International Journal of Technology, Leadership and Sciences (IJTLS)

ISSN: 3107-908
www.ijtls.com
Research Paper
DOI: https://doi.org/10.5281/zenodo.20772276

PREDICTIVE CYBER ATTACK DETECTION IN CLOUD COMPUTING USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

SANAKA ANUSHA[1],D. SRIDHAR[2] ,Dr.CHAVA HARI BABU[3], DR.VUNNAVA DINESH BABU[4], R.VAMSI KRISHNA[5]

[1]M.Tech Student,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.

[2]Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.

[3]Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.

[4]Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.

[5]Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.

ABSTRACT:

The scalability, adaptability, and cost-effectiveness of cloud computing have become it an indispensable element of contemporary digital infrastructure. The system's decentralized architecture renders it susceptible to data breaches, insider threats, zero-day vulnerabilities, distributed Denial of Service (DDoS) assaults, and several other cyber threats. Traditional intrusion detection systems struggle to identify novel and new threats in real time. This study introduces a novel approach for identifying cyber assaults in cloud systems via the use of machine learning techniques. The approach utilizes a hybrid deep learning architecture that integrates CNN and LSTM networks. The proposed method effectively identifies harmful activities by scrutinizing extensive network data, hence uncovering previously unrecognized attack patterns. Incorporating Explainable Artificial Intelligence (XAI) methodologies to elucidate model decisions improves transparency and fosters confidence. The proposed method provides a comprehensive and perceptive resolution to the issue of cloud computing security, as shown by experimental data demonstrating improved performance in recall, accuracy, precision, and false positive rate.

Keywords: Cloud Computing Security, Cyber Attack Detection, Machine Learning, Deep Learning, CNN-LSTM, Explainable Artificial Intelligence (XAI), Intrusion Detection System, DDoS Detection.

Received Date: 5 June 2026; **Accepted Date:** 15 June 2026; **Published Date:** 20 June 2026

I. INTRODUCTION

The advent of cloud computing, allowing users to access consolidated computer resources over the Internet as needed, has profoundly altered the ways in which organizations handle data storage, management, and processing. It facilitates rapid scaling, diminished infrastructure costs, and improved operational efficiency. Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) are essential elements of modern business operations. Cloud computing offers several benefits; yet, it has also become a prominent target for assaults due to the

security weaknesses linked to its extensive use. Cloud systems are inherently complicated and dynamic because to their multi-tenant structures, virtualization, and dispersed data storage. These characteristics hamper the implementation of conventional security measures and broaden the attack surface. Cloud systems are susceptible to many cyber dangers, including DDoS assaults, malware penetration, data breaches, insider threats, and Advanced Persistent dangers (APTs). Conventional rule-based security systems and intrusion detection systems (IDS) are inadequate in identifying novel threats since they depend on predefined signatures and patterns. In recent years, machine learning (ML) has shown to be an effective instrument for improving cybersecurity. Machine learning systems may detect unusual behavior by independently recognizing patterns throughout large datasets. In cloud systems, where significant amounts of user behavior and network traffic data are perpetually produced, this feature becomes more essential. The real-time analysis of this data allows ML-based systems to identify dangers, both known and unknown, with more accuracy than conventional methods. The identification of cyber threats has advanced considerably with the use of advanced machine learning methodologies, especially deep learning frameworks like CNN and LSTM networks. These models may more efficiently discern intricate assault patterns by capturing the complicated spatial and temporal relationships inherent in network data. Furthermore, the amalgamation of several algorithms using hybrid methodologies may enhance detection effectiveness while diminishing the incidence of false alarms. Modern cybersecurity solutions also prioritize explainability. The decision-making process becomes more opaque as machine learning models grow in complexity. To resolve this problem and bolster confidence in automated security systems, Explainable Artificial Intelligence (XAI) solutions clarify model behavior. In cloud systems, security considerations are crucial since they profoundly affect data privacy and regulatory compliance. This project seeks to provide a sophisticated framework using machine learning to identify cyber assaults in cloud computing systems. The suggested methodology seeks to improve detection precision, reduce false positives, and accommodate new threat categories. The system provides a sophisticated and resilient solution for protecting cloud infrastructure via the integration of deep learning and Explainable AI techniques.

This study highlights the need of using artificial intelligence (AI) skills to create defenses that are more robust and adaptable in response to the increasing threats to cloud security.

II.LITERATURE REVIEW

- S. N. Tirumala Rao and S. M. P. Dinakar Rao suggested a machine learning-based intrusion detection system using classification methods, including Decision Trees and Support Vector Machines (SVM). They effectively decreased false positives and improved detection accuracy for identified assaults using their technique. The research results underscored the significance of feature selection in improving model efficacy in cloud security contexts.
- A deep learning anomaly detection model using an autoencoder was proposed by A. Javaid, Q. Niyaz, W. Sun, and M. Alam. Their system may detect novel threats by examining patterns in typical network traffic. Compared to conventional intrusion detection approaches, the suggested strategy shown enhanced effectiveness in detecting zero-day assaults.
- K. Modi, D. Patel, B. Borisaniya, H. Patel, and A. Patel conducted an exhaustive examination of cloud intrusion detection techniques. Their research analyzed the merits and drawbacks of signature-based and anomaly-based techniques. The report highlighted the need for intelligent and adaptive cloud security solutions.
- M. Alom, T. M. Taha, C. Yakopcic, and others investigated deep neural networks for the detection of cyber threats in cloud systems. Their suggested approach, including automated learning techniques, improved system security and precisely detected intricate assault patterns.
- N. Moustafa and J. Slay used machine learning models, trained on benchmark datasets like UNSW-NB15, to create an intrusion detection system. Their results demonstrated that machine learning techniques substantially improved detection rates for contemporary cyber threats.
- R. Vinayakumar, K. Soman, and P. Poornachandran introduced a hybrid model that amalgamates deep learning with conventional machine learning techniques. Their methodology
- improved detection precision and reduced false alarm rates, demonstrating efficacy in large-scale cloud data processing.

- B. Arrieta et al. concentrated on integrating Explainable Artificial Intelligence (XAI) into intrusion detection systems, so augmenting the dependability and credibility of machine learning-based security systems by elucidating the logic behind model choices, thus promoting transparency.
- R. K. Banyal, P. Jain, and V. K. Jain examined the use of artificial intelligence approaches in cloud security. Their efforts focused on automating threat detection and optimizing reaction time using machine learning, leading to enhanced protection against cyber threats.

III.EXISTING SYSTEM

Conventional security methods, such as firewalls, signature-based intrusion detection systems (IDS), and rule-based monitoring tools, are the foundation of contemporary cyber attack detection systems in cloud computing. These systems are limited to recognizing established threats, identifying possible hazards only via the surveillance of network activity according to predetermined signatures or criteria. Their efficacy in contemporary cloud systems is constrained, since they are unable of identifying unknown or zero-day assaults. Administering rule-based systems on extensive cloud infrastructures is arduous due to their inflexibility and the need for frequent human interaction. Certain systems use rudimentary anomaly detection algorithms; however, these approaches often rely on too simplistic statistical methodology, resulting in a heightened occurrence of false positives and false negatives. Moreover, existing systems lack real-time threat detection capabilities and have scalability issues due to the vast amounts of data generated by the cloud. Intelligent, automated, and adaptive security solutions using machine learning are essential, since dependence on human intervention prolongs response time.

DISADVANTAGES

- Current techniques have limited scalability,
- often generate several false alerts, and fail to identify fresh or continuously developing threats.
- Existing systems are inadequate for identifying intricate or developing attack patterns, leading to security violations and unnoticed assaults.

IV.PROPOSED SYSTEM

The suggested system presents an enhanced framework for detecting cyberattacks in cloud computing environments via the use of machine learning methods. It can identify both existing and emerging threats in real time with a hybrid deep learning model that combines CNN and LSTM networks. To improve the accuracy of attack detection, CNN extracts critical information from network traffic data, while LSTM analyzes temporal patterns and user behavior over time. The system includes data acquisition, cleansing, feature extraction, model training, and real-time threat detection. The model training starts with the creation of network traffic and system logs to eliminate noise, standardize the data, and identify critical characteristics. The trained system utilizes anomaly detection and classification to recognize malicious activity. To enhance transparency, we include Explainable Artificial Intelligence (XAI) approaches, such as SHAP or LIME, to clarify model conclusions. The suggested methodology offers automated cloud security surveillance, low false alarm rates, scalability, and elevated accuracy.

ADVANTAGES

- The system distinguishes between recognized and unknown threats by trend analysis and anomaly detection, in contrast to conventional signature-based systems.
- Advanced algorithms like CNN and LSTM improve the accuracy of cyber threat detection via the analysis of intricate data pattern

V.SYSTEM MODEL

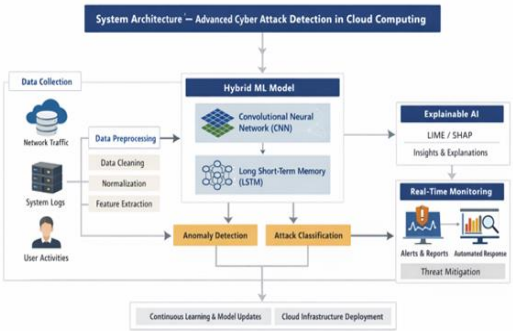


Fig.1 System Model

The proposed cyber attack detection system utilizes advanced machine learning techniques to safeguard cloud computing environments. Cyber threat detection is facilitated by the comprehensive and diverse data provided by cloud infrastructures, including user actions, system records, and network traffic. The system's primary features are improved detection accuracy, real-time monitoring, scalability, and adaptability to evolving threats. It utilizes a hybrid machine learning approach for attack classification and anomaly detection, surpassing the limitations of prior systems. The system model consists of data acquisition, data purification, feature extraction, model training, and real-time threat identification. Security, scalability, reliability, and performance are essential non-functional criteria. The model is tailored for distributed cloud systems, exhibiting exceptional performance metrics, including low false alarm rates and fast response times. This technology's scalable, automated, and intelligent methodology has streamlined the safeguarding of cloud infrastructure from modern cyber threats.

VI.MODULES

Data Collection Module – Network traffic, user activity, and system logs from the cloud environment are consolidated.

Preprocessing Module – Prepares data for analysis via cleaning, conversion, and normalization operations.

Feature Extraction Module – Identifies critical components of cyber attack detection.

Model Training Module – Trains the hybrid machine learning model to identify and categorize anomalies.

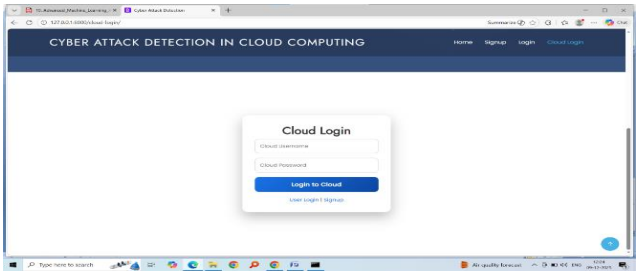
Detection Module – Instantaneously detects and classifies attacks.

Alert & Response Module – Upon danger identification, notifications will be sent, and security measures will be enacted.

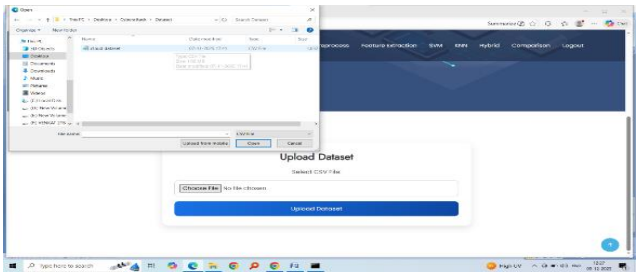
Cloud Security Management Module – Guarantees the scalability, stability, and ongoing surveillance of distributed cloud systems.

VII.SCREENSHOTS

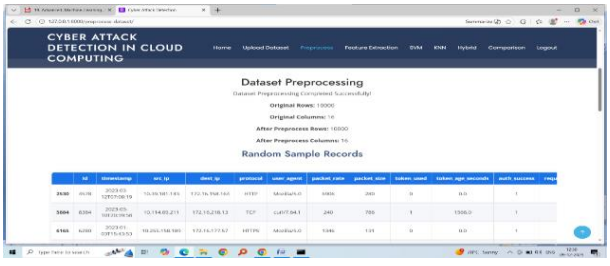
Select "Cloud Login" at the application's initiation.

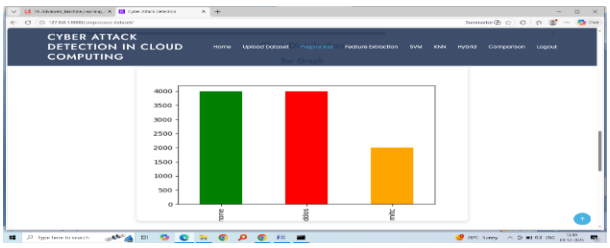


The cloud password is "cloud," and the username is "cloud. The cloud dashboard will appear upon pressing the Login to cloud button.

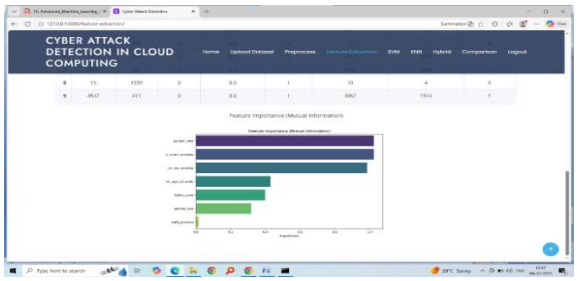


Upload the dataset to the cloud and choose it.

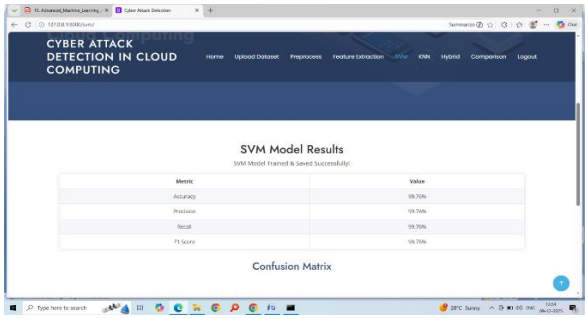




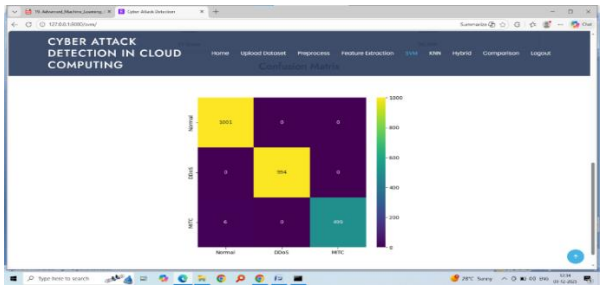
Analyze the intricacies of the preprocessed dataset. Advancing to the next module.



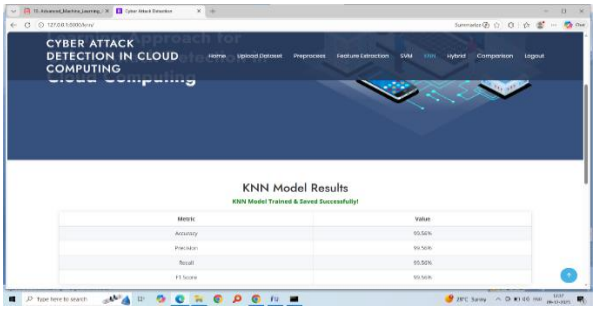
In our project, feature extraction entails gathering pertinent properties of network traffic from cloud communication logs, including packet size, authentication success, token use, packet rate, and request patterns. Thereafter, these characteristics are normalized and converted into numerical vectors to improve the precision of attack detection models in machine learning and deep learning.

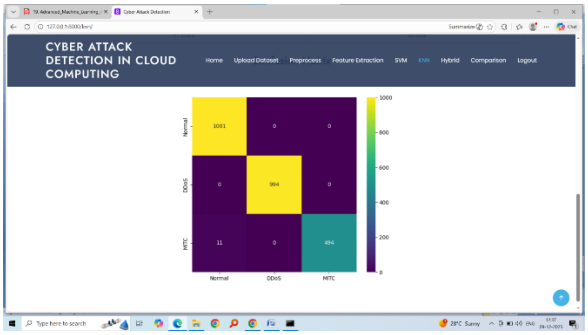


To go to the next module, click here.



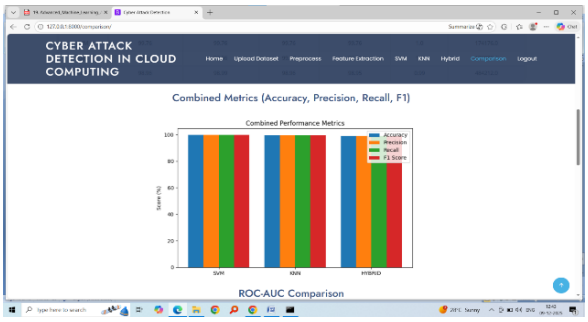
The SVM model proficiently detects network traffic, as shown by the confusion matrix. Almost all samples are accurately identified as Normal (1001), DDoS (994), or MITC (499), with just a negligible number of occurrences remaining undeclared. The very precise and reliable SVM model for cyber attack detection was shown by the low count of MITC samples (6) that were incorrectly categorized as Normal.

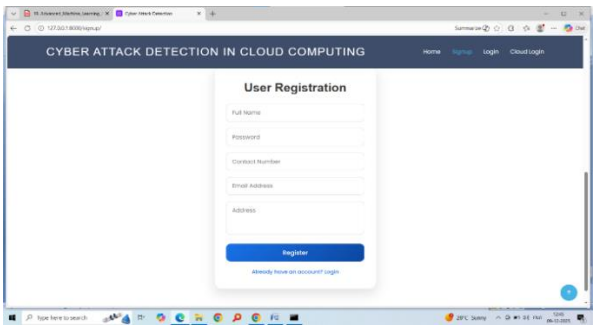




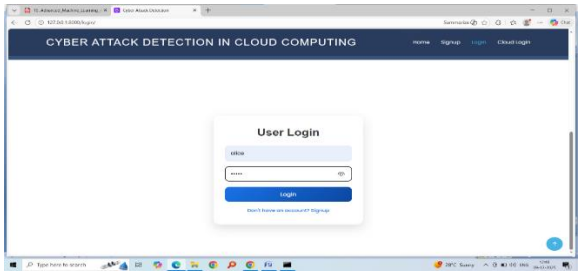
The KNN model precisely categorizes Normal (1001), DDoS (994), and MITC (494) classifications. Despite accurate classification of DDoS traffic, a limited quantity of MITC samples (11 in total) were mistakenly categorized as Normal. The KNN model accurately detects cyber breaches with little mistakes.

To go to the next module, click here.

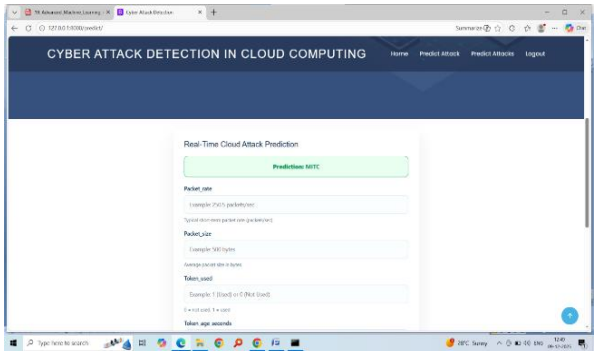




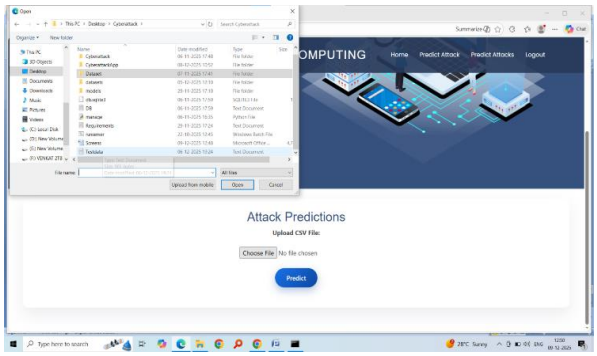
Complete the signup process as if you were a first-time user.

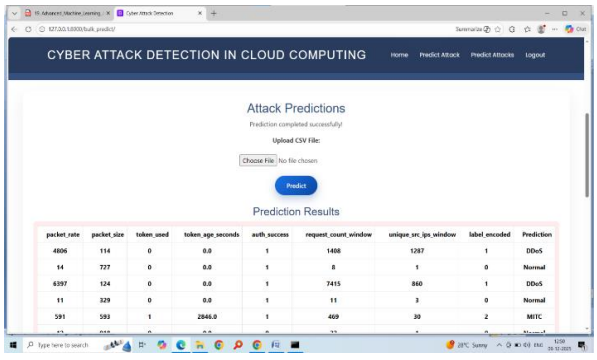


Authenticate as the user at completion of registration.



My conjecture was correct: MITC. To go to the next module, click here.





This module allows for the prediction of the number of concurrent assaults.

VIII.CONCLUSION

Therefore, strong and intelligent security mechanisms are increasingly vital to safeguard private information and assets from hackers, due to the growing dependence on cloud computing. Conventional intrusion detection systems are inadequate because to their high false alarm rates, rigid architecture, and incapacity to adapt to changing situations.

This study introduced an innovative machine learning approach for cyber threat identification in cloud computing, using a hybrid model that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The suggested method efficiently detects both known and emerging cyber risks, examines vast cloud data, and reveals complex patterns.

To improve the system, Explainable Artificial Intelligence (XAI) approaches are included. These tactics improve the clarity and comprehensibility of decision-making, promoting trust and dependability. The system's real-time monitoring and automatic reaction capabilities substantially mitigate the effects of cyber assaults.

The suggested system ultimately exceeds the constraints of current techniques by providing enhanced accuracy, scalability, flexibility, and efficiency. It offers a dependable and advanced approach to protect cloud environments from current and emerging cyber threats. This study improves cloud security via the comprehensive use of machine learning, enabling the development of next-generation intelligent intrusion detection systems.

IX.FUTURE ENHANCEMENTS

The suggested technique successfully detects cyber dangers in the cloud; nonetheless, there is room for improvement and more study in this area.

To tackle intricate assault patterns and boost detection precision, the system may be augmented in the future using more sophisticated deep learning models, including Transformer-based architectures. These models exceed conventional techniques in their capacity to capture interdependencies within network traffic data.

To improve scalability and expedite the processing of extensive cloud data streams, it is crucial to include real-time big data processing frameworks like Hadoop or Apache Spark. This will improve the efficiency of large-scale cloud infrastructures for enterprises.

Incorporating federated learning methodologies might enhance the system further. These approaches enable the cooperation of several cloud environments in model training without the exchange of sensitive information. This improves security and privacy without affecting detection effectiveness.

Future endeavors may focus on improving the Explainable AI (XAI) component by creating more intuitive visualization tools to aid security analysts in comprehending model choices and threat trends.

To improve reaction time and reduce human intervention, the system may integrate with security orchestration systems and automated incident response processes. A self-sustaining security architecture will eventually be attainable.

An further improvement is ensuring the model's relevance to new threats by using real-time threat intelligence feeds to update the system with the most recent attack patterns and vulnerabilities.

Ultimately, to verify and improve the suggested system's robustness and efficacy, it is crucial to evaluate it in actual cloud settings using varied datasets. Future study may investigate deployment across multi-cloud and hybrid cloud infrastructures, as well as cross-platform interoperability.

These upgrades will improve the system's overall efficiency, scalability, security, and adaptability, hence boosting intelligent cybersecurity solutions in the cloud.

X.REFERENCES

[1] S. M. P. Dinakar Rao and S. N. Tirumala Rao, “Intrusion detection system using machine learning algorithms,” International Journal of Computer Science and Information Security (IJCSIS), 2018.

[2] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” in Proc. IEEE Conf. Communications and Network Security (CNS), 2016.

[3] K. Modi, D. Patel, B. Borisaniya, H. Patel, and A. Patel, “A survey of intrusion detection techniques in cloud,” Journal of Network and Computer Applications, Elsevier, vol. 36, no. 1, pp. 42–57, 2013.

[4] M. Alom, T. M. Taha, C. Yakopcic, et al., “The history began from AlexNet: A comprehensive survey on deep learning approaches,” arXiv preprint arXiv:1803.01164, 2018.

[5] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” in Proc. Military Communications and Information Systems Conf. (MilCIS), 2015, pp. 1–6.

[6] R. Vinayakumar, K. P. Soman, and P. Poornachandran, “Deep learning approach for intelligent intrusion detection system,” IEEE Access, vol. 7, pp. 41525–41550, 2019.

[7] A. B. Arrieta et al., “Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI,” Information Fusion, vol. 58, pp. 82–115, 2020.

[8] R. K. Banyal, P. Jain, and V. K. Jain, “Multi-factor authentication framework for cloud computing,” in Proc. Int. Conf. Computational Intelligence and Communication Networks (CICN), 2013, pp. 105–110.

[9] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[10] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson Education, 2017.