Cloud Computing Security Based Intrusion Detection Using ANN

[1]A.Vishnuvardhan Reddy, [2]K.V.Rameswara Reddy, [3]O.Roopa Devi
[4]B.Thimma Reddy, [5]V.Jemima Jyothi
[1,2,4] Associate Professor, Department of Computer Science & Engineering,
G Pulla Reddy Engineering College (Autonomous), Kurnool.
[3,5]Assistant Professor, Department of Computer Science & Engineering,
G Pulla Reddy Engineering College (Autonomous), Kurnool.

ABSTRACT: Cloud computing has become a vital part of modern digital infrastructure, offering scalable, on-demand computing resources. With the increasing demand and popularity in the usage of cloud computing, there has been a necessity to prevent common attacks and security threats to cloud computing services. The consumers of cloud services are constantly concerned about the cyber-security risks, data loss, and slowdown of services. Actually, intrusion detection system (IDS) is an enhanced mechanism used to control traffic within networks and detect abnormal activities. However, the widespread adoption of cloud services has also raised significant security concerns. This paper addresses the imperative need for enhancing security in cloud computing environments through the application of anomaly detection techniques powered by ANN. The ubiquity of cloud computing has ushered in a new era of digital transformation, enabling organizations to streamline operations and achieve unprecedented efficiency. Nevertheless, the dynamic nature of the cloud, coupled with the evolving threat landscape, has exposed organizations to a spectrum of security challenges. These challenges encompass data breaches, insider threats, and vulnerabilities inherent to the shared responsibility model, which necessitates a collaborative approach between cloud service providers and customers. Anomaly detection, a key facet of cloud security, offers a proactive and adaptive defense mechanism against a wide range of security threats. At its core, anomaly detection relies on the establishment of a baseline of normal system behavior. This paper proposes a Artificial Neural Network (ANN) model in cloud security and investigates the key steps for integrating such models into cloud security strategies. Lastly, the data's performance is evaluated using Accuracy, Precision, Recall, and F1-Score.

KEYWORDS: Cloud Computing Security, Anomaly Detection, Implementing anomaly detection in cloud computing, Intrusion Detection System (IDS), Artificial Neural Network (ANN).

I.INTRODUCTION

Cloud Computing is the latest internet-based online programme that allows users to access and interact with a number of cloud apps in a simple and personalised manner. Cloud computing allows you to connect to a cloud application via the Internet and store and access cloud data from anywhere. By choosing cloud services users are able to store their location data on a remote data server. Information stored on a remote data centre can be accessed or managed through cloud services provided by cloud service providers. Therefore, data stored in a remote data centre for data processing should be processed with the utmost care. Cloud Computing security is one of the biggest concerns to deal with these days. Data is at risk if security measures are not adequately implemented in data processing and transfer. Because cloud computing allows a number of users to access stored data, there is a greater danger of data loss. To identify security concerns and answers

to these challenges, strong safety measures must be established. There has recently been a lot of interest in learning more about network and cloud security.

Cloud Computing has become a popular trend in the Information Technology (IT) business, serving as an advanced extension of traditional technologies. It enables direct communication between users and service providers within a cloud environment, offering benefits such as centralized data access, automatic software updates, high availability, flexibility to scale services and infrastructure, cost savings, mobility, security measures for theft detection and prevention, and improved quality control. Cloud services can be easily accessed from anywhere on-demand. A key emerging trend in IT management is "Distributed Computing," which enables dynamic changes in computing resources without concerns about account administration, location, or operating system. These resources are virtualized. The rise of pervasive technology has been driven by the integration of wired and wireless devices accessible anytime and anywhere. High-Performance Computing (HPC) is commonly represented by computer clusters, where a group of interconnected, homogeneous computers work together on a shared task, managed by an application.

Cloud computing is a technological advance that offers the facilities, platform and software of information technology as Internet services. It is considered to be the conversion of a long-lasting dream called ‘‘Computing for Use’’ and it is being gradually embraced by organizations as private, public or hybrid Clouds [1]. Its main objective is to let users use and pay for what they want, promising on-demand services for their software or infrastructure needs.

In an era defined by the relentless growth of digital data and the pervasive adoption of cloud computing, the paramount concern of organizations is ensuring the security and integrity of their data and systems. Artificial Intelligence (AI) and Machine Learning (ML), driven by their capacity to analyze vast datasets, identify patterns, and make real-time decisions, have emerged as the vanguards of cloud security. From the evolution of cyber threats to the limitations of conventional security measures, we embark on a journey to unravel the transformative potential of AI and ML in safeguarding cloud environments.

User authentication in cloud systems can be conducted using four widely recognized methods: knowledge-based (what the user knows), ownershipbased (what the user has), characteristic-based (what the user is), and location-based (where the user is). Common authentication techniques such as passwords and user names pose significant risks to online banking services, financial systems, and users [2]. However, these risks can be effectively managed by implementing multi-factor authentication (MFA). An MFA uses different levels of authentication, making it difficult for hackers to penetrate the system because they must bypass multiple steps before compromising the security. An MFA is vital for cloud security because it requires users to provide multiple forms of verification before accessing resources or services. This enhances security in the digital age for several reasons. They offer better protection against theft, meet compliance requirements, secure remote access, prevent unauthorized access, support risk-based authentication, protect against insider threats, and foster customer trust and confidence. As a crucial element of a robust cybersecurity strategy, MFA provides an essential defense layer against various threats and vulnerabilities in the interconnected digital world.

Although Cloud computing is seen as a significant and positive IT infrastructure shift, much security work is still needed to minimize its deficiencies. Since a significant amount of personal and corporate information is placed in the Cloud data centers, those Cloud security issues and vulnerabilities need to be identified and prevented. Because Cloud infrastructure runs through standard Internet protocols and uses virtualization techniques, it may be vulnerable to attacks. Those attacks may come from traditional sources such as Address Resolution Protocol, IP spoofing, Denial of Service (DoS) etc.,. They may also come from other sources. Zero-day attacks, for example, referred to as unknown attacks, are seen as a significant challenge in the cyber security domain [3]. Traditional techniques used for detection and prevention are not efficient enough to handle those attacks while also dealing with a large data flow.

Machine Learning (ML) techniques are very helpful for identifying attacks, whether traditional or zero-day attacks. Machine learning includes a series of algorithms that can learn patterns from data and predict accordingly. ML combines computer science and statistics to enhance the prediction. ML comprises three main types of learning, supervised, unsupervised and semi-supervised [4]. The main objective of this study is to conduct a systematic review of the ML techniques used to solve, detect or prevent Cloud security issues and vulnerabilities

The remainder of this study is divided into five sections: Section II provides the literature review. The methodology for conducting this review is described in Section III. The findings and results are listed in Section IV. Lastly, the paper is concluded in Section V.

II.LITERATURE SURVEY

Chiew et al. [5] demonstrated that various machine learning algorithms can effectively detect network intrusions, with the Convolutional Neural Networks (CNNs) - Long Short-Term Memory (LSTM) -DT approach outperforming traditional classifiers. The CNN-LSTM-DT method achieved the highest F1 score of 93.26% and an accuracy of 93.72% in both the binary and multiclass tests. Future research could explore more sophisticated methods for deep learning and machine learning to further improve the detection performance.

Gordon et al., [6] highlights the detailed study on hybrid cloud computing techniques and demonstrate the ways of security and risk management at the enterprise level. A recent study proposed the use of a deep learning algorithm for the detection of anomalies in cloud services. A detailed study has been carried out using deep learning approaches and the performance of different models has been compared based on the accuracy. Other studies proposed the use of a secured cloud management log based on temporal data that records the history and transactional data at various time points to provide security to the customers using encryption services for the log data within a particular period as requested by the user.

Khan et al. [7] presented a secure system that authenticated patients by using their names, passwords, and biometric data. The SHA-512 algorithm was used to ensure data integrity. Once verified, the patient's mobile sensor device is activated and continuously sends information to the cloud system. To securely transmit sensor information, the system employs a Caesar cipher and enhanced elliptic-curve cryptography (IECC). The combination of improved ECC and SHA-512 enhances data integrity and security, with the

upgraded ECC incorporating an additional secret key for increased security. However, the report did not provide a comprehensive comparison with the other encryption algorithms.

According to Khorshed et al. [8], gaps in Cloud computing are defined as the trust issues between customers and Cloud providers, where customers fear policies that are hidden from them. On the other hand, Cloud providers are afraid that customers might take advantage and conduct attacks using their Cloud services. The main determinants of the selection of a Cloud provider are the expectations of their organizations and what facilities they will obtain from a specific provider.

Kumar et al., [9] developed a biometric authentication system to grant user access to a cloud-based environment. The system combines biometric authentication with cryptographic methods. It captures fingerprint features from images using a self-learning algorithm, stores them in a database for authentication, and converts them into bio keys using hash functions. The suggested approach is more costeffective in terms of computing and communication resources than the current techniques. Researchers have suggested that future improvements could involve the use of other biometric methods to enhance user authentication processes.

Vulnerabilities, according to Modi et al., [10] are defined as Cloud safety loopholes, which an opponent can use to obtain access to the network and other infrastructure resources. A Cloud threat is a possible negative occurrence that can be malicious or incidental. An attack involves a Cloud resource damage activity, and a vulnerability exploitation may influence the accessibility of Cloud computing and financial benefits.

J. Mohammed Ubada et al. [22] proposed the Multi-Factor Authentication (MFA) scheme to enhance cloud security authentication by incorporating multiple factors. This method focuses on efficiently restricting access and dynamically generating a one-time-use password (OTUP) for services. It prioritizes confirming the user's OTUP before granting access to a cloud. Once the OTUP is verified, user authentication is validated through graphical user authentication. This innovative approach is highly efficient and streamlines cloud-computing tasks. Future security measures could include facial recognition

Nenvani et al., [11] delve into the security aspects of cloud computing architecture, particularly focusing on the Infrastructure as a Service (IaaS) layer. The paper comprehensively examines vulnerabilities within IaaS, specifically addressing issues related to virtualization, such as attacks on VM image sharing, VM isolation violation, insecure VM migration, and VM escape, while also proposing corresponding solution.

A. Punia et al., [12] explored blockchain applications in various domains and identified secure data sharing and decentralized control as key benefits in cloud systems. They discussed how ML, when combined with blockchain, can mitigate common security threats in cloud and IoT environments, such as man-in-the-middle and DDoS attacks.

Sagar et al. [13] proposed a password authentication framework that enhances security by integrating elliptic curve cryptography (ECC) and attribute-based encryption. In this framework, passwords are converted into hash values using ECC, and then transformed into negative passwords using a specialized algorithm. These negative passwords are further

encrypted into Encrypted Negative Passwords (ENPs) using multi-iteration encryption that combines cryptographic hash functions, negative passwords, and symmetric key algorithms. This method strengthens the protection against dictionary attacks without requiring additional elements.

Saleem et al. [14] introduced a convenient and affordable multi-factor authentication system that did not require any special setups. During registration, users choose and memorize three images as graphical passwords, that they must correctly identify when logging in. This system effectively prevents keyloggers and screen capture attacks. However, there are potential security risks associated with relying solely on graphical passwords, such as vulnerabilities related to image memorization.

Selamat et al., [15] provide a study that uses three ML algorithms to identify and examine the data to determine the malware issues in CC and then selects the best model based on the accuracy achieved. With the advances in ML algorithms to identify and detect the threats in computing technologies, there has been a rise in attackers as well such as the Denial of Service (DoS) attacks in Distributed DoS (DDoS) systems. The DDoS attacks have been identified as one of the major threats in the cloud computing system.

More targeted contributions include Shrestha et al. [16], who proposed a hybrid system combining blockchain for decentralized access and ML for behavioral policy evaluation, achieving improved anomaly detection and enforcement efficiency. They provided a foundational overview of blockchain architecture and consensus algorithms, which underpins many ML-integrated security systems. Lastly, conducted a systematic literature review summarizing various approaches where blockchain and ML were co-applied in the cloud to ensure data integrity, threat prediction, and autonomous decision-making.

III. Enhancing Intelligent Cardiovascular Health Monitoring using deep learning

In this section, Cloud Computing Security Based Intrusion Detection Using ANN is presented. This section describes the methodology employed to construct the proposed model, illustrated in figure1.

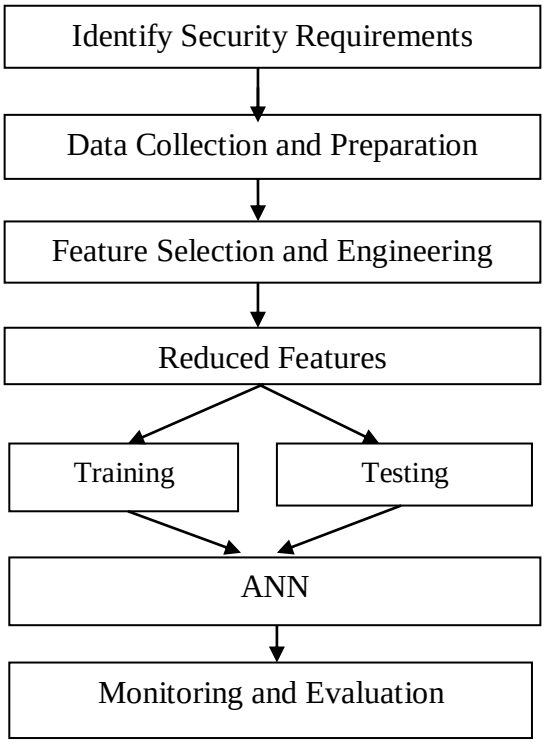

Fig. 1. The architecture of proposed system

Artificial Neural Network (ANN) models play a crucial role in enhancing cloud computing security. These models are utilized in various cloud security applications, including intrusion detection, malware detection, anomaly detection, log analysis, access control etc. As already

mentioned, the biggest value of ANN models lies in the ability to learn complex patterns, detect anomalies, and adapt to evolving threats. However, when it comes to choosing the specific models for the cloud security, it fully depends on the nature of the problem, availability of computational resources, data, sensitivity and the architecture of the existing system and other requirements case-specific to the organization.

Organizations can integrate ANN techniques into their cloud security strategies in several ways. As already discussed, organizations can have multiple benefits from integration of ANN in cloud computing security. Regardless of the application in tasks such as Data Analysis, Anomaly Detection, Malware Detection and Classification, Intrusion Detection, Prevention, User Authentication, and Access Control, the successful implementation of ANN model requires adequate strategies and resources.

In Figure 1 are shown key steps to integrate ANN into cloud security. By following these steps, organizations can successfully integrate ANN into their cloud computing security strategies. However, for the organizations that want to integrate the ANN in existing solutions and architectures of security, the process would require a more thorough evaluation. The first phase towards implementation requires assessment of strengths and weaknesses of the existing system. This would allow easier identification of areas and tasks that might require or allow ANN integration.

The phase of finding the areas and tasks that could be enhanced using ANN is closely related to pre-defined objectives or goals the organization has. Having clearly defined objectives, to determine the specific tasks or challenges that ANN can address within the cloud security system is very important for the optimization of strategies. The latter has direct indication to the model selection that is suitable for the identified tasks and purposes. Training the model requires vast amount of data that are pre-processed and carefully selected for the given task. Given the importance of dataset selection, data processing and preparation, this phase requires a thorough investigation. The whole success of the model depends on dataset and data preparation.

Aiming to determine the effect of factors on cloud security costs, we present a new approach using a feed forward propagation ANN model. Based on homogeneous encryption technology, the suggested method may immediately train and create a simple ANN model for encrypted data. For the implementation of the approach there are three phases: the training phase, the testing phase, and the validation phase, which are linked across a cloud environment.

ANNs are trained using labeled data, where the input features are known, and the corresponding outputs are provided for learning. The training process involves presenting the input data to the network, computing the output, comparing it with the expected output, and adjusting the weights and biases through back propagation. The ANN method can be applied to various tasks, including classification, regression, pattern recognition, and time-series forecasting. Its effectiveness depends on factors such as the quality and quantity of the training data, the choice of network architecture, and the optimization algorithm used for weight adjustment.

The dataset is usually divided into three subsets for training, validation, and testing. The training subset is used to train the ANN model. It comprises a large portion of the dataset and is used to optimize the network's weights and biases through the learning process. The test subset is used to evaluate the final performance of the trained ANN model. It provides an unbiased assessment of the model's generalization capabilities on unseen data.

In anomaly detection, the choice of features (data attributes) is critical. Feature selection and engineering involve determining which data points are most relevant for detecting anomalies and extracting meaningful information from raw data. Cloud security practitioners must carefully curate and preprocess the data, selecting attributes that encapsulate important characteristics of the cloud environment. Feature engineering often involves transforming and scaling data to improve the performance of ANN models. Carefully select the features (attributes) that are most relevant to the anomaly detection task. These features should capture the behavior or characteristics of the cloud environment that you want to monitor. Feature engineering may involve creating new features or transforming existing ones to better represent the data's underlying patterns.

Our intrusion detection model includes feature selection to identify and combine useful features for accurate detection. The graphic data visualization task is used to select the optimum feature subset that can enhance the prediction of the proposed model. Once the subset is selected, the ANN algorithm is applied to obtain a reliable classifier to distinguish between normal or abnormal activities.

IV.RESULT ANALYSIS

In this section, Cloud Computing Security Based Intrusion Detection Using ANN is presented. It is crucial to compute a range of evaluation metrics, including accuracy, precision, recall, and F1-score, to evaluate and compare the performance of the ANN model utilized in this research. The effectiveness of the models can be evaluated by analyzing these metrics based on specific criteria. These metrics provide important information regarding the precision and reliability of the models, and further analysis can be conducted based on these calculations. The experiment was performed, obtaining the results as shown in table 1.

Precision: Precision indicates the proportion of accurate positive predictions. This was computed using the following equation: The equation 1 is defined as:

$$Precision = \frac{TP}{(TP+FP)} X100 \quad (1)$$

Recall: Recall, also known as the amount of sensitivity or true-positive rate, is the percentage of genuine positive cases recognized properly by the model. The formula used to calculate the recall is as follows: The equation 2 is defined as:

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

F1-score: The F1-score is a balanced statistic that includes precision and recall using a weighted average. F1 Score can be viewed as the measure that balances precision and recall, yielding one score for assessing the performance of the model. This computation can be performed using the following equation: The mathematical representation of the equation 3 is defined as:

$$F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (3)$$

Accuracy: Accuracy, commonly known as the true positive rate, assesses the overall accuracy of a model's predictions. This value was determined using the following formula: Accuracy can be calculated as equation 4:

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \ldots \quad (4)$$

By computing these metrics, we gained a comprehensive understanding of the model's effectiveness, encompassing accuracy, precision, recall, and the overall balance between precision and recall, as represented by the F1-score.

Table 1. Performance analysis evaluation

Models	Precision (%)	Recall (%)	F1-Score (%)	Accuracy (%)
RF	74.78	77.35	82.98	87.82
SVM	77.67	84.88	93.56	94.67
ANN	83.59	89.89	94.68	98.98

The figure 2 shows the Precision comparison between Random Forest (RF), Support Vector Machine (SVM) and proposed ANN. The x-axis shows models and y-axis shows precision percentage. Described model achieves high precision than the Random Forest (RF), Support Vector Machine (SVM).

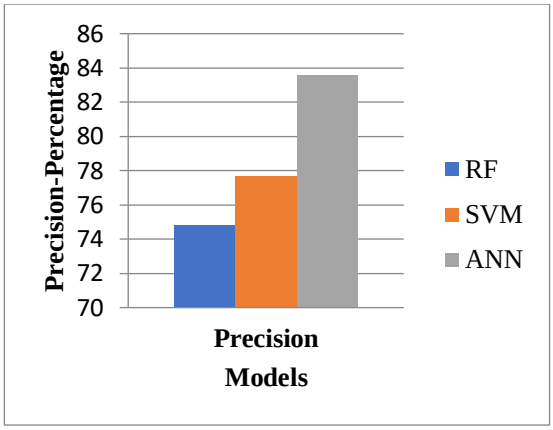

Fig. 2. PRECISION COMPARISION GRAPH

Figure 3 compares the Recall of the proposed ANN technique with that of the Random Forest (RF), Support Vector Machine (SVM)-based approach. Models are displayed on the x-axis, while Recall percentage is displayed on the y-axis. The Recall of the described model is higher than the Random Forest (RF), Support Vector Machine (SVM) models.

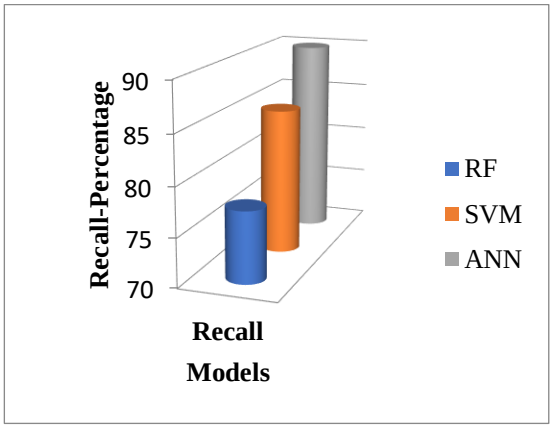

Fig. 3. RECALL COMPARISION GRAPH

The F1-Score comparison between the proposed ANN strategy and the Random Forest (RF), Support Vector Machine (SVM)-based approach is displayed in figure 4. The y-axis displays the F1-Score percentage, while the x-axis displays the models. Compared to Random Forest (RF), Support Vector Machine (SVM) models, the described model shows higher F1-Score.

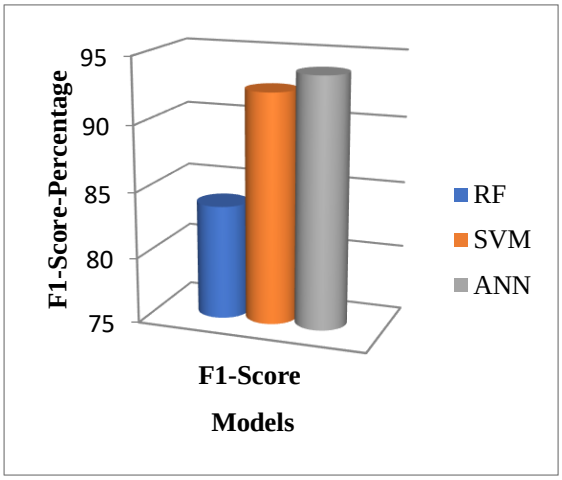

Fig. 4. F1-SCORE COMPARISION GRAPH

The proposed ANN technique's accuracy is compared with the Random Forest (RF), Support Vector Machine (SVM)-based methods in figure 5. The y-axis shows the accuracy percentage, and the x-axis shows the models. The model that is being discussed has a higher accuracy than the Random Forest (RF), Support Vector Machine (SVM) models.

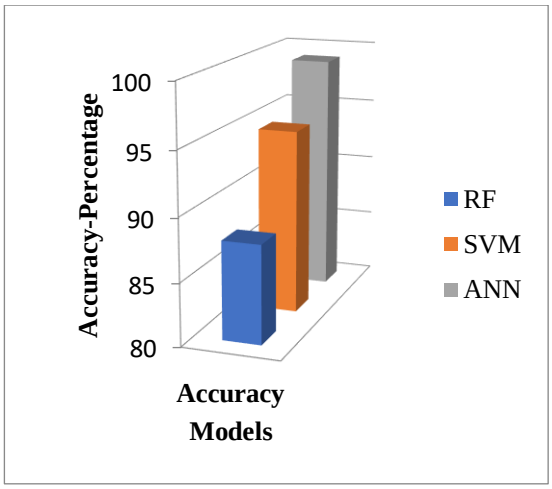

Fig. 5. ACCURACY COMPARISION GRAPH

V.CONCLUSION

In this section, Cloud Computing Security Based Intrusion Detection Using ANN is presented. To give an overview of the simple task implementing a deep learning technique, we proposed a Artificial Neural Network (ANN) model in cloud security. The model was trained and developed for encrypted data, enabling efficient analysis for the evaluation of the efficiency in cloud security. The effectiveness of the model depends on factors such as the quality and quantity of training data, network architecture design, and optimization algorithms. The integration of deep learning techniques and the implementation of ANN models offer cost-effective solutions for enhancing cloud computing security, improving threat detection, and optimizing resource allocation. A continuation of this work will further focus on certain effective elements in the overall costs of the security in cloud, being analyzed separately and as parts of a larger group classification. Addressing such objectives and research directions, ANN model can continue to advance and provide cost-effective solutions and enhance security in cloud computing. Compared to other based architectures, the presented ANN architecture has better performance in terms of Precision 83.59%, Recall 89.89%, F1-Score 94.68% and Accuracy 98.98%.

VI.REFERENCES

1. A. P. Achilleos, K. Kritikos, A. Rossini, G. M. Kapitsaki, J. Domaschka, M. Orzechowski, D. Seybold, F. Griesinger, N. Nikolov, D. Romero, and G. A. Papadopoulos, ‘‘The cloud application modelling and execution language,’’ J. Cloud Comput., vol. 8, no. 1, p. 20, Dec 2019, doi: 10.1186/s13677-019-0138-7.
2. A. Alhothaily, C. Hu, A. Alrawais, T. Song, X. Cheng, and D. Chen, “A secure and practical authentication scheme using personal devices,” IEEE

Access, vol. 5, pp. 11677–11687, 2017, doi: 10.1109/ACCESS.2017.2717862.
3. A. AlEroud and G. Karabatis, ‘‘A contextual anomaly detection approach to discover zero-day attacks,’’ in Proc. Int. Conf. Cyber Secur., pp. 40–45, Dec 2012, doi: 10.1109/CyberSecurity.2012.12.
4. J. Arshad, P. Townend, and J. Xu, ‘‘A novel intrusion severity analysis approach for clouds,’’ Future Gener. Comput. Syst., vol. 29, no. 1, pp. 416–428, Jan. 2013, doi: 10.1016/j.future.2011.08.009.
5. K. L. Chiew and B. Hui, “An improved network intrusion detection method based on CNN-LSTM-SA,” J. Adv. Res. Appl. Sci. Eng. Technol., vol. 44, no. 1, pp. 225–238, 2025, doi: 10.37934/araset.44.1.225238
6. A. Gordon, “The hybrid cloud security professional,” IEEE Cloud Comput. vol. 3, no. 1, pp. 82–86, 2016, doi: 10.1109/MCC.2016.21.
7. M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, “A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data,” IEEE Access, vol. 8, pp. 52018–52027, 2020, doi: 10.1109/ACCESS.2020.2980739.
8. M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, ‘‘Trust issues that create threats for cyber attacks in cloud computing,’’ in Proc. IEEE 17th Int. Conf. Parallel Distrib. Syst., Dec. 2011, pp. 900–905, doi: 10.1109/ICPADS.2011.156.
9. Kumar Venkatachalam, P. Prabu, A. Almutairi, and M. Abouhawwash, “Secure biometric authentication with de-duplication on distributed cloud storage,” PeerJ Comput. Sci., vol. 7, no. e569, 2021, doi: 10.7717/peerj-cs.569.
10. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, ‘‘A survey on security issues and solutions at different layers of cloud computing,’’ J. Supercomput., vol. 63, pp. 561–592, Oct 2013, doi: 10.1007/s11227-012-0831-5.
11. J. Mohammed Ubada and M. Mohamed Surputheen, “Evaluation of multifactor user security through multi authentication verifiable hybrid revert encryption for cloud computing environment,” Int. J. Comput. Sci. Netw. Secur., vol. 22, no. 9, pp. 481–488, 2022, doi: 10.22937/IJCSNS.2022.22.9.62.
12. G. Nenvani, and H. Gupta, “A survey on attack detection on cloud using supervised learning techniques,” In 2016 Symposium on Colossal Data Analysis and Networking (CDAN), pp. 1-5, 2016, doi: 10.1109/CDAN.2016.7570872.
13. A. Punia, P. Gulia and N. S. Gill, et al. “A systematic review on blockchain-based access control systems in cloud environment,” J Cloud Comp vol. 13, pp. 146, 2024, doi: 10.1186/s13677-024-00697-7.
14. S. A. Sagar, O. Bhat, M. Raina, and S. Patil, “Authentication system using cryptographic secure password storage,” Int. J. Innov. Res. Eng. Multidisciplinary Phys. Sci., vol. 6, no. 6, pp. 76–78, 2018.
15. B. O. ALSaleem and A. I. Alshoshan, “Multi-factor authentication to systems login,” in Proc. Nat. Comput. Colleges Conf., pp. 1–4, 2021, doi: 10.1109/NCCC49330.2021.9428806.
16. N.S. Selamat and F.H.M. Ali, "Comparison of malware detection techniques using machine learning algorithm," Indones. J. Electr. Eng. Comput. Sci. vol. 16, no. 1, pp. 435–440, 2019, doi: 10. 11591/ijeecs.v16.i1.pp435-440.
17. S. J. Suji Prasad, S. R. Ramprasad, P. Sivaraman, K. V. Reddy, B. P. Battula and R. Manikandan, "Enhancing Blockchain-Based Access Control in Cloud Computing with Machine Learning Techniques," 2024

International Conference on Emerging Research in Computational Science (ICERCS), Coimbatore, India, pp. 1-5, 2024, doi: 10.1109/ICERCS63125.2024.10895227.

18. E. K. Subramanian and L. Tamilselvan, ‘A focus on future cloud: machine learning-based cloud security’, SOCA, vol. 13, no. 3, pp. 237–249, Sep 2019, doi: 10.1007/s11761-019-00270-0.
19. D. V. K. Vengala, D. Kavitha, and A. S. Kumar, “Three factor authentication system with modified ECC based secured data transfer: Untrusted cloud environment,” Complex Intell. Syst., vol. 9, no. 3, pp. 2915–2928, 2023, doi: 10.1007/s40747-021-00305-0.
20. H. Xu, ‘Cybersecurity and Data Quality in Cloud Computing: A Research Framework’, in Information Systems, M. Papadaki, P. Rupino da Cunha, M. Themistocleous, and K. Christodoulou, Eds., in Lecture Notes in Business Information Processing. Cham: Springer Nature Switzerland, 2023, pp. 201–208. doi: 10.1007/978-3-031-30694-5_15.