International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(23s) 2026 pp. 348-361
https://doi.org/10.70917/ijcisim-2026-5579
Article

DEEP LEARNING-DRIVEN NETWORK SECURITY THREAT IDENTIFICATION AND MITIGATION

M. Prajwala Priyanka[1], Debasish Saha Roy[2], Jagannath Dayal Pradhan[3], Fazal Noorbasha[4], Dr. Sunil Gagare[5], C. Sathish[6]

[1]Department of Computer Science and Engineering, Cyber Security, Geethanjali College of Engineering and Technology, Hyderabad 501301, Telangana, India. Email: gprajwalapriyanka123@gmail.com ORCID:https://orcid.org/0009-0006-4360-1713
[2]Assistant Professor, Department of Computer Science and Engineering, Specialization: AI-ML and Deep Learning, JIS College of Engineering, West Bengal – 741235, India. Email: debasish.saharoy@jiscollege.ac.in
ORCID: https://orcid.org/0009-0004-1063-2906
[3]C. V. Raman Global University, Bhubaneswar, Odisha, India. Email: Jagannath2464@gmail.com
[4]Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Green Fields, Vaddeswaram, Guntur – 522302, Andhra Pradesh, India. Email: fazalnoorbasha@kluniversity.in
[5]Assistant Professor, Department of Electronics & Telecommunication Engineering, Amrutvahini College of Engineering, Sangamner, Affiliated to Savitribai Phule Pune University, Pune, Maharashtra, India. Email: sunilgagare@yahoo.co.in
[6]Associate Professor, Department of Information Technology, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India. Email: sathishinfy@gmail.com
Corresponding Author: M. Prajwala Priyanka

Abstract: The rapid evolution of cyber threats has increased the demand for intelligent and efficient approaches to network security. Deep learning has gained considerable attention in this context because of its ability to learn complex patterns and automatically extract relevant features from large and diverse cybersecurity data. The present paper examines the application of deep learning for network security threat identification and mitigation, with emphasis on the capabilities of different deep learning architectures and their suitability for cybersecurity tasks. CNN, DBN, RBM, Autoencoder, Stacked Autoencoder, RNN, LSTM, and GAN-based approaches are examined in relation to malware detection, intrusion detection, phishing and spam detection, botnet detection, and ransomware detection. The paper further considers recent developments in hybrid deep learning models, GAN-based approaches, federated learning, attention-based techniques, and Transformer-based methods for improving threat detection. Along with these developments, important challenges involving parameter optimization, evaluation metrics, datasets, model architecture, inference, and interpretability are considered. The analysis highlights the growing role of deep learning in developing automated and adaptive security mechanisms and emphasizes the need for reliable datasets, suitable model selection, improved generalization, and explainable approaches for effective cybersecurity applications.
Keywords: Deep Learning, Network Security, Cybersecurity, Threat Detection, Malware Detection, Intrusion Detection

1. INTRODUCTION

Network security has become a fundamental requirement for protecting modern digital infrastructure from unauthorized access, data breaches, malicious activities, and service disruptions. It involves the implementation of technologies, policies, and procedures designed to maintain the confidentiality, integrity, and availability of information transmitted across networks. The rapid adoption of cloud computing, Internet of Things (IoT) devices, mobile technologies, online services, and interconnected systems has significantly increased the scale and complexity of network environments. As organizations increasingly depend on digital networks for communication, business operations, financial transactions, and information exchange, the potential consequences of security breaches have

also become more serious. Conventional security mechanisms, including firewalls, antivirus programs, access-control systems, and signature-based detection techniques, continue to provide essential protection; however, their dependence on predefined rules and known attack patterns can limit their effectiveness against sophisticated and continuously evolving cyber threats.[1]

The cybersecurity landscape has experienced a substantial increase in the frequency, diversity, and sophistication of cyberattacks. Threats such as malware, ransomware, phishing, botnet activities, denial-of-service attacks, network intrusions, and unauthorized access can target individual users as well as organizational and critical infrastructure systems. Modern attackers increasingly employ automated tools, encryption, obfuscation, polymorphic techniques, social engineering, and rapidly changing attack strategies to avoid conventional detection mechanisms. In addition, the growing number of connected devices and distributed network environments creates a larger attack surface and generates enormous volumes of security-related data. Security systems must therefore analyse network traffic and system activities continuously while distinguishing legitimate behaviour from malicious behaviour. These developments demonstrate the limitations of relying solely on traditional security approaches and emphasize the importance of intelligent methods capable of adapting to changing threat patterns.[2]

Deep learning has emerged as a significant artificial intelligence-based approach for addressing several challenges in cybersecurity. Unlike conventional machine-learning methods that frequently require manually engineered features, deep learning models can automatically learn complex and hierarchical representations from large and heterogeneous datasets. This capability allows deep learning techniques to analyse different forms of cybersecurity information, including network traffic, packet characteristics, system logs, executable files, URLs, emails, and user behaviour. Various architectures provide specific advantages for different security tasks. Convolutional Neural Networks (CNNs) can identify important local and structural patterns, while Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks can model sequential and temporal relationships in network activities. Autoencoders can learn representations of normal behaviour for anomaly detection, whereas Generative Adversarial Networks (GANs) can generate additional data and address certain data imbalance problems. More recently, attention-based and Transformer architectures have provided additional capabilities for capturing complex and long-range relationships within cybersecurity data.[3]

The increasing complexity of cyber threats creates a strong need for deep learning-based threat detection and mitigation mechanisms that can provide accurate, adaptive, and timely security responses. Effective cybersecurity systems should not only identify previously known attacks but should also have the capability to recognize abnormal patterns associated with emerging and previously unseen threats. Deep learning can contribute to this objective by learning from historical security data and continuously analysing new observations to identify suspicious behaviour. Its application across malware detection, intrusion detection, phishing and spam detection, botnet identification, and ransomware detection demonstrates its broad potential for cybersecurity. Furthermore, combining deep learning with hybrid architectures, attention mechanisms, federated learning, and other advanced approaches can improve adaptability, privacy, and detection capability. Therefore, the development of deep learning-driven network security systems represents an important direction for strengthening threat identification and mitigation in increasingly complex and dynamic digital environments.

2. LITERATURE REVIEW

Khalaf et,al (2025) Protection of infrastructure is becoming increasingly demanding, and the sophistication and severity of cyber threats are increasing daily. Traditional threat detection techniques cannot match the ever-evolving nature of cyber threats, which increases the number of false positives and attack misses. AI-driven methods address these shortfalls via the use of advanced learning algorithms to detect and respond to newly discovered threats in real time. They are largely static rule-based or signature-based attacks, and they do not perform effectively against zero-day attacks and highly organized, advanced attacks. Given the critical need to protect digital infrastructures such as energy, transport, and communications from destruction, which threatens security and operational integrity, an adaptive means for real-time and accurate threat detection must evolve. This research aims to determine the optimum

method for designing and testing an AI-based real-time threat detection system that is suitable for use in critical infrastructure environments.[4]

Aljaramiz et,al (2025) Cybersecurity threats in the healthcare industry, particularly in Saudi Arabia, pose significant challenges. As institutions adopt digital technologies under Saudi Arabia's Vision 2030, vulnerabilities to ransomware, phishing, and data breaches escalate. This paper investigates the role of Bidirectional Long Short-Term Memory (Bi-LSTM) and Convolutional Neural Networks (CNN) models in enhancing threat detection and mitigation strategies tailored to Saudi Arabia's unique healthcare requirements. The proposed model achieves 94 % accuracy, with high precision, recall, and F1-score, confirming its reliability in identifying cyber threats. Additionally, we introduce a hybrid deep learning architecture that integrates real-time threat monitoring and adaptive mitigation strategies. Experimental results demonstrate its effectiveness in safeguarding sensitive health care data and ensuring service continuity. These findings underscore the potential of deep learning in strengthening cybersecurity defenses in critical sectors.[5]

Afraji et,al (2025) The kind of cyber threat prevalent and most dangerous to networked systems is the Distributed Denial of Service (DDoS), especially with expanded connection of Internet of Things (IoT) devices. This article categorizes DDoS attacks into three primary types: volumetric, protocol based and application layer of cyber attacks. It discusses the application of security threats that arise from the use of the DL models, accusing recently introduced ideas and stressing pitfalls: the issues of data and methods scarcity. There is the same need for the greater use of explainable and transparent AI to improve confidence in such security systems as is noted in the review. It also reveals that present detection performance is constrained and frequently obstructed by the poor quality of the datasets. The future work is proposed to build superior datasets and use accurate algorithm to improve the security models. This paper focuses on explainability as a way of making the AI model creation process and any consequent decisions explainable and transparent. The use of deep learning enhances the capability of cybersecurity in handling DDoS attacks and preventing or controlling them. But it has to be a part of a more large-scope platform, based on multiple types of longitudinal or cross-sectional data combined with high efficiency, explainable AI. The article ends with call to proceed with studying and advancing the AI application in response to new threats, and make the most of it to enhance protection of the contemporary networked environment.[6]

Abughali et,al (2024) Due to the substantial interdependencies between water and energy infrastructures, the water-energy nexus (WEN) is regarded as an appealing focal point for potential malicious intruders, particularly in the context of smart cities. Driven by the increasing vulnerability of these critical infrastructures to sophisticated cyber-attacks and the lack of comprehensive protection strategies, this study aims to address these challenges. This paper introduces a pioneering deep learning-driven framework for detecting, locating, and mitigating stealthy false data injection attacks (FDIAs) targeting electrical and water networks within the WEN. The proposed framework, which leverages two lightweight deep learning models, is designed to accurately detect and locate cyber-attacks in real-time while effectively mitigating their impact, thereby enhancing the operational resilience and security of the WEN. These models undergo training and testing using a wide range of challenging cyber-attack scenarios, including Pulse, Random, Ramp, and Scaling attacks, to ascertain their efficacy and resilience.[7]

Kumar et,al (2021) The recent burgeoning of Internet of Things (IoT) technologies in the maritime industry is successfully digitalizing Maritime Transportation Systems (MTS). In IoT-enabled MTS, the smart maritime objects, infrastructure associated with ship or port communicate wirelessly using an open channel Internet. The intercommunication and incorporation of heterogeneous technologies in IoT-enabled MTS brings opportunities not only for the industries that embrace it, but also for cyber-criminals. Cyber Threat Intelligence (CTI) is an effective security strategy that uses artificial intelligence models to understand cyber-attacks and can protect data of IoT-enabled MTS proficiently. Unsurprisingly, most of the existing CTI-based solutions uses manual analysis to extract relevant threat information, and has low detection and high false alarm rate. Therefore, to tackle aforementioned challenges, an automated framework called DLTIF is developed for modeling cyber threat intelligence and identifying threat types.[8]

Thamilarasu et,al (2019) Cyber-attacks on the Internet of Things (IoT) are growing at an alarming rate as devices, applications, and communication networks are becoming increasingly connected and integrated. When attacks on IoT networks go undetected for longer periods, it affects availability of critical systems for end users, increases the number of data breaches and identity theft, drives up the costs and impacts the revenue. It is imperative to detect attacks on IoT systems in near real time to provide effective security and defense. In this paper, we develop an intelligent intrusion-detection system tailored to the IoT environment. Specifically, we use a deep-learning algorithm to detect malicious traffic in IoT networks. The detection solution provides security as a service and facilitates interoperability between various network communication protocols used in IoT. We evaluate our proposed detection framework using both real-network traces for providing a proof of concept, and using simulation for providing evidence of its scalability. Our experimental results confirm that the proposed intrusion-detection system can detect real-world intrusions effectively.[9]

Research gap: The reviewed studies demonstrate the effectiveness of deep learning in detecting cyber threats across critical infrastructure, healthcare, IoT, maritime transportation, and smart-city environments; however, most existing research focuses on specific attack types, sectors, or individual deep learning models. Limited attention has been given to a comprehensive examination of different deep learning architectures, including CNN, DBN, Autoencoder, RNN, LSTM, GAN, attention-based, and Transformer models, across multiple cybersecurity applications. Moreover, challenges related to zero-day attacks, dataset quality, class imbalance, model generalization, computational complexity, and explainability continue to restrict practical deployment. Existing studies also tend to emphasize threat detection rather than integrating detection with effective and timely mitigation. Therefore, a research gap exists in developing a broader and theoretically integrated perspective on deep learning-driven network security that connects threat identification with mitigation while considering different attack categories, model capabilities, data requirements, and practical deployment challenges. The present paper addresses this gap by examining major deep learning methods, their applications in malware, intrusion, phishing, botnet, and ransomware detection, recent technological advances, and the key challenges that influence the development of adaptive, accurate, robust, and explainable cybersecurity systems.

3. OVERVIEW OF DEEP LEARNING METHODS

Deep learning (DL) is a branch of machine learning that uses neural networks with multiple processing layers to learn complex patterns from data. Unlike conventional machine-learning methods that often require manually engineered features, DL models can automatically learn relevant features from large and complex datasets. This capability makes DL particularly useful in cybersecurity, where network traffic, system logs, malware, and other security data are often high-dimensional and heterogeneous. Major DL architectures used in cybersecurity include Convolutional Neural Networks (CNNs), Deep Belief Networks (DBNs), Autoencoders (AEs), Recurrent Neural Networks (RNNs), Generative Adversarial Networks (GANs), and hybrid models.

Convolutional Neural Networks: Convolutional Neural Networks (CNNs) are deep-learning architectures designed to extract spatial and local patterns from structured data. A typical CNN consists of an input layer, convolutional layers, pooling layers, and fully connected layers. Convolutional layers use learnable filters to generate feature maps, while pooling layers reduce their dimensions and computational requirements. Fully connected layers then use the extracted features for classification or prediction. [10]

In cybersecurity, CNNs are used for malware classification, intrusion detection, and malicious traffic identification. Their ability to automatically extract hierarchical features makes them suitable for identifying complex patterns associated with cyber threats.

Deep Belief Networks: Deep Belief Networks (DBNs) are probabilistic deep-learning models that combine unsupervised learning with hierarchical feature representation. A DBN is generally constructed by stacking multiple Restricted Boltzmann Machines (RBMs), with each layer learning a representation from the output of the preceding layer.

DBNs can handle high-dimensional cybersecurity data and learn increasingly abstract features through layer-wise training. They can therefore be applied to intrusion detection, security-event classification, and abnormal behaviour identification.[11]

A Restricted Boltzmann Machine (RBM) consists of visible and hidden layers. The visible units receive the input data, while the hidden units learn abstract representations. The energy function of an RBM is given by:

$$E(h) = -\sum_{i} \quad a_i v_i - \sum_{j} \quad b_j h_j - \sum_{i,j} \quad v_i h_j w_{ij} \quad (1)$$

where $a_i$and $b_j$are the visible and hidden biases, respectively, and w_{ij}represents the weight connecting the i^{th}visible unit to the j^{th}hidden unit.

The joint probability distribution is expressed as:

$$P(h) = \frac{e^{-E(h)}}{Z} \quad (2)$$

where $Z$is the partition function. RBMs are commonly trained using contrastive divergence, and their learned representations can be used successively to construct a DBN.

Autoencoders: Autoencoders (AEs) are neural networks designed to learn compact representations of input data and reconstruct the original input. They consist of an encoder and a decoder. The encoder transforms input Xinto a latent representation Z, while the decoder reconstructs the input.

The encoding operation is represented as:

$$Z = f(WX + b) \quad (3)$$

where $f$is the activation function, $W$is the weight matrix, and $b$is the bias vector.

The decoder is expressed as:

$$X' = g(W'Z + b') \quad (4)$$

where $g$is the decoder activation function, $W'$is the decoder weight matrix, and $b'$is the decoder bias.

The reconstruction error can be measured using Mean Squared Error (MSE):

$$L(X') = (X - X')^2 \quad (5)$$

In cybersecurity, autoencoders are widely useful for feature extraction, dimensionality reduction, and anomaly detection. Higher reconstruction errors can indicate unusual or potentially malicious network behaviour.[12]

Stacked Autoencoders (SAEs) consist of multiple autoencoder layers arranged sequentially. The output of one layer becomes the input to the next, allowing the model to learn increasingly complex representations. The layers can initially be trained using unsupervised learning and subsequently fine-tuned for the target task. SAEs are useful for feature extraction, anomaly detection, and intrusion detection.

Recurrent Neural Networks: Recurrent Neural Networks (RNNs) are designed to process sequential and time-dependent data. They maintain a hidden state that carries information from previous observations, making them suitable for network traffic, system logs, and user-activity sequences.[13]

The hidden state at time $t$is represented as:

$$h_t = f(x_t) \quad (6)$$

where $h_t$is the current hidden state, $h_{t-1}$is the previous hidden state, and $x_t$is the current input.

The output can be expressed as:

$$y_t = W_y h_t \quad (7)$$

where $W_y$represents the output weight matrix. RNNs can therefore capture temporal relationships and sequential patterns associated with cyber threats.

Long Short-Term Memory (LSTM) is a specialized RNN architecture developed to overcome the vanishing-gradient problem. It uses a memory cell and three gates: input, forget, and output gates. These gates regulate the information stored, discarded, and transferred through the network.

LSTM models are useful in cybersecurity for sequential intrusion detection, network traffic monitoring, behavioural analysis, and identification of evolving attack patterns.

Generative Adversarial Networks: Generative Adversarial Networks (GANs) consist of two competing neural networks: a generator and a discriminator.[14] The generator creates synthetic samples, while the discriminator attempts to distinguish generated samples from real ones.

The minimax objective of GANs is given by:

$$\min_{\theta_g}\max_{\theta_d} E_{x\sim p_{data}(x)}\left[log\ log\ D_{\theta_d}(x)\right] + E_{z\sim p(z)}\left[log\left(1 - D_{\theta_d}\left(G_{\theta_g}(z)\right)\right)\right] \quad (8)$$

where $\theta_g$and $\theta_d$represent the parameters of the generator and discriminator, respectively. $p_{data}(x)$represents the real-data distribution, $z$is a noise vector, and $G_{\theta_g}(z)$represents the generated sample.

In cybersecurity, GANs can generate synthetic security data, address class imbalance, and augment datasets containing limited attack samples. They can also support the development of more robust threat-detection models.

Hybrid and Ensemble Deep Learning Models: Hybrid and ensemble models combine two or more deep-learning architectures to exploit their complementary strengths. For example, CNN-LSTM models can combine CNN-based feature extraction with LSTM-based temporal analysis. Similarly, autoencoders can be combined with classifiers for feature extraction and threat classification.

Such models are particularly useful for cybersecurity because network data may contain both spatial and temporal characteristics. Hybrid approaches can therefore improve feature representation and support more effective intrusion, malware, and anomaly detection.

Comparative Characteristics of Different DL architectures provide different capabilities for cybersecurity applications. CNNs are effective for pattern and feature extraction, DBNs support hierarchical representation learning, autoencoders are useful for reconstruction and anomaly detection, RNNs and LSTMs handle sequential data, and GANs support synthetic data generation. Hybrid models combine these capabilities to address complex security problems.

Table 1. Comparative Characteristics of Major Deep Learning Methods in Cybersecurity

Deep Learning Method	Primary Capability	Major Cybersecurity Applications	Key Advantage
CNN	Feature and pattern extraction	Malware and intrusion detection	Automatic feature learning

DBN	Hierarchical representation learning	Intrusion detection and classification	Learns abstract features
RBM	Probabilistic feature learning	Feature learning and intrusion detection	Compact representation
Autoencoder	Reconstruction and feature learning	Anomaly detection	Detects abnormal patterns
Stacked Autoencoder	Hierarchical feature extraction	Intrusion and anomaly detection	Learns multiple feature levels
RNN	Sequential learning	Traffic and behaviour analysis	Captures temporal patterns
LSTM	Long-term sequence learning	Intrusion detection and attack analysis	Retains long-term information
GAN	Data generation	Data augmentation and imbalance handling	Generates synthetic samples
Hybrid/Ensemble DL	Combined learning	Advanced threat detection	Combines strengths of multiple models

Overall, these deep-learning architectures provide complementary capabilities for cybersecurity threat identification and mitigation. Their effectiveness depends on the type of security data, nature of the threat, detection objective, and computational requirements of the application.

4. APPLICATIONS OF DEEP LEARNING TECHNOLOGY IN THE FIELD OF CYBERSECURITY

The increasing digitization of modern systems has resulted in the rapid growth of cybersecurity threats across computers, mobile devices, communication networks, financial services, and online platforms. Traditional machine-learning algorithms such as Support Vector Machine (SVM), Decision Tree (DT), and Naïve Bayes (NB) have been widely used for cybersecurity.[15] However, their effectiveness may be limited when processing large-scale and heterogeneous security data. Deep learning (DL) addresses these limitations by automatically extracting high-level features and learning complex patterns from large datasets. Therefore, DL has become useful for malware detection, intrusion detection, phishing and spam detection, botnet detection, and ransomware detection.

Malware Detection

Malware is malicious software designed to damage systems, steal information, or gain unauthorized access. Common types include worms, Trojan horses, spyware, and adware. Deep learning can detect malware using static, dynamic, and hybrid analysis. Static analysis examines code, metadata, and opcode sequences, while dynamic analysis observes program behaviour during execution. Hybrid analysis combines both approaches.[16] DL models automatically learn meaningful patterns from malware samples and distinguish malicious software from legitimate programs.

PC-Based Malware Detection: Traditional signature-based detection identifies malware using known signatures but can be bypassed through encryption and code obfuscation. Deep learning can instead learn malicious patterns directly from data. Features such as API calls, opcode sequences, code structures, and behavioural characteristics can be analysed to classify software as malicious or benign. This also helps in identifying modified and previously unseen malware.

Android-Based Malware Detection: Android devices are important targets because they store sensitive personal and financial information. Malware may use code obfuscation, dynamic payloads, and drive-by downloads to compromise devices. Deep learning models can analyse application code, behaviour, system calls, API calls, network communication, and runtime activities to identify malicious applications.

Intrusion Detection

Intrusion detection identifies unauthorized or malicious activities in computer systems and networks. Intrusion Detection Systems (IDS) commonly use signature-based and anomaly-based approaches.[17] Deep learning improves intrusion detection by automatically extracting features from network traffic and learning complex patterns associated with malicious activities.

Signature-Based Detection: Signature-based detection compares network activities with previously identified attack signatures. Deep learning models can learn from large datasets of known attacks and extract features such as packet headers, payload characteristics, flow statistics, and communication patterns. These learned representations can help identify known malicious activities and reduce false-positive detections.

Anomaly Detection: Anomaly detection identifies activities that differ from normal network behaviour. Unlike signature-based approaches, it can support the detection of unknown and zero-day attacks. RNNs, LSTMs, and Autoencoders (AEs) can learn normal traffic patterns and identify unusual activities. This makes DL-based anomaly detection suitable for changing network environments.

Phishing and Spam Detection

Deep learning is widely used to detect phishing and spam across email, websites, SMS, and social media. DL models can automatically analyse textual, structural, behavioural, and metadata features to distinguish legitimate communication from suspicious content.

Phishing Detection: Phishing attacks impersonate legitimate sources to obtain sensitive information from users. Deep learning models can analyse email content, headers, metadata, URLs, embedded links, website content, and sender characteristics. These features help identify suspicious communication and distinguish phishing attempts from legitimate sources.

Spam Detection: Spam consists of unwanted messages distributed through email, social media, and text messaging. Deep learning models can learn from large collections of spam and legitimate messages. Features such as textual content, headers, metadata, links, and sender information can be used to classify messages as spam or non-spam.

Botnet Detection

A botnet is a network of compromised devices controlled by an attacker for malicious activities such as DDoS attacks, spam distribution, and malware propagation. Deep learning models can analyse network traffic, communication patterns, packet characteristics, and device behaviour to identify botnet activity. CNNs, RNNs, LSTMs, and Autoencoders can help detect abnormal communication and compromised devices.

Ransomware Detection

Ransomware is malware that restricts access to data or systems, commonly by encrypting files and demanding payment. Deep learning can detect ransomware by analysing file activities, system calls, API calls, process behaviour, and network traffic. By learning ransomware-related behavioural patterns, DL models can identify suspicious activities even when the specific ransomware signature is unknown.

Table 2. Applications of Deep Learning Technology in Cybersecurity

Application Area	Description
Malware Detection	Identifies malicious software using code, API calls, opcode sequences, and behavioural features.
PC-Based Malware Detection	Detects malicious computer programs using static, dynamic, and behavioural characteristics.

Android-Based Malware Detection	Analyses application behaviour, code, system calls, and network activities.
Intrusion Detection	Identifies unauthorized and malicious network activities.
Signature-Based Detection	Detects known attacks using learned attack patterns and network features.
Anomaly Detection	Identifies deviations from normal behaviour and supports unknown attack detection.
Phishing Detection	Analyses emails, websites, URLs, links, and metadata to identify phishing.
Spam Detection	Classifies messages as spam or legitimate using textual and metadata features.
Botnet Detection	Identifies compromised devices and malicious communication patterns.
Ransomware Detection	Detects ransomware through suspicious file, system, process, and network behaviour.

Overall, deep learning provides effective capabilities for identifying a wide range of cybersecurity threats. Its ability to automatically learn complex patterns makes it useful for malware, intrusion, phishing, spam, botnet, and ransomware detection.

5. RECENT ADVANCES IN DEEP LEARNING-BASED THREAT DETECTION

Recent advances in deep learning have shifted cybersecurity research from conventional single-model detection toward hybrid architectures, generative models, federated learning, attention mechanisms, transformer-based models, and cross-dataset evaluation. Publicly available datasets are increasingly used to evaluate these approaches, allowing researchers to compare models under common experimental conditions. Important datasets include CIC-IDS2017 for network intrusion detection, CIC-MalMem-2022 for malware memory analysis, and publicly collected phishing URL datasets. These developments have improved the ability of DL models to address complex, imbalanced, evolving, and previously unseen cyber threats.

Hybrid Deep Learning for Intrusion Detection: Hybrid deep-learning architectures combine the strengths of different neural networks to improve threat detection. CNNs can extract local and statistical patterns, whereas RNNs and LSTMs can learn temporal dependencies in network traffic. Recent research has therefore explored combinations of CNNs, recurrent networks, attention mechanisms, and other architectures for intrusion detection. Such models are particularly useful when network traffic contains both spatial and sequential characteristics. Public benchmark datasets such as CIC-IDS2017 and other network intrusion datasets are commonly used to evaluate these approaches.

GAN-Based Data Augmentation for Threat Detection: Data imbalance is a major problem in cybersecurity because normal traffic often contains substantially more samples than individual attack categories. Andresini et al. [18] proposed **MAGNETO**, which combines two-dimensional representations of network flows, GAN-based data augmentation, and a CNN for intrusion detection. The GAN generates additional samples representing potential attacks, helping the CNN learn from minority attack classes. The approach was evaluated on four benchmark datasets and demonstrated the usefulness of GAN-based augmentation for improving intrusion detection under imbalanced conditions.

5.3 Federated Deep Learning for Privacy-Preserving Security

Federated learning has emerged as an important advancement because cybersecurity data may contain sensitive information that cannot easily be transferred to a central server. Tabassum et al. [19] proposed **FEDGAN-IDS**, which combines federated learning and GAN-based data augmentation for intrusion detection in smart IoT environments. The approach distributes model training across IoT devices while using GANs to address data imbalance. The study

considered smart-home, healthcare, and smart-city environments and showed the potential of combining privacy-preserving learning with deep-learning-based intrusion detection.

5.4 Attention-Based Deep Learning for Malware Detection

Attention mechanisms have become increasingly important for malware detection because they allow models to focus on the most relevant features within complex malware data. Qazi et al. [20] proposed **MAD-ANET**, an attention-based DNN-CNN model for binary and multiclass malware classification using the publicly available CIC-MalMem-2022 dataset. The study considered benign, Trojan horse, ransomware, and spyware classes and demonstrated the application of attention-based deep learning to malware memory analysis.

5.5 Transformer-Based Phishing Detection

Transformer-based architectures represent another major advancement in phishing detection. Wang and Chen [21] proposed **TCURL**, a hybrid architecture combining a convolution branch and a transformer branch for phishing URL detection. The model was designed to capture both local relationships and long-term dependencies among URL characters. Their experiments on multiple datasets demonstrated that combining CNN-based feature extraction with transformer-based modelling can improve phishing URL classification.

More recently, integrated transformer-based approaches have further combined URL embeddings, residual networks, temporal convolution, multi-head self-attention, and pretrained language models. One such study reported evaluation on four datasets, including Ebbu2017, PhishCrawl, 420K-PD, and 1M-PD, demonstrating the growing use of transformer-based models for malicious URL identification.

5.6 Cross-Dataset Generalization of Phishing Detection

An important recent advance is the evaluation of whether a phishing detection model can perform effectively on data collected from a different source. Rashid et al. [22] demonstrated that phishing URL classifiers can experience substantial performance degradation when evaluated on datasets different from those used for training. They proposed an unsupervised domain-adaptation framework to improve transferability between datasets. Their experiments showed an average cross-dataset F1-score improvement of 0.06, with improvements approaching 0.2 in some cases. This highlights the importance of generalization rather than relying only on high performance within a single dataset.

5.7 Advanced Malware Detection Using Public Datasets

Recent malware research has also focused on dynamic and memory-based analysis rather than relying only on traditional signatures. Alzahrani [23] investigated deep-learning-based dynamic malware detection using the publicly available CIC-MalMem-2022 dataset, which contains benign and malicious memory records, including ransomware, spyware, and Trojan samples. Such approaches demonstrate the movement toward behavioural and memory-based detection for identifying malware variants that may evade conventional signature-based systems.

Table 3. Recent Advances in Deep Learning-Based Cybersecurity

Recent Advance	Deep Learning Approach	Publicly Available Data	Main Contribution
Hybrid intrusion detection	CNN, RNN, LSTM and hybrid models	CIC-IDS2017 and other IDS datasets	Combines spatial and temporal feature learning
GAN-based augmentation	GAN + CNN	Benchmark IDS datasets	Addresses attack-data imbalance
Federated threat detection	Federated DL + GAN	IoT/IDS datasets	Supports privacy-preserving threat detection
Attention-based malware detection	Attention + DNN-CNN	CIC-MalMem-2022	Focuses on important malware features

Transformer-based phishing detection	CNN + Transformer	Phishing URL datasets	Captures local and long-range URL patterns
Cross-dataset phishing detection	Deep learning + UDA	Multiple phishing URL datasets	Improves model generalization
Dynamic malware detection	Deep learning	CIC-MalMem-2022	Detects malware using memory/behavioural information

Overall, recent advances demonstrate a clear transition from conventional deep-learning classifiers toward hybrid, attention-based, GAN-assisted, federated, and transformer-based cybersecurity models. The increasing use of publicly available datasets has also made comparative evaluation more practical. However, recent studies indicate that issues such as class imbalance, privacy, adversarial behaviour, and cross-dataset generalization remain important challenges for reliable real-world deployment.

6. DISCUSSION

Deep learning has emerged as an important approach for identifying and mitigating cybersecurity threats because of its ability to learn complex patterns directly from large and heterogeneous security datasets. Unlike conventional machine-learning approaches that often depend on manually selected features, deep learning models can automatically learn representations from network traffic, system logs, executable files, URLs, emails, and other security-related data. The applications discussed in this paper show that different deep learning architectures provide different advantages depending on the characteristics of the security problem. CNNs are effective in learning local and structural patterns, while RNNs and LSTMs are more suitable for sequential and temporal network behaviour. Autoencoders are useful for anomaly detection, whereas GANs can address data imbalance and generate additional training samples. Hybrid and attention-based models further improve the ability to capture complex relationships within cybersecurity data.

The theoretical significance of deep learning in network security lies in its ability to represent cybersecurity threats as patterns that can be learned from historical observations. In intrusion detection, for example, normal and malicious traffic can be represented through multiple network characteristics, allowing a model to distinguish abnormal behaviour without relying entirely on predefined signatures. This is particularly important for detecting previously unseen attacks. Similarly, malware detection can benefit from learning behavioural, structural, and sequential characteristics of malicious programs. In phishing and spam detection, deep learning can analyse textual information, URLs, metadata, and communication patterns to identify suspicious content. Thus, deep learning provides a common theoretical framework for transforming complex cybersecurity data into meaningful representations for classification, detection, and prediction.

The recent advances discussed in this paper also indicate a shift from isolated deep learning architectures toward more integrated and adaptive security systems. Hybrid CNN-LSTM models can combine feature extraction with temporal learning, while attention mechanisms allow models to concentrate on the most informative features. GAN-based approaches provide a theoretical solution to the problem of imbalanced security datasets by generating additional samples for underrepresented attack classes. Federated learning further extends this concept by allowing models to learn from distributed security data without requiring all sensitive data to be transferred to a central location. Transformer-based approaches represent another important development because their attention mechanisms can capture long-range relationships in sequential data such as URLs, network flows, and communication sequences.

However, the effectiveness of deep learning in cybersecurity is influenced by several theoretical and practical challenges. Parameter optimization remains important because model performance depends on the selection of learning rate, number of layers, neurons, batch size, activation functions, dropout, and optimization algorithms. A poorly optimized model may either fail to learn important threat patterns or become unnecessarily complex. Therefore, systematic hyperparameter optimization is required to obtain an appropriate balance between detection performance and computational cost.

Evaluation metrics are another important consideration. Accuracy alone is insufficient for cybersecurity applications, particularly when datasets contain a large proportion of normal traffic and relatively few attack samples. A model may obtain high accuracy while failing to detect important attacks. Consequently, precision, recall, F1-score, sensitivity, specificity, false-positive rate, and false-negative rate should be considered together. From a theoretical security perspective, reducing false negatives is particularly important because an undetected malicious event can have considerably greater consequences than an incorrectly classified normal event.

Dataset quality and availability also strongly influence the generalization capability of deep learning models. Public datasets such as CIC-IDS2017, UNSW-NB15, and CIC-MalMem-2022 provide valuable resources for developing and evaluating cybersecurity models. However, cybersecurity environments continuously change, and datasets may become outdated, imbalanced, or insufficiently representative of emerging attack behaviours. Consequently, a model trained on one dataset may perform well in controlled experiments but show reduced performance when applied to traffic from a different environment. This creates a theoretical requirement for diverse, updated, balanced, and cross-domain datasets.

Deep learning architecture selection is similarly dependent on the nature of the cybersecurity problem. No single architecture is theoretically optimal for all threat-detection tasks. CNNs are appropriate for extracting local patterns, RNNs and LSTMs for temporal dependencies, autoencoders for learning normal behaviour and detecting deviations, and transformers for modelling long-range relationships. Hybrid architectures can combine these capabilities, but they generally increase model complexity and computational requirements. Therefore, architecture selection should be guided by the characteristics of the input data and the intended security objective.

Finally, inference and interpretability remain major concerns for the practical adoption of deep learning-based security systems. Deep models often operate as complex representations whose decisions are difficult for security analysts to interpret. In a cybersecurity environment, it is not sufficient to identify an event as malicious; analysts may also need to understand which traffic characteristics, behavioural patterns, or features contributed to the decision. Explainable artificial intelligence can therefore complement deep learning by providing interpretable information about model predictions. Faster inference is also necessary for real-time threat detection because delays in identifying and responding to an attack can increase potential damage.

Overall, the theoretical discussion indicates that deep learning provides a flexible foundation for network security threat identification and mitigation by combining automated feature learning, anomaly detection, classification, sequential modelling, and adaptive learning. Nevertheless, its effectiveness depends not only on model accuracy but also on data quality, architecture selection, optimization, evaluation methodology, computational efficiency, and interpretability. The future development of cybersecurity systems should therefore move toward robust, explainable, adaptive, and privacy-preserving deep learning frameworks capable of operating effectively against both known and emerging threats.

7. CONCLUSION

The study concludes that deep learning has emerged as a powerful approach for strengthening network security by enabling accurate, automated, and adaptive identification of complex cyber threats. Different architectures, including CNN, DBN, Autoencoder, RNN, LSTM, GAN, attention-based models, and Transformer-based approaches, provide distinct capabilities for analysing network traffic, malware behaviour, intrusion patterns, phishing activities, botnets, and ransomware. Recent developments further demonstrate the potential of hybrid models, federated learning, data augmentation, and advanced attention mechanisms to improve detection performance and address issues such as class imbalance and privacy. However, challenges related to zero-day attacks, dataset quality, model optimization, generalization, computational requirements, evaluation, and interpretability continue to limit large-scale practical deployment. Therefore, future cybersecurity systems should focus not only on improving detection accuracy but also on developing robust, explainable, real-time, and adaptive models that integrate threat identification with timely mitigation. Overall, deep learning-driven cybersecurity offers significant potential for building more resilient network security systems capable of responding effectively to the evolving cyber threat landscape.

REFERENCES

1. Peca, L., & Țurcanu, D. (2023). Network security: Practical examples solved to be introduced in network security.
2. Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.
3. Wang, X., Zhao, Y., & Pourpanah, F. (2020). Recent advances in deep learning. *International Journal of Machine Learning and Cybernetics*, *11*(4), 747-750.
4. Khalaf, N. Z., Barazanchi, A., Ibraheem, I., Radhi, A. D., Shah, P., & Sekhar, R. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. *Mesopotamian Journal of CyberSecurity*, *5*(2), 501-513.
5. Aljaramiz, M., Khurana, M., Aljarameez, F., & Alnasiry, N. (2025, April). Deep Learning-Driven Cybersecurity Threat Detection and Mitigation in Saudi Arabia Healthcare System. In *2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD)* (pp. 1-5). IEEE.
6. Afraji, D. M. A. A., Lloret, J., & Peñalver, L. (2025). Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments. *Cyber Security and Applications*, *3*, 100085.
7. Abughali, A., Alansari, M., & Al-Sumaiti, A. S. (2024). Deep learning strategies for detecting and mitigating cyber-attacks targeting water-energy nexus. *IEEE Access*, *12*, 129690-129704.
8. Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., & Hassan, M. M. (2021). DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2472-2481.
9. Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors*, *19*(9), 1977.
10. Baba, A., & Bonny, T. (2023). FPGA-based parallel implementation to classify Hyperspectral images by using a Convolutional Neural Network. Integration, 92, 15-23. https://doi.org/10.1016/j.vlsi.2023.04.003
11. Sohn, I. (2021). Deep belief network based intrusion detection techniques: A survey. Expert Systems with Applications, 167, 114170. https://doi.org/10.1016/j. eswa.2020.114170
12. T. Bonny, S. Vaidyanathan, A. Sambas, K. Benkouider, W. A. Nassan and O. Naqaweh, "Multistability and Bifurcation Analysis of a Novel 3D Jerk Sys-tem: Electronic Circuit Design, FPGA Implementation, and Image Cryptog-raphy Scheme," in IEEE Access, vol. 11, pp. 78584-78600, 2023, doi: 10.1109/AC-CESS.2023.3299171.
13. Torre, D., Mesadieu, F. & Chennamaneni, A. Deep learning techniques to detect cybersecurity attacks: a systematic mapping study. Empir Software Eng 28, 76 (2023). https://doi.org/10.1007/s10664-023-10302-1
14. Yinka-Banjo, C., Ugot, OA. A review of generative adversarial networks and its application in cybersecurity. Artif Intell Rev 53, 1721–1736 (2020). https: //doi.org/10.1007/s10462-019-09717-4
15. Bhowmik T., Bhadwaj A., Kumar A., Bhushan B. (2022) Machine Learning and Deep Learning Models for Privacy Management and Data Analysis in Smart Cites. In: Balas V.E., Solanki V.K., Kumar R. (eds) Recent Advances in Internet of Things and Machine Learning. Intelligent Systems Reference Library, vol 215. Springer, Cham. https://doi.org/10.1007/978-3-030-90119-6_13
16. C. -C. Sun, D. J. Sebastian Cardenas, A. Hahn and C. -C. Liu, "Intrusion Detection for Cybersecurity of Smart Meters," in IEEE Transactions on Smart Grid, vol. 12, no. 1, pp. 612-622, Jan. 2021, doi: 10.1109/TSG.2020.3010230.
17. Disha, R.A., Waheed, S. Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. Cybersecurity 5, 1 (2022). https://doi.org/ 10.1186/s42400-021-00103-8
18. G. Andresini, A. Appice, L. De Rose, and D. Malerba, "GAN augmentation to deal with imbalance in imaging-based intrusion detection," Future Generation Computer Systems, vol. 123, pp. 108–127, 2021. doi: 10.1016/j.future.2021.04.017.
19. A. Tabassum, A. Erbad, W. Lebda, A. Mohamed, and M. Guizani, "FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning," Computer Communications, vol. 192, pp. 299–310, 2022. doi: 10.1016/j.comcom.2022.06.015.
20. E. U. H. Qazi, M. H. Faheem, W. K. Al-Ghanem, T. Zia, M. Imran, and I. Ahmad, "MAD-ANET: Malware Detection Using Attention-Based Deep Neural Networks," Computer Modeling in Engineering & Sciences, vol. 143, no. 1, pp. 1009–1027, 2025. doi: 10.32604/cmes.2025.058352.
21. C. Wang and Y. Chen, "TCURL: Exploring hybrid transformer and convolutional neural network on phishing URL detection," Knowledge-Based Systems, vol. 258, article 109955, 2022. doi: 10.1016/j.knosys.2022.109955.
22. F. Rashid, B. Doyle, S. C. Han, and S. Seneviratne, "Phishing URL detection generalisation using Unsupervised Domain Adaptation," Computer Networks, vol. 245, article 110398, 2024. doi: 10.1016/j.comnet.2024.110398.
23. T. Alzahrani, "Advanced Techniques for Dynamic Malware Detection and Classification in Digital Security Using Deep Learning," Computers, Materials & Continua, vol. 83, no. 3, pp. 4575–4606, 2025. doi: 10.32604/cmc.2025.063448.