Journal for Educators, Teachers and Trainers
The PROFESIOLab electronic, peer-reviewed, open-access Magazine

ISSN 1989-9572

DOI:10.47750/jett.2024.15.05.38

Enhanced Data Privacy and Security in Cloud Storage: A Robust Authentication Scheme for Cyber-Physical-Social Systems

S.Mahesh Reddy 1, M.Sana 2, M.Sushma 2, M.Divya Sri2

Journal for Educators, Teachers and Trainers, Vol.15(5)

https://jett.labosfor.com/

Date of Reception: 24 Oct 2024

Date of Revision: 20 Nov 2024

Date of Publication : 31 Dec 2024

S.Mahesh Reddy 1, M.Sana 2, M.Sushma 2, M.Divya Sri2 (2024). Enhanced Data Privacy and Security in Cloud Storage: A Robust Authentication Scheme for Cyber-Physical-Social Systems,Vol.15(5).383-392

Journal for Educators, Teachers and Trainers
The LabOSfor electronic, peer-reviewed, open-access Magazine

Journal for Educators, Teachers and Trainers, Vol. 15(5)

ISSN1989 –9572

Enhanced Data Privacy and Security in Cloud Storage: A Robust Authentication Scheme for Cyber-Physical-Social Systems

S.Mahesh Reddy [1], M.Sana [2], M.Sushma [2], M.Divya Sri[2]

[1] Assistant Professor, [2] UG Student

[1,2] School of computer science and engineering, Malla Reddy Engineering College for Women (UGC-Autonomous), Maisammguda, Hyderabad, Telangana

Abstract
Cloud storage services are increasingly being adopted by organizations for managing and storing data due to their cost-effectiveness and resource scalability. However, the rise in cloud usage brings concerns regarding data security and user authentication, particularly in Cyber-Physical-Social Systems (CPSS). According to recent reports, over 60% of cloud users experience data breaches, and more than 30% are concerned about unauthorized access to personal data. Existing cloud security mechanisms such as encryption often fall short in ensuring user anonymity and preventing impersonation attacks. To address these gaps, the proposed paper introduces a robust authentication scheme aimed at enhancing data privacy and security in cloud storage. The core innovations lie in two critical aspects: user anonymity and protection against user/cloud impersonation attacks. User identities, including usernames and biometric data, are anonymized through hashing, ensuring that cloud servers cannot track or misuse this information. Additionally, sessions are dynamically created and terminated during login/logout, preventing the cloud server from logging activities or accessing sensitive data. The paper outlines a comprehensive approach involving user registration, login verification, file upload and download, and session management, along with the application of advanced encryption techniques like Elliptic Curve Cryptography (ECC) and CHACHA. The computation performance of these algorithms is also evaluated through a comparison graph, highlighting their efficiency. The novel contributions enhance data security while ensuring seamless cloud data access and sharing.

Keywords: Cloud storage, data security, authentication, user anonymity, elliptic curve cryptography, CHACHA, impersonation attacks

1. Introduction

Cloud storage has emerged as a vital solution for organizations and individuals to manage and store their data at a lower cost. According to a report by Gartner, the global cloud services market is expected to grow to $600 billion by 2025, with nearly 80% of organizations leveraging cloud platforms for storing critical data. Despite the undeniable benefits of cloud storage, security remains a significant concern. A study by McAfee revealed that 21% of cloud users have experienced a data breach, and 60% of cloud users worry about unauthorized access to sensitive information. These statistics highlight the critical need for enhanced security measures to ensure data confidentiality and user privacy, especially in sensitive environments like Cyber-Physical-Social Systems (CPSS).

The demand for secure and efficient cloud storage solutions is growing exponentially across various domains, including healthcare, finance, and social networking. In these applications, users share highly sensitive data, such as medical records, financial transactions, and personal information, making it essential to adopt robust mechanisms to safeguard this data. Additionally, the need for secure user authentication and data sharing mechanisms is crucial in modern systems where multiple users from diverse backgrounds access the cloud. As cloud platforms become more central to digital transformation, it is paramount to develop security solutions that not only protect the data but also ensure seamless access and sharing across diverse platforms, thus maintaining the integrity of applications that rely on cloud storage.

Existing manual methods for securing data in cloud systems primarily revolve around encryption and traditional access control mechanisms. While techniques such as data encryption provide a level of security, they are often insufficient for protecting user privacy and preventing sophisticated attacks like impersonation or identity theft. Furthermore, conventional methods of user authentication, such as username and password-based systems, are vulnerable to various forms of cyberattacks, including phishing, brute-force, and session hijacking. Although some systems incorporate biometric authentication, these measures often lack the sophistication required to provide robust protection in modern cloud environments, leading to potential security vulnerabilities and data breaches.

Given these challenges, there is a compelling need for a more advanced and comprehensive security methodology in cloud storage, particularly in environments like CPSS, where users require secure and anonymous data access. The need for an authentication system that combines cutting-edge encryption, biometric verification, and dynamic session management is critical. Existing solutions fail to address the growing complexity of modern cloud security challenges. Therefore, there is an urgent requirement to develop a multi-layered, novel authentication and data-sharing scheme that provides user anonymity, protects against impersonation attacks, and ensures seamless access to data while optimizing computational efficiency. This paper presents such a solution, leveraging state-of-the-art encryption techniques and user privacy preservation strategies to overcome existing shortcomings.

2. Literature Survey

In [1], authors presented an overview of cloud computing and discussed the fundamental aspects and applications of cloud technologies. They highlighted the various computing models, such as SaaS, PaaS, and IaaS, in cloud architectures. The paper also addressed the challenges in implementing and managing cloud systems. The drawback of this approach was the lack of a deeper exploration into emerging technologies such as blockchain integration for enhanced security. In [2], authors reviewed the state-of-the-art in cloud computing and identified key research challenges, such as resource management and service provisioning. They also explored various cloud computing paradigms and frameworks to improve system performance and scalability. However, the study did not thoroughly investigate the security and privacy concerns related to cloud data storage and transmission.

In [3], authors provided a survey on cloud computing security, focusing on issues like data confidentiality, integrity, and availability. They also discussed existing solutions such as encryption and access control mechanisms. The main drawback was the limited discussion on the integration of advanced technologies like blockchain for enhancing cloud security. In [4], authors examined recent security challenges in cloud computing and identified various threats like data breaches, denial of service attacks, and insider threats. They proposed solutions to mitigate these risks, such as multi-layered security models and advanced encryption techniques. However, the research failed to address the scalability of the proposed security solutions in large cloud environments.

In [5], authors explored cloud computing methodologies, systems, and applications, providing insights into the benefits and complexities of cloud adoption. They focused on the technical aspects of cloud infrastructure and service models, emphasizing system optimization. A limitation of the paper was its insufficient focus on the integration of blockchain for ensuring trust and transparency in cloud computing systems. In [6], authors reviewed the challenges faced in the design and security of cloud computing architectures. They discussed various architectural models and design patterns aimed at improving performance and reliability. However, the study did not explore how emerging technologies like blockchain could address security challenges in cloud systems.

In [7], authors critically reviewed cloud computing, analyzing the gap between researchers' desires and practical realities. They provided a detailed evaluation of cloud services and discussed user expectations versus actual service delivery. The drawback of this study was its insufficient focus on the security and privacy aspects in real-world cloud computing scenarios. In [8], authors proposed the use of blockchain technology in cloud computing for enhancing security through decentralized trust management. They discussed several use cases where blockchain could provide tamper-resistant data storage. The main limitation was the paper's focus on theoretical aspects rather than practical implementations and performance evaluations.

In [9], authors examined the use of blockchain in cloud computing, emphasizing its potential to solve architectural and security challenges. They outlined key blockchain-based architectures designed to improve cloud systems. The drawback was the limited exploration of the scalability and real-time implementation challenges of blockchain in cloud environments. In [10], authors presented a review of blockchain-based trust management in cloud systems. They categorized various trust management models and identified future research directions in blockchain integration. However, the paper did not fully address the challenges related to integrating blockchain with existing cloud service architectures.

In [11], authors discussed the benefits and challenges of integrating blockchain technology with cloud computing. They explored various applications where blockchain could enhance cloud services such as secure data sharing and transparent auditing. The main drawback was the lack of a comprehensive analysis on the scalability and performance implications of integrating blockchain with cloud platforms. In [12], authors proposed a Blockchain-based Secure Cloud Identity and Access Management (BSCIAM) framework to enhance the security of cloud systems. They demonstrated how blockchain could ensure the integrity and authentication of cloud resources. The drawback was the limited testing of the framework in large-scale cloud environments.

In [13], authors provided an overview of blockchain technology, discussing its architecture, consensus mechanisms, and potential future trends. They highlighted blockchain’s role in enhancing security and transparency across various industries. The limitation was the insufficient practical application of the technology in real-world cloud systems. In [14], authors explored the applications and open issues in blockchain technology. They identified various challenges in deploying blockchain across different sectors, including scalability and energy consumption. The main drawback was the lack of focus on cloud-specific blockchain integration challenges. In [15], authors reviewed the state-of-the-art in blockchain technology and identified research challenges in adopting blockchain for cloud and other industries. They provided a detailed analysis of blockchain's potential impact on various systems.

However, the paper did not focus on how blockchain could be used specifically to address security issues in cloud computing systems.

3. Proposed System

The proposed methodology introduces a novel, multi-layered approach to cloud storage security in Cyber-Physical-Social Systems (CPSS) by combining unique elements that are not seen in existing surveys as shown in Figure 1. The algorithm starts with user anonymity achieved through hashed usernames and biometric data, ensuring that the cloud server cannot trace individual identities. This is followed by a dynamic session management mechanism that prevents impersonation attacks by creating and terminating sessions at login and logout. The data encryption is handled by a dual-layer system, where ECC is used for initial encryption, followed by CHACHA, a lighter encryption method, for re-encryption before sharing the data. This combination of ECC and CHACHA ensures both high-level security and optimized performance. Additionally, the cloud server applies secure file access by verifying users through multi-factor authentication before granting permission to upload, download, or alter files. This multi-layered encryption and authentication approach enhances both privacy and security, which are critical in CPSS environments.

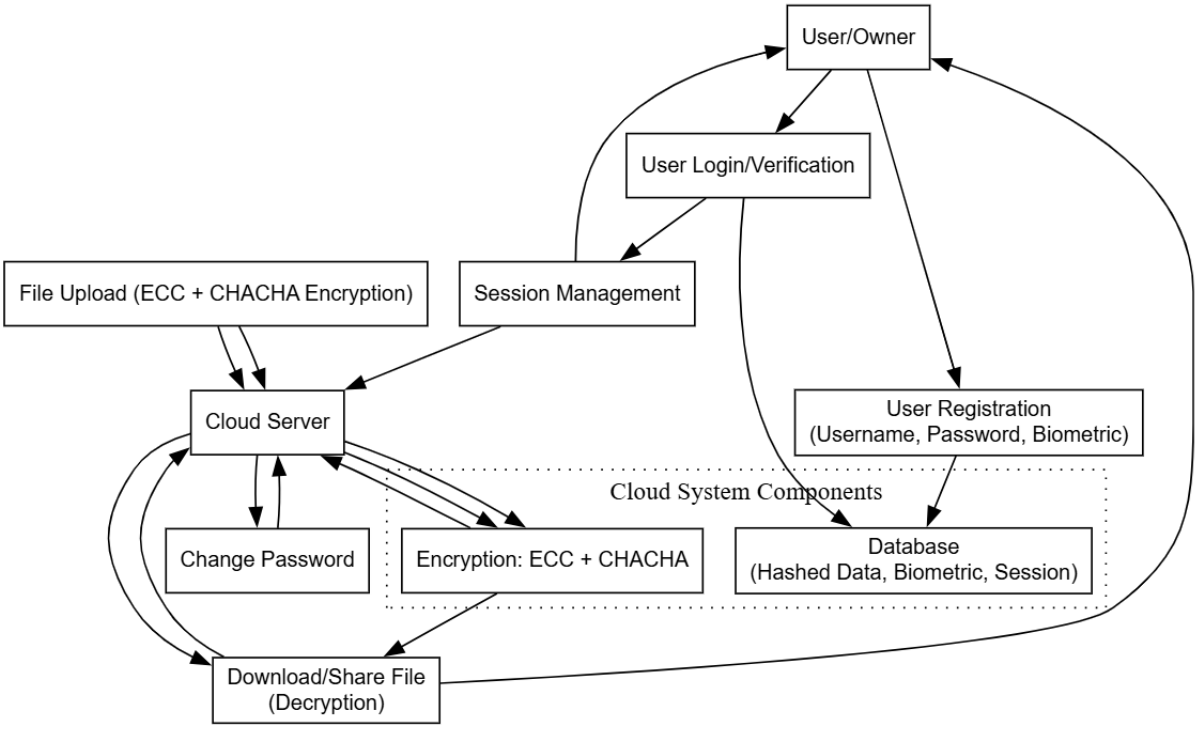


Figure 1. Proposed System Architecture.

User Registration: The user initiates the process by registering on the cloud platform, providing a username, password, and biometric details (such as a fingerprint or facial image). The username and biometric data are then hashed before being stored in the cloud database, ensuring that these sensitive details are anonymized. The biometric data, once hashed, is also enrolled in a secure biometric authentication system to ensure robust identity verification during future interactions.

User Login/Verification: When the user logs in, they provide their username, password, and biometric data. The system verifies the provided credentials against the previously hashed data stored in the cloud database. If the credentials are valid, a dynamic session is created, enabling the user to access their data securely. This session is automatically terminated after the user logs out, further preventing impersonation attacks.

File Upload: The data owner uploads a file, which is first encrypted using Elliptic Curve Cryptography (ECC), ensuring a high level of data security. The cloud server then re-encrypts this file using the CHACHA encryption algorithm, which is more lightweight than ECC, optimizing performance without compromising security. The re-encrypted file is then shared with valid users who have been authenticated via the dynamic session management system.

Change Password: Users or data owners can request a password change through the cloud system. Once the request is validated through multi-factor authentication, the new password is hashed and securely stored in the database.

Download Own/Shared Files: Users who need to download their own or shared files must first go through the authentication process, ensuring that only authorized users can access the data. After successful verification, the files are decrypted, either by the original owner or the valid recipient, allowing them to access the shared data securely.

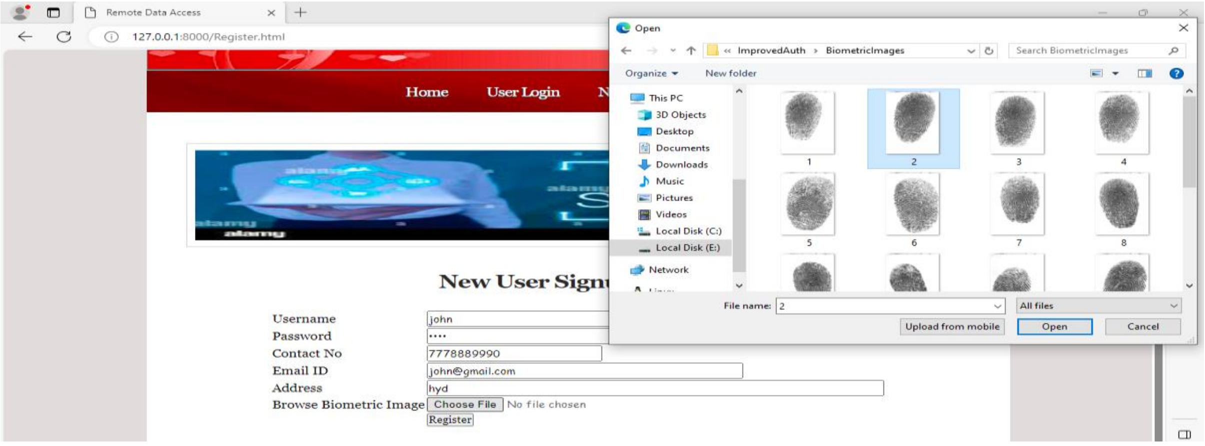
Computation Graph: To evaluate the performance of the encryption methods, the system plots a comparison graph between the ECC computation time and CHACHA computation time. This visual representation highlights the efficiency of using CHACHA as an extension to ECC, showcasing the practical benefits of the proposed encryption scheme in real-world scenarios.

4. Results and Discussions

Figure 2 shows the Register screen where the user enters their signup details, uploads their biometric image, and clicks on the 'Register' button to proceed to the next page. Figure 3 shows the User Login screen, where after completing the sign-up, the user clicks on the 'User Login' link to access the login page for authentication.

Figure 4 shows the Fingerprint Selection screen, where the user enters login credentials, uploads their biometric image, and presses buttons to proceed to the next step. Figure 5 shows the Upload File screen, which appears after a successful login. The user can click on the ‘Upload File’ link to upload files into the system.

Figure 6 shows the File Uploaded screen, displaying the uploaded file saved in the cloud. The file is now visible in an encrypted format, ensuring security. Figure 7 shows the Download Own/Share File screen, where the file cannot be opened since it is encrypted. The user can click on the ‘Download Own/Share File’ link to access files uploaded by other users. In the Download Own/Share File screen, users can view files from all data owners and download them by clicking on the 'Click Here' link, after which they are directed to a page where the file is downloaded in a decrypted format. In the Change Password screen, after downloading the file in decrypted format, the user clicks on the ‘Change Password’ link to update their account credentials for enhanced security.

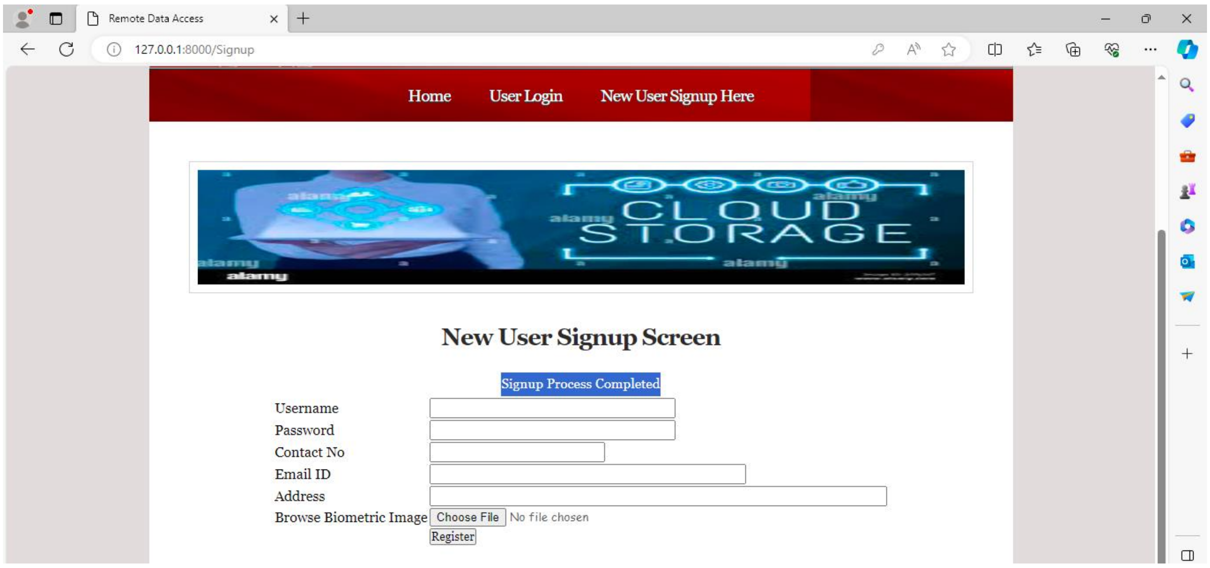


New User Signu

File name: 2

Username	john
Password	••••
Contact No	7778889990
Email ID	john@gmail.com
Address	hyd
Browse Biometric Image	Choose File No file chosen
	Register

Figure 2. Register

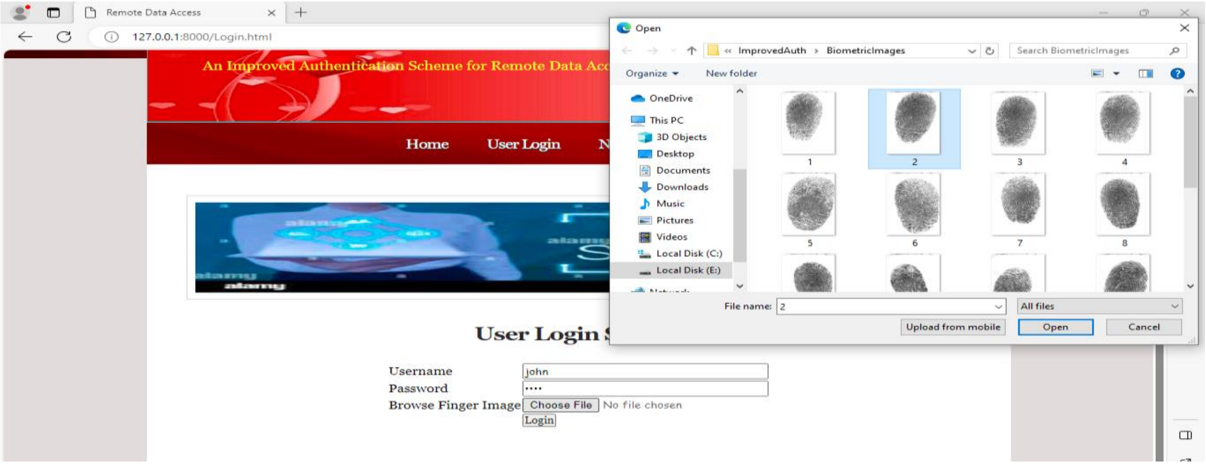


New User Signup Screen

Signup Process Completed

Username	
Password	
Contact No	
Email ID	
Address	
Browse Biometric Image	Choose File No file chosen
	Register

Figure 3. User Login



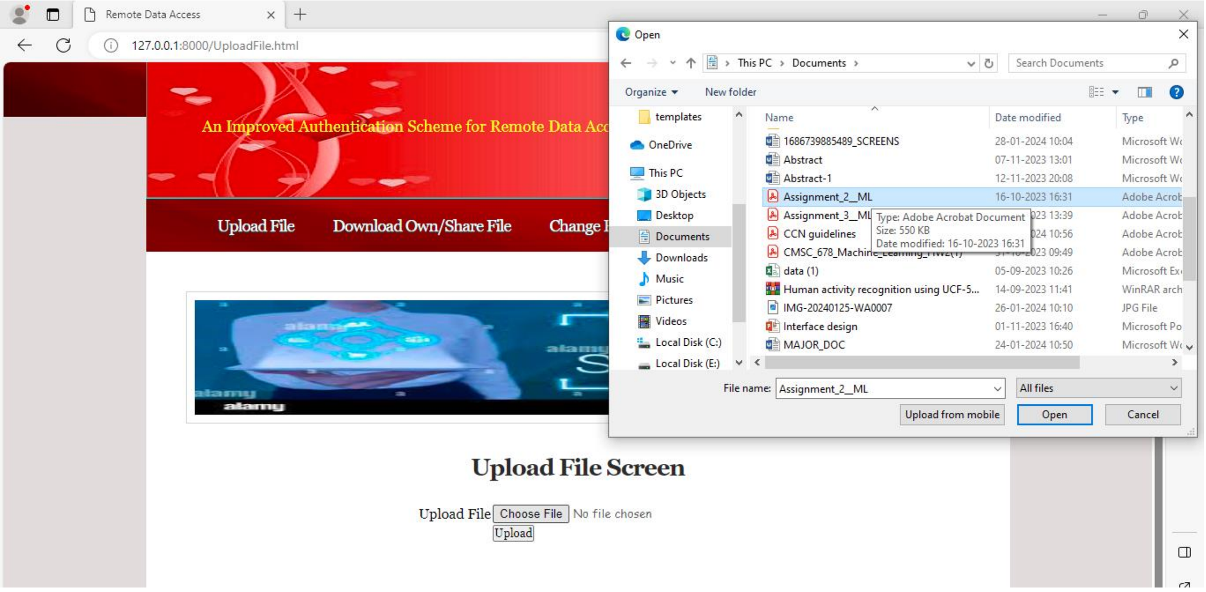
An Improved Authentication Scheme for Remote Data Acc

User Login S

File name: 2

Username	john
Password	••••
Browse Finger Image	Choose File No file chosen
	Login

Figure 4. Fingerprint Selection

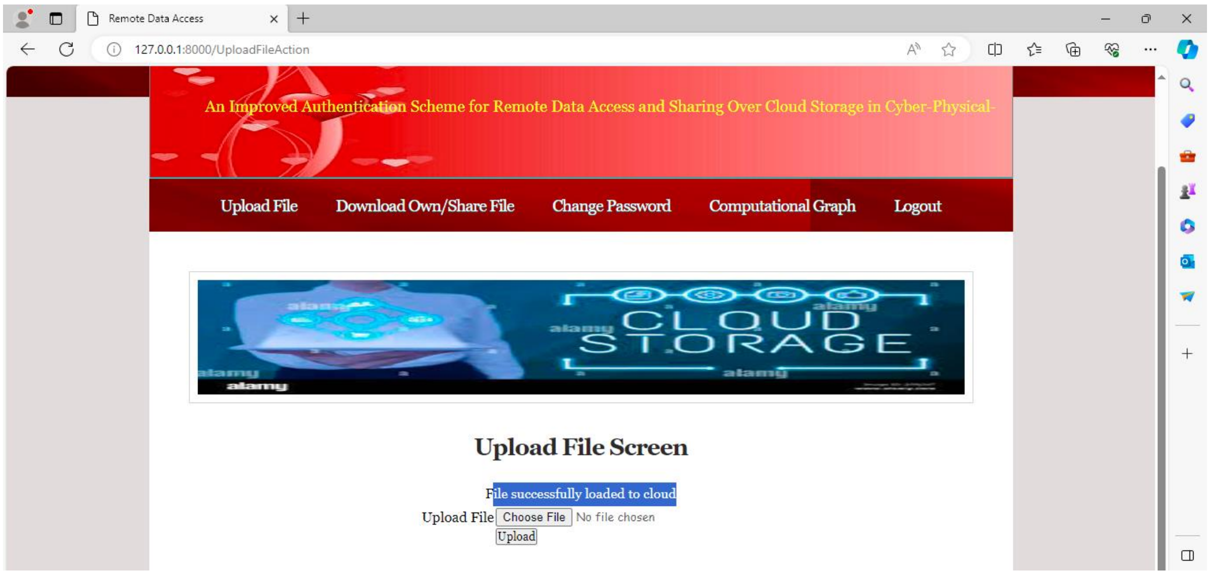


Name	Date modified	Type
1686739885489_SCREENS	28-01-2024 10:04	Microsoft W
Abstract	07-11-2023 13:01	Microsoft W
Abstract-1	12-11-2023 20:08	Microsoft W
Assignment_2__ML	16-10-2023 16:31	Adobe Acrol
Assignment_3__ML	023 13:39	Adobe Acrol
CCN guidelines	024 10:56	Adobe Acrol
CMSC_678_Machine_Learning_HW2(1)	023 09:49	Adobe Acrol
data (1)	05-09-2023 10:26	Microsoft Ex
Human activity recognition using UCF-5...	14-09-2023 11:41	WinRAR arch
IMG-20240125-WA0007	26-01-2024 10:10	JPG File
Interface design	01-11-2023 16:40	Microsoft Po
MAJOR_DOC	24-01-2024 10:50	Microsoft W

Type: Adobe Acrobat Document
Size: 550 KB
Date modified: 16-10-2023 16:31

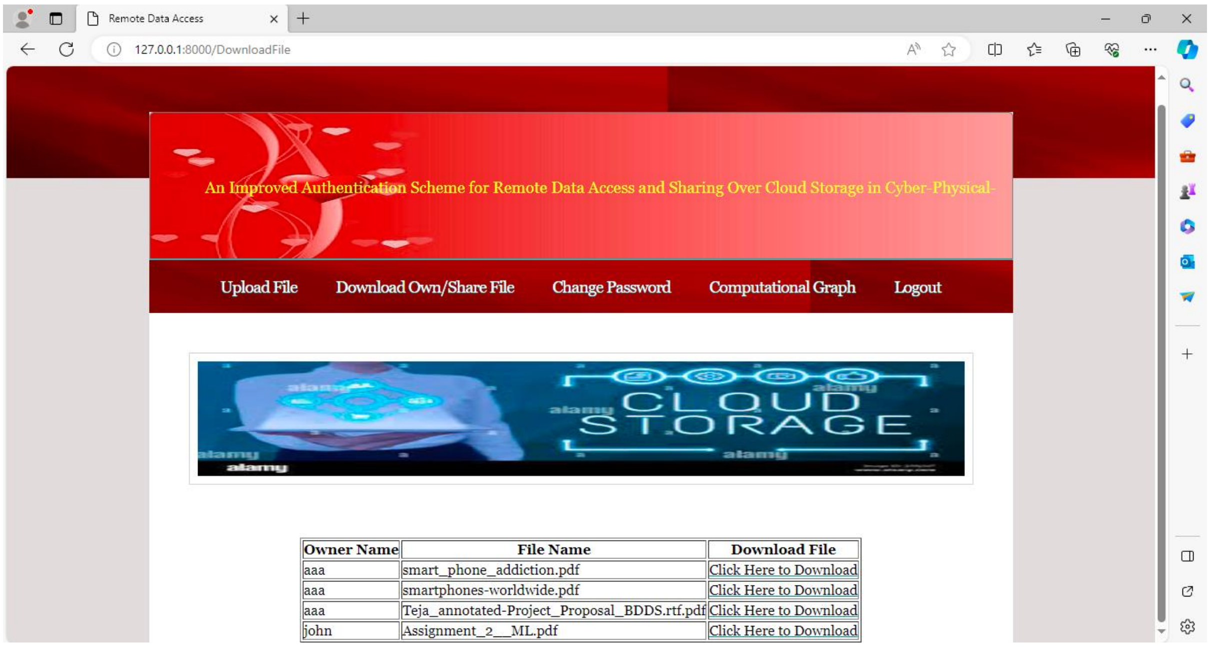
File name: Assignment_2__ML

Figure 5. Upload File


Remote Data Access
127.0.0.1:8000/UploadFileAction
An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-
Upload File
Download Own/Share File
Change Password
Computational Graph
Logout
CLOUD STORAGE
Upload File Screen
Upload File Choose File No file chosen
Upload

File successfully loaded to cloud

Figure 6. File Uploaded.


Remote Data Access
127.0.0.1:8000/DownloadFile
An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-
Upload File
Download Own/Share File
Change Password
Computational Graph
Logout
CLOUD STORAGE

Owner Name	File Name	Download File
aaa	smart_phone_addiction.pdf	Click Here to Download
aaa	smartphones-worldwide.pdf	Click Here to Download
aaa	Teja_annotated-Project_Proposal_BDDS.rtf.pdf	Click Here to Download
john	Assignment_2__ML.pdf	Click Here to Download

Figure 7. Download Own/Share File.

5. Conclusion

In conclusion, the proposed authentication scheme significantly enhances data security and privacy in cloud storage for Cyber-Physical-Social Systems (CPSS) by addressing critical vulnerabilities such as user anonymity and impersonation attacks. By employing advanced techniques like hashing for user identity anonymization and dynamic session management, the system ensures that unauthorized access and internal threats are mitigated. Additionally, the integration of Elliptic Curve Cryptography (ECC) and CHACHA for encryption optimizes data confidentiality while maintaining computational efficiency. The comparison of these encryption algorithms further underscores the practicality of the proposed approach in real-world scenarios. However, future research can explore further improvements in encryption methods to enhance scalability and reduce computational overhead in larger systems. Additionally, integrating multi-factor authentication and blockchain technology could provide even more robust security and transparency in cloud-based CPSS environments. The adoption of these advanced technologies would pave the way for more secure, scalable, and user-friendly cloud storage solutions.

References

1. Qian, L.; Luo, Z.; Du, Y.; Guo, L. Cloud computing: An overview. In *Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, 1–4 December 2009. Proceedings 1*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 626–631

2. Zhang, Q.; Cheng, L.; Boutaba, R. Cloud computing: State-of-the-art and research challenges. *J. Internet Serv. Appl.* **2010**, *1*, 7–18.

3. Singh, S.; Jeong, Y.S.; Park, J.H. A survey on cloud computing security: Issues, threats, and solutions. *J. Netw. Comput. Appl.* **2016**, *75*, 200–222.

4. Subramanian, N.; Jeyaraj, A. Recent security challenges in cloud computing. *Comput. Electr. Eng.* **2018**, *71*, 28–42.

5. Wang, L.; Ranjan, R.; Chen, J.; Benatallah, B. *Cloud Computing: Methodology, Systems, and Applications*; CRC Press: Boca Raton, FL, USA, 2017.

6. Hu, F.; Qiu, M.; Li, J.; Grant, T.; Taylor, D.; McCaleb, S.; Butler, L.; Hamner, R. A review on cloud computing: Design challenges in architecture and security. *J. Comput. Inf. Technol.* **2011**, *19*, 25–55.

7. Venters, W.; Whitley, E.A. A critical review of cloud computing: Researching desires and realities. *J. Inf. Technol.* **2012**, *27*, 179–197.

8. Park, J.H.; Park, J.H. Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry* **2017**, *9*, 164.

9. Murthy, C.V.B.; Shri, M.L.; Kadry, S.; Lim, S. Blockchain based cloud computing: Architecture and research challenges. *IEEE Access* **2020**, *8*, 205190–205205.

10. Li, W.; Wu, J.; Cao, J.; Chen, N.; Zhang, Q.; Buyya, R. Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions. *J. Cloud Comput.* **2021**, *10*, 35.

11. Habib, G.; Sharma, S.; Ibrahim, S.; Ahmad, I.; Qureshi, S.; Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet* **2022**, *14*, 341.

12. Das, S.; Sahil, M.; Pandit, N.K.; Priyadarshini, R.; Gochhayat, S.P. BSCIAM: A Blockchain based Secure Cloud Identity and Access Management Framework. In Proceedings of the 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 24–25 February 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6.

13. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 557–564.

14. Das, S.; Rout, J.; Mishra, M. Blockchain Technology: Applications and Open Issues. In Proceedings of the 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 10–11 March 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.

15. Namasudra, S.; Deka, G.C.; Johri, P.; Hosseinpour, M.; Gandomi, A.H. The revolution of blockchain: State-of-the-art and research challenges. *Arch. Comput. Methods Eng.* **2021**, *28*, 1497–1515.