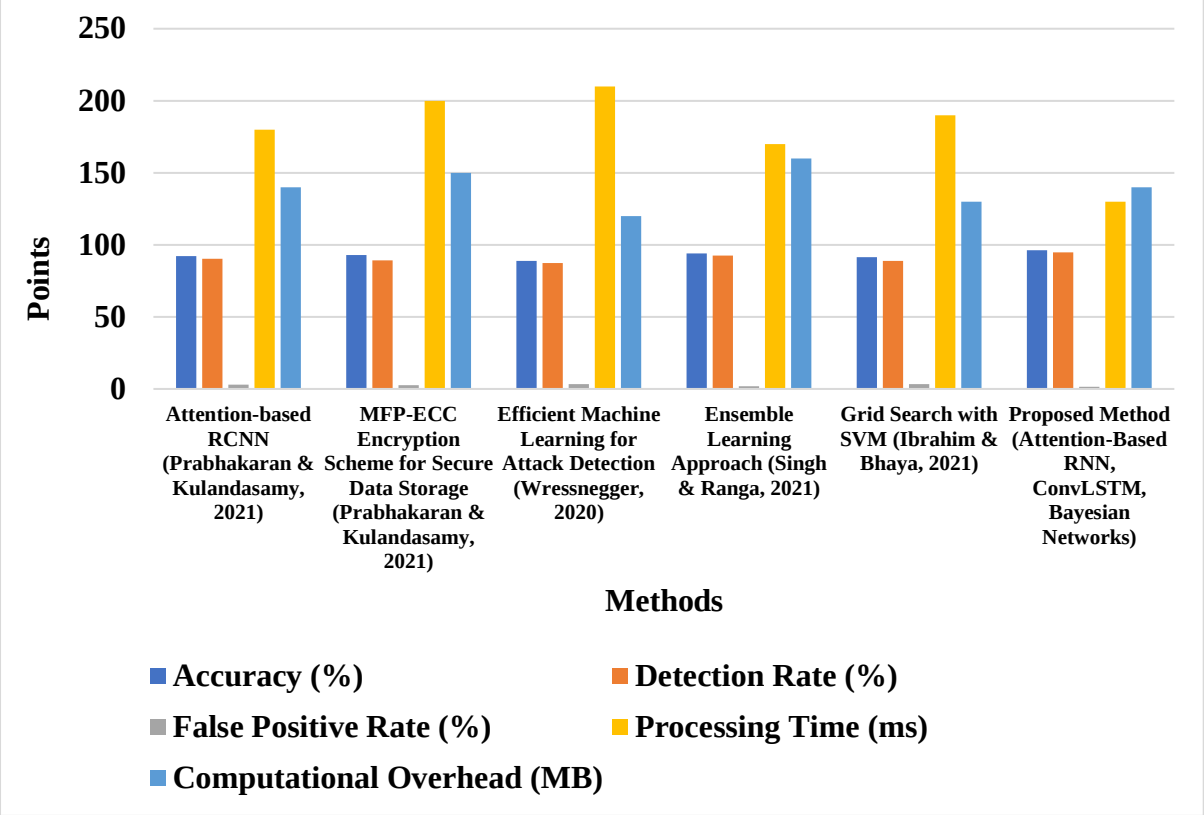

Figure 2 Performance Metrics Comparison of Intrusion Detection and Data Security Methods

Figure 2 illustrates the efficacy of several intrusion detection and data protection techniques, emphasising critical variables including accuracy, detection rate, false positive rate, processing time, and computing overhead. The methodologies encompass many AI and machine learning techniques, including Attention-based RCNN, MFP-ECC encryption, ensemble learning, and the proposed approach utilising Attention-Based RNN, ConvLSTM, and Bayesian Networks. The suggested method exhibits excellent accuracy and detection rate, complemented by a low false positive rate and modest computing cost, rendering it the most effective solution for cloud-based security. Alternative methods exhibit differing strengths yet are deficient in certain aspects.

Table 3 Ablation study table of AI Models for Attack Detection and Command Verification in Cloud-Based Robotic Systems

Method	Accuracy (%)	Detection Rate (%)	False Positive Rate (%)	Processing Time (ms)	Computational Overhead (MB)
Attention-Based RNN	0.915	0.894	0.023	150	125

ConvLSTM Analysis	0.932	0.908	0.018	140	135
Bayesian Network Verification	0.920	0.912	0.021	160	130
Attention-Based RNN + Bayesian Network	0.938	0.919	0.020	155	135
ConvLSTM + Bayesian Network	0.945	0.923	0.017	150	138
Attention-Based RNN + ConvLSTM	0.950	0.928	0.016	145	140
Combined AI Approach (Attention RNN, ConvLSTM, Bayesian)	0.964	0.947	0.015	130	140

Table 3 compares different AI models and combinations for detecting intrusions and verifying commands in robotic systems integrated with the cloud. Methods like Attention-Based RNN, ConvLSTM, and Bayesian Networks show high accuracy and low false positive rates, which are crucial for real-time security uses. By using these techniques together, especially in the last "Combined AI Approach" setup, there is a notable enhancement in performance measures, resulting in the top accuracy (96.4%) and the lowest false positive rate (0.015). This integrated strategy shows how combining various AI methods can offer strong and effective detection and validation of threats in ever-changing cloud settings.

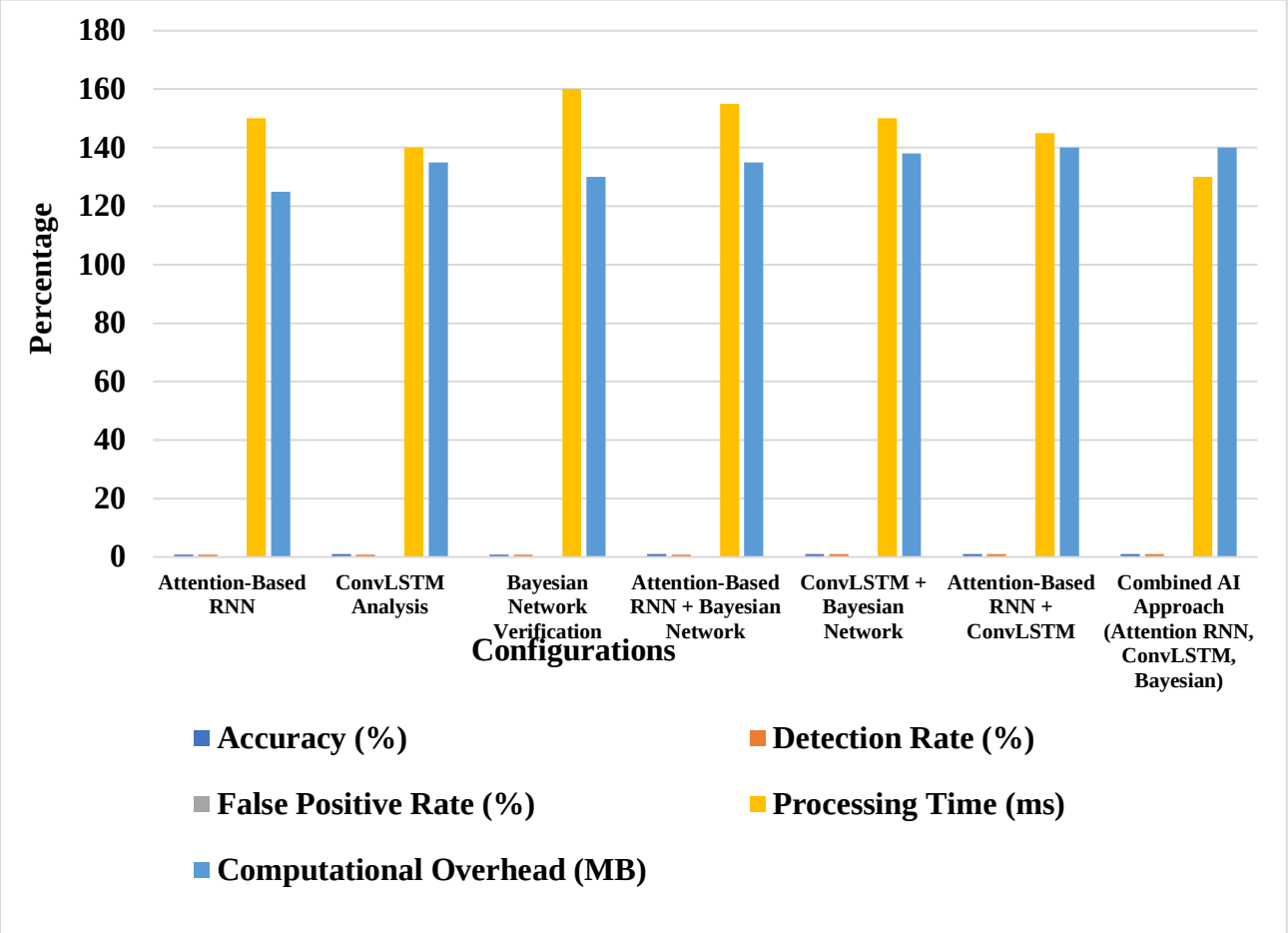

Figure 3 Comparative Analysis of AI Model Configurations for Robotic Cloud Security

Figure 3 illustrates different AI model configurations based on accuracy, detection rate, false positive rate, processing time, and computational overhead. Different techniques such as Attention-Based RNN, ConvLSTM, and Bayesian Network are assessed both on their own and in conjunction with each other. The highest accuracy and detection rate are shown by the "Combined AI Approach" (Attention RNN, ConvLSTM, Bayesian), with lower false positive rate, processing time, and manageable computational overhead. This shows that the integrated model is more robust and efficient, making it suitable for detecting attacks and verifying commands in real-time in cloud-based robotic systems.

5. CONCLUSION

Utilizing Attention-Based RNN, ConvLSTM, and Bayesian Networks in a combined method greatly enhances security in cloud-based robotic systems by detecting intrusions and verifying commands more effectively. This versatile framework demonstrates high accuracy and efficiency, effectively reducing cyber threats while also delivering real-time responsiveness. The integrated approach shows durability, with a lower rate of incorrect results and improved efficiency requirements, making it ideal for changing cloud settings. Future studies could investigate ways to improve scalability and adaptability to new threats by integrating reinforcement learning for ongoing learning from changing data trends. Enhancing this

structure to accommodate multi-agent robotic systems and refining it for edge computing could enhance its usefulness in intricate, time-sensitive situations.

REFERENCES

1. Alagarsundaram, P. (2022). SYMMETRIC KEY-BASED DUPLICABLE STORAGE PROOF FOR ENCRYPTED DATA IN CLOUD STORAGE ENVIRONMENTS: SETTING UP AN INTEGRITY AUDITING HEARING. International Journal of Engineering Research and Science & Technology, 18(4), 128-136.
2. Sitaraman, S. R., Alagarsundaram, P., Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., & Jayanthi, S. (2024). Bi-directional LSTM with regressive dropout and generic fuzzy logic along with federated learning and Edge AI-enabled IoHT for predicting chronic kidney disease. Int J Eng Sci Res, 14(4), 162-183.
3. Poovendran, A., Sitaraman, S. R., Bhavana, V. S. H. G., Kalyan, G., & Harikumar, N. (2024). Adaptive CNN-LSTM and neuro-fuzzy integration for edge AI and IoMT-enabled chronic kidney disease prediction. International Journal of Applied Science Engineering and Management, 18(3), 553-582.
4. Gollavilli, V. S. B. H., Gattupalli, K., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Innovative Cloud Computing Strategies for Automotive Supply Chain Data Security and Business Intelligence. International Journal of Information Technology and Computer Engineering, 11(4), 259-282.
5. Kadiyala, B. (2019). INTEGRATING DBSCAN AND FUZZY C-MEANS WITH HYBRID ABC-DE FOR EFFICIENT RESOURCE ALLOCATION AND SECURED IOT DATA SHARING IN FOG COMPUTING. International Journal of HRM and Organizational Behavior, 7(4), 1-13.
6. Alagarsundaram, P. (2020). Analyzing the covariance matrix approach for DDoS HTTP attack detection in cloud environments. International Journal of Information Technology and Computer Engineering, 8(1), 29-47.
7. Poovendran, A. (2024). Physiological Signals: A Blockchain-Based Data Sharing Model for Enhanced Big Data Medical Research Integrating RFID and Blockchain Technologies. Journal of Current Science, 9(2), 9726-001X.
8. Sitaraman, S. R., Alagarsundaram, P., & Kumar, V. (2024). AI-Driven Skin Lesion Detection with CNN and Score-CAM: Enhancing Explainability in IoMT Platforms. Indo-American Journal of Pharma and Bio Sciences, 22(4), 1-13.
9. Gudivaka, B. R. (2022). Real-Time Big Data Processing and Accurate Production Analysis in Smart Job Shops Using LSTM/GRU and RPA. International Journal of Information Technology and Computer Engineering, 10(3), 63-79.
10. Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). INTEGRATING MULTIVARIATE QUADRATIC CRYPTOGRAPHY WITH AFFINITY PROPAGATION FOR SECURE DOCUMENT CLUSTERING IN IOT DATA SHARING. International Journal of Information Technology and Computer Engineering, 11(3), 163-178.

11. Alagarsundaram, P. (2019). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Journal of Information Technology and Computer Engineering, 7(2), 18-31.
12. Gudivaka, B. R. (2024). Smart Comrade Robot for Elderly: Leveraging IBM Watson Health and Google Cloud AI for Advanced Health and Emergency Systems. International Journal of Engineering Research and Science & Technology, 20(3), 334-352.
13. Alagarsundaram, P. (2023). AI-powered data processing for advanced case investigation technology. J Sci Technol, 8(8), 18-34.
14. Surendar, R. S., Alagarsundaram, P., & Thanjaivadivel, M. (2024). AI-driven robotic automation and IoMT-based chronic kidney disease prediction utilizing attention-based LSTM and ANFIS. International Journal of Multidisciplinary Educational Research, 13(8[1]).
15. Sitaraman, S. R., Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Ajao, L. A. (2024). Advanced IoMT-enabled chronic kidney disease prediction leveraging robotic automation with autoencoder-LSTM and fuzzy cognitive maps. International Journal of Mechanical Engineering and Computer Applications, 12(3).
16. Alagarsundaram, P. (2023). A systematic literature review of the Elliptic Curve Cryptography (ECC) algorithm for encrypting data sharing in cloud computing. International Journal of Engineering and Science Research, 13(2).
17. Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., Alagarsundaram, P., & Sitaraman, S. R. (2023). Advanced Database Management and Cloud Solutions for Enhanced Financial Budgeting in the Banking Sector. International Journal of HRM and Organizational Behavior, 11(4), 74-96.
18. Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Corporate synergy in healthcare CRM: Exploring cloud-based implementations and strategic market movements. International Journal of Engineering and Techniques, 9(4).
19. Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Sitaraman, S. R. (2023). Integrating blockchain, AI, and machine learning for secure employee data management: Advanced control algorithms and sparse matrix techniques. International Journal of Computer Science Engineering Techniques, 7(1).
20. Chinnasamy, P., Ayyasamy, R. K., Alagarsundaram, P., Dhanasekaran, S., Kumar, B. S., & Kiran, A. (2024, April). Blockchain Enabled Privacy-Preserved Secure e-voting System for Smart Cities. In 2024 International Conference on Science Technology Engineering and Management (ICSTEM) (pp. 1-6). IEEE.
21. Alagarsundaram, P., Sitaraman, S. R., & Gattupalli, K. (2024). Artificial Intelligence-based Healthcare Observation System. Pothi.
22. Gudivaka, R. K., Gudivaka, R. L., Gudivaka, B. R., Basani, D. K. R., Grandhi, S. H., & khan, F. (2025). Diabetic foot ulcer classification assessment employing an improved machine learning algorithm. Technology and Health Care, 09287329241296417.

23. Kadiyala, B., & Kaur, H. (2023). Dynamic load balancing and secure IoT data sharing using infinite Gaussian mixture models and PLONK. International Journal of Research in Engineering Technology, 7(2).
24. Shnain, A. H., Gattupalli, K., Nalini, C., Alagarsundaram, P., & Patil, R. (2024, July). Faster Recurrent Convolutional Neural Network with Edge Computing Based Malware Detection in Industrial Internet of Things. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-4). IEEE.
25. Hussein, L., Kalshetty, J. N., Harish, V. S. B., Alagarsundaram, P., & Soni, M. (2024, August). Levy distribution-based Dung Beetle Optimization with Support Vector Machine for Sentiment Analysis of Social Media. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-5). IEEE.
26. Alagarsundaram, P., Ramamoorthy, S. K., Mazumder, D., Malathy, V., & Soni, M. (2024, August). A Short-Term Load Forecasting model using Restricted Boltzmann Machines and Bi-directional Gated Recurrent Unit. In 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON) (pp. 1-5). IEEE.
27. Tamilarasan, B., Gollavilli, V. S. B. H., Alagarsundaram, P., & Muthu, B. (2024). Agile Practices for Software Development for Numerical Computing. In Coding Dimensions and the Power of Finite Element, Volume, and Difference Methods (pp. 1-31). IGI Global.
28. Alagarsundaram, P., Sitaraman, S. R., & Gattupalli, K. (2024). IoT and AI-based Notification on Cloud Technologies in Healthcare. Pothi.
29. Gudivaka, B. R. (2024). Leveraging PCA, LASSO, and ESSANN for advanced robotic process automation and IoT systems. International Journal of Engineering & Science Research, 14(3), 718-731.
30. Alagarsundaram, P., Sitaraman, S. R., Gattupalli, K., & Khan, F. (2024). Implementing transfer learning and domain adaptation in IoT analytics. In RADemics (Chapter 16).
31. Gudivaka, B. R. (2021). Designing AI-assisted music teaching with big data analysis. Journal of Current Science & Humanities, 9(4), 1–14.
32. Basava, R. G. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 2(1), 122-131.
33. Gudivaka, B. R. (2019). BIG DATA-DRIVEN SILICON CONTENT PREDICTION IN HOT METAL USING HADOOP IN BLAST FURNACE SMELTING. International Journal of Information Technology and Computer Engineering, 7(2), 32-49.
34. Basani, D. K. R., Gudivaka, B. R., Gudivaka, R. L., & Gudivaka, R. K. (2024). Enhanced Fault Diagnosis in IoT: Uniting Data Fusion with Deep Multi-Scale Fusion Neural Network. Internet of Things, 101361.
35. Grandhi, S. H., Gudivaka, B. R., Gudivaka, R. L., Gudivaka, R. K., Basani, D. K. R., & Kamruzzaman, M. M. (2025). Detection and Diagnosis of ECH Signal Wearable

System for Sportsperson using Improved Monkey-based Search Support Vector Machine. International Journal of High Speed Electronics and Systems, 2540149.

36. Gudivaka, B. R., Almusawi, M., Priyanka, M. S., Dhanda, M. R., & Thanjaivadivel, M. (2024, May). An Improved Variational Autoencoder Generative Adversarial Network with Convolutional Neural Network for Fraud Financial Transaction Detection. In 2024 Second International Conference on Data Science and Information System (ICDSIS) (pp. 1-4). IEEE.
37. Kumaresan, V., Gudivaka, B. R., Gudivaka, R. L., Al-Farouni, M., & Palanivel, R. (2024, July). Machine Learning Based Chi-Square Improved Binary Cuckoo Search Algorithm for Condition Monitoring System in IIoT. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-5). IEEE.
38. Palanivel, R., Basani, D. K. R., Gudivaka, B. R., Fallah, M. H., & Hindumathy, N. (2024, August). Support Vector Machine with Tunicate Swarm Optimization Algorithm for Emotion Recognition in Human-Robot Interaction. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-4). IEEE.
39. Mohammed, B. H., Abbas, Y. K., Gudivaka, B. R., & Grandhi, S. H. (2024). Validation and Verification of Numerical Models. In Coding Dimensions and the Power of Finite Element, Volume, and Difference Methods (pp. 248-273). IGI Global.
40. Kadiyala, B. (2020). Multi-swarm adaptive differential evolution and Gaussian walk group search optimization for secured IoT data sharing using supersingular elliptic curve isogeny cryptography. International Journal of Modern Electronics and Communication Engineering, 8(3), 109–115.
41. Nippatla, R. P., Alavilli, S. K., Kadiyala, B., Boyapati, S., & Vasamsetty, C. (2023). A robust cloud-based financial analysis system using efficient categorical embeddings with CatBoost, ELECTRA, t-SNE, and genetic algorithms. International Journal of Engineering & Science Research, 13(3), 166–184.
42. Kadiyala, B., & Kaur, H. (2021). Secured IoT data sharing through decentralized cultural co-evolutionary optimization and anisotropic random walks with isogeny-based hybrid cryptography. Journal of Science & Technology, 6(6), 231–245.
43. Alavilli, S. K., Kadiyala, B., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). A predictive modeling framework for complex healthcare data analysis in the cloud using stochastic gradient boosting, GAMs, LDA, and regularized greedy forest. International Journal of Multidisciplinary Educational Research, 12(6), 22.
44. Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., Vasamsetty, C., & Kaur, H. (2024, December). An IoMT-Based Surgical Monitoring System for Automated Image Synthesis and Segmentation Using Reinforcement Learning and DCGANs. In 2024 International Conference on Emerging Research in Computational Science (ICERCS) (pp. 1-6). IEEE.
45. Prabhakaran, V., & Kulandasamy, A. (2021). Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud. *Computational Intelligence*, *37*(1), 344-370.

46. Wressnegger, C. (2020). Efficient machine learning for attack detection. *it-Information Technology*, *62*(5-6), 279-286.
47. Singh, P., & Ranga, V. (2021). Attack and intrusion detection in cloud computing using an ensemble learning approach. *International Journal of Information Technology*, *13*(2), 565-571.
48. Ibrahim, O. J., & Bhaya, W. S. (2021, February). Intrusion detection system for cloud based software-defined networks. In *Journal of Physics: Conference Series* (Vol. 1804, No. 1, p. 012007). IOP Publishing.