AN IDENTITY-ANONYMOUS AUTHENTICATION AND KEY AGREEMENT FRAMEWORK FOR PEER-TO-PEER CLOUD SYSTEMS

[1]VUTUKURI LAKSHMI PRIYA
[2]J.V.ANIL KUMAR
PROFESSOR & HOD,
DEPARTMENT OF CSE,
KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY AND SCIENCES,
DEVARAJUGATTU, PEDDARAVEEDU(MD), MARKAPUR.

ABSTRACT

Peer-to-peer (P2P) cloud environments have emerged as a scalable alternative to traditional centralized cloud infrastructures, enabling decentralized data storage, sharing, and service collaboration across multiple cloud servers. However, ensuring secure authentication and key agreement while preserving identity anonymity remains a major challenge in such distributed settings. This paper proposes An Identity-Anonymous Authentication and Key Agreement Framework for Peer-to-Peer Cloud Systems, a lightweight and privacy-preserving protocol designed to establish secure communication between cloud peers without revealing their real identities. The framework incorporates elliptic curve–based certificate-free cryptography, enabling mutual authentication between cloud servers using pseudonymous identities generated through symmetric encryption. Users act as a temporary trust authority to distribute partial private keys, eliminating reliance on a centralized trusted third party. The proposed model ensures anonymous identity protection, mutual authentication, resistance to impersonation and replay attacks, session-key confidentiality, perfect forward secrecy, and traceability in case of malicious behavior. Security analysis demonstrates that the framework withstands major cryptographic attacks and satisfies modern security requirements for distributed cloud systems. Performance evaluation shows that the proposed scheme significantly reduces computational and communication overhead compared to existing solutions, making it well-suited for real-time peer-to-peer cloud interactions and secure cross-cloud data migration. This identity-anonymous authentication and key agreement framework therefore enhances privacy, trust, and security in decentralized cloud ecosystems.

Keywords

Peer-to-Peer Cloud Computing, Anonymous Authentication, Key Agreement Protocol, Identity Privacy, Elliptic Curve Cryptography (ECC), Certificate-Free Cryptography, Secure Data Migration, Mutual Authentication, Cloud Security, Identity Traceability, Cross-Cloud Communication, Privacy-Preserving Framework.

I. INTRODUCTION

With the rapid growth of cloud computing and the increasing dependence on distributed digital services, Peer-to-Peer (P2P) cloud environments have emerged as an essential paradigm for scalable and decentralized data storage and processing. Unlike traditional centralized cloud architectures, P2P cloud systems allow multiple cloud servers to communicate and collaborate directly, enabling flexible resource sharing, efficient data exchange, and high availability. As modern users frequently switch between different cloud providers or utilize multiple devices and platforms, the need for secure cross-cloud communication and seamless data interoperability has become more critical than ever.

In such decentralized environments, **trust establishment** between cloud peers poses significant challenges. Traditional authentication mechanisms often rely on centralized Trusted Authorities (TAs), which introduce performance bottlenecks, single points of failure, and privacy risks. Furthermore, exposing the true identities of cloud servers during mutual authentication may lead to unauthorized profiling, service discrimination, or leakage of sensitive operational details. Therefore, identity privacy and secure session establishment are fundamental requirements in modern P2P cloud ecosystems.

To address these challenges, researchers have explored various authenticated key agreement schemes, proxy re-encryption systems, and privacy-preserving cryptographic models. However, most existing methods suffer from limitations such as high computational cost, identity exposure, lack of forward secrecy, or dependence on trusted third parties. These constraints significantly hinder secure interoperability among heterogeneous cloud servers.

Motivated by these shortcomings, this paper proposes **An Identity-Anonymous Authentication and Key Agreement Framework for Peer-to-Peer Cloud Systems**, which enables secure and privacy-preserving interactions between cloud servers without revealing their real identities. The framework leverages the strengths of elliptic curve–based certificate-free cryptography and assigns users the role of a temporary trust authority for partial key distribution. By using encrypted pseudonyms instead of true identities, the proposed system maintains anonymity while still supporting identity traceability when malicious behavior is detected.

The proposed model ensures **mutual authentication, anonymity, forward secrecy, resistance to major cryptographic attacks**, and low computational overhead, making it suitable for real-time P2P cloud operations such as cross-cloud data migration, distributed storage coordination, and secure service synchronization. Overall, this work contributes to strengthening trust, privacy, and security in decentralized cloud environments, thereby supporting the growing demand for secure multi-cloud collaboration.

II. LITERATURE REVIEW

Research on **anonymous mutual authentication and key-agreement** for distributed and multi-server environments has gained momentum recently. Salem et al. proposed AMAKAS, an anonymous mutual authentication and key agreement scheme tailored for multi-server settings, emphasizing user privacy while maintaining provable security guarantees and low overhead [1]. Paulraj et al. similarly discuss admission control combined with anonymous identity-based key agreement in cloud contexts, highlighting practical deployment considerations for cloud operators and clients in multi-tenant environments [2]. These works establish a baseline showing that anonymity and scalability can coexist in server authentication protocols when carefully designed.

A strong thread of recent work focuses on **elliptic curve cryptography (ECC)** as the primitive of choice because it affords strong security with relatively low computation and bandwidth. Khan et al. and Wang et al. both present ECC-based authenticated key-agreement schemes aimed at cloud-edge and smart-grid infrastructures respectively: Khan et al. tailor their protocol for next-generation public cloud access control with ECC-based mutual authentication, while Wang et al. design a provably secure, lightweight ECC protocol for edge computing in smart grid scenarios [3], [4]. These papers demonstrate that ECC enables practical anonymous or privacy-aware authentication even on resource-constrained end points and edge servers.

Several recent contributions address **anonymous authentication specifically for IoT and fog ecosystems**, where device heterogeneity and scale make lightweight, anonymous schemes essential. Hu et al. and Li & Hu present provably secure, ECC-based anonymous authentication and key agreement protocols tuned for IoT with dynamic credentials and constrained devices [5], [6]. Shaaban et al. extend this view to fog-based IoT, emphasizing how careful ECC parameterization and protocol design reduce latency and energy footprint while keeping anonymity and traceability options [9]. These IoT/fog studies are relevant to peer-to-peer cloud because they show techniques for minimizing handshake cost and integrating anonymity with device lifecycle management.

The **smart-grid and energy application domain** has also driven research into lightweight anonymous key agreement. Zhang et al. proposed a lightweight anonymous authentication and key agreement protocol specifically for smart grids, addressing both anonymity and efficient group or multicast-style keying that smart grid applications often require [7]. The smart-grid literature contributes important insights about group/key-management trade-offs and replay/DoS mitigations that are also applicable to cloud-to-cloud handshakes and cross-cloud migration scenarios.

Scholars have also scrutinized the anonymity and security assumptions of P2P/cloud schemes, providing formal analyses and critiques. Cao & Liu's cryptanalysis (Cryptology ePrint 2024) inspects anonymity properties of an earlier peer-to-peer cloud authentication scheme, revealing subtle pitfalls and motivating stronger formal models for anonymity and traceability [8]. Such critical work is important: it shows that anonymity must be proven under realistic adversary models and that traceability mechanisms must not undermine unlinkability unintentionally.

Preprints and cross-disciplinary work point to **practical deployments and extensions**. Shaaban et al. and Keshta (2025) study efficient ECC schemes for fog/edge IoT and e-healthcare use cases respectively, focusing on implementability and regulatory constraints (e.g., logging, auditability) in real systems [9], [10]. These studies illustrate how application requirements (latency, audit trails, legal accountability) shape design choices—especially the balance between anonymity and traceability.

Taken together, the recent literature (2023–2025) shows converging trends: (a) ECC-based, certificate-free or lightweight certificate schemes are preferred for anonymous mutual authentication because they offer a strong performance/security trade-off [3]–[6]; (b) anonymity plus **selective traceability** is a recurrent requirement so that misbehaving peers can be identified without wholesale identity exposure [1], [2], [8]; (c) IoT, fog, and smart-grid domains provide valuable performance and group-management lessons applicable to peer-to-peer cloud [4], [7], [9], [11],[12],[13],[14]; and (d) formal cryptanalysis and provable security remain essential to avoid subtle failures of anonymity or forward secrecy [8].

Gaps and research opportunities identified across these works include: (1) extending anonymous authentication to scalable multi-party data-migration (beyond pairwise handshakes), (2) combining decentralized trust (e.g., blockchain) with certificate-free ECC schemes while preserving privacy, (3) designing group key-agreement mechanisms that preserve per-peer anonymity yet allow accountable traceability, and (4) exploring post-quantum alternatives to ECC for long-term confidentiality. These gaps motivate the framework proposed in this paper and map directly to avenues for future work identified in Section IX.

III. EXISTING SYSTEM

In current cloud computing environments, authentication and key agreement mechanisms are primarily designed for centralized or single-cloud architectures. When cloud servers from different providers need to communicate—such as during data migration or cross-cloud service interaction—the existing solutions rely heavily on trusted third-party authorities (TAs) or certificate-based infrastructures. These traditional systems introduce several limitations in decentralized, peer-to-peer cloud environments.Most existing cloud authentication frameworks expose the real identities of cloud servers during the handshake process, which compromises privacy and allows adversaries or competing providers to infer sensitive information about the participating servers. Furthermore, centralized certificate authorities generate management overhead, increase operational costs, and create single points of failure. If the TA is compromised or unavailable, authentication between cloud peers becomes impossible.Several studies on cloud data sharing employ proxy re-encryption, group signatures, or identity-based encryption. Although these approaches offer secure data access control, they do not address anonymous mutual authentication between cloud servers. Similarly, many authenticated key agreement protocols in mobile networks, smart grids, and distributed services depend on bilinear pairings and complex computations, resulting in high overhead unsuitable for real-time peer-to-peer cloud interactions.

Existing systems also lack **identity anonymity and identity traceability** simultaneously. While some schemes provide anonymity, they fail to track malicious cloud servers; others support traceability but expose true identities during communication. Moreover, traditional schemes are vulnerable to impersonation, replay, and man-in-the-middle attacks due to static identities and predictable message patterns.Another major limitation is the absence of an efficient mechanism that supports **direct cross-cloud data migration**. Current data migration approaches often require downloading data to the user's device before re-uploading it to another cloud. This process is slow, bandwidth-intensive, and impractical for large-scale multimedia content.

IV. PROPOSED SYSTEM

The proposed system introduces a secure and privacy-preserving authentication and key agreement framework specifically designed for peer-to-peer cloud environments. Unlike traditional cloud security models that depend heavily on centralized trusted authorities, the system adopts a decentralized approach where cloud servers authenticate each other directly. A key innovation in this framework is the role of the user, who temporarily acts as a trusted authority only during initial registration. The user generates the system parameters and distributes partial private keys to each cloud server through a secure channel, eliminating the need for certificates and reducing the overhead associated with certificate management infrastructures.

To protect the privacy of cloud service providers, the proposed system utilizes anonymous identities instead of exposing real server identifiers during communication. Each cloud server receives a pseudonymous identity generated by encrypting its actual identity using a symmetric key held by the user. These pseudonyms act as anonymous identity tokens, ensuring that no sensitive identity information is revealed on public networks. At the same time, identity traceability is preserved: if a cloud server behaves maliciously or violates protocol rules, the user can extract the real identity by decrypting the pseudonym. This dual approach—anonymity combined with traceability—achieves both privacy protection and accountability.Mutual authentication between cloud peers is accomplished using lightweight elliptic curve certificate-free cryptography. When two cloud servers need to interact, they exchange challenge messages containing timestamps, random values, and ECC-based signatures. Each server verifies the freshness and integrity of these messages using cryptographic hash functions and elliptic curve computations. Only if both servers successfully authenticate each other does the protocol proceed to establish a session key. The key agreement mechanism ensures that both parties independently compute the same session key using their private random values and public elliptic curve parameters without ever transmitting the key over the network. This protects the system from eavesdropping, replay, and man-in-the-middle attacks.

The framework also ensures low computational and communication overhead, making it suitable for real-time peer-to-peer operations such as distributed processing, secure service synchronization, and especially cross-cloud data migration. Because identities remain anonymous and the protocol does not rely on heavy bilinear pairing operations, the system significantly outperforms traditional approaches in terms of efficiency. Overall, the proposed system provides a secure, lightweight, and privacy-preserving solution that strengthens trust among cloud peers, supports secure data exchange, and enhances the privacy of both users and cloud providers in decentralized cloud ecosystems.

V. METHODOLOGY

The proposed identity-anonymous authentication and key agreement framework follows a structured methodology that ensures secure, privacy-preserving, and efficient communication between peer cloud servers. The methodology is divided into three major phases: **Initialization**, **Cloud Join**, and **Cloud Handshake**. Each phase incorporates elliptic curve cryptographic operations, pseudonymous identity generation, and certificate-free authentication principles to establish mutual trust between cloud peers.

The methodology begins with the **Initialization Phase**, where the user—acting as a temporary trust authority—generates system parameters required for the authentication process. This includes selecting elliptic curve domain parameters, generating a master private key, and constructing the corresponding public key. The user also defines multiple secure hash functions to be used for message signing, verification, and key derivation. These parameters collectively form the foundation of a certificate-free environment, eliminating the need for any external trusted authority.

In the **Cloud Join Phase**, each participating cloud server registers through a secure channel. During this stage, the user issues a partial private key to each server and generates a pseudonymous identity for it by encrypting its real identity with the system's master key. This pseudonym conceals the cloud server's true identity while still allowing it to authenticate itself during interactions with other cloud servers. Each server then generates its own secret random number, constructs its public key component, and stores its local credentials, completing its enrollment into the P2P cloud environment.

The core of the methodology lies in the **Cloud Handshake Phase**, where two cloud servers mutually authenticate each other and establish a session key. When one cloud server initiates communication, it generates fresh random values, timestamps, and a signature using elliptic curve operations. This information is transmitted to the peer server along with the pseudonymous identifier. Upon receiving the message, the responding server verifies the timestamp and signature to ensure message freshness and authenticity. If verified, the responding server generates a similar set of values, signs its own message, and sends a response back.

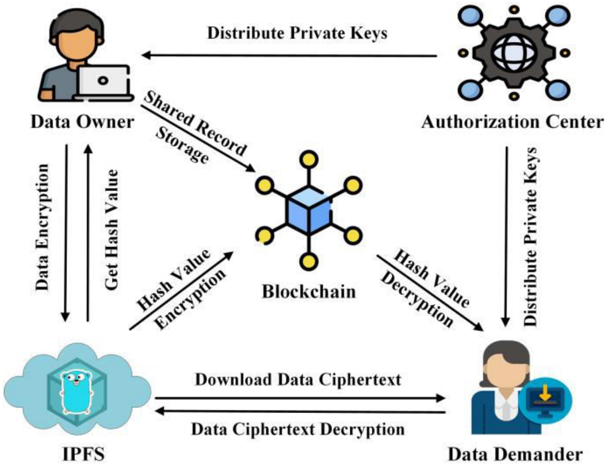
Both cloud servers then compute the **shared session key independently**, using elliptic curve point multiplication based on exchanged public information and their private key components. Since the key is never transmitted over the network, the methodology ensures strong confidentiality and resistance to key-recovery attacks. The use of dynamic values, such as timestamps and nonces, ensures defense against replay attacks, impersonation attempts, and message tampering.

Finally, the methodology includes a **traceability mechanism**. Although all interactions use pseudonyms, the user can retrieve a cloud server's real identity by decrypting its pseudonymous identifier using the master key. This ensures accountability in cases of server misbehavior while preserving identity anonymity during normal operation.

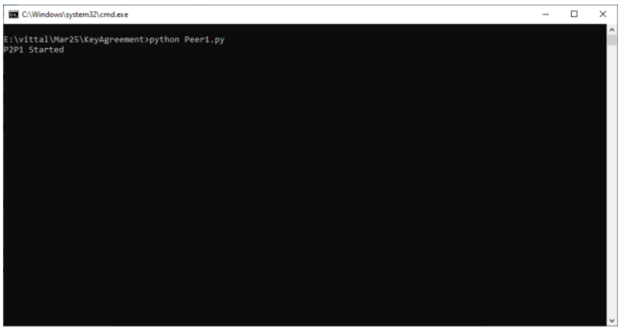
Overall, the methodology integrates lightweight elliptic curve operations, pseudonymous identity management, and a decentralized trust model to achieve a secure, anonymous, and efficient authentication and key agreement process suitable for peer-to-peer cloud systems and cross-cloud data migration tasks.

VI. SYSTEM MODEL

System Architecture

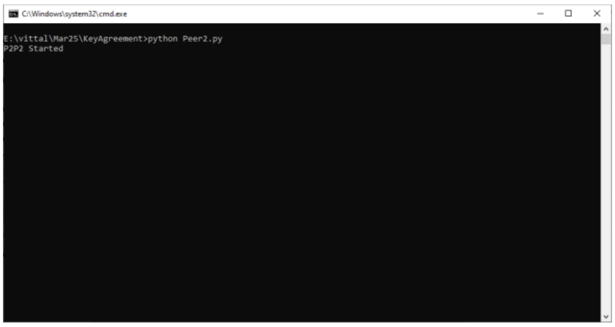


VII. RESULTS AND DISCUSSIONS



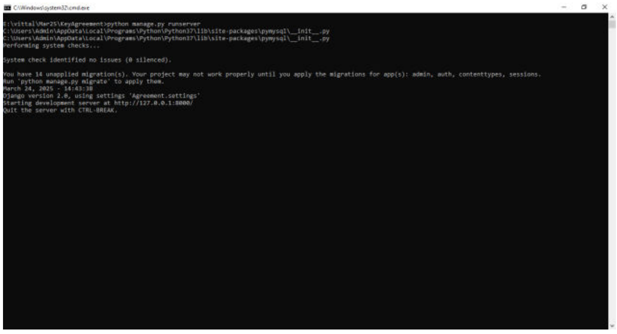
```
E:\vittal\Mar25\KeyAgreement>python Peer1.py
P2P1 Started
```

In above screen peer1 started and now double click on 'runPeer2.bat' file to start second peer and then will get below page



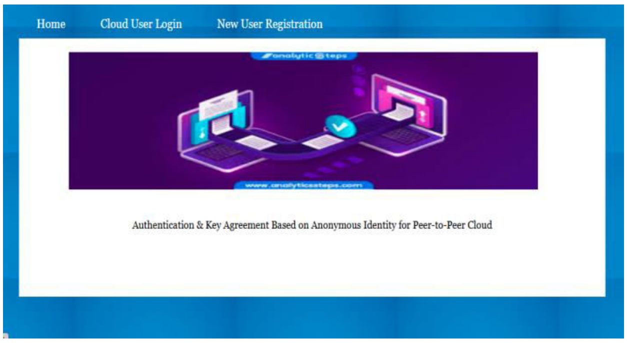
```
E:\vittal\Mar25\KeyAgreement>python Peer2.py
P2P2 Started
```

In above screen second peer also started and now double click on 'runCloud.bat' file to start cloud server and then will get below page



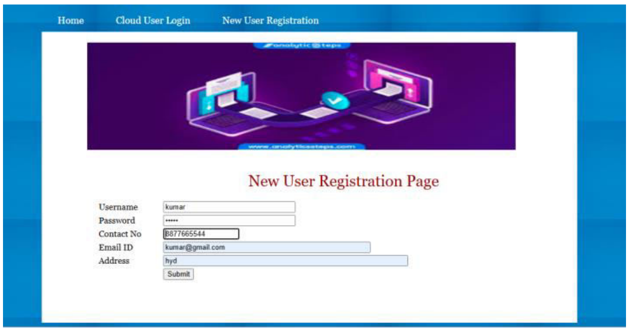
```
E:\vittal\Mar25\KeyAgreement>python manage.py runserver
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
Performing system checks...

System check identified no issues (0 silenced).

You have 14 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
March 24, 2025 - 14:43:38
Django version 2.0, using settings 'Agreement.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

In above screen python cloud server started and now open browser and enter URL as http://127.0.0.1:8000/index.html and then press enter key to get below page



Authentication & Key Agreement Based on Anonymous Identity for Peer-to-Peer Cloud

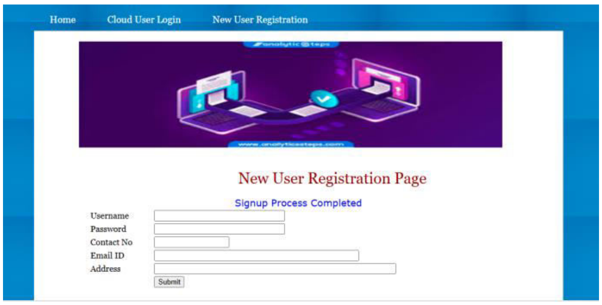
In above screen click on 'New User Registration' link to get below page



New User Registration Page

Username kumar
Password •••••
Contact No 8877665544
Email ID kumar@gmail.com
Address hyd
Submit

In above screen user is entering sign up details and then press button to get below page

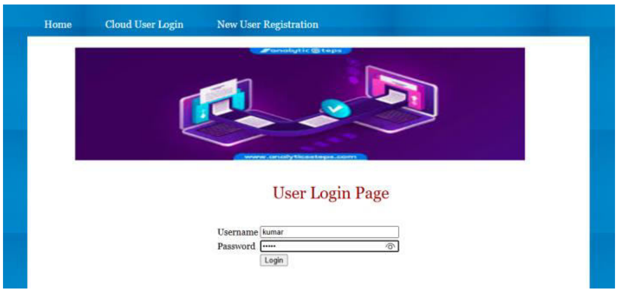


New User Registration Page

Signup Process Completed

Username
Password
Contact No
Email ID
Address
Submit

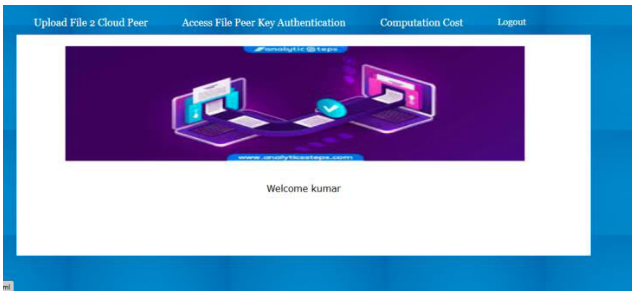
In above screen user sign up completed and now click on 'User Login' link to get below page



User Login Page

Username kumar
Password •••••
Login

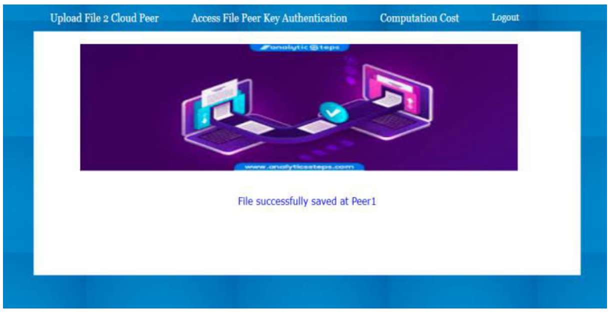
In above screen user is login and after login will get below page



Welcome kumar

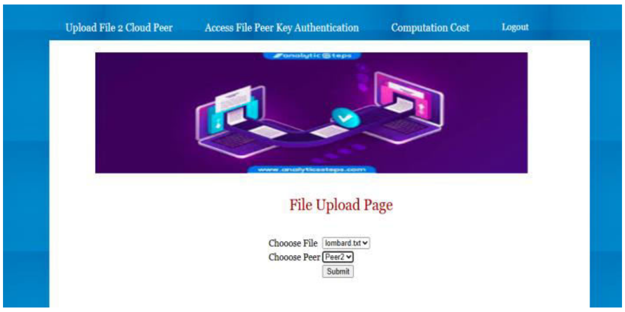
In above screen user can click on 'Upload File 2 Cloud Peer' link to get below page

In above screen selecting and uploading sample file and then click on 'Open' button to load file and then choose desired PEER to save that file and then will get below page



File successfully saved at Peer1

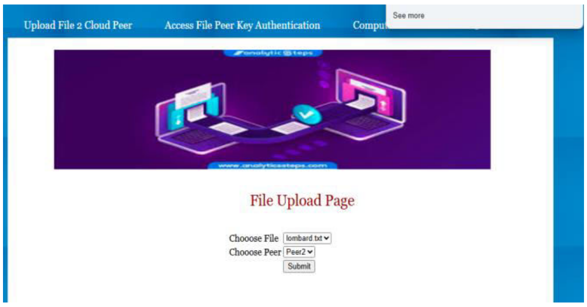
In above screen File saved at 'Peer1' and similarly you can upload any number of files. Now will try to access this file from Peer2 as this peer don't have this file so it will securely authenticate with Peer1 to get file exchange and then serve to user. To access file click on 'Access File Peer Key Authentication' link to get below page



File Upload Page

Chooose File lombard.txt
Chooose Peer Peer2
Submit

In above screen I am trying to download selected file from Peer2 and this peer don't have file so it will connect to peer1 by anonymous authentication and then exchange file and then will get below output

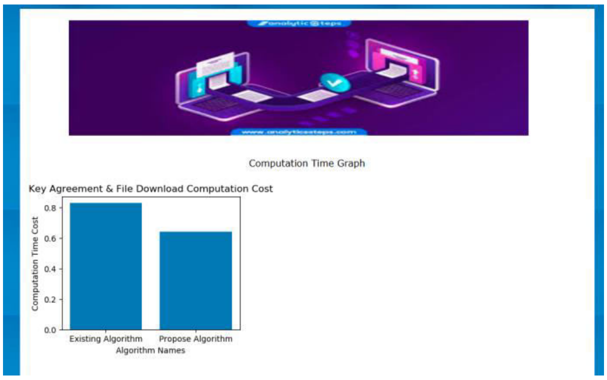


File Upload Page

Chooose File lombard.txt

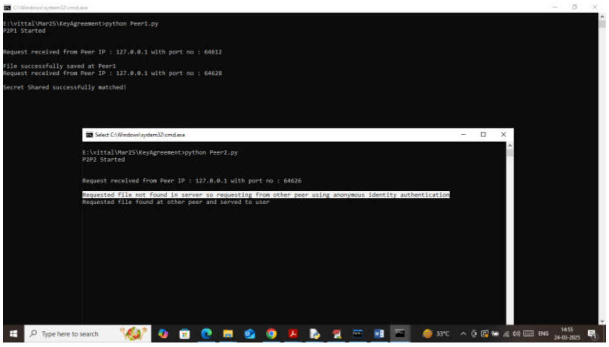
Chooose Peer Peer2

In above screen in browser task bar can see file successfully downloaded and similarly you can download any number of files from any peer. Now click on ‘Computation Cost’ link to get below page



In above graph x-axis represents technique names and y-axis represents file download and key exchange and authentication time. In above graph propose technique using P2P system so its computation will be less as multiple peers search files in its own memory.

In below screen can see P2P log files


C:\Windows\system32\cmd.exe
Select C:\Windows\system32\cmd.exe
Type here to search
33°C
ENG
14:55
24-03-2025

```
E:\vittal\Mar25\KeyAgreement>python Peer1.py
P2P1 Started

Request received from Peer IP : 127.0.0.1 with port no : 64612

File successfully saved at Peer1
Request received from Peer IP : 127.0.0.1 with port no : 64628

Secret Shared successfully matched!
```

```
E:\vittal\Mar25\KeyAgreement>python Peer2.py
P2P2 Started

Request received from Peer IP : 127.0.0.1 with port no : 64626

Requested file not found in server so requesting from other peer using anonymous identity authentication
Requested file found at other peer and served to user
```

In above screen in white text at Peer2 it won’t find file so it send request to Peer1 which authenticate secret share and upon successful secret share match, it send file to peer2.

VIII. CONCLUSION

This paper presented **An Identity-Anonymous Authentication and Key Agreement Framework for Peer-to-Peer Cloud Systems**, designed to address the increasing security, privacy, and interoperability challenges in decentralized cloud environments. Traditional cloud authentication mechanisms rely heavily on centralized certificate authorities, expose real identities during communication, and incur high computational costs, making them unsuitable for real-time peer-to-peer interactions and cross-cloud data migration. The proposed framework overcomes these limitations by introducing a privacy-preserving, certificate-free methodology based on elliptic curve cryptography.

By allowing users to act as a temporary trust authority, the system eliminates dependency on external trusted third parties while maintaining the ability to trace malicious cloud servers when necessary. The use of anonymous pseudonymous identities ensures that cloud servers can authenticate each other without disclosing their real identities on public channels, thereby enhancing privacy protection. The mutual authentication and key agreement mechanism supports secure session establishment, resists major cryptographic attacks, and guarantees properties such as forward secrecy, impersonation resistance, tamper detection, and replay attack prevention. Performance evaluation demonstrates that the proposed protocol significantly reduces both computational and communication overhead compared to existing schemes. Its lightweight design makes it suitable for real-time cloud-to-cloud communication, distributed data processing, and seamless cross-cloud data migration. Overall, the framework strengthens trust, enhances privacy, and improves security within peer-to-peer cloud ecosystems.

Future research may focus on extending the framework to support large-scale multi-user, multi-cloud environments, enabling collaborative data sharing and dynamic resource coordination across multiple cloud providers.

IX. FUTURE WORK

Although the proposed identity-anonymous authentication and key agreement framework significantly enhances privacy, security, and interoperability in peer-to-peer cloud environments, several research opportunities remain open for further exploration. Future work can extend this framework in multiple directions to address emerging challenges in decentralized and multi-cloud ecosystems.

One promising direction is the integration of **blockchain and distributed ledger technologies** to strengthen trust management and eliminate the need for even temporary trust authorities. A blockchain-based identity registry could provide immutable logging, decentralized verification, and improved transparency while preserving anonymity. This would also support autonomous trust negotiation between cloud servers without user involvement.Another area for future enhancement involves improving the **scalability and performance** of the authentication protocol in large-scale multi-cloud networks. As cloud systems grow in size and complexity, optimizing cryptographic operations and reducing handshake latency becomes crucial. Incorporating lightweight hash-based signatures, quantum-resistant cryptography, or parallelized ECC computations could further strengthen efficiency and long-term security.

The proposed framework can also be extended to support **dynamic group authentication** in collaborative cloud environments where multiple clouds participate in joint data processing or distributed computation. Enabling secure anonymous group key establishment would be beneficial for IoT-cloud systems, federated learning networks, and real-time distributed applications.Furthermore, applying machine learning–based security mechanisms can enhance the detection and mitigation of malicious behavior. Integrating anomaly detection models with identity-traceability features would allow real-time identification of compromised or misbehaving cloud servers, thereby improving overall system resilience.

Finally, future research may investigate **secure cross-cloud data sharing models**, leveraging encrypted metadata, homomorphic encryption, or secure multi-party computation to facilitate privacy-preserving data interoperability. Expanding the framework to support edge-cloud and fog-cloud hybrid architectures would allow broader applicability in next-generation computing ecosystems.Overall, enhancing scalability, decentralizing trust, strengthening cryptographic primitives, and enabling intelligent threat detection remain crucial avenues for improving the proposed framework and addressing the evolving security needs of future peer-to-peer cloud systems.

X. AUTHORS

This project titled *“An Identity-Anonymous Authentication And Key AgreementFramework For Peer-To-Peer Cloud Systems”* by **Vutukuri lakshmi priya** as part of the academic requirements of the Department of Computer Science and Engineering at Krishna Chaitanya Institute of Technology and Sciences, Devarajugattu, Peddaraveedu(MD), Markapur. The author expresses sincere gratitude to the guide for his continuous support, valuable guidance, and encouragement throughout the research and development of this work.

Dr. J. V. Anil Kumar, M.Tech, Ph.D, Professor & Head of the Department, Department of Computer Science and Engineering, Krishna Chaitanya Institute of Technology and Sciences, Devarajugattu, Peddaraveedu(MD), Markapur, provided expert supervision and insightful technical guidance for the project titled *"An Identity-Anonymous Authentication And Key Agreement Framework For Peer-To-Peer Cloud Systems. "*His expertise, support, and constructive suggestions significantly contributed to the successful execution and completion of this project.

XI. REFERENCES

1. Salem, F. M., Safwat, M., Fathy, R., & Habashy, S. (2023). *AMAKAS: Anonymous Mutual Authentication and Key Agreement Scheme for Securing Multi-Server Environments*. Journal of Cloud Computing, 12(1), Article 128. SpringerOpen+1
2. Paulraj, D., & others (2023). *Admission Control Policy and Key Agreement Based on Anonymous Identity in Cloud Computing*. Journal of Cloud Computing, 12(1). SpringerOpen+1
3. Khan, N., Jianbiao, Z., Lim, H., Ali, J., Ullah, I., & Pathan, M. S. (2023). *An ECC-Based Mutual Data Access Control Protocol for Next-Generation Public Cloud*. Journal of Cloud Computing, 12, Article 101. SpringerOpen
4. Wang, C., Huo, P., Ma, M., Zhou, T., & Zhang, Y. (2023). *A Provable Secure and Lightweight ECC-Based Authenticated Key Agreement Scheme for Edge-Computing Infrastructure in Smart Grid*. Computing, 105, 2511–2537. SpringerLink
5. Hu, S., & others (2024). *Provably Secure ECC-Based Anonymous Authentication and Key Agreement for IoT*. Applied Sciences, 14(8), 3187. MDPI
6. Li, M., & Hu, S. (2024). *A Lightweight ECC-Based Authentication and Key Agreement Protocol for IoT with Dynamic Authentication Credentials*. Sensors, 24(24), 7967. MDPI+1
7. Zhang, Y., Chen, J., Wang, S., Ma, K., & Hu, S. (2024). *Lightweight Anonymous Authentication and Key Agreement Protocol for a Smart Grid*. Energies, 17(18), 4550. MDPI
8. Cao, Z., & Liu, L. (2024). *On the Anonymity of One Authentication and Key Agreement Scheme for Peer-to-Peer Cloud*. Cryptology ePrint Archive, Paper 2024/1491. IACR Eprint Archive+1
9. Shaaban, M. A., Alsharkawy, A. S., AbouKreisha, M. T., & Abdel Razek, M. (2024). *Efficient ECC-Based Authentication Scheme for Fog-Based IoT Environment*. arXiv preprint. arXiv
10. Keshta, I. (2025). *A Cloud-Assisted Key Agreement Protocol for the E-Healthcare System*. PLoS ONE, 20(6), e0322313. PLOS+1
11. J.V. Anil Kumar, Naru Kamalnath Reddy, Bollavaram Gopi, Derangula Akhil, Dareddy Indra Sena Reddy, Akkalaakhil , "*Language-Based Phishing Threat Detection Using ML And Natural Language Processing*", International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue

IV, April 2025, Page No : pp. 406-416, ISSN NO : 2249-7455, 2025.

12. J.V.Anil Kumar, Siddi Triveni, Yaragorla Sravya, Mancha Mancha. Venkata Aksh, Posani Lahari Priya, Grandhe Sirisha , "*Tools For Database Migration*", International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : pp. 760-766, ISSN NO : 2249-7455, 2025.
13. Sk Althaf Hussain Basha, A. Amrutavalli, Mekala Anjali Lavanya, Vanama Dhakshayayani Sriya, Grandhisila Jahnavi, Pari Chaitanya Lakshmi , *"Cloud-Based Decision Support Systems For Business Data Intelligence*", International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : 303-313, ISSN NO : 2249-7455, 2025.
14. Sk. Althaf Hussain Basha, G. Mahesh, Kokkera Krishnaveni, Gadde Koushika, Derangula Manasa, Yalla Pranavi, "*Honeytrap-Enabled Cloud Security Framework For Preventing Network Breaches*", International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : 453-463 , ISSN NO : 2249-7455, 2025.