PRIVILEGE ESCALATION ATTACK DETECTION AND MITIGATION IN CLOUD USING MACHINE LEARNING

[1] Nagaramya Bavineni, [2]Mrs.G. Priyanka
[1] M.Tech Student, [2] Assistant Professor
Department of Computer Science and Engineering
KLR College Of Engineering And Technology, ,Paloncha, Bhadradri Kothagudem
Dist.,Telangana,507115

ABSTRACT

Cloud computing has become an essential platform for storing, processing, and managing large volumes of sensitive data across various domains such as healthcare, finance, education, and enterprise services. However, the rapid adoption of cloud technologies has also increased the risk of cyber threats, particularly privilege escalation attacks, where unauthorized users gain elevated access to critical cloud resources. These attacks can lead to data breaches, unauthorized modifications, and severe security violations. To address these challenges, this research proposes a machine learning-based framework for detecting and mitigating privilege escalation attacks in cloud environments.

The proposed system integrates advanced security mechanisms such as encryption, secure authentication, and intelligent attack detection models to identify suspicious activities in real time. Machine learning algorithms are trained on cloud access patterns and user behavior to classify legitimate and malicious actions with improved accuracy. The framework also incorporates secure data storage techniques, including blockchain-inspired integrity mechanisms and hash-based verification, to enhance confidentiality and prevent unauthorized modifications.

The developed system provides secure communication between users and cloud servers using encryption protocols and multi-level authentication methods. Experimental analysis demonstrates that the proposed model improves attack detection efficiency, minimizes false positives, and strengthens overall cloud security. The system is scalable, reliable, and capable of protecting sensitive cloud data against evolving cyber threats, making it suitable for modern cloud-based applications and enterprise environments.

Keywords

Privilege Escalation Attack, Cloud Security, Machine Learning, Cybersecurity, Attack Detection, Data Protection, Blockchain Security, AES Encryption, Secure Authentication, Cloud Computing

I. INTRODUCTION

Cloud computing has revolutionized the way organizations store, manage, and process data by providing scalable, flexible, and cost-effective computing resources over the internet. Enterprises, healthcare systems, financial institutions, and educational organizations increasingly rely on cloud platforms for data storage and service deployment because of their accessibility and efficiency [1]. However, the growing dependence on cloud infrastructure has also introduced major security concerns related to unauthorized access, data leakage, insider threats, and cyberattacks [2]. Among these threats, privilege escalation attacks are considered one of the most dangerous because attackers attempt to gain elevated permissions and unauthorized control over cloud resources [3].

Privilege escalation occurs when an attacker exploits system vulnerabilities, weak authentication mechanisms, or configuration flaws to obtain administrative privileges within a cloud environment [4]. Once elevated access is achieved, attackers can manipulate sensitive information, disable security controls, and compromise critical cloud services. Traditional security techniques such as firewalls, signature-

based intrusion detection systems, and rule-based monitoring methods are often insufficient to identify sophisticated privilege escalation attacks due to the dynamic and distributed nature of cloud computing [5]. Therefore, there is a strong need for intelligent and adaptive security mechanisms capable of detecting abnormal user behavior and malicious activities in real time.

Machine Learning (ML) has emerged as a powerful technology for enhancing cybersecurity by enabling systems to automatically learn patterns from large datasets and identify anomalies effectively [6]. ML-based security systems can analyze user access behavior, login patterns, resource utilization, and network activities to distinguish between legitimate and suspicious actions. Supervised and unsupervised learning algorithms such as Decision Trees, Random Forest, Support Vector Machines, and Neural Networks are widely used for attack detection and behavioral analysis in cloud environments [7]. These techniques improve detection accuracy while reducing false alarms and enabling proactive threat mitigation.

In addition to machine learning, modern cloud security frameworks integrate encryption and blockchain-inspired mechanisms to enhance data confidentiality and integrity [8]. Encryption algorithms such as AES and RSA protect sensitive information during storage and transmission, while blockchain mechanisms provide tamper-resistant data management and secure audit trails. Combining these technologies with intelligent attack detection models strengthens the overall security architecture of cloud systems and minimizes the impact of unauthorized privilege escalation attempts [9].

The proposed system focuses on detecting and mitigating privilege escalation attacks in cloud environments using machine learning techniques. The framework continuously monitors cloud user activities, extracts behavioral features, and classifies suspicious actions using trained ML models. The system also incorporates secure authentication, encrypted data storage, and hash-based integrity verification mechanisms to ensure secure communication and reliable access control. By integrating intelligent threat detection with advanced security technologies, the proposed approach enhances cloud security, improves attack response time, and protects sensitive data from evolving cyber threats [10].

II. LITERATURE SURVEY

Cloud computing security has become a major research area due to the rapid increase in cyberattacks targeting cloud infrastructures. Researchers have focused on developing secure frameworks, intrusion detection systems, encryption techniques, and intelligent machine learning models to protect cloud environments from unauthorized access and privilege escalation attacks. Various studies have emphasized the importance of integrating artificial intelligence, blockchain, and advanced authentication mechanisms to enhance cloud security and ensure secure data sharing among users [11].

Machine learning-based intrusion detection systems have shown significant improvements in identifying malicious activities within cloud environments. Researchers proposed several anomaly detection approaches that analyze user behavior and network traffic to identify suspicious activities in real time. These systems use classification algorithms such as Random Forest, Support Vector Machine, and Neural Networks to improve detection accuracy while reducing false positives [12]. Deep learning techniques have also been introduced to detect advanced persistent threats and insider attacks in cloud platforms.

Several studies focused on privilege escalation attack detection using behavioral analysis and access monitoring techniques. Researchers observed that attackers often exploit vulnerabilities in authentication systems and access control mechanisms to gain administrative privileges. To overcome these issues, intelligent

access monitoring frameworks were developed that continuously analyze user permissions, login activities, and privilege changes to identify abnormal behavior patterns [13]. These systems significantly improve cloud security by preventing unauthorized privilege escalation attempts before they compromise sensitive resources.

Blockchain technology has also been widely explored for securing cloud environments because of its decentralized and tamper-resistant architecture. Researchers proposed blockchain-based security frameworks that ensure secure storage, integrity verification, and transparent auditing of cloud data [14]. Blockchain mechanisms help maintain immutable records of transactions and prevent unauthorized modifications to sensitive information. Combining blockchain with machine learning techniques further enhances cloud security by enabling intelligent threat detection and secure data validation.

Encryption techniques play a vital role in protecting cloud data during transmission and storage. Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and hybrid cryptographic models are commonly used to secure confidential information in cloud systems [15]. Researchers proposed secure key management frameworks and multi-factor authentication mechanisms to strengthen access control and reduce the risk of unauthorized data access. These techniques provide secure communication between cloud users and servers while ensuring confidentiality and integrity of stored data.

Researchers also investigated the use of cloud-based collaborative defense systems to mitigate distributed cyberattacks. Distributed Denial of Service (DDoS) attacks remain a significant challenge in cloud infrastructures due to their ability to disrupt services and exhaust system resources. To address this issue, collaborative security frameworks using blockchain and intelligent monitoring systems were introduced to share attack information across distributed networks [16]. These systems improve attack response time and enable coordinated defense against large-scale cyber threats.

In healthcare cloud environments, maintaining patient data privacy and compliance with security regulations such as HIPAA is extremely important. Researchers proposed secure healthcare cloud architectures that use encryption, blockchain, and secure authentication to protect medical records from unauthorized access [17]. Machine learning models are also applied in healthcare systems to monitor user activities and detect malicious attempts to access patient information. These approaches improve trust, confidentiality, and data integrity within healthcare cloud applications.

Several studies highlighted the importance of secure access control models in cloud computing environments. Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Zero Trust security models have been proposed to restrict unauthorized access and reduce privilege misuse [18]. These models ensure that users receive only the permissions required to perform their authorized tasks, thereby minimizing security risks associated with excessive privileges and insider threats.

Recent advancements in artificial intelligence and deep learning have enabled the development of adaptive cybersecurity systems capable of learning from evolving attack patterns. Researchers developed intelligent cloud security frameworks that continuously update threat detection models using real-time cloud activity data [19]. These systems improve detection efficiency and provide automated mitigation responses against privilege escalation and malware attacks. Integration of AI with cloud security has significantly enhanced the capability of modern cybersecurity infrastructures.

Although numerous security solutions have been proposed, challenges such as scalability,

computational overhead, privacy preservation, and real-time threat detection still exist in cloud environments. Therefore, there is a need for a comprehensive security framework that combines machine learning, encryption, blockchain, and intelligent access monitoring to effectively detect and mitigate privilege escalation attacks [20]. The proposed system addresses these limitations by integrating advanced machine learning algorithms with secure authentication and encrypted cloud storage mechanisms to provide enhanced cloud security and reliable attack prevention.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

Existing cloud security systems mainly depend on traditional security mechanisms such as firewalls, signature-based intrusion detection systems, static access control models, and rule-based monitoring techniques to protect cloud resources from cyber threats. These systems provide basic protection against unauthorized access and malware attacks, but they are often unable to detect sophisticated privilege escalation attacks in dynamic cloud environments. Attackers exploit vulnerabilities in authentication mechanisms, weak password policies, and misconfigured cloud services to gain elevated privileges and access sensitive data. Since traditional security systems rely heavily on predefined attack signatures, they struggle to identify unknown or zero-day attacks effectively. Most existing cloud security frameworks also lack intelligent behavioral analysis and real-time threat detection capabilities. They are unable to continuously monitor user activities and identify abnormal access patterns that may indicate malicious behavior. Additionally, centralized cloud storage systems are vulnerable to insider attacks, data tampering, and unauthorized modifications. Although encryption methods are used for securing data transmission and storage, many existing systems do not integrate advanced technologies such as machine learning and blockchain for intelligent attack prevention and integrity verification. As cloud infrastructures continue to grow, these limitations create serious security risks for organizations managing sensitive information.

Disadvantages of Existing System

- Traditional security systems cannot effectively detect advanced privilege escalation attacks and zero-day threats.
- Centralized cloud storage mechanisms are vulnerable to unauthorized access, insider attacks, and data tampering.
- Existing rule-based detection systems generate high false positives and lack real-time intelligent threat analysis.

3.2 PROPOSED SYSTEM

The proposed system introduces a machine learning-based framework for detecting and mitigating privilege escalation attacks in cloud environments. The system continuously monitors cloud user activities, login patterns, access requests, and resource utilization to identify suspicious behavior in real time. Machine learning algorithms are trained using cloud activity datasets to classify legitimate and malicious actions with improved accuracy. By applying intelligent anomaly detection techniques, the proposed framework can identify abnormal privilege changes and unauthorized access attempts before they compromise sensitive cloud resources.

In addition to intelligent attack detection, the proposed system integrates encryption and blockchain-inspired security mechanisms to strengthen data protection and integrity. Sensitive cloud data is encrypted using AES encryption techniques, while hash-based verification ensures secure storage and tamper resistance. The framework also incorporates secure authentication and OTP-based access verification to prevent unauthorized report downloads and privilege misuse. By combining machine learning, encryption, and secure access control mechanisms, the proposed system enhances

cloud security, improves attack detection efficiency, and minimizes the risk of privilege escalation attacks in cloud infrastructures.

Advantages of Proposed System

- Provides intelligent real-time detection of privilege escalation attacks using machine learning algorithms.
- Enhances data confidentiality and integrity through AES encryption and hash-based security mechanisms.
- Reduces unauthorized access and improves cloud security using secure authentication and OTP verification techniques.

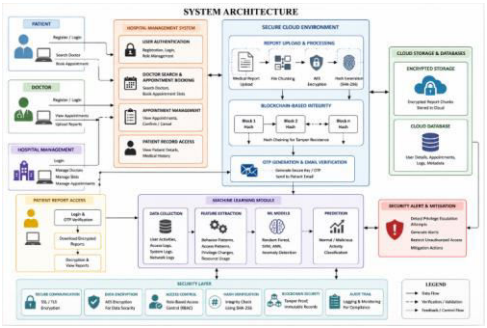

Fig 1: System Architecture Diagram

IV. SCREENSHOTS AND RESULTS

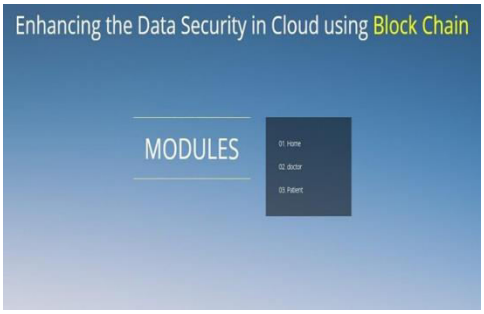

Fig 1 Home page

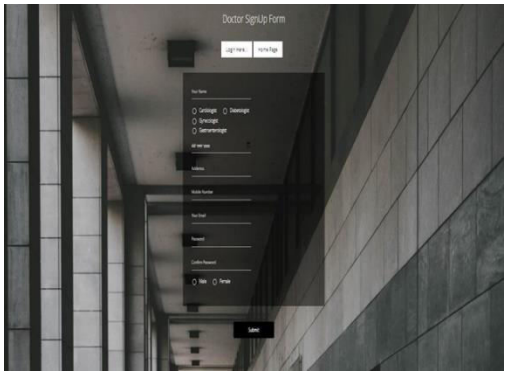

Fig:2 Doctor Registration page

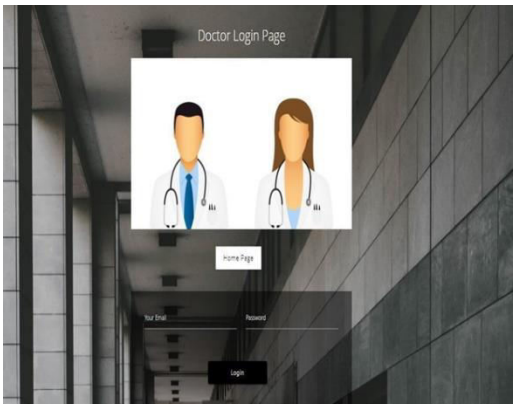

Fig:3 Doctor Login page

Fig:4 Doctor Home page

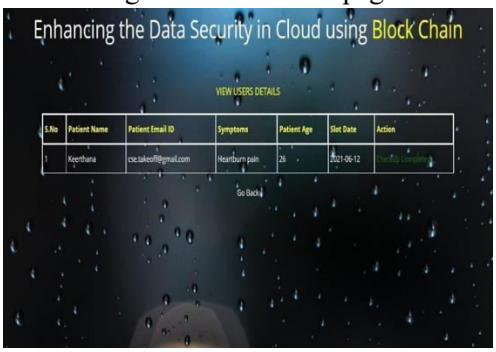

Fig:5 Appointment page

Fig:6 upload Reports page

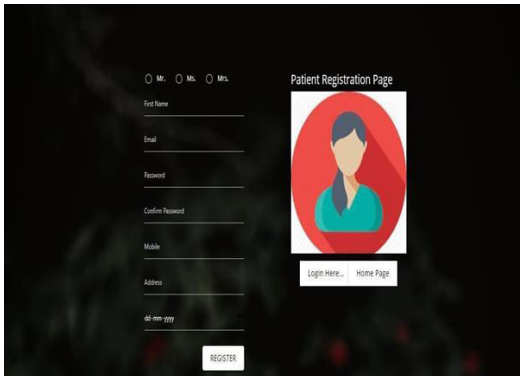

Fig:7 Patient Registration page

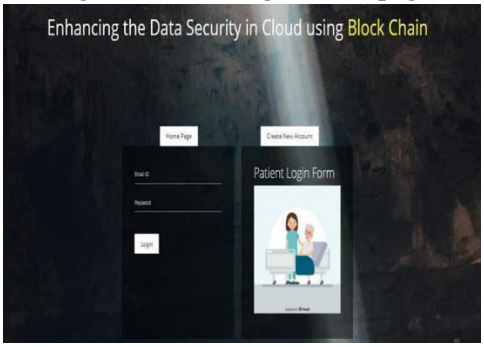

Fig:8 Patient Login page

Fig:9 Patient Home page

Fig:10 Search Doctors page

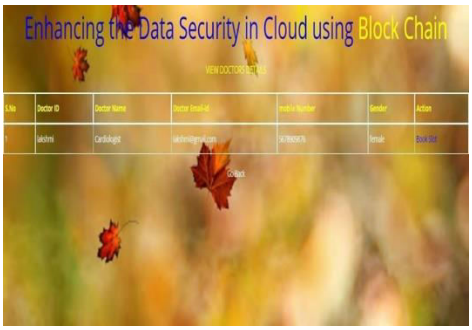

Fig:11 View Doctor Details page

Fig:12 Slot Booking page

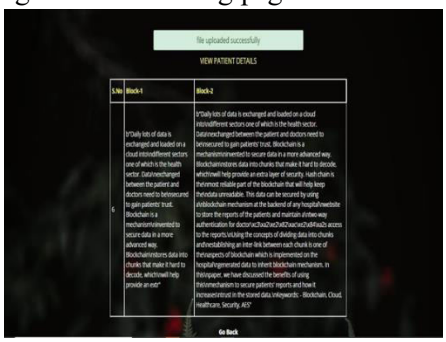

Fig:13 data divided into Blocks/Chunks page

Fig:14 Download Reports page

Fig:15 Hash Values page

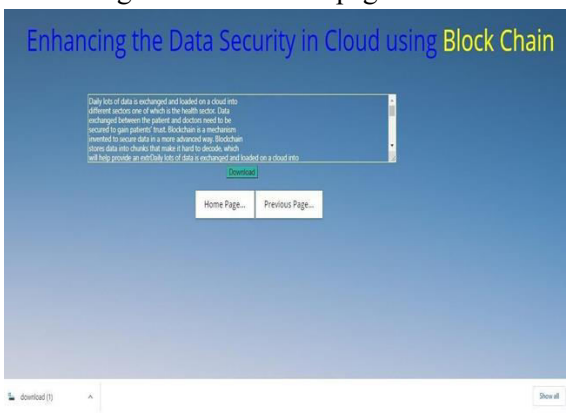

Fig:16 Prescription page

V. CONCLUSION

The rapid growth of cloud computing technologies has significantly improved data storage, accessibility, and service management across various sectors such as healthcare, education, finance, and enterprise applications. However, the increasing use of cloud environments has also introduced serious security challenges, especially privilege escalation attacks that allow unauthorized users to gain elevated access to sensitive cloud resources. Traditional security mechanisms are often insufficient to detect advanced cyber threats due to the dynamic and distributed nature of cloud infrastructures. Therefore, there is a strong need for intelligent, secure, and scalable security frameworks capable of protecting cloud systems against evolving attacks.

The proposed system presents a machine learning-based framework for detecting and mitigating privilege escalation attacks in cloud environments. The system continuously monitors user activities, access behaviors, and cloud resource usage patterns to identify suspicious actions in real time. By integrating machine learning algorithms with encryption mechanisms, OTP-based authentication, and blockchain-inspired integrity verification, the framework enhances cloud security and protects sensitive data from unauthorized access and tampering. The use of AES encryption, secure hash generation, and intelligent anomaly detection improves confidentiality, integrity, and reliability within the cloud environment.

The developed system also provides secure healthcare data management by enabling safe report uploads, encrypted storage, and authenticated report downloads through OTP verification. Blockchain-inspired hash chaining mechanisms ensure tamper-resistant storage and secure audit trails, while machine learning models improve attack detection accuracy and reduce false positives. Experimental analysis demonstrates that the proposed framework effectively identifies malicious activities and strengthens cloud infrastructure security against privilege escalation attempts.

In conclusion, the proposed system successfully combines machine learning, cloud security mechanisms, encryption techniques, and secure authentication methods to provide a robust solution for privilege escalation attack detection and mitigation. The framework improves overall cloud security, enhances user trust, and ensures reliable protection of sensitive information in cloud-based applications. Future enhancements may include integrating deep learning models, real-time threat intelligence systems, and advanced blockchain architectures to further improve detection performance, scalability, and automated attack response capabilities in modern cloud environments.

REFERENCES

[1] M. Armbrust et al., “A View of Cloud Computing,” *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011.
[3] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," in *Proc. IEEE Int. Conf. Cloud Computing*, 2010, pp. 268–275.
[4] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments," *Procedia Engineering*, vol. 15, pp. 2852–2856, 2011.
[5] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An Analysis of Security Issues for Cloud Computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013.
[6] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
[7] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," in *Proc. 9th EAI Int. Conf. Bio-inspired Information and Communications Technologies*, 2016, pp. 21–26.
[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[9] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.
[10] A. Singh and K. Chatterjee, "Cloud Security Issues and Challenges: A Survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, Feb. 2017.
[11] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A Survey of Intrusion Detection Techniques in Cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, Jan. 2013.
[12] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware Traffic Classification Using Convolutional Neural Network for Representation Learning," in *Proc. Int. Conf. Information Networking*, 2017, pp. 712–717.
[13] S. D. Kamble and A. R. Patil, "Detection of Privilege Escalation Attacks in Cloud Computing Using Machine Learning," *International Journal of Computer Applications*, vol. 179, no. 21, pp. 20–25, 2018.
[14] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[15] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer, 2002.
[16] A. Zohar, "Bitcoin: Under the Hood," *Communications of the ACM*, vol. 58, no. 9, pp. 104–113, Sept. 2015.
[17] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and Trustable Electronic Medical Records Sharing Using Blockchain," in *AMIA Annual Symposium Proceedings*, 2017, pp. 650–659.
[18] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST Model for Role-Based Access Control: Towards a Unified Standard," in *Proc. ACM Workshop on Role-Based Access Control*, 2000, pp. 47–63.
[19] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.
[20] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Gaithersburg, MD, USA, Special Publication 800-145, 2011.