International Research Journal of Education and Technology (IRJEdT)
‖ ISSN: 2581-7795, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 09 | Issue: 08 | Aug 2026 | www.irjweb.com ‖

Deep Learning for Cybersecurity

A Systematic Review of Methods, Applications, Datasets, and Emerging Trends

Vishnu Priya B[0009-0004-9250-7841]
Assistant Professor
Department of IT & Cognitive Systems
Sri Krishna Arts and Science College
Coimbatore, India

Karthick S[0009-0007-2744-4567]
Assistant Professor
Department of IT & Cognitive Systems
Sri Krishna Arts and Science College
Coimbatore, India

Abstract **- The increasing complexity of cyber threats has created a need for intelligent and adaptive security solutions. Deep Learning (DL) has emerged as an effective approach for detecting complex and previously unseen attacks by automatically learning patterns from security data. This survey reviews major deep learning architectures and their applications in intrusion, malware, phishing, DDoS, ransomware, and IoT threat detection. It also discusses commonly used datasets, key challenges, and emerging approaches such as explainable AI, federated learning, and Transformer-based models. Finally, the survey identifies research gaps and future directions for developing robust and reliable cybersecurity systems.**

Keywords: Deep Learning, Cybersecurity, Intrusion Detection, Malware Detection, IoT Security.

I. INTRODUCTION

The rapid growth of cloud computing, Internet of Things (IoT), mobile technologies, and interconnected networks has increased the number and complexity of cybersecurity threats. Attacks such as malware, phishing, ransomware, Distributed Denial-of-Service (DDoS), and network intrusions pose serious challenges to individuals and organizations. Traditional security mechanisms mainly rely on predefined rules and attack signatures, which can be effective against known threats but may struggle to identify new and evolving attacks.

Machine Learning (ML) has improved automated threat detection by learning patterns from security data. However, conventional ML techniques often depend on manual feature selection and domain expertise. Deep Learning (DL) addresses some of these limitations by automatically learning complex representations from large datasets. Architectures such as DNNs, CNNs, RNNs, LSTMs, Autoencoders, GANs, Transformers, and Graph Neural Networks (GNNs) have been applied to intrusion detection, malware detection, phishingsdetection, DDoS detection, ransomware detection, and IoT security.

Despite its advantages, deep learning in cybersecurity faces challenges such as class imbalance, computational complexity, limited interpretability, adversarial attacks, and zero-day threat detection. This survey reviews major deep learning architectures and their cybersecurity applications, discusses key challenges and emerging approaches, and identifies research gaps and future directions for developing robust and adaptive cybersecurity systems.

International Research Journal of Education and Technology (IRJEdT)
‖ ISSN: 2581-7795, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 09 | Issue: 08 | Aug 2026 | www.irjweb.com ‖

II. BACKGROUND OF DEEP LEARNING IN CYBERSECURITY

The increasing use of cloud computing, Internet of Things (IoT) devices, mobile applications, and interconnected networks has resulted in more complex cybersecurity threats, including malware, phishing, ransomware, DDoS attacks, and network intrusions. This growth has created a need for intelligent and automated threat-detection mechanisms.

A. Traditional Cybersecurity Approaches

Traditional cybersecurity systems mainly use signature-based and rule-based methods to identify known attacks. Although effective against previously identified threats, these methods may have difficulty detecting new, modified, or zero-day attacks. Anomaly-based approaches can detect unusual activities but may generate false alarms when legitimate behavior differs from established patterns.

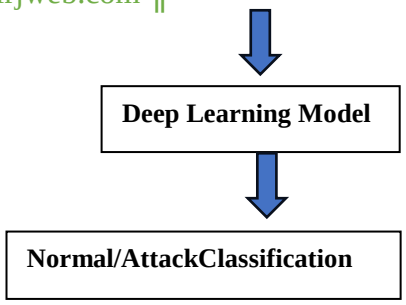
B. Machine Learning in Cybersecurity

Machine Learning (ML) provides data-driven threat detection using algorithms such as Decision Trees, Random Forests, Support Vector Machines (SVM), and Logistic Regression. These techniques have been widely applied to intrusion, malware, and phishing detection. However, conventional ML approaches often depend on manual feature engineering and domain expertise.

Security Data → Preprocessing → Feature Extraction → ML Model → Threat Detection

C. Emergence of Deep Learning

Deep Learning (DL) extends machine learning by using multilayer neural networks to automatically learn complex representations from security data. DL models can process network traffic, system logs, executable files, URLs, emails, and behavioral data with reduced dependence on manual feature engineering.



Architectures such as DNNs, CNNs, RNNs, LSTMs, Autoencoders, GANs, Transformers, and GNNs have been investigated for intrusion detection, malware detection, phishing detection, DDoS detection, and IoT security.

D. Advantages and Limitations

Deep learning provides automatic feature learning and the ability to identify complex patterns in large and high-dimensional security datasets. However, its effectiveness can be affected by limited or imbalanced datasets, high computational requirements, lack of interpretability, adversarial attacks, and difficulties in detecting evolving threats. Therefore, current research focuses on developing more accurate, explainable, robust, and adaptive deep learning-based cybersecurity systems.

III. DEEP LEARNING ARCHITECTURES FOR CYBERSECURITY

Deep learning architectures are widely used in cybersecurity to learn complex patterns from network traffic, system logs, malware, and other security data. The major architectures and their applications are summarized below.

A. Artificial Neural Networks (ANN)

ANNs consist of interconnected neurons organized into input, hidden, and output layers. In cybersecurity, they are used to classify security data as normal or malicious.

Applications: Intrusion detection, malware detection, phishing detection, and spam detection.

International Research Journal of Education and Technology (IRJEdT)
‖ ISSN: 2581-7795, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 09 | Issue: 08 | Aug 2026 | www.irjweb.com ‖

Limitation: Requires sufficient training data and may have limited interpretability.

B. Convolutional Neural Networks (CNN)

CNNs automatically extract important local patterns from security data. They can analyze network traffic, packet representations, and malware represented as byte sequences or images.

Applications: Malware detection, intrusion detection, malicious traffic classification, and phishing detection.
Advantage: Automatic feature extraction.
Limitation: Computationally expensive and less suitable for long-term sequential relationships.

C. Recurrent Neural Networks (RNN)

RNNs are designed to process sequential data by retaining information from previous inputs. They are suitable for analyzing packet sequences, login activities, API calls, and system logs.

Applications: Intrusion detection, malware behavior analysis, and network traffic analysis.
Limitation: May suffer from vanishing or exploding gradients.

D. Long Short-Term Memory (LSTM)

LSTM is an advanced type of RNN that uses memory cells and gates to capture long-term dependencies in sequential data.

Applications: Intrusion, DDoS, botnet, and user-behavior detection.
Advantage: Effective for long-term sequential patterns.
Limitation: High computational and memory requirements.

E. Autoencoders

Autoencoders learn compact representations of input data using an encoder and decoder. They can learn normal network behavior and identify abnormal activities through reconstruction errors.

Applications: Anomaly detection, intrusion detection, and malware detection.
Advantage: Useful when labelled attack data are limited.
Limitation: Performance depends on training data and anomaly-threshold selection.

F. Generative Adversarial Networks (GAN)

GANs consist of a generator and discriminator that compete during training. In cybersecurity, they are mainly used to generate synthetic attack data and address class imbalance.

Applications: Data augmentation, intrusion detection, and adversarial-security research.
Advantage: Generates additional attack samples for training.
Limitation: Training can be unstable.

G. Transformers

Transformers use self-attention mechanisms to identify relationships within long sequences of data.

Applications: Intrusion detection, phishing detection, security-log analysis, malicious URL detection, and threat intelligence.
Advantage: Captures long-range contextual relationships.
Limitation: Requires considerable computational resources.

H. Graph Neural Networks (GNN)

GNNs analyze graph-structured data in which nodes represent entities such as users, devices, or IP addresses and edges represent their relationships.

Applications: Botnet detection, fraud detection, intrusion analysis, and network anomaly detection.
Advantage: Effectively captures relationships among network entities.
Limitation: Graph construction and large-scale processing can be complex.

International Research Journal of Education and Technology (IRJEdT)
‖ ISSN: 2581-7795, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 09 | Issue: 08 | Aug 2026 | www.irjweb.com ‖

IV. APPLICATIONS OF DEEP LEARNING IN CYBERSECURITY

Deep learning is widely applied in cybersecurity to identify complex attack patterns from network traffic, system activities, and application data. Major applications include intrusion, malware, phishing, DDoS, ransomware detection, and IoT security.

A. Intrusion Detection

Deep learning-based Intrusion Detection Systems (IDS) analyze network traffic to distinguish normal activities from malicious attacks. DNNs, CNNs, LSTMs, Autoencoders, and Transformers are commonly applied for this purpose. Popular datasets include NSL-KDD, UNSW-NB15, CICIDS2017, and CSE-CIC-IDS2018.

B. Malware Detection

Deep learning detects malicious software by analyzing features such as byte sequences, API calls, system calls, and runtime behavior. CNNs are useful for extracting malware patterns, while RNNs and LSTMs can analyzebehavioral sequences.

C. Phishing Detection

Deep learning models identify phishing attacks by analyzing URLs, emails, webpage content, and HTML structures. CNNs, LSTMs, and Transformers can distinguish legitimate content from phishing attempts.

D. DDoS Detection

Deep learning can detect DDoS attacks by identifying abnormal network traffic patterns. DNNs, CNNs, LSTMs, and Autoencoders are used to distinguish legitimate traffic from malicious traffic flooding.

E. Ransomware Detection

Deep learning-based ransomware detection analyzes file activities, API calls, processes, and network behavior. CNNs, LSTMs, and Autoencoders can help identify suspicious behavior before extensive data encryption occurs.

F. IoT Security

Deep learning helps protect IoT environments by detecting abnormal device and network behavior. CNNs, LSTMs, Autoencoders, and GNNs are used for intrusion, botnet, and anomaly detection. Common datasets include Bot-IoT, N-BaIoT, and IoT-23.

Overall, deep learning provides effective techniques for detecting diverse cybersecurity threats. However, real-world deployment must consider detection accuracy, false alarms, computational cost, explainability, and the ability to detect previously unseen attacks.

V. CYBERSECURITY DATASETS

The performance of deep learning-based cybersecurity systems depends strongly on the quality and diversity of training data. Common datasets used for evaluating cybersecurity models include NSL-KDD, UNSW-NB15, CICIDS2017, CSE-CIC-IDS2018, Bot-IoT, N-BaIoT, and IoT-23. These datasets contain normal and malicious network activities representing attacks such as DoS/DDoS, botnets, brute-force attacks, and network intrusions.

VI. COMPARATIVE ANALYSIS OF EXISTING STUDIES

Existing studies have applied different deep learning architectures depending on the type of cybersecurity problem. CNNs are effective for extracting local patterns, LSTMs are suitable for sequential security data, Autoencoders support anomaly detection, Transformers capture long-range contextual information, and GNNs model relationships among network entities.

TABLE I

Model	Major Application	Key Strength
ANN/DNN	Intrusion detection	General classification
CNN	Malware, intrusion	Feature extraction
RNN/LSTM	DDoS, intrusion	Sequential analysis
Autoencoder		

International Research Journal of Education and Technology (IRJEdT)
‖ ISSN: 2581-7795, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 09 | Issue: 08 | Aug 2026 | www.irjweb.com ‖

	Anomaly detection	Unsupervised learning
GAN	Data augmentation	Generates synthetic samples
Transformer	Phishing, intrusion	Contextual analysis
GNN	Botnet, network security	Relationship analysis

The comparison indicates that no single architecture is optimal for every cybersecurity problem. Model selection depends on the characteristics of the data, security application, computational requirements, and expected detection performance.

VII. CHALLENGES AND LIMITATIONS

Despite their effectiveness, deep learning-based cybersecurity systems face several challenges. Important limitations include imbalanced datasets, high computational requirements, limited model interpretability, false-positive detection, adversarial attacks, privacy concerns, and difficulties in detecting zero-day attacks. The availability of representative and accurately labelled real-world security data is another major concern.

VIII. EMERGING TRENDS

Recent developments are focused on improving the intelligence, robustness, and privacy of cybersecurity systems. Important emerging approaches include Explainable Artificial Intelligence (XAI), federated learning, Transformer-based models, Graph Neural Networks, adversarially robust learning, and lightweight deep learning models for IoT and edge environments.

IX. RESEARCH GAPS AND FUTURE DIRECTIONS

Although deep learning has demonstrated considerable potential in cybersecurity, several research gaps remain. Future research should focus on improving zero-day attack detection, model explainability, real-time threat detection, adversarial robustness, privacy preservation, and computational efficiency. Hybrid deep learning architectures and adaptive models capable of responding to continuously changing attack patterns are also promising research directions.

X. CONCLUSION

Deep learning has become an important approach for detecting complex cybersecurity threats. Architectures such as CNNs, LSTMs, Autoencoders, GANs, Transformers, and GNNs have been applied to intrusion, malware, phishing, DDoS, ransomware, and IoT threat detection. However, challenges related to computational cost, interpretability, data quality, and emerging attacks remain. Future research should therefore focus on developing robust, explainable, efficient, and adaptive deep learning-based cybersecurity systems.

REFERENCES

1. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). "A survey of deep learning methods for cyber security." *Information*, 10(4), 122. This is a useful general reference for deep-learning applications such as malware and intrusion detection.
2. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). "IntruDTree: A machine learning based cyber security intrusion detection model." *Symmetry*, 12(5), 754.
3. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study." *Journal of Information Security and Applications*, 50, 102419. DOI: 10.1016/j.jisa.2019.102419. This is particularly valuable for your Cybersecurity Datasets and Comparative Analysis sections because

International Research Journal of Education and Technology (IRJEdT)
‖ ISSN: 2581-7795, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 09 | Issue: 08 | Aug 2026 | www.irjweb.com ‖

it reviews multiple deep-learning architectures and 35 cybersecurity datasets.

4. **Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues." *Knowledge-Based Systems*, 189, 105124.**

DOI: 10.1016/j.knosys.2019.105124. Useful for challenges, taxonomy, open issues, and future research directions.

5. **Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). "Deep learning approach for intelligent intrusion detection system." *IEEE Access*, 7, 41525–41550.**