JOURNAL OF THE ROYAL LAUREATES ACADEMY

www.rlaindia.org

ENHANCING USER DATA PROTECTION IN PUBLIC CLOUD ENVIRONMENTS THROUGH INTELLIGENT IDENTITY VERIFICATION AND SECURE ACCESS CONTROL MECHANISMS

Mudusu Mahesh Kumar

Research Scholar, Dept. of CSE, Sikkim Alpine University, Namchi Sikkim

Dr. Pankaj Khairnar

Research Supervisor, Dept. of CSE, Sikkim Alpine University, Namchi Sikkim

ABSTRACT

The increasing utilization of public cloud computing has created new opportunities for digital information management while introducing complex challenges concerning user privacy, identity security, and unauthorized data access. Protecting user information requires intelligent identity verification and secure access control mechanisms capable of responding to continuously evolving cybersecurity threats. This research paper examines an integrated approach to enhancing user data protection through intelligent authentication, behavioural analysis, multi-factor verification, identity federation, and dynamic authorization. It emphasizes the importance of evaluating user identity, device characteristics, access behaviour, and contextual risk before granting permission to cloud resources. The proposed approach combines artificial intelligence-assisted identity verification with role-based and attribute-based access control to strengthen security and minimize unnecessary privileges. Furthermore, the study explores implementation challenges, privacy considerations, and the effectiveness of continuous security monitoring in public cloud environments.

Keywords: Public Cloud Computing, User Data Protection, Intelligent Identity Verification, Secure Access Control, Artificial Intelligence, Identity Management, Multi-Factor Authentication, Data Privacy.

I. INTRODUCTION

Public cloud computing has become an important technological foundation for modern digital services because it enables individuals, businesses, and institutions to access computing resources through internet-based platforms. Cloud environments provide flexible storage, processing capabilities, application hosting, and collaborative information-sharing facilities without requiring organizations to maintain extensive physical infrastructure. The widespread adoption of cloud-based technologies has improved operational efficiency and reduced infrastructure-related expenses. However, the increasing volume of personal, financial, educational, and organizational information stored in public cloud environments has created significant concerns regarding data protection, privacy, identity theft, and unauthorized access. These challenges have made secure identity management and access control essential components of contemporary cloud computing architecture.

Traditional security systems generally rely on passwords and predefined access permissions to protect cloud resources. Although these mechanisms provide basic protection, they may not adequately address advanced cyberattacks involving stolen credentials, phishing, malicious applications, compromised devices, and unauthorized account sharing. Attackers may exploit weak authentication practices to impersonate legitimate users and obtain access to confidential information. Furthermore, static authorization policies may continue granting access even when a user's responsibilities, device conditions, or security circumstances have changed. Consequently, modern cloud environments require intelligent mechanisms that can evaluate the legitimacy of access requests and continuously assess potential security risks.

Intelligent identity verification provides opportunities to improve conventional authentication procedures through artificial intelligence, machine learning, biometric recognition, behavioural analysis, and contextual risk assessment. These technologies can examine multiple characteristics associated with an access request to determine whether it is consistent with the legitimate user's identity and normal behaviour. Secure access control complements this process by determining which cloud resources an authenticated user can access and what operations may be performed. Role-based access control, attribute-based access control, and zero-trust security principles can establish more flexible and reliable authorization mechanisms. Integrating these technologies can reduce unauthorized access opportunities while maintaining appropriate levels of accessibility for legitimate users.

The present research investigates approaches for enhancing user data protection in public cloud environments through intelligent identity verification and secure access control mechanisms. It examines the contribution of artificial intelligence-assisted authentication, behavioural monitoring, identity federation, and dynamic authorization to cloud security. The study also considers the technical, operational, and privacy-related challenges associated with implementing intelligent security systems. Its primary objective is to establish an integrated protection approach that verifies user identities accurately, evaluates access requests according to security conditions, and prevents unnecessary exposure of confidential information. The research highlights the importance of continuous verification, least-privilege access, and systematic security evaluation in developing trustworthy public cloud infrastructures.

II. INTELLIGENT IDENTITY VERIFICATION AND ARTIFICIAL INTELLIGENCE-BASED AUTHENTICATION

Intelligent identity verification represents an advanced approach to establishing the authenticity of individuals and devices requesting access to cloud-based resources. Unlike conventional authentication systems that primarily depend on fixed credentials, intelligent verification evaluates multiple identity-related characteristics and contextual information. These characteristics may include registered credentials, biometric features, device information, geographical patterns, network conditions, and previous access behaviour. By analysing different indicators, intelligent authentication systems can identify suspicious access attempts and determine whether additional verification is necessary. This approach is particularly relevant to public cloud infrastructures where users frequently access resources through different devices and geographical locations.

Artificial intelligence provides important capabilities for improving identity verification by analysing large volumes of authentication-related information. Machine learning algorithms can identify recurring behavioural patterns and distinguish between ordinary and potentially suspicious activities. For example, a cloud platform may learn that a particular user generally accesses organizational applications during specific working hours through recognized devices. If an authentication request suddenly originates from an unfamiliar device and demonstrates unusual activity, the system can assign a higher risk score. Depending on predefined policies, additional verification may be required before the requested access is granted. Such intelligent evaluation can strengthen identity protection without requiring identical security procedures for every access request.

Biometric authentication is another important component of intelligent identity verification. Fingerprint recognition, facial identification, voice recognition, and other biometric methods can provide additional evidence regarding a user's identity. These technologies can reduce dependence on easily compromised passwords and improve the convenience of authentication. However, biometric information must be processed through secure and privacy-conscious mechanisms because biometric characteristics cannot be replaced as easily as conventional credentials. Organizations should use protected biometric templates, encrypted storage, liveness detection, and controlled retention policies. Biometric authentication should also be combined with appropriate alternative verification and recovery procedures to prevent legitimate users from being permanently excluded when biometric verification becomes unavailable.

Behavioural authentication strengthens identity verification by examining the manner in which individuals interact with digital systems. Typing patterns, navigation behaviour, device interaction, session characteristics, and application usage may provide additional information about the legitimacy of an access request. Unlike conventional verification, which generally occurs at the beginning of a session, behavioural authentication can operate continuously during user activity. If the observed behaviour significantly differs from established patterns, the system may request reauthentication or temporarily restrict sensitive operations. Nevertheless, behavioural characteristics should not be treated as conclusive proof of identity because legitimate user behaviour may change due to workload, device replacement, accessibility requirements, or environmental conditions.

Intelligent authentication can also incorporate risk-based verification mechanisms. These systems evaluate the potential security risk associated with individual access requests by considering identity assurance, device security, location, network conditions, requested resources, and previous incidents. Low-risk requests may proceed through standard authentication procedures, whereas high-risk requests may require additional factors or stronger verification. This approach enables organizations to allocate security controls according to the sensitivity of information and the likelihood of unauthorized access. The integration of risk-based authentication with multi-factor verification can improve security while reducing unnecessary interruptions for legitimate users.

Despite these advantages, artificial intelligence-based identity verification introduces challenges related to algorithmic accuracy, explainability, data quality, and privacy. Incorrectly trained models may generate false-positive alerts or fail to identify sophisticated

attacks. Behavioural models may also produce inaccurate assessments when legitimate users change their working patterns. Therefore, intelligent verification systems require regular model evaluation, representative training data, secure data processing, and human oversight for sensitive decisions. Organizations should establish transparent procedures for handling authentication failures and provide suitable alternatives when automated identity verification is unsuccessful. Through responsible implementation, intelligent authentication can become an effective component of comprehensive public cloud data protection.

III. SECURE ACCESS CONTROL MECHANISMS AND IDENTITY MANAGEMENT

Secure access control is a fundamental requirement for protecting cloud information because authentication alone does not determine whether a user should be permitted to access a particular resource. After establishing identity, cloud systems must evaluate the user's permissions and determine which activities are authorized. Weak access-control policies can expose confidential information even when authentication procedures are technically strong. Therefore, organizations must establish structured authorization mechanisms that regulate access to applications, databases, storage systems, administrative interfaces, and shared cloud services. Effective access control ensures that users receive only the permissions necessary to fulfil their legitimate responsibilities.

Role-based access control is widely used to manage permissions according to organizational responsibilities. Under this approach, users are assigned predefined roles, and each role is associated with specific access permissions. For example, an administrator may manage system configurations, while an ordinary employee may access only designated organizational applications. Researchers may receive permission to use approved datasets without obtaining administrative control over the underlying infrastructure. This structure simplifies permission management in organizations containing large numbers of users. It also reduces the possibility of inconsistent authorization decisions because permissions are managed through centrally defined roles rather than individually assigned privileges.

Attribute-based access control offers greater flexibility by evaluating multiple characteristics associated with users, resources, actions, and environmental conditions. Attributes may include department, employment status, security clearance, device compliance, data classification, time of access, and geographical location. Access decisions are made by evaluating these attributes against established organizational policies. For instance, a

healthcare employee may be permitted to view specific patient information only when working within an approved organizational environment and performing an authorized professional activity. This approach supports more detailed authorization decisions and is particularly useful in complex public cloud environments where access requirements may change according to operational conditions.

The principle of least privilege is another essential element of secure access management. It requires that every user, application, and service receive only the minimum permissions necessary to complete assigned tasks. Excessive permissions increase the consequences of compromised accounts and create opportunities for unauthorized information access. Organizations should periodically review user privileges, remove unnecessary permissions, and immediately update access rights when employees change roles or leave the organization. Privileged accounts require additional safeguards because they can provide access to critical infrastructure and confidential information. Administrative operations should therefore involve stronger authentication, restricted permissions, and detailed activity monitoring.

Identity federation provides an effective mechanism for managing authentication across multiple cloud applications and organizational platforms. Through federated identity systems, a trusted identity provider can authenticate a user and communicate relevant identity information to other authorized service providers. This reduces the need to maintain separate credentials for every application and supports centralized identity governance. Technologies and standards such as Security Assertion Markup Language, OpenID Connect, and OAuth 2.0 support different aspects of federated authentication and delegated authorization. Organizations must nevertheless configure trust relationships carefully, protect identity assertions, validate tokens, and establish secure session-management procedures to prevent unauthorized access through federated accounts.

Zero-trust architecture further strengthens cloud access management by eliminating the assumption that users or devices should automatically be trusted because of their network location or organizational ownership. Each access request must be evaluated according to identity, device condition, requested resource, and applicable security policies. Authentication and authorization are performed before establishing access to protected resources, while continuous assessment helps identify changing security conditions. This approach is particularly appropriate for public cloud environments because users, applications, and data are distributed across different networks and infrastructure platforms. Combining zero-trust

principles with role-based permissions, attribute-based authorization, and identity federation can create a more resilient and adaptable cloud access-control environment.

IV. IMPLEMENTATION STRATEGY, DATA PROTECTION CHALLENGES AND SECURITY EVALUATION

The successful implementation of intelligent identity verification and secure access control requires a systematic security architecture that integrates identity management, authentication, authorization, and monitoring. The initial stage involves establishing reliable digital identities through appropriate identity-proofing and user-enrollment procedures. During registration, organizations should verify relevant identity information, associate users with approved accounts, and establish secure authentication credentials. Each identity should be linked to an appropriate level of assurance according to the sensitivity of the resources being protected. These procedures help prevent fraudulent account creation and reduce the possibility of unauthorized individuals entering organizational cloud environments.

The second stage involves integrating intelligent authentication with contextual risk assessment. When a user attempts to access a cloud resource, the system evaluates available identity credentials, registered devices, authentication factors, and relevant contextual information. Machine learning models may assist in identifying unusual access patterns, while predefined security policies determine the verification requirements. If the request presents a higher risk, the system may require additional authentication or temporarily restrict access. Importantly, automated risk assessment should operate within clearly established governance policies to prevent inaccurate model decisions from unnecessarily disrupting legitimate cloud services.

The third stage involves implementing secure authorization policies. Following successful authentication, the access-control system evaluates the user's role, attributes, resource classification, and requested activity. Role-based access control can manage standard organizational permissions, while attribute-based access control can introduce additional restrictions according to contextual requirements. Privileged access management should be implemented for administrative operations, and access rights should be reviewed periodically. Short-lived access tokens, secure session management, and timely credential revocation can further reduce the opportunities for unauthorized use of active accounts.

Continuous monitoring and security analytics form another important component of the implementation strategy. Cloud environments generate substantial quantities of authentication records, access events, application logs, and administrative activity information. Security monitoring systems can analyse these records to identify unusual behaviour and potential security incidents. Automated alerts may be generated when users attempt to access restricted information, repeatedly fail authentication, or perform unexpected data transfers. Security teams can investigate these alerts and initiate appropriate responses, including reauthentication, account suspension, session termination, and incident reporting. Continuous monitoring also provides information that can support the improvement of authentication policies.

However, implementing intelligent identity and access-control mechanisms creates several technical challenges. Integration with existing enterprise applications, legacy information systems, and different cloud service providers may require significant customization. Machine learning-based systems may generate inaccurate predictions when training datasets are incomplete or unrepresentative. Biometric authentication may also introduce privacy concerns, while extensive monitoring can create questions regarding the collection and use of personal information. Organizations must therefore balance security requirements with privacy protection, transparency, operational efficiency, and user convenience. Appropriate encryption, data minimization, retention policies, and access restrictions should be established for identity-related information.

The effectiveness of the proposed approach should be evaluated through measurable security and operational indicators. Relevant indicators include unauthorized access attempts, authentication success rates, false-positive and false-negative detection rates, average incident detection time, access-policy violations, and the number of excessive user permissions. Organizations should also evaluate system response time, implementation expenses, user satisfaction, and service availability. Periodic penetration testing, vulnerability assessments, compliance reviews, and independent security audits can help determine whether implemented mechanisms provide the expected protection. The evaluation process should support continuous improvement rather than treating security implementation as a one-time activity. Through systematic deployment and regular assessment, intelligent identity verification and secure access control can contribute substantially to stronger user data protection in public cloud environments.

V. CONCLUSION

The increasing use of public cloud computing has made user data protection an essential requirement for individuals, businesses, and institutions. Although cloud platforms provide flexibility, scalability, and cost-effective information management, they also create security challenges involving identity theft, unauthorized access, compromised credentials, and privacy violations. Traditional authentication and static authorization mechanisms may not provide sufficient protection against sophisticated cyber threats. The integration of intelligent identity verification and secure access control therefore represents an important approach to strengthening information security in modern cloud environments.

The research highlights the importance of artificial intelligence-assisted authentication, biometric identification, behavioural analysis, and risk-based verification in improving the accuracy of identity management. These technologies can evaluate different characteristics associated with users and their access activities to identify potentially suspicious requests. Furthermore, role-based access control, attribute-based access control, identity federation, and zero-trust architecture can establish stronger authorization policies. The combined application of these mechanisms ensures that users receive appropriate permissions while reducing unnecessary exposure of confidential information.

The study also emphasizes that successful cloud data protection requires more than advanced technological solutions. Organizations must establish effective identity governance, secure credential management, encryption policies, continuous monitoring, and periodic security assessments. Privacy protection, regulatory compliance, algorithmic reliability, and implementation costs must also be considered when introducing intelligent security systems. A balanced implementation strategy can help organizations maintain security without unnecessarily affecting the accessibility and performance of cloud-based services. Continuous evaluation of authentication and authorization mechanisms is necessary to respond effectively to emerging cybersecurity threats.

Overall, intelligent identity verification and secure access control provide a comprehensive foundation for enhancing user data protection in public cloud environments. Their integration can strengthen identity assurance, minimize unauthorized access, improve security monitoring, and increase confidence in cloud-based information systems. Future research should focus on explainable artificial intelligence, privacy-preserving biometric authentication, decentralized digital identities, intelligent threat prediction, and adaptive zero-

trust security architectures. These developments may contribute to more reliable, transparent, and resilient cloud computing environments in which user privacy and information confidentiality remain fundamental priorities.

REFERENCES

1. Al-Mezel, S. A., Alzahrani, A. I., & Javaid, A. Y. (2016). A survey of authentication mechanisms in cloud computing. Journal of Computer and Communications, 4(11), 1-9.

2. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. In Proceedings of the 2016 International Conference on Cloud Computing Research and Innovation (ICCCRI) (pp. 58-64).

3. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. In Proceedings of the 2016 International Conference on Cloud Computing Research and Innovation (ICCCRI) (pp. 58-64).

4. Al-Souly, Hanan & Alsheddi, Abeer & Kurdi, Heba. (2013). Lightweight Symmetric Encryption Algorithm for Secure Database. International Journal of Advanced Computer Science and Applications. 3. 53-63. 10.14569/SpecialIssue.2013.030407.

5. Ambekar, Kimaya & Kamatchi, R.. (2016). Enhanced User Authentication Model in Cloud Computing Security. 530. 327-338. 10.1007/978-3-319-47952-1_26.

6. Anbazhagan, Subramanian & K, Somasundaram. (2014). Cloud Computing Security through Symmetric Cipher Model. International Journal of Computer Science and Information Technology. 6. 57-66. 10.5121/ijcsit.2014.6304.

7. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

8. Ashish Kumar Singh et al., "CAESAR CLOUD: A Comprehensive Approach for Enhancing Security and Service Availability Based on Reputation for Cloud User Environment", International journal of network security and its applications, 2014, pp. 2164-2175.

9. Ashish Singh and Kakali Chatterjee, "A Secure Multi–tier Authentication Scheme in Cloud Computing Environment", International Conference on Circuit, Power and Computing Technologies (ICCPCT), IEEE, ISBN 978-1-4799-7075-9, 2015.

10. Bhavana A., Alekhya V., Deepak K. and Sreenivas V, "Password Authentication System (PAS) for Cloud Environment", Cloud Publications, International Journal of Advanced Computer Science and Information Technology, Volume 2, Issue 1, 2013, ISSN 2320-0235. pp. 29-33.