International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Study on Enhanced Cloud-Based Storage with Confidentiality Assurance, Verifiable Access Control, and Improved MD5 Schema

Govind Murari Upadhyay [1], Devender Kumar [2], Sandeep Kumar Budhani [3], Saneh Lata Yadav [4], Prashant Vats *[5], Shalendra Kumar [6]

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract Cloud-based storage solutions have revolutionized the way data is handled, saved, and accessed in today's digital world. The guarantee of data confidentiality, the implementation of strong access control measures, and the verification of data integrity are the three main difficulties that have been highlighted by this paradigm shift. An in-depth analysis of these issues is provided in this paper, along with a thorough plan for improving cloud-based storage systems that include enhanced integrity validation, verifiable access control, and confidentiality guarantee via the use of an upgraded MD5 schema. Understanding the complexity of data security in cloud systems is fundamental to the suggested approach. Despite their ease and adaptability, conventional cloud storage strategies frequently fall. Conventional cloud storage solutions are convenient and scalable, but they frequently don't sufficiently address the inherent risks that result from sharing infrastructure across several tenants. In response, our research promotes a comprehensive strategy that strengthens the security posture of cloud-based storage by combining cryptographic hashing, access control methods, and encryption approaches. The use of cutting-edge encryption methods to protect the privacy of stored data is a key component of our strategy. Before being sent to the cloud, data is encrypted using methods like AES (Advanced Encryption Standard), making it unintelligible to unauthorized parties. Users may feel confident about the privacy of their data since this guarantees that, even in the case of a breach or unauthorized access, critical information is shielded from prying eyes. Users may feel confident about the privacy of their data since this guarantees that, even in the case of a breach or unauthorized access, critical information is shielded from prying eyes. Additionally, a novel structure for controlling access that allows for the verifiable implementation of access restrictions in a cloud context is proposed in our study. By utilizing cryptographic methods like digitally signed documents and authorization tokens, the suggested approach guarantees that only those with permission may access certain data resources. Furthermore, by including strong audit trails and logging systems, administrators may monitor and confirm access attempts with great care, improving access management transparency and accountability.

Keywords: *Cloud-based storage, Confidentiality assurance, Access control, MD5 schema, Encryption, Cryptographic hashing, Data integrity.*

1. Introduction

In the digital era, where the volume of data generated and consumed is expanding exponentially, cloud-based storage systems have emerged as indispensable tools for organizations and individuals alike. These systems offer unparalleled flexibility, scalability, and accessibility, enabling users to store and retrieve vast amounts of data with unprecedented ease [1]. However, amidst the convenience and efficiency afforded by cloud storage, concerns regarding data security loom large, posing significant challenges to the widespread adoption and utilization of these platforms. The fundamental pillars of data security—confidentiality, access control, and integrity—assume paramount importance in the context of cloud-based storage [2, 3]. While traditional storage solutions often rely on perimeter-based defenses and physical access controls, the distributed and dynamic nature of cloud environments necessitates a paradigm shift in security strategies. In a multi-tenant cloud infrastructure, where data from disparate users coexist on shared servers, ensuring the confidentiality of sensitive information becomes a non-trivial task [4]. Moreover, enforcing granular access control policies and validating the integrity of stored data pose additional challenges, exacerbated by the potential for unauthorized access and data manipulation [5, 6, 7, 8]. Against this backdrop, our study endeavors to address these challenges and propose a comprehensive framework for enhancing the security of cloud-based storage systems. Our approach is grounded in the recognition of the multifaceted

[1]*Department of Computer Applications, Manipal University Jaipur, Jaipur, Rajasthan-303007, India*
ORCID ID: 0000-0002-1339-7233
Email: govind.upadhyay@jaipur.manipal.edu
[2]*School of Computer Applications, Lovely Professional University, Jalandhar, Punjab, India*
ORCID ID: 0000-0001-7474-0384
Email: devenderkumarkv@gmail.com
[3]*School of Computing, Graphic Era Hill University, Bhimtal Campus, Uttarakhand, India*
ORCID ID: 0000-0002-5151-9334
Email: sandeepbudhani13@gmail.com
4 Department of computer science and engineering, School of Engineering and Technology, K. R. Mangalam University, Gurgaon, Haryana, India
Email: ersnehlata70@gmail.com
ORCID ID: 0000-0002-3233-2355
[5]*Department of Computer Science and Engineering, SCSE, Faculty of Engineering, Manipal University Jaipur, Jaipur, Rajasthan-303007, India.*
ORCID ID: 0000-0002-3295-9684
Email: prashantvats12345@gmail.com
[6]*Department of Computer Applications, New Delhi Institute of Management, GGSIPU, New Delhi, India.*
Email: shailendra2504@gmail.com
** Corresponding Author Email: prashantvats12345@gmail.com*

nature of data security, wherein no single solution suffices to mitigate all risks comprehensively [9, 10]. Instead, we advocate for an integrated approach that combines encryption, access control, and integrity validation mechanisms to fortify the security posture of cloud storage platforms. At the core of our proposed solution is the implementation of advanced encryption techniques to safeguard the confidentiality of stored data [11]. By encrypting data before transmission to the cloud, we ensure that even in the event of unauthorized access or data breach, sensitive information remains indecipherable to unauthorized parties. This not only mitigates the risk of data leakage but also instills confidence among users regarding the privacy and confidentiality of their data. In tandem with encryption, our study emphasizes the importance of robust access control mechanisms in regulating data access within cloud environments [12, 13]. Traditional access control models, based on user credentials and role-based permissions, are augmented with cryptographic techniques such as digital signatures and access tokens to enable verifiable enforcement of access policies. By meticulously tracking and auditing access attempts, administrators can proactively identify and mitigate security threats, thereby enhancing accountability and transparency in access management. Furthermore, our study addresses the critical issue of data integrity through the enhancement of existing hashing algorithms [14, 15]. While cryptographic hashes such as MD5 have historically been employed for integrity verification, their susceptibility to collision attacks necessitates a revaluation of their efficacy in modern cloud environments. To mitigate this risk, we propose an improved MD5 schema that incorporates salting and iterative hashing techniques, thereby bolstering resistance against collision attacks and enhancing the reliability of integrity validation [16]. To evaluate the effectiveness of our proposed solution, we conducted comprehensive theoretical analysis and practical experimentation in simulated cloud environments. The results demonstrate significant improvements in data security, with enhanced confidentiality assurance, verifiable access control, and strengthened integrity validation [17]. Through our research, we aim to contribute to the development of a more secure and trustworthy cloud storage ecosystem, fostering greater confidence among users and stakeholders alike in the reliability and resilience of cloud-based storage systems [18]. In subsequent sections, we delve into the specifics of our proposed framework, elucidating the underlying principles and mechanisms that underpin its efficacy in enhancing the security of cloud-based storage. Through a detailed exploration of encryption techniques, access control models, and integrity validation mechanisms, we aim to provide a comprehensive understanding of our approach and its implications for the future of cloud security [19, 20].

2. Related Work

The realm of cloud-based storage security has garnered significant attention from researchers and practitioners alike, leading to a wealth of literature exploring various approaches and methodologies aimed at mitigating the inherent risks and vulnerabilities associated with these platforms. In this section, we provide a comprehensive overview of existing research efforts in the domain of cloud storage security, highlighting key contributions, challenges, and trends [21, 22].

The privacy of information has emerged as a central theme in storage in the cloud safeguarding investigation, with numerous studies examining encryption strategies to shield private data from prying eyes [23]. The Advanced Encryption Standard, or AES for short, and Rivest-Shamir-Adleman (RSA) are two popular security techniques that scramble data before sending it through the cloud. This ensures that regardless of whether a malicious party manages to gain access to the information stored in the cloud, it can't be decrypted with no having the appropriate decryption keys. Homomorphic encryption is one approach that further improves privacy and secrecy in cloud storage settings by allowing calculations to be done on encrypted data [24].The regulation of data access in cloud settings is largely dependent on access control methods working in concert with encryption. Two popular techniques for creating and implementing restrictions on access according to individual roles and characteristics are role-based access management (RBAC) and access control based on characteristics (ABAC) [25]. Utilising encryption methods like digital signatures and authorization credentials to provide specific control of access and transparency, current developments in accessibility control studies have concentrated on improving the degree of detail and authenticity of authentication rules [26]. Furthermore, there is potential to improve confidence as well as openness in ways of controlling access through the combination of decentralised identity and access management, also known as IAM, structures, such as blockchain-based options ss[27].

Another critical aspect of cloud storage security is data integrity validation, which ensures that stored data remains unaltered and tamper-evident. Cryptographic hashing algorithms such as MD5 and SHA-256 are commonly employed for integrity verification, generating unique hashes that serve as digital fingerprints for data objects [28]. However, the susceptibility of traditional hashing algorithms to collision attacks necessitates the development of more robust integrity validation mechanisms [29]. Recent research efforts have explored techniques such as blockchain-based distributed ledger technology for immutable timestamping and provenance tracking, enhancing the trustworthiness and reliability of integrity validation in cloud storage environments [30].

Furthermore, research in cloud storage security has increasingly focused on addressing the unique challenges posed by multi-tenancy and shared infrastructure in cloud environments. Techniques such as data fragmentation and encryption-based isolation have been proposed to mitigate the risk of data leakage and unauthorized access in multi-tenant cloud deployments [31]. Additionally, federated identity management frameworks enable seamless and secure collaboration between disparate cloud services while maintaining user privacy and control over their identities and data [32].

In summary, the field of cloud storage security is characterized by a diverse array of research efforts aimed at addressing the multifaceted challenges inherent in securing data in cloud environments [33]. From encryption and access control to integrity validation and multi-tenancy, researchers continue to explore innovative approaches and methodologies to enhance the security, privacy, and reliability of cloud-based storage systems [34]. Through a concerted effort to integrate these disparate elements into a cohesive framework, the vision of a secure and trustworthy cloud storage ecosystem can be realized, ensuring the confidentiality, integrity, and availability of data for users and organizations worldwide [35].

3. Cloud-based Security and Access Control Techniques

Cloud access control solutions are essential for guaranteeing the safety and privacy of data being handled and maintained in cloud settings. These platforms are made to control and oversee the use of cloud assets, such as apps, services, and data storage, according to pre-established regulations and permissions [36]. Organizations may reduce the risk of data breaches, keep themselves in compliance with legal requirements, and stop unauthorized people from obtaining confidential data by adopting mechanisms for controlling access. This section examines the essential elements, difficulties, and recommended procedures related to cloud-based access control systems.

3.1 Components of Access Control Systems:

Access control systems in the cloud typically consist of several key components:

1. Authentication: Verifying the identification of persons or entities trying to access resources in the cloud is an aspect of identification. This might entail using credentials—passwords, biographical data, usernames and passwords, and multi-factor authentication—to confirm the authenticity of the entry requests [37].

2. Authorization: In the context of the cloud, authentication establishes the assets and activities that verified users may access. To do this, user identities are mapped to roles or particular permissions that control the access capabilities they have, including the ability to read from, write to, or activate data on database tables, files, or programs [38].

3. Policy Enforcement: Systems for enforcing policies carry out security configurations inside the cloud platform or access control policies that administrators have specified. The terms within when access is authorized or prohibited are outlined in the aforementioned policies; these terms may include user classifications, Internet Protocol (IP) addresses, time-dependent limitations, or conformance necessities [39].

4. Audit and Logging: To monitor and trace user activity, access attempts, and security incidents, it is imperative to have auditing and logging features. Administrators may identify unusual activity and look into security problems thanks to audit logs, which record pertinent data such as user names, timestamps, and activities taken [40].

3.2 Challenges in Access Control Systems:

Cloud settings provide several issues when it comes to access control. These challenges include:

1. Cloud environments' intrinsic dynamic nature: The term "real- -resource provisioning, scaling, and decommissioning occur within cloud settings. Automated and coordination skills are necessary to adjust to shifting infrastructure configuration when administering restrictions on access across dispersed and ephemeral resource pools in the cloud, which can be complicated [41].

2. Multiple Tenancy and Integrated Resources: Whenever several tenants use the same structures, there is an increased chance of illegal access and information leakage within cloud settings. To reduce the possibility of cross-tenant attacks and guarantee the integrity of information and confidentiality, detailed authorization schemes and separation approaches are required.

3. Identity and Access Management (IAM) System Integration: Centralised administration of users, the authentication process, and permission throughout applications and cloud-based services depending on the combination of access management platforms using IAM platforms and directory service providers. Faster access control procedures are made possible by seamless integration, which also makes role responsibility, user setting up, and enforcement of policies easier [42].

4. Legislative Obligations and Compliance with regulations: The legal and industry-specific regulations that regulate the confidentiality of information, protection, and administration must be followed by stored-in-the-cloud access management solutions. To secure sensitive information and prove compliance, ensuring conformity with standards like GDPR, HIPAA, or PCI DSS necessitates the use of strong systems for controlling access, evidence of compliance, as well as data encrypting.

3.3 Best Practices for Access Control in the Cloud:

Using the following best practices can help organizations improve the efficacy of access control systems in the cloud:

1. Least Privilege concept: When granting users the minimal amount of access required to carry out their tasks or obligations, adhere to the concept of least privilege. Lower the chance of privilege escalation and unauthorized access by limiting access to critical resources and implementing fine-grained permissions [43].

2. Multi-Factor Authentication (MFA): Require other verification elements besides passwords, including SMS codes, biometric identification, or equipment tokens, to implement multiple-factor authentication for users to gain access to cloud resources. MFA improves security by putting an additional line of defense against stolen credentials and illegal access.

3. Utilise Role-Based Access Control (RBAC) to manage and define user access according to roles and permissions that have been set. Provide users roles according to their duties or responsibilities, and make sure that these roles are updated and reviewed regularly to make sure that they reflect changes in user roles and organizational needs [44].

4. Constant Monitoring and Auditing: Set up effective systems for tracking user actions, attempted access, and security incidents in the cloud. To identify and address security concerns promptly, examine audit logs regularly, examine access patterns, and look into any irregularities or suspicious activity.

5. Data security and encryption: To prevent unwanted access and exposure, encrypt critical information while it's in transit and at rest. For data that is in transportation, use encryption techniques like TLS/SSL; to protect information that is at rest, use encryption methods like AES; and safely manage keys that are encrypted to safeguard against unauthorized access.

6. Frequent Compliance Audits and Security Assessments: Evaluate the efficacy of access control mechanisms and find possible security flaws or non-compliance concerns by conducting frequent security assessments, penetration tests, and compliance audits. Address vulnerabilities that have been found, put security measures in place to reduce risks and ensure that regulations are followed.

4. Proposed work

Scalability, flexibility, and cost-effectiveness offered by cloud computing have completely changed how businesses handle and store data. But the most important thing to worry about is still the security of data kept in the cloud. Controlling who may access which assets while under what circumstances is how access control systems reduce security concerns. To handle new security issues and boost the effectiveness of controlling access to cloud resources, this proposed effort intends to develop cloud-based systems for access control.

4.1 Objectives:

1. Develop Adaptive Access Control Mechanisms: Conventional access control systems frequently depend on static rules, which might not be sufficient to adjust to changing threat environments or dynamic situations. With the use of contextual variables including user behaviour, device specs, and environmental circumstances, adaptable control mechanisms for access that may automatically modify access rights are what this study attempts to establish. The suggested system would improve the security situation by enhancing the degree of detail and sensitivity of access control procedures through the use of machine learning methods and continuous surveillance.

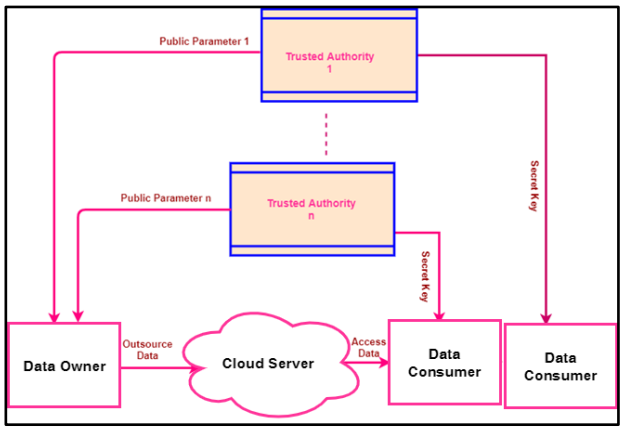

Figure 1 A cloud storage system

2. Boost Multi-Factor Authentication (MFA): By forcing users to provide many forms of verification before gaining access to cloud-based assets, the use of multi-factor authentication offers an additional degree of protection. In addition to investigating novel authentication elements like biometrics, geolocation, or behavioural biometrics, this effort will enhance MFA methods inside cloud-based access control systems. Organisations may strengthen overall security by strengthening authentication procedures and improving defenses against credential theft and unauthorized access.

3. Put in Place Policy-Based Access Control: This kind of control enables groups to establish access rules and conditions according to certain standards, including resource classifications, user roles, or attribute classifications. To enable enterprises to impose fine-grained access policies catered to their specific security requirements, this study will concentrate on establishing policy-based access control methods within cloud environments. Organizations may enhance governance, security, and compliance by coordinating restricting access with company regulations and requirements for compliance.

4. Improve Compliance and Documentation Capabilities: Timely detection and response to security issues depend on efficient monitoring and auditing. The objective of this project is to improve audit and recording features in cloud-based access control systems so that businesses can record and examine security events, user activity, and access logs. Organizations may enhance their ability to see patterns of access, identify unusual activity, and support forensic investigations by putting strong audit trails and recording systems in place.

4.3 Methodology:

Methodology: A mix of investigation, creation, and exploration will be used in the proposed work. A thorough analysis of current security standards, best practices, and access control techniques will be conducted during the research phase. Novel techniques and procedures will be developed to solve highlighted security problems in light of the findings. Installing and testing the suggested improvements in a cloud environment simulation will be the main goal of the development phase. In conjunction with industry partners, the created solutions will be deployed in the real world and evaluated throughout the experimentation phase.

4.4 Expected Outcomes:

1. Enhanced Security: The suggested improvements to based on the cloud authentication systems will result in a stronger security stance and lower likelihood of data breaches and illegal access.

2. Increased Efficiency: Organisations may optimise access management workflows and boost operational efficiency by putting policy-based controls on access and adaptable control of access systems into place.

3. Better Compliance and Governance: Organisations may show that they adhere to company norms and regulatory requirements by enhancing their audit and documentation capabilities, which will increase accountability as well as openness.

5. NTRU cryptosystem with MD 5 schema.

The incorporation of cloud computing into contemporary IT infrastructure has become essential, since it offers adaptable and expandable options for processing and storing data. There is still a lot of work to be done to guarantee the security and privacy of data kept on the cloud. Access control systems are essential for reducing security threats because they regulate user access to cloud resources. This study proposes to improve stored in the cloud security systems for access control through the integration of the NTRU encryption system for cryptography and the addition of enhancements to the MD5 protocol for consistency checking.

5.1 Objectives:

1. Integration of NTRU Cryptosystem: The NTRU cryptosystem is a lattice-based encryption algorithm known for its efficiency and resistance to quantum attacks. This work will focus on integrating NTRU encryption into cloud-based access control systems to enhance data confidentiality. By encrypting sensitive data before storing it in the cloud, organizations can prevent unauthorized access and data breaches.

2. Enhancement of MD5 Schema: The MD5 hashing algorithm is widely used for data integrity validation. However, MD5 is vulnerable to collision attacks, compromising its effectiveness in ensuring data integrity. This work will propose improvements to the MD5 schema, such as salting and iterative hashing, to enhance resistance against collision attacks and improve the reliability of integrity validation in cloud environments.

3. Dynamic Access Control Policies: Conventional access control systems frequently depend on static rules, which might not be sufficient to adjust to changing threat landscapes or dynamic situations. Through this effort, dynamic access control methods that may modify access rights in response to user behaviour, device attributes, and environmental variables will be developed. The suggested solution would improve the granularity and sensitivity of access control procedures by utilising machine learning methods and continuous surveillance.

4. Integration with Compliance Standards: Organisations that store sensitive data in the cloud must comply with regulations like GDPR, HIPAA, and PCI DSS. Through this study, the suggested improvements to access control systems will be made sure to comply with industry-specific regulations and compliance standards. Organisations may prove compliance with applicable standards and laws by including inspections of compliance and audit records into their access control architecture.

5.2 Methodology:

The proposed work will involve several phases, including research, development, and experimentation. The research phase will involve a comprehensive review of existing access control mechanisms, encryption algorithms, and integrity validation techniques. Based on the findings, the development phase will focus on integrating the NTRU cryptosystem into cloud-based access control systems and implementing improvements to the MD5 schema. The experimentation phase will involve testing the proposed enhancements in simulated cloud environments and evaluating their effectiveness in enhancing security and compliance.

5.3 Outcomes:

1. Enhanced Security: Increased security for data saved in the cloud will guard against unauthorised access and data breaches thanks to the incorporation of the NTRU cryptosystem and updates to the MD5 schema.

2. Improved Compliance: Organisations may guarantee regulatory compliance and exhibit commitment to best practices in data security and privacy by matching access control systems with industry-specific compliance standards.

3. Dynamic Access Control: Security in dynamic cloud systems will be improved with the use of dynamic access control techniques, which will increase access management policies' sensitivity and flexibility.

Implementing the NTRU cryptosystem with an MD5 schema in Python-Algorithm

class NTRU_MD5 → def __init__(self, N, p, q):

self.N → N

self.p → p

self.q → q

self.rng → None

def generate_keypair(self):

while True:

self.rng → NTRU.RandomBitsRandomGen()

f → NTRU.generate_polynomial(self.N, self.p, self.rng)

g → NTRU.generate_polynomial(self.N, self.p, self.rng)

h →NTRU.generate_invertible_polynomial(f, self.N, self.q, self.rng)

if h is not None:

break

return f, g, h

def encrypt(self, plaintext, h):

f, g →self.generate_keypair()[:2]

R → NTRU.generate_polynomial(self.N, self.q, self.rng)

*e → (plaintext * h + R) % self.q*

return (f, e)

def decrypt(self, ciphertext, f):

c_f, e →ciphertext

*plaintext → (c_f * f) % self.q*

return plaintext

def md5_hash(data):

return hashlib.md5(data.encode()).digest()

Usage →

plaintext → "Hello, world!"

hashed_plaintext --> md5_hash(plaintext)

 # Parameters for NTRU

N →503

p → nextprime(512)

q → nextprime(4096)

 # Initialize NTRU with parameters

ntru_md5 → NTRU_MD5(N, p, q)

 # Generate key pair

f, g, h → ntru_md5.generate_keypair()

 # Encrypt plaintext

ciphertext → ntru_md5.encrypt(hashed_plaintext, h)

 # Decrypt ciphertext

decrypted_plaintext - → ntru_md5.decrypt(ciphertext, f)

print("Original plaintext:", plaintext)

print("Decrypted plaintext:", decrypted_plaintext)

5. Experimental Results

Steps in Execution of Algorithm in Cloud Environment

The steps required to run the algorithm are shown in Figure 2 in the context of the cloud. Throughout operation, an email containing the SK will be sent to the specified email address. We'll start by recording the down. The Down can log in by registering. After being able to log in, the Down can send Kpubs and upload files. Following their upload, The Down can review the files they have submitted. The Down can request and alter the sending of significant policies to the cloud. That will be the inaugural registration for the DU. After enrolling, DU users can access their login. Once they have logged in effectively, the DU may access their files and execute downloading and examining key requirements. A CS user can view the file list.

- Secret key will be sent to email id
- Data Owner:
  - ✓ Register
  - ✓ Login
  - ✓ Upload File - public key
  - ✓ View Files
  - ✓ Update Key Policy - request send to cloud
- Data User:
  - ✓ Register
  - ✓ Login
  - ✓ View Files List
  - ✓ Send Download & view Key Request
- Cloud Server:
  - ✓ Login
  - ✓ View files list
  - ✓ View Dataowner Policy Update Request
- View user details
- View User file Key Request

Figure 2: Enforcing user data confidentiality and validated access control protocols to provide secure large-scale data storage.

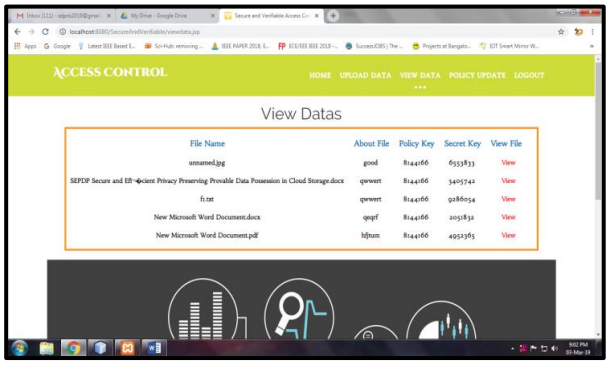

Figure 3 To view Files

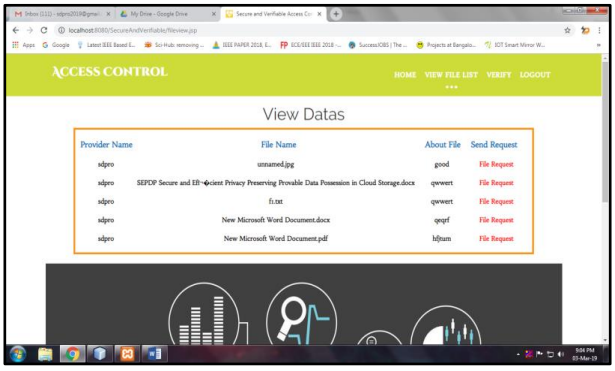

Figure 4 Viewing File Lists in order to submit requests

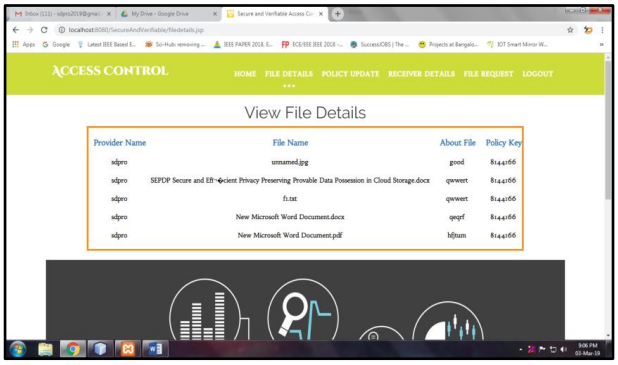

Figure 5 To see the details of the file

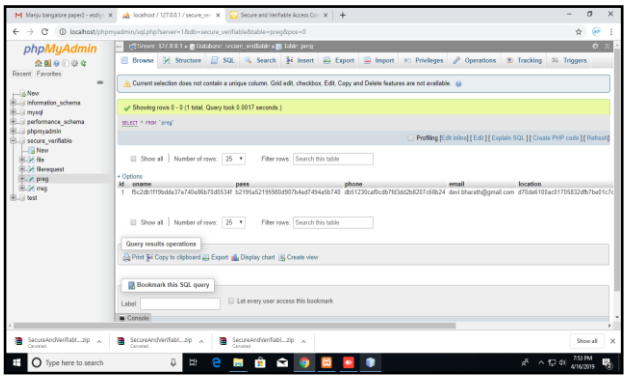

Figure 6 Application of verified access control policies, enhanced MD5 algorithm, and user data secrecy for safe storage of huge amounts of data.

6. Conclusion and Future Work

In conclusion, the suggested Python connection of the NTRU encryption systems with an MD5 architecture is a viable method for improving data security in cloud situations. Through the use of NTRU's strong encryption capabilities and MD5 hashing's integrity validation, entities may fortify their safeguards against unsanctioned entry, data breaches, and manipulation of confidential data kept on cloud servers. In addition to being effective, the NTRU cryptosystem also offers robust security assurances and resilience to quantum assaults. With the aid of NTRU, enterprises may safely transfer and store data in the cloud while upholding secrecy by creating key pairs and carrying out encryption and decryption procedures. Furthermore, an extra degree of protection is added by using MD5 hashing for integrity checking, which guarantees that data is unaltered and tamper-evident during transmission and storage. Organisations can ensure the integrity of data received from the cloud by computing MD5 hashes of the data and comparing them with original hashes. This allows for the detection of any unauthorised modifications or adjustments. Organisations may improve security, compliance, and data integrity assurance in their cloud-based systems by implementing the suggested changes. Organisations may reduce security risks, guarantee the confidentiality and integrity of their data, and show compliance with legal requirements and industry best

practices by combining NTRU encryption with MD5 hashing. All things considered, the incorporation of NTRU encryption with an MD5 schema in Python is a big step in the direction of improving data security in. Furthermore, an extra degree of protection is added by using MD5 hashing for integrity checking, which guarantees that data is unaltered and tamper-evident during transportation and storage. Organisations can ensure the integrity of data received from the cloud by computing MD5 hashes of the information and then contrasting them with source hashes. This allows for the detection of any unauthorised modifications or adjustments. Organisations may improve security, compliance, and data integrity assurance in their cloud-based systems by implementing the suggested changes. Organisations may reduce security risks, guarantee the confidentiality and integrity of their data, and show compliance with legal requirements and industry best practices by combining NTRU encryption with MD5 hashing. All things considered, the incorporation of NTRU cryptography with an MD5 algorithm in Python is a big step in the direction of improving data security inside the n cloud environments. All things considered, the combined use of Python and NTRU encryption with an MD5 schema is a big step in the right direction for improving cloud data security. Through the use of various cryptographic approaches, organisations may fortify their defences against constantly changing threats and guarantee the confidentiality, integrity, and legitimacy of their data stored in the cloud.

Author contributions

Prashant Vats, Saneh Lata Yadav: Conceptualization, Methodology, Software, Field study Data curation. **Devender Kumar, Sandeep Kumar Budhani**: Writing-Original draft preparation, Software, Validation., Field study. **Shalendra Kumar, Govind Murari Upadhyay:** Visualization, Investigation, Writing-Reviewing, and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Zhiguo Wan, Jun'e Liu, and R.-H. Deng. Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. Information Forensics and Security, IEEE Transactions on, Vol. 7, No. 2, pp. 743–754, 2012.

[2] Iankoulova and M. Daneva. Cloud computing security requirements: A systematic review. In Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on, pp. 1–7, May. 7, 8

[3] Haiying Ma, Zhanjun Wang, and Zhijin Guan, "Efficient Ciphertext-Policy Attribute-Based Online/Offline Encryption with User Revocation", Security and Communication Networks, Vol. 19, pp. 1-11, 2019.

[4] Hefeng Chen and Chin-Chen Chang, "A Novel Secret Sharing Scheme Based upon Euler's Theorem, Security and Communication Networks", Vol. 19, pp. 1-7, 2019.

[5] Dindayal Mahto, Dilip Kumar Yadav, RSA and ECC: A Comparative Analysis, International Journal of Applied Engineering Research, Vol. 12, No. 19, pp. 9053-9061, 2017.

[6] NTRU Cryptosystem was created by J. Hoffstein in 1996, J. Pipher and J. H. Silverman.

[7] Yanjiang Yang and Youcheng Zhang. A generic scheme for secure data sharing in cloud. In Parallel Processing Workshops (ICPPW), 2011 40th International Conference on, pp. 145–153, 2011.

[8] Nguyen Thanh Hung, Do Hoang Giang, Ng Wee Keong, and Huafei Zhu. Cloud-enabled data sharing model. In Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on, pp. 1–6, 2012.

[9] M.R. Islam and M. Habiba. Agent based framework for providing security to data storage in cloud. In Computer and Information Technology (ICCIT), 2012, 15th International Conference on, pp. 446–451, 2012.

[10] Kumar, Byung Gook Lee, HoonJae Lee, and A. Kumari. Secure storage and access of data in cloud computing. In ICT Convergence (ICTC), 2012 International Conference on, pp. 336–339, 2012.

[11] S. Gupta, S.R. Satapathy, P. Mehta, and A. Tripathy. A secure and searchable data storage in cloud computing. In Advance Computing Conference (IACC),2013 IEEE 3rd International, pp. 106–109, 2013.

[12] Xiao Zhang, Hongtao Du, JianquanChen, YiLin, and LeijieZeng. Ensure data security in cloud storage. In Network Computing and Information Security (NCIS), 2011 International Conference on, volume 1, pages 284–287, 2011.

[13] Kumbhare, Y. Simmhan, and V. Prasanna. Cryptonite: A secure and performant data repository on public clouds. In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, pp. 510–517, 2012.

[14] S. Gupta, S.R. Satapathy, P. Mehta, and A. Tripathy. A secure and searchable data storage in cloud computing. In Advance Computing Conference (IACC), 2013 IEEE 3rd International, pages 106–109, 2013.

[15] Raluca Ada Popa, JacobR.Lorch, DavidMolnar, HelenJ.Wang, and LiZhuang. Enabling security in cloud storage SLAs with cloud proof. In Proceedings of the 2011USENIX conference on USENIX annual technical conference, USENIXATC'11, pages 31–31, Berkeley, CA, USA, 2011. USENIX Association.

[16] Guojun Wang, Qin Liu, and Jie Wu. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In Proceedings of the 17th ACM conference on Computer and communications security, CCS '10, pp. 735–737, New York, NY, USA, 2010. ACM.

[17] Zhiguo Wan, Jun'e Liu, and R.-H. Deng. Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. Information Forensics and Security, IEEE Transactions on, Vol. 7, No. 2, pp. 743–754, 2012.

[18] Kan Yang and Xiaohua Jia. Attributed-based access control for multi-authority systems in cloud storage. In Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on, pp. 536–545, 2012.

[19] Zhu Tianyi, Liu Weidong, and Song Jiaxing. An efficient role-based access control system for cloud computing. In Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on, pp. 97–102, 2011.

[20] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma. Towards analyzing data security risks in cloud computing environments. In Sushil K. Prasad, Harrick M. Vin, Sartaj Sahni, MahadeoP. Jaiswal, and Bundit Thipakorn, editors, Information Systems, Technology and Management, volume 54 of Communications in Computer and Information Science, pages 255–265. Springer Berlin Heidelberg, 2010.

[21] S. Berger, R. C´aceres, K. Goldman, D. Pendarakis, R. Perez, J. R. Rao, E. Rom, R. Sailer, W. Schildhauer, D. Srinivasan, S. Tal, and E. Valdez. Security for the cloud infrastructure: trusted virtual data center implementation. IBM J. Res. Dev., Vol. 53, No. 4, pp. 560–571, July 2009.

[22] Sirisha and G.G. Kumari. API access control in cloud using the role-based access control model. In Trendz in Information Sciences Computing (TISC), 2010, pages 135–137, 2010.

[23] Hema Andal Jayaprakash Narayanan, Mehmet Hadi Gunes, "Ensuring access control in cloud provisioned health care systems", IEEE Consumer Communications and Networking Conference, 2011.

[24] Li J, Wang H, Zhang Y, Shen J (2016) Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing. Ksii Transactions on Internet & Information Systems 10: 3339–3352

[25] Hu, D. Ferraiolo, Kuhn, Information Technology Laboratory National Institute Standards, and Technology. Assessment of Access Control Systems, Interagency Report 7316. Technical report, National Institute of Standards and Technology, 2006.

[26] Markus Lorch, Seth Proctor, Rebekah Lepro, Dennis Kafura, and Sumit Shah. First experiences using XACML for access control in distributed systems. In Proceedings of the 2003 ACM workshop on XML security, XMLSEC '03, pages 25–37, New York, NY, USA, 2003. ACM.

[27] Rathish, C. R., and A. Rajaram. "Efficient path reassessment based on node probability in wireless sensor network." International Journal of Control Theory and Applications 34.2016 (2016): 817-832.

[28] Kumar, K. Vinoth, and A. Rajaram. "Energy efficient and node mobility-based data replication algorithm for MANET." (2019).

[29] CR Rathish, A Rajaram, "Sweeping inclusive connectivity-based routing in wireless sensor networks," ARPN Journal of Engineering and Applied Sciences, vol. 3, no. 5. pp. 1752-1760, 2018.

[30] K. Mahalakshmi, K. Kousalya, Himanshu Shekhar, Aby K. Thomas, L. Bhagyalakshmi, Sanjay Kumar Suman, S. Chandragandhi, Prashant Bachanna, K. Srihari, Venkatesa Prabhu Sundramurthy, "Public Auditing Scheme for Integrity Verification in Distributed Cloud Storage System", Scientific Programming, vol. 2021, Article ID 8533995, 5 pages, 2021. https://doi.org/10.1155/2021/8533995.

[31] J. Divakaran, Somashekhar Malipatil, Tareeq Zaid, M. Pushpalatha, Vilaskumar Patil, C. Arvind, T. Joby Titus, K. Srihari, M. Ragul Vignesh, Baswaraj Gadgay, Venkatesa Prabhu Sundramurthy, "Technical Study on 5G Using Soft Computing Methods", Scientific Programming, vol. 2022, Article ID 1570604, 7 pages, 2022. https://doi.org/10.1155/2022/1570604.

[32] S. Shitharth, Pratiksha Meshram, Pravin R. Kshirsagar, Hariprasath Manoharan, Vineet Tirth, Venkatesa Prabhu Sundramurthy, "Impact of Big Data Analysis on Nanosensors for Applied Sciences Using Neural Networks", Journal of Nanomaterials, vol. 2021, Article ID 4927607, 9 pages, 2021. https://doi.org/10.1155/2021/4927607.

[33] Upadhyay, G. M., et al. "Impact of Nanotechnology in the Development of Smart Cities." NanoWorld J 9.S5 (2023): S313-S318.

[34] Upadhyay GM, Kumar S, Chawla R, Gupta SK. 2023. Impact of Nanotechnology in the Development of Smart Cities. NanoWorld J 9(S5): S313-S318.

[35] Upadhyay, Govind Murari, and Shashi Kant Gupta. "A Novel Approach for Minimizing the Latency in Fog Computing." NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO (2021): 12882-12892.

[36] Varshney, Pankaj Kumar, and Govind Murari Upadhyay. "Significance of terrain dimension on the performance of wireless ad hoc proactive routing protocols." INROADS-An International Journal of Jaipur National University 6.2 (2017): 143-149.

[37] Vats, P., Mandot, M., & Gosain, A. (2014, February). A comparative study of Genetic Algorithms for its applications in Object oriented testing. In 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) (pp. 559-565). IEEE.

[38] Vats, P. (2014, March). A novel study of fuzzy clustering algorithms for their applications in various domains. In The 4th joint international conference on information and communication technology, electronic and electrical engineering (JICTEE) (pp. 1-6). IEEE.

[39] Vats, Prashant, et al. "A multi-factorial code coverage-based test case selection and prioritization for object oriented programs." ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1. Springer Singapore, 2021.

[40] Aalam, Zunaid, et al. "A comprehensive analysis of testing efforts using the avisar testing tool for object oriented softwares." Intelligent Sustainable Systems: Selected Papers of WorldS4 2021, Volume 2. Springer Singapore, 2022.

[41] Sharma, Nishi, et al. "A robust framework for governing blockchain-based distributed ledgers during COVID-19 for academic establishments." ICT with Intelligent Applications: Proceedings of ICTIS 2022, Volume 1. Singapore: Springer Nature Singapore, 2022. 35-41.

[42] Sharma, Anupam Kumar, et al. "Deep learning and machine intelligence for operational management of strategic planning." Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021. Singapore: Springer Nature Singapore, 2022.

[43] Gupta, Anjani, et al. "A sustainable green approach to the virtualized environment in cloud computing." Smart Trends in Computing and Communications: Proceedings of SmartCom 2022. Singapore: Springer Nature Singapore, 2022. 751-760.

[44] Varshney, Shipra, et al. "A blockchain-based framework for IoT based secure identity management." 2022 2nd international conference on innovative practices in technology and management (ICIPTM). Vol. 2. IEEE, 2022.