JOURNAL OF THE ROYAL LAUREATES ACADEMY

www.rlaindia.org

INTELLIGENT THREAT DETECTION IN INTERNET OF THINGS NETWORKS USING DIMENSIONALITY REDUCTION AND ADVANCED CLASSIFICATION TECHNIQUES

Ravi Govil

Research Scholar, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan

Dr. Sushma Agrawal

Research Supervisor, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan

ABSTRACT

The rapid growth of the Internet of Things (IoT) has transformed various sectors by enabling interconnected devices to communicate and exchange data seamlessly. Despite its numerous advantages, IoT networks are increasingly becoming targets of sophisticated cyberattacks due to their heterogeneous architecture, resource limitations, and large-scale deployment. Traditional security mechanisms often struggle to detect emerging and complex threats in dynamic IoT environments. Intelligent threat detection systems based on machine learning and data analytics have emerged as effective solutions for identifying malicious activities and enhancing network security. However, the high dimensionality of IoT-generated data presents challenges related to computational complexity, storage requirements, and classification accuracy. Dimensionality reduction techniques help overcome these limitations by selecting or extracting the most informative features while eliminating redundant information. This research paper explores the integration of dimensionality reduction methods and advanced classification techniques for intelligent threat detection in IoT networks. The study discusses methodologies, advantages, challenges, and future directions for developing efficient and scalable cybersecurity frameworks capable of protecting IoT ecosystems against evolving cyber threats.

Keywords: Internet of Things, Threat Detection, Dimensionality Reduction, Machine Learning, Classification Techniques, Cyber security, Intrusion Detection.

I. INTRODUCTION

The Internet of Things (IoT) represents a technological revolution that connects billions of devices, sensors, machines, and systems through internet-based communication networks. IoT applications have become widespread in healthcare, transportation, industrial automation, agriculture, smart cities, energy management, and home automation. The increasing deployment of IoT devices has significantly enhanced operational efficiency and decision-making capabilities. However, the interconnected nature of IoT networks has also expanded the attack surface for cybercriminals, making security a major concern.

IoT devices often operate with limited computational power, memory, and energy resources, which restrict the implementation of traditional security mechanisms. Moreover, the continuous generation of massive amounts of network traffic data creates additional challenges for monitoring and detecting malicious activities. Cyber attacks such as distributed denial-of-service (DDoS), malware infections, botnet attacks, spoofing, phishing, data injection, and unauthorized access pose serious threats to IoT infrastructure. Consequently, intelligent threat detection systems capable of identifying abnormal behaviors and emerging attack patterns have become essential components of modern cyber security frameworks.

Machine learning and artificial intelligence technologies have demonstrated remarkable potential in detecting cyber threats through automated pattern recognition and anomaly analysis. However, the effectiveness of these approaches often depends on the quality and dimensionality of the input data. Large numbers of features may introduce redundancy, noise, and computational overhead that reduce classification performance. Therefore, dimensionality reduction techniques combined with advanced classification algorithms provide an effective solution for improving threat detection accuracy while reducing resource consumption.

II. DIMENSIONALITY REDUCTION TECHNIQUES

Dimensionality reduction techniques play a crucial role in the development of intelligent threat detection systems for Internet of Things (IoT) networks, particularly when combined with advanced classification algorithms for cybersecurity applications. The rapid expansion of IoT ecosystems has resulted in the generation of massive volumes of network traffic data characterized by high dimensionality, complexity, and heterogeneity. IoT devices continuously exchange information through various communication protocols, producing datasets that contain hundreds of features related to network behavior, packet characteristics, communication patterns, device activities, and system events. While these extensive datasets provide valuable information for identifying malicious activities and cyber threats, they also introduce significant challenges associated with computational complexity, increased storage requirements, longer processing times, and reduced classification performance. Many features within such datasets may be redundant, irrelevant, highly correlated, or noisy, thereby negatively affecting the efficiency and accuracy of machine learning models used for intrusion detection. Dimensionality reduction techniques address these challenges by transforming high-dimensional datasets into more compact and informative representations while preserving the most relevant information required for accurate threat detection. As a result, these techniques have become fundamental components of modern IoT cybersecurity frameworks designed to provide intelligent, scalable, and resource-efficient protection against evolving cyberattacks.

Dimensionality reduction can generally be classified into two major categories: feature selection and feature extraction. Feature selection focuses on identifying and retaining the most informative attributes from the original dataset while removing irrelevant and redundant features. Unlike feature extraction, feature selection preserves the original meaning and interpretability of the selected variables. In IoT intrusion detection systems, feature selection helps reduce computational burden and improve classifier performance by focusing only on those network characteristics that significantly contribute to distinguishing normal activities from malicious behavior. Several feature selection methods have been widely applied in cybersecurity research. Filter-based approaches evaluate features independently of classification algorithms using statistical measures such as Information Gain, Chi-Square Analysis, Mutual Information,

Correlation Coefficients, Fisher Scores, and ReliefF algorithms. These techniques rank features according to their relevance and select the most important attributes for further analysis. Because filter methods are computationally efficient and scalable, they are particularly suitable for large IoT datasets containing numerous features.

Wrapper-based feature selection methods represent another important category of dimensionality reduction techniques. Unlike filter methods, wrapper approaches evaluate subsets of features by directly measuring their impact on the performance of a specific machine learning algorithm. Common wrapper techniques include Forward Selection, Backward Elimination, Recursive Feature Elimination, Sequential Feature Selection, and Genetic Algorithms. These methods iteratively search for optimal feature subsets that maximize classification accuracy while minimizing redundancy. Although wrapper methods generally achieve superior predictive performance compared to filter approaches, they require significantly greater computational resources due to repeated model training and evaluation. Nevertheless, advances in computing power and optimization algorithms have enabled the successful application of wrapper techniques in IoT threat detection systems where accuracy is a critical requirement.

Embedded feature selection methods combine the advantages of filter and wrapper approaches by integrating feature selection directly into the model training process. Machine learning algorithms such as Decision Trees, Random Forests, LASSO Regression, Gradient Boosting Machines, and XGBoost inherently evaluate feature importance during learning. These methods automatically identify the most relevant attributes while simultaneously constructing predictive models. Embedded approaches provide an effective balance between computational efficiency and classification performance, making them highly attractive for resource-constrained IoT environments. Random Forest feature importance analysis, for example, has become a widely used technique for selecting optimal network traffic attributes in intrusion detection applications due to its robustness and ability to handle complex feature interactions.

In addition to feature selection, feature extraction techniques constitute another essential branch of dimensionality reduction. Feature extraction transforms the original high-dimensional data into a new lower-dimensional feature space while preserving the most significant information. One of the most widely used feature extraction methods is Principal Component Analysis (PCA),

which projects data onto a smaller set of orthogonal components that capture the maximum variance within the dataset. PCA effectively reduces dimensionality by eliminating correlations among features and generating compact representations suitable for machine learning algorithms. In IoT cybersecurity applications, PCA has been extensively used to improve intrusion detection performance by reducing data complexity while maintaining critical attack-related information. Another popular technique is Linear Discriminant Analysis (LDA), which focuses on maximizing class separability by identifying projection directions that best distinguish different categories of network activities. LDA is particularly useful in supervised learning environments where labeled attack and normal traffic data are available.

Recent advancements in artificial intelligence have introduced sophisticated nonlinear dimensionality reduction techniques capable of capturing complex relationships within high-dimensional IoT datasets. Autoencoders, which are specialized neural network architectures, learn compressed representations of input data by encoding and reconstructing observations through hidden layers. These deep learning-based approaches can automatically identify latent features that may not be captured by traditional linear techniques. Variational Autoencoders and Deep Autoencoders have demonstrated remarkable effectiveness in reducing dimensionality while preserving important cybersecurity characteristics. Similarly, t-Distributed Stochastic Neighbor Embedding (t-SNE) and Uniform Manifold Approximation and Projection (UMAP) are advanced nonlinear techniques commonly used for data visualization and exploratory analysis. These methods preserve local and global data structures, enabling researchers to better understand attack patterns and network behavior within complex IoT environments.

The application of dimensionality reduction techniques provides numerous benefits for intelligent threat detection systems. By reducing the number of features processed by machine learning models, computational complexity is significantly lowered, resulting in faster training and prediction times. Reduced dimensionality also decreases memory consumption and storage requirements, which is particularly important for IoT devices with limited hardware resources. Furthermore, eliminating irrelevant and redundant features improves model generalization capability and reduces the risk of overfitting. Classification algorithms trained on optimized feature subsets often achieve higher accuracy, precision, recall, and F1-scores compared to

models using the full feature set. Additionally, dimensionality reduction contributes to lower false positive rates by minimizing noise and improving the clarity of underlying data patterns. These advantages collectively enhance the practicality and scalability of intrusion detection systems deployed in large-scale IoT ecosystems.

In conclusion, dimensionality reduction techniques constitute a fundamental component of intelligent threat detection frameworks designed for Internet of Things networks. Through feature selection and feature extraction methods, these techniques effectively address challenges associated with high-dimensional cybersecurity datasets while improving computational efficiency and classification performance. Traditional approaches such as Information Gain, Chi-Square Analysis, Recursive Feature Elimination, Principal Component Analysis, and Linear Discriminant Analysis continue to play important roles in optimizing intrusion detection systems. At the same time, emerging deep learning-based techniques such as Autoencoders provide powerful tools for capturing complex patterns within modern IoT environments. By integrating dimensionality reduction with advanced classification algorithms, researchers and cybersecurity professionals can develop more accurate, scalable, and resource-efficient threat detection systems capable of protecting IoT networks against increasingly sophisticated cyber threats.

III. Convolutional Neural Networks (CNN) for Intelligent Threat Detection in Internet of Things Networks

Convolutional Neural Networks (CNNs) have emerged as one of the most powerful deep learning architectures for intelligent threat detection in Internet of Things (IoT) networks due to their exceptional ability to automatically extract complex features and identify hidden patterns within large-scale cybersecurity datasets. Originally developed for image recognition and computer vision applications, CNNs have been successfully adapted for network intrusion detection, malware classification, anomaly detection, and cybersecurity analytics. The rapid growth of IoT ecosystems has led to an unprecedented increase in the volume, variety, and velocity of network traffic generated by interconnected devices. These networks continuously produce multidimensional data containing information related to communication patterns, packet transmissions, protocol behaviors, device interactions, and system events. Traditional machine learning algorithms often require extensive manual feature engineering and may struggle to

capture intricate relationships within such high-dimensional datasets. In contrast, CNNs can automatically learn hierarchical feature representations directly from raw or preprocessed network traffic data, making them highly suitable for intelligent threat detection frameworks that incorporate dimensionality reduction and advanced classification techniques. Their capability to identify both known and previously unseen attack patterns has significantly enhanced the effectiveness of modern intrusion detection systems designed for securing IoT environments.

The architecture of a Convolutional Neural Network consists of several interconnected layers that work together to extract meaningful features and perform classification tasks. The primary components include input layers, convolutional layers, activation functions, pooling layers, fully connected layers, and output layers. In cybersecurity applications, network traffic data are first transformed into structured representations suitable for CNN processing. These representations may take the form of matrices, traffic flow images, packet feature maps, or multidimensional tensors generated through preprocessing and dimensionality reduction techniques. The convolutional layers apply multiple learnable filters across the input data to detect local patterns and important characteristics associated with normal or malicious network behavior. Each filter generates feature maps that highlight specific data structures, enabling the network to learn increasingly sophisticated representations at deeper layers. This automated feature extraction capability eliminates the need for extensive manual selection of network attributes and allows CNNs to discover subtle indicators of cyber threats that may be difficult to identify using conventional methods.

One of the key advantages of CNNs in IoT threat detection is their ability to perform hierarchical learning. During the early stages of training, convolutional layers learn basic traffic characteristics such as packet distributions, protocol patterns, connection statistics, and communication behaviors. As information passes through successive layers, the network gradually constructs more abstract representations capable of distinguishing complex attack signatures and anomalous activities. This hierarchical learning process enables CNNs to effectively capture both low-level and high-level features associated with cyberattacks such as Distributed Denial-of-Service (DDoS) attacks, botnet activities, malware infections, port scanning, spoofing attacks, and unauthorized access attempts. The learned representations often

provide superior classification performance compared to traditional machine learning approaches that rely on manually engineered features.

Pooling layers constitute another important component of CNN architectures used in intelligent threat detection systems. These layers reduce the dimensionality of feature maps by summarizing local information while preserving essential characteristics. Common pooling operations include max pooling and average pooling. By reducing feature map size, pooling layers decrease computational requirements, improve processing efficiency, and reduce the risk of overfitting. This characteristic is particularly valuable in IoT environments where computational resources are often limited and real-time threat detection is required. The dimensionality reduction achieved through pooling complements external feature reduction techniques such as Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), Information Gain, and Recursive Feature Elimination, resulting in more efficient cybersecurity frameworks.

The integration of dimensionality reduction techniques with CNN models further enhances intrusion detection performance in IoT networks. High-dimensional datasets frequently contain redundant, irrelevant, or noisy features that may negatively affect learning efficiency and classification accuracy. Techniques such as PCA, Autoencoders, Chi-Square Analysis, Mutual Information, and Correlation-Based Feature Selection help eliminate unnecessary information while retaining the most informative attributes. By reducing dataset complexity before CNN training, these methods decrease computational overhead, accelerate convergence, and improve generalization performance. The resulting optimized datasets enable CNN models to focus on critical threat-related information and achieve higher detection accuracy with lower processing costs. Such optimization is essential for deploying deep learning-based intrusion detection systems within resource-constrained IoT ecosystems.

CNNs have demonstrated remarkable effectiveness in detecting a wide variety of cyber threats affecting IoT networks. Distributed Denial-of-Service attacks, one of the most common threats targeting connected devices, generate distinctive traffic patterns that CNNs can identify with high accuracy. Similarly, botnet infections often exhibit characteristic communication behaviors that can be captured through deep feature extraction processes. CNN-based intrusion detection systems have also shown strong performance in detecting malware propagation, network

reconnaissance activities, data exfiltration attempts, and insider threats. Their ability to learn complex nonlinear relationships within network traffic data enables the identification of subtle attack indicators that may evade traditional signature-based detection systems. Furthermore, CNNs can adapt to evolving attack strategies through continuous training and model updates, providing resilience against emerging cybersecurity threats.

Another significant advantage of CNN-based threat detection systems is their ability to support real-time security monitoring. Once trained, CNN models can rapidly analyze incoming network traffic and classify activities as normal or malicious with minimal latency. This capability is essential for IoT applications where immediate threat identification and response are necessary to prevent service disruptions, data breaches, and infrastructure damage. The use of optimized architectures, lightweight convolutional layers, and efficient dimensionality reduction strategies further enhances real-time performance, making CNN-based solutions practical for deployment in smart cities, industrial control systems, healthcare networks, and other critical IoT environments.

Despite their advantages, CNNs also face several challenges in cybersecurity applications. Training deep neural networks requires substantial computational resources and large labeled datasets, which may not always be readily available. Overfitting can occur when models learn dataset-specific patterns rather than generalizable threat characteristics. Additionally, deep learning models are often criticized for their limited interpretability, making it difficult for security analysts to understand the reasoning behind specific predictions. Researchers are actively addressing these limitations through explainable artificial intelligence techniques, transfer learning approaches, federated learning frameworks, and lightweight CNN architectures specifically designed for resource-constrained environments.

In conclusion, Convolutional Neural Networks represent a highly effective and intelligent approach for threat detection in Internet of Things networks. Their ability to automatically learn hierarchical feature representations, process high-dimensional network traffic data, and accurately classify complex cyber threats makes them valuable components of modern intrusion detection systems. When combined with dimensionality reduction techniques and advanced classification strategies, CNNs provide enhanced detection accuracy, reduced computational

complexity, and improved scalability for IoT cybersecurity applications. As cyber threats continue to evolve and IoT deployments expand globally, CNN-based intelligent threat detection frameworks are expected to play an increasingly important role in safeguarding connected ecosystems and ensuring secure digital infrastructures.

IV. CONCLUSION

The increasing complexity of cyber threats in Internet of Things environments necessitates intelligent and adaptive security solutions. Dimensionality reduction techniques and advanced classification algorithms offer a powerful combination for enhancing threat detection performance while minimizing computational overhead. By reducing data dimensionality and leveraging sophisticated machine learning models, intelligent intrusion detection systems can efficiently identify malicious activities and protect IoT networks from evolving cyberattacks. As IoT adoption continues to expand globally, the development of scalable, accurate, and resource-efficient threat detection frameworks will remain essential for ensuring the security and reliability of connected ecosystems.

V. REFERENCES

1. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *Military Communications and Information Systems Conference*, 1–6.

2. Aljawarneh, S., Aldwairi, M., &Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *25*, 152–160.

3. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection systems. *IEEE Access*, *7*, 41525–41550.

4. Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2020). Deep learning for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *22*(2), 1352–1393.

5. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). Deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50.

6. Verma, A., & Ranga, V. (2020). Machine learning-based intrusion detection systems for IoT applications. *Wireless Personal Communications, 111*(4), 2287–2310.

7. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system using machine learning classification techniques. *Computers, Materials & Continua, 66*(1), 803–819.

8. Khraisat, A., Gondal, I., Vamplew, P., &Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*(1), 1–22.

9. Sethi, K., Kumar, R., Prajapati, N., Bera, P., & Choudhury, T. (2020). IoT security challenges and machine learning approaches. *Journal of Information Security and Applications, 52*, 102472.

10. Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems. *Journal of Ambient Intelligence and Humanized Computing, 11*(11), 1–18.