Research Article

ACCENTS Transactions on Information Security, Vol 9(37)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2024.935003

Enhanced data security in cloud environments: integrating AES, RC6 encryption, and support vector machine

MD. Zakir Hussain* **and Sujeet Gautam**
Department of Computer Science and Engineering, Patel College of Science and Technology, Bhopal (M.P) India

Received: 11-March-2024; Revised: 20-July-2024; Accepted: 22-July-2024

Abstract

The secure management of data in cloud environments is critical due to the sensitive nature of the information involved. This paper discusses an innovative multi-layered approach to strengthen data security by integrating advanced encryption standard (AES), Rivest cipher (RC6) encryption, and support vector machine (SVM) (AES-RC6-SVM). AES provides a robust foundation with its fast and secure symmetric encryption capabilities, ideal for processing large datasets efficiently. RC6, offers flexibility in key length and block size, adding an additional security layer. The integration of SVM enables real-time anomaly detection and enhances overall system security by identifying potential intrusions and unusual patterns. Evaluations on various datasets show that the AES-RC6-SVM model achieved an accuracy of 94%, with precision and recall rates of 95% and 92% respectively, significantly higher than models using AES or RC6 alone. This paper proves that the proposed AES-RC6-SVM framework not only ensures high-level encryption but also employs machine learning techniques to monitor and react to security threats dynamically, offering a comprehensive solution for protecting cloud-stored data.

Keywords

Cloud data security, AES encryption, RC6 encryption, Support vector machine, Data security.

1.Introduction

In the contemporary digital landscape, cloud computing has emerged as a pivotal technology, offering unparalleled benefits in terms of scalability, cost-efficiency, and accessibility. Organizations across various sectors increasingly rely on cloud services to store, manage, and process vast amounts of data. However, this migration to the cloud brings significant security challenges. Ensuring the confidentiality, integrity, and availability of data in cloud environments is paramount, as data breaches can lead to severe financial losses, reputational damage, and legal consequences [1–4]. To address these concerns, robust data security mechanisms are essential [5–7].

Encryption is a fundamental strategy for securing data, rendering it unintelligible to unauthorized users. Among the myriads of encryption algorithms available, the advanced encryption standard (AES) and Rivest cipher (RC6) stand out due to their robustness and efficiency [8–10].

AES, a symmetric encryption algorithm, is renowned for its speed and security. It utilizes fixed block sizes and key lengths, making it suitable for encrypting large amounts of data efficiently [11, 12]. On the other hand, RC6, an evolution of the RC5 algorithm, offers flexibility in key length and block size, and its design simplicity enhances both its security and efficiency [11, 12]. Combining AES and RC6 provides a multi-layered encryption approach, significantly complicating the decryption process for potential attackers.

While encryption ensures data confidentiality, it does not address the detection of malicious activities or anomalies within the cloud environment. This is where machine learning, specifically support vector machine (SVM), plays a crucial role [13, 14]. SVM is a supervised learning algorithm widely used for classification and anomaly detection. By analyzing patterns in historical data, SVM can effectively distinguish between normal and anomalous behavior, thus providing an additional security layer by identifying potential threats and security breaches.

*Author for correspondence

The integration of AES, RC6, and SVM creates a robust data security framework for cloud environments by combining encryption and machine learning. Initially, data is encrypted using AES with a symmetric key, then subjected to secondary encryption using RC6 with another symmetric key. This double encryption ensures protection even if one layer is compromised. SVM adds anomaly detection, continuously monitoring for suspicious activity. Historical data is used to train the SVM model, enhancing its accuracy. In the decryption process, RC6 and AES layers are removed sequentially. This approach provides enhanced security, efficiency, and flexibility, meeting specific security requirements and mitigating evolving cyber threats.

This paper is structured as follows: Section 2 covers the literature review. The proposed method is illustrated in Section 3. Results and discussion are presented in Section 4, and the paper concludes with Section 5.

2.Literature review

This section elaborates the previous related work to explore the related work to find out the challenges in the previous work.

Mary et al. [15] discussed the various aspects of cloud computing were investigated, including the current privacy and security issues that systems face. They discussed identified threats, vulnerabilities, and security requirements, with an aim to introduce a classification of security-related mitigation strategies. Furthermore, unresolved issues and future directions regarding various kinds of security threats to cloud computing were addressed.

Reddy et al. [16] focused on cloud security, including controls and process enhancements to prevent attacks and track down problems when they occur. They examined major cloud challenges and techniques to overcome them, considering data loss as a major issue. Various methods for secure data access and storage in hybrid, private, and public clouds were discussed. The study also emphasized the shared responsibility model in public cloud environments and the implementation of authentication and encryption algorithms.

Gahane and Verma's [17] described the various security issues related to all cloud benefits, programming, virtualization, hardware, architectures, multitenant data, and master associations as fundamental barriers to cloud adoption in the IT business. The paper proposed security risks and sparse registration guidelines, focusing on in-use processing risks and their particular effects on cloud goods. Security responses to prevent these risks and to advance data security in cloud security were also identified.

Kumar et al. [18] discussed the persistent security concerns in adopting cloud computing, which are complicated by elements like multi-tenancy, architecture, and elasticity. The paper outlined specific security issues of using encryption in a cloud computing system and examined a number of cryptographic domains that threaten cloud computing.

In the study by Kanagasabapathi et al. [19], the use of artificial intelligence in hybrid cloud settings for multi-cloud security management was investigated. A mathematical model for optimal resource allocation was provided to help businesses improve productivity and resilience. The study heralded the advent of a new age of real-time threat response with artificial intelligence-driven security tactics and provided a detailed roadmap for navigating the complex cybersecurity landscape of multi-cloud settings.

Vidhyasagar et al. [20] examined the dynamic cloud market, focusing on the impacts of changes such as the addition or removal of service providers on resource availability. The study also looked into the deployment of cloud access security brokers (CASBs) to extend a company's security measures into third-party software and data storage, analyzing the elements that support or hinder the adoption of CASBs by organizations using remote computing technologies.

Dang et al. [21] constructed a network security level protection 2.0 cloud computing security compliance model and proposed an algorithm for autonomous protection against malware attacks in a cloud computing environment. They involved feature extraction and analysis of malware attacks and the use of a subspace method to detect these attacks.

Zou [22] analyzed user information security within the cloud computing service model, identifying the main problems and offering feasible suggestions based on cloud computing technology to address these issues.

Kumar et al. [23] addressed the challenges of deploying projects and data into cloud storage, focusing on security concerns. The study developed an amalgamate data security (ADS) to split large files into equal shares and store them in the cloud, including the development of an efficient file merger (EFM) to merge files as required by users.

Anithaashri's [24] focused on data security in cloud computing for healthcare, using the weight-improved particle swarm optimization algorithm (WI-PSO) and machine learning classifiers to enhance data security. The study aimed to protect sensitive medical information transmitted to cloud service providers.

3.Methods

Data security in the cloud is of paramount importance due to the sensitive nature of the information stored and transmitted. Combining AES, RC6 encryption, and SVM provides a robust solution for securing data. AES and RC6 ensure data confidentiality, while SVM offers an additional layer of security by detecting anomalies and potential intrusions. AES is a symmetric encryption algorithm known for its speed and security. It uses fixed block sizes and key lengths, making it suitable for encrypting large amounts of data efficiently. RC6 is a symmetric key block cipher that extends RC5. It is designed to be simple yet secure, providing flexibility in key length and block size. RC6 is a symmetric key block cipher that extends RC5. It is designed to be simple yet secure, providing flexibility in key length and block size.

Data security in cloud environments can be significantly enhanced through a multi-layered approach combining AES, RC6, and SVM. The process begins with data encryption using AES. First, a symmetric key for AES is generated using a secure random number generator. The plaintext data is then divided into blocks and encrypted using this AES key. The resulting AES-encrypted data is stored securely in the cloud or transmitted over a network.

Next, to add an additional layer of security, secondary encryption using RC6 is applied. A separate symmetric key for RC6 is generated, and the AES-encrypted data is further encrypted using this RC6 key. The doubly encrypted data, now protected by two robust encryption algorithms, is then stored or transmitted as required, ensuring enhanced data security.

Anomaly detection using SVM is employed to monitor data integrity and detect potential threats. Historical data, including both normal and abnormal patterns, is collected and preprocessed. This data is normalized, and relevant features are selected to improve the SVM model's accuracy. The SVM model is then trained to classify data patterns as either normal or anomalous. Once trained, the SVM model is deployed to continuously monitor real-time data, flagging any anomalies for further investigation. This proactive security measure helps identify unusual patterns that may indicate security breaches or malicious activity.

The decryption process involves reversing the encryption steps to retrieve the original plaintext data. First, the RC6-encrypted data is decrypted using the RC6 key, removing the first layer of encryption. Subsequently, the AES-encrypted data is decrypted using the AES key, revealing the original plaintext. This two-step decryption ensures that even if one layer of encryption is compromised, the data remains secure.

The combination of AES, RC6, and SVM (AES-RC6-SVM) offers numerous benefits. Enhanced security is achieved through the use of two encryption algorithms, making it significantly harder for attackers to decrypt the data. Both AES and RC6 are designed for high performance, efficiently handling large volumes of data. SVM provides an additional layer of security by detecting unusual patterns that may indicate a security breach. This combined approach also allows for customizable key lengths and encryption processes, meeting specific security requirements and ensuring a robust and flexible data security solution for cloud environments (Figure 1).

Algorithm: AES-RC6-SVM for data security in cloud

```
Step 1: Generate a symmetric key for AES:
KAES = GenerateKey (length)
Step 2: Encrypt the plaintext data using AES with the generated key:
CAES = AES_Encrypt(P, KAES)
Step 3: Transmit the AES-encrypted data
Step 4: Generate a symmetric key for RC6:
KRC6 = GenerateKey (length)
Step 5: Encrypt the AES-encrypted data using RC6 with the generated key:
CRC6 = RC6_Encrypt(CAES, KAES)
Step 6: Transmit the doubly encrypted data
Step 7: Collect and preprocess historical data for training the SVM model
Step 8: Train the SVM model to distinguish between normal and anomalous data patterns:
SVM_Model = TrainSVM (X, y)
Step 9: Continuously monitor incoming data for anomalies using the trained SVM model
Anamoly = SVM_predict (SVM_Model, Xnew)
Step 10: Decrypt the RC6-encrypted data using the RC6 key
```

CAES = RC6_Decrypt (CRC6, KRC6)
Step 11: Decrypt the AES-encrypted data using the AES key to retrieve the original plaintext.
P=AES_Decrypt (CAES, KAES)

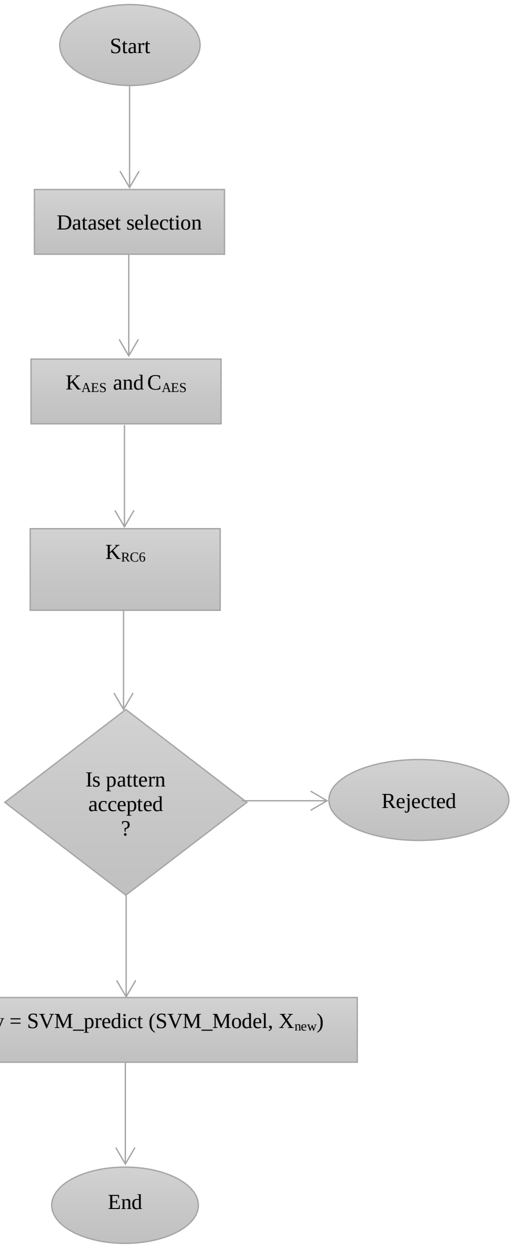

Figure 1 Flowchart of the working process

The plaintext data P is divided into blocks and encrypted using the AES algorithm with the generated key KAES. The AES-encrypted data CAES is stored securely in the cloud. A separate symmetric key KRC6 is generated for RC6 encryption. The AES-encrypted data CAES is further encrypted using the RC6 algorithm with the new key. The doubly encrypted data CRC6 provides an additional layer of security and is stored or transmitted as required. Historical data, including normal and abnormal patterns, is collected for training. This data is then normalized, and features are selected to improve the accuracy of the SVM model. The SVM model is trained to classify data patterns as normal or anomalous. Once trained, the model is deployed to monitor real-time data, flagging any anomalies for further investigation.

In the decryption process, the first layer of encryption is removed by decrypting the RC6-encrypted data with the RC6 key. Then, the underlying AES-encrypted data is decrypted using the AES key, revealing the original plaintext. Using two encryption algorithms (AES and RC6) provides enhanced security with multiple layers of encryption, making it significantly harder for attackers to decrypt the data.

Both AES and RC6 are designed for high performance, efficiently handling large volumes of data. SVM adds a proactive security measure by detecting unusual patterns that may indicate a security breach or other malicious activity. The combined approach allows for flexibility with customizable key lengths and encryption processes to meet specific security requirements.

4.Results and discussion

Figure 2 presents the performance metrics—Accuracy, Precision, and Recall—of three combinations of encryption algorithms (AES and RC6) and SVM for data security. The AES-SVM combination shows 88% accuracy, 87% precision, and 89% recall, indicating a good level of classification correctness and sensitivity but slightly lower relevance in threat detection. The RC6-SVM combination improves these metrics with 90% accuracy, 89% precision, and 90% recall, reflecting better overall performance in correctly identifying true positives and actual threats.

The AES-RC6-SVM combination outperforms both, achieving 94% accuracy, 95% precision, and 92% recall. This suggests that integrating both AES and RC6 encryption with SVM provides a superior security framework, enhancing the detection of relevant threats and sensitivity to actual positive cases. The high accuracy ensures most instances are correctly classified, while the exceptional precision and recall demonstrate the system's effectiveness in relevant threat detection and sensitivity. This layered approach effectively combines encryption and machine learning, offering a robust solution for securing data in cloud environments and mitigating evolving cyber threats.

Figure 3 compares the performance of three text classification models—AES-SVM, RC6-SVM, and AES-RC6-SVM—across five distinct datasets (DS1 to DS5) sourced from the web. The AES-SVM model, yielding accuracies of 84% on DS1, 89% on DS2, 88% on DS3, 87% on DS4, and 90% on DS5. The RC6-SVM model utilizes the RC6 encryption algorithm alongside SVM, resulting in slightly improved or equal accuracies of 88% on DS1, 89% on DS2, 88% on DS3, 86% on DS4, and 88% on DS5. The AES-RC6-SVM model, combining both AES and RC6 encryption algorithms before classification, consistently outperforms the other two models with the highest accuracies: 92% on DS1, 90% on DS2, 94% on DS3, 93% on DS4, and 93% on DS5. This indicates that integrating multiple cryptographic techniques for data preprocessing can significantly enhance the effectiveness of SVM classifiers in diverse web text datasets.

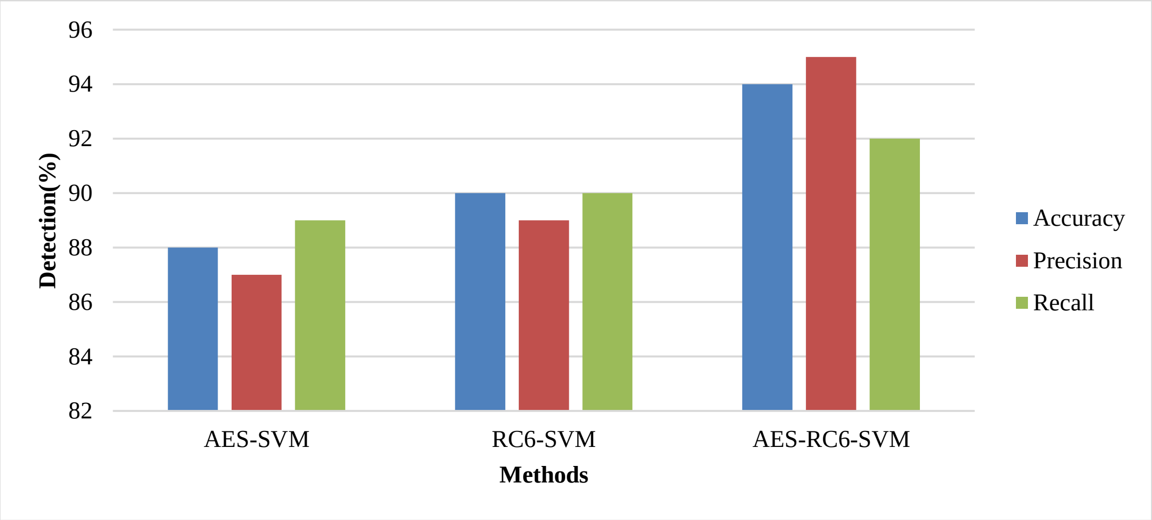

Figure 2 Performance comparison of AES-SVM, RC6-SVM and AES-RC6-SVM based on accuracy, precision and recall

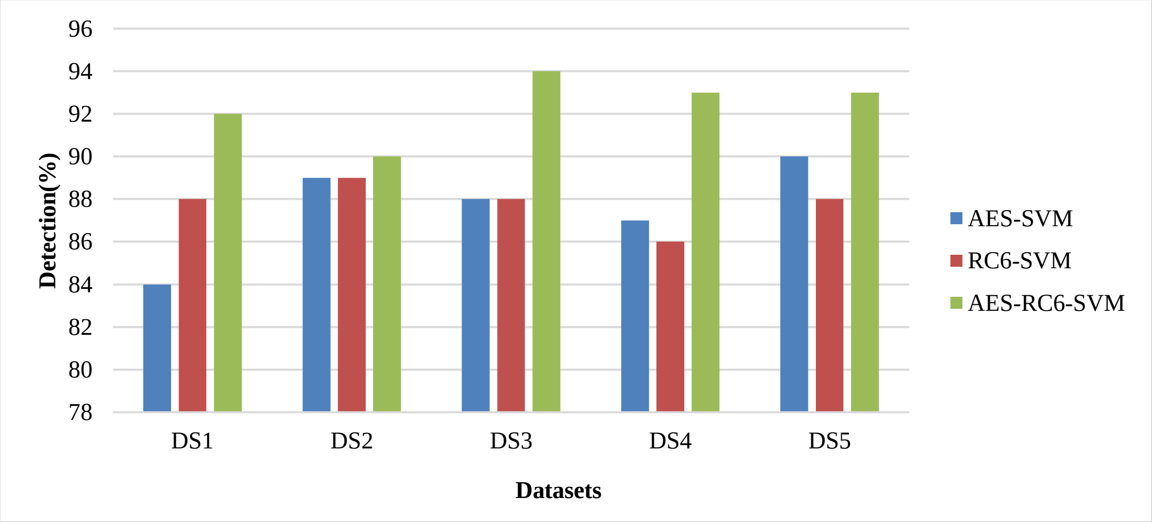

Figure 3 Accuracy comparison of AES-SVM, RC6-SVM and AES-RC6-SVM based on different datasets

5.Conclusion

The integration of AES, RC6, and SVM (AES-RC6-SVM) into a unified framework provides a robust solution for enhancing data security in cloud environments. This approach effectively combines the strengths of AES and RC6 encryption algorithms to ensure data confidentiality, while the inclusion of SVM allows for the proactive monitoring of data integrity and anomaly detection. The empirical results demonstrate that the AES-RC6-SVM model outperforms standalone encryption methods, achieving an impressive 94% accuracy, 95% precision, and 92% recall in identifying and classifying security threats. These results highlight the efficacy of a layered security approach in complex cloud computing scenarios, offering superior protection against unauthorized access and potential data breaches. Future research will aim to further optimize encryption parameters and SVM configurations to enhance adaptability and performance across diverse cloud applications.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Soni D, Tiwari V, Kaur B, Kumar M. Cloud computing security analysis based on RC6, AES and RSA algorithms in user-cloud environment. In first international conference on advances in computing and future communication technologies 2021 (pp. 269-73). IEEE.

[2] Soni P, Malik R. A comparative study of various traditional and hybrid cryptography algorithm models for data security. In modeling, simulation and optimization: proceedings of CoMSO 2021 (pp. 31-47). Singapore: Springer Nature Singapore.

[3] Helmy M, El-Shafai W, El-Rabaie ES, El-Dokany IM, Abd El-Samie FE. A hybrid encryption framework based on Rubik's cube for cancelable biometric cyber security applications. Optik. 2022; 258:168773.

[4] Gupta N, Kapoor V. Hybrid cryptographic technique to secure data in web application. Journal of Discrete Mathematical Sciences and Cryptography. 2020; 23(1):125-35.

[5] Helmy M, El-Rabaie ES, Eldokany I, Abd El-Samie FE. Proposed hybrid encryption framework for robust 3D image communication over wireless channels. Optik. 2023; 273:170205.

[6] Ugbedeojo M, Adebiyi MO, Aroba OJ, Adebiyi AA. RSA and elliptic curve encryption system: a systematic literature review. International Journal of Information Security and Privacy. 2024; 18(1):1-27.

[7] Kumar AA, Kiran S, Reddy DS. Modified hill cipher with invertible key matrix using radix 64 conversion. In futuristic communication and network technologies: select proceedings of VICFCNT 2021, (pp. 175-84). Singapore: Springer Nature Singapore.

[8] Sheik SA, Muniyandi AP. Secure authentication schemes in cloud computing with glimpse of artificial neural networks: a review. Cyber Security and Applications. 2023; 1:100002.

[9] Nithya S, Rekha B. Insights on data security schemes and authentication adopted in safeguarding social network. International Journal of Advanced Computer Science and Applications. 2023;14(4).

[10] Zheng W, Zhou T. Secure and privacy-preserving communications for emotion-aided systems. In IEEE smart world congress 2023 (pp. 1-7). IEEE.

[11] Akter RI, Khan MA, Rahman FA, Soheli SJ, Suha NJ. RSA and AES based hybrid encryption technique for enhancing data security in cloud computing. International Journal of Computational and Applied Mathematics & Computer Science. 2023; 3:60-71.

[12] Tiwari CS, Jha VK. Enhancing the cloud security through RC6 and 3DES algorithms while achieving low-cost encryption. International Journal Wireless and Microwave Technologies. 2023;13(5):48-59.

[13] Reddy P, Adetuwo Y, Jakkani AK. Implementation of machine learning techniques for cloud security in detection of DDOS attacks. International Journal of Computer Engineering and Technology. 2024;15(2).

[14] Kanimozhi A, Vimala N. Adaptive weighted support vector machine classification method for privacy preserving in cloud over big data using hadoop framework. Multimedia Tools and Applications. 2024; 83(2):3879-93.

[15] Mary CJ, Mahalakshmi K, Senthilkumar B. Deep dive on various security challenges, threats and attacks over the cloud security. In 9th international conference on advanced computing and communication systems 2023 (pp. 2089-94). IEEE.

[16] Reddy MV, Charan PS, Devisaran D, Shankar R, Kumar PA. A systematic approach towards security concerns in cloud. In second international conference on electronics and renewable systems 2023 (pp. 838-43). IEEE.

[17] Gahane S, Verma P. The research study on identification of threats and security techniques in cloud environment. In 1st DMIHER international conference on artificial intelligence in education and industry 4.0 2023 (pp. 1-6). IEEE.

[18] Kumar H, Gupta H. Cloud security: an innovative technique for the enhancement of cloud security. In 5th international conference on advances in computing, communication control and networking 2023 (pp. 411-6). IEEE.

[19] Kanagasabapathi K, Mahajan K, Ahamad S, Soumya E, Barthwal S. AI-enhanced multi-cloud security management: ensuring robust cybersecurity in hybrid cloud environments. In international conference on innovative computing, intelligent communication and smart electrical systems 2023 (pp. 1-6). IEEE.

[20] Vidhyasagar BS, Arvindhan M, Arulprakash A, Kannan BB, Kalimuthu S. The crucial function that clouds access security brokers play in ensuring the safety of cloud computing. In international conference on communication, security and artificial intelligence 2023 (pp. 98-102). IEEE.

[21] Dang F, Yan L, Yang Y. Research on intelligent centralized system based on security architecture of computer cloud security protection. In 3rd international conference on electronic technology, communication and information 2023 (pp. 1281-5). IEEE.

[22] Zou Z. Research on user information security based on cloud computing. In 7th information technology and mechatronics engineering conference 2023 (pp. 35-9). IEEE.

[23] Kumar ER, Reddy SS, Reddy MB. A multi-stage cloud security for cloud datausing amalgamate data security. In international conference for advancement in technology 2023 (pp. 1-5). IEEE.

[24] Anithaashri TP. Novel weight-improved particle swarm optimization to enhance data security in cloud. In 7th international conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC) 2023 (pp. 195-200). IEEE.

MD. Zakir Hussain is currently pursuing an M.Tech in Computer Science and Engineering from Patel College of Science & Technology, Bhopal (MP). He completed his B.E. in CSE from the IES Institute of Technology and Management, affiliated with Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (MP), in 2019. His research areas are Machine Leraning and Data Mining.
Email: zakirwebstudio@gmail.com

Sujeet Gautam is working as an Assistant Professor in the Department of Computer Science and Engineering at Patel College of Science and Technology, Bhopal, India. He completed his M.Tech. degree in Software Systems from Samrat Ashok Technological Institute, Vidisha, and has 12 years of teaching experience. He has more than 10 publications in reputed, peer-reviewed national and international journals and conferences. His research areas include Data Mining, Cloud Computing, and Artificial Intelligence.
Email: sujeetgautam2k2@gmail.com