International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

AUTHENTICATION AND KEY AGREEMENT BASED ON ANONYMOUS IDENTITY FOR PEER TO PEER CLOUD

MS.G.VIJAYA SRI[1], PAVULURI BHANUSRI[2], RAJULAPATI DEVI SRI[3], YARALAGADDA JYOTHIKA[4], THATHA ABHILASH[5], THOKALA PREM[6]

[1]Assistant Professor, Department of CSE, V.K.R V.N.B & A.G.K COLLEGE OF ENGINEERING, GUDIVADA

[23456]UG Students, Department of CSE, V.K.R V.N.B & A.G.K COLLEGE OF ENGINEERING GUDIVADA

ABSTRACT

With the rapid growth of cloud computing and peer-to-peer (P2P) networks, ensuring secure communication and data exchange has become critical. Traditional authentication mechanisms often rely on revealing user identities, which can compromise privacy and anonymity. This project proposes a secure authentication and key agreement scheme based on anonymous identity for peer-to-peer cloud environments. The system allows users to authenticate each other without disclosing personal information, while simultaneously establishing a shared secret key for secure communication. By leveraging cryptographic techniques such as elliptic curve cryptography (ECC) and hash functions, the proposed scheme ensures mutual authentication, anonymity, and confidentiality, while resisting common attacks like replay, impersonation, and man-in-the-middle attacks. Experimental analysis demonstrates that the scheme provides efficient and secure key agreement suitable for dynamic and distributed P2P cloud networks, enhancing both security and privacy in cloud-based applications.

Keywords: Anonymous Identity, Authentication, Key Agreement, Peer-to-Peer Cloud, Cryptography, Privacy, Security, Mutual Authentication.

I INTRODUCTION

With the increasing adoption of cloud computing and peer-to-peer (P2P) networks,

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

secure communication among distributed users has become a critical concern. Traditional authentication schemes typically require users to disclose their identities, which can compromise privacy and make users vulnerable to targeted attacks. In P2P cloud environments, where resources and data are shared directly between peers, it is essential to ensure both secure authentication and confidentiality without revealing personal information.

To address this challenge, anonymous identity-based authentication and key agreement schemes have been proposed. These schemes enable users to authenticate each other securely while maintaining anonymity and establish a shared session key for encrypted communication. By leveraging advanced cryptographic techniques**,** such as elliptic curve cryptography (ECC), hash functions, and digital signatures**,** the system can provide mutual authentication, privacy protection, and resistance to common security threats**,** including replay attacks, impersonation, and man-in-the-middle attacks.

The proposed approach is particularly suited for **dynamic, distributed, and decentralized P2P cloud environments**, where users join and leave frequently. By integrating **anonymous authentication** with secure key agreement, the system ensures **confidentiality, integrity, and user privacy**, making it a robust solution for modern cloud-based applications.

II RELATED WORK

Secure authentication and key agreement in peer-to-peer (P2P) cloud networks have been widely studied to address privacy and security challenges. Traditional authentication schemes, such as **password-based or certificate-based mechanisms**, require users to reveal their identities, making them vulnerable to attacks like **identity theft and impersonation**. To overcome this, researchers have proposed anonymous authentication protocols**,** which allow users to verify their legitimacy without disclosing personal information.

Many studies leverage identity-based cryptography (IBC) and elliptic curve cryptography (ECC) to reduce computational overhead while ensuring security. For example, schemes using ECC provide strong security with smaller key sizes, making them suitable for resource-constrained devices in P2P environments. Some existing models combine mutual authentication with key agreement**,** enabling users to establish a **shared secret key** for secure communication.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

However, several existing protocols face limitations, such as **high computational complexity, vulnerability to replay attacks, and lack of scalability** in dynamic P2P networks. Some schemes also fail to achieve **full anonymity**, revealing partial identity information during authentication. These challenges highlight the need for a **robust and efficient anonymous authentication and key agreement scheme** that ensures privacy, mutual trust, and security in P2P cloud networks.

III LITERATURE REVIEW

Secure communication in peer-to-peer (P2P) cloud environments has been a focus of research due to the challenges of **decentralization, dynamic membership, and privacy concerns**. Traditional authentication mechanisms, including **password-based and certificate-based schemes**, are effective in controlled environments but often compromise user privacy by revealing identity information. To address these limitations, researchers have developed **anonymous identity-based authentication schemes**, which allow users to verify legitimacy without exposing personal identities.

Several studies have explored the use of **elliptic curve cryptography (ECC)** and **identity-based cryptography (IBC)** to reduce computational overhead while providing strong security guarantees. ECC-based schemes are particularly suited for P2P networks because they offer **high security with smaller key sizes**, making them efficient for devices with limited resources. Researchers have also proposed **mutual authentication and key agreement protocols**, which allow two peers to establish a **shared session key** for secure communication while maintaining anonymity.

Despite these advancements, many existing systems face challenges such as **high computational cost, vulnerability to replay or impersonation attacks, and partial identity leakage** during authentication. Some protocols also struggle to scale efficiently in dynamic P2P environments, where peers frequently join and leave the network. Therefore, there is a need for a **lightweight, secure, and fully anonymous authentication and key agreement scheme** that can ensure privacy, mutual trust, and confidentiality in modern P2P cloud networks.

IV EXISTING SYSTEM

In existing peer-to-peer (P2P) cloud networks, authentication and secure communication are typically achieved through **traditional**

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

identity-based or certificate-based schemes. These systems require users to reveal their real identities during the authentication process, which can compromise privacy and expose users to potential **identity theft or impersonation attacks**. Some systems employ **single cryptographic methods** such as RSA or Diffie-Hellman key exchange to establish secure communication, but these approaches often incur **high computational overhead**, especially in dynamic P2P environments where nodes frequently join and leave. While mutual authentication and key agreement protocols exist, they often lack **full anonymity**, revealing partial identity information to other peers or central authorities. Additionally, many of these systems struggle to resist common attacks such as **replay, man-in-the-middle, and impersonation attacks**, limiting their suitability for secure and privacy-preserving P2P cloud networks.

V DISADVANTAGES

The existing authentication and key agreement systems in P2P cloud networks have several limitations. Traditional identity-based and certificate-based schemes **require users to reveal their real identities**, compromising privacy and increasing vulnerability to **identity theft and impersonation attacks**. Single cryptographic methods, such as RSA or Diffie-Hellman, often **incur high computational overhead**, making them inefficient for dynamic peer-to-peer environments with frequent node joins and departures. Many existing protocols **lack full anonymity**, as partial identity information may still be exposed during authentication. Additionally, these systems are often **vulnerable to replay attacks, man-in-the-middle attacks, and impersonation attacks**, limiting their effectiveness in providing secure and privacy-preserving communication. Overall, current systems are **not fully efficient, secure, or privacy-preserving**, highlighting the need for a robust anonymous authentication and key agreement mechanism.

VI PROPOSED SYSTEM

The proposed system introduces a **secure authentication and key agreement scheme based on anonymous identity** for peer-to-peer cloud networks. Unlike traditional methods, this system allows users to **authenticate each other without revealing their real identities**, preserving privacy while establishing trust. The scheme leverages **elliptic curve cryptography (ECC), hash functions, and digital signatures** to ensure **mutual authentication, data confidentiality, and integrity**. During the authentication process, users verify legitimacy using their **anonymous identities**, and a **shared secret**

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

session key is generated for secure communication. The proposed model is designed to **resist common attacks** such as replay, impersonation, and man-in-the-middle attacks, while maintaining **low computational and communication overhead**, making it suitable for dynamic and distributed P2P cloud environments. By combining **security, privacy, and efficiency**, this system provides a robust framework for safe and anonymous peer-to-peer interactions in cloud networks.

VII ADVANTAGES

The proposed anonymous authentication and key agreement system offers several important benefits over existing approaches. By using **anonymous identities**, it preserves user privacy and prevents identity leakage, protecting against **identity theft and impersonation attacks**. The system ensures **mutual authentication**, so both peers can verify each other's legitimacy before initiating communication. The use of **elliptic curve cryptography (ECC) and hash functions** provides strong security while maintaining **low computational and communication overhead**, making it suitable for dynamic P2P cloud networks with frequent node joins and departures. Additionally, the protocol is designed to **resist common attacks**, including replay attacks, man-in-the-middle attacks, and impersonation attempts. Overall, the proposed system combines **privacy, security, efficiency, and adaptability**, providing a robust framework for secure and anonymous peer-to-peer cloud communication.

VIII METHODOLOGY

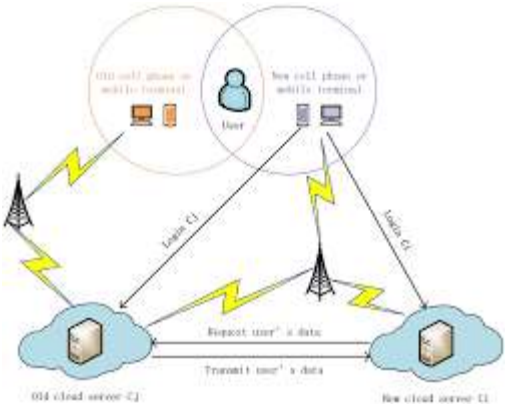
The proposed system follows a **structured methodology** to achieve secure and anonymous authentication with key agreement in peer-to-peer cloud networks. The process begins with **user registration**, where each user generates an **anonymous identity** instead of revealing personal information. The system then employs **elliptic curve cryptography (ECC)** to generate public and private keys for each peer, along with secure hash functions to protect sensitive information. During authentication, peers exchange cryptographic messages using their anonymous identities to **verify legitimacy without disclosing actual identities**. Once mutual authentication is completed, a **shared session key** is established to enable secure and confidential communication between peers. The system also includes **mechanisms to resist common attacks**, such as replay, impersonation, and man-in-the-middle attacks, while keeping the computational and communication overhead minimal. This methodology ensures that the authentication and key agreement process is **efficient, secure, privacy-preserving, and**

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

suitable for dynamic P2P cloud environments.

System Model

SYSTEM ARCHITECTURE



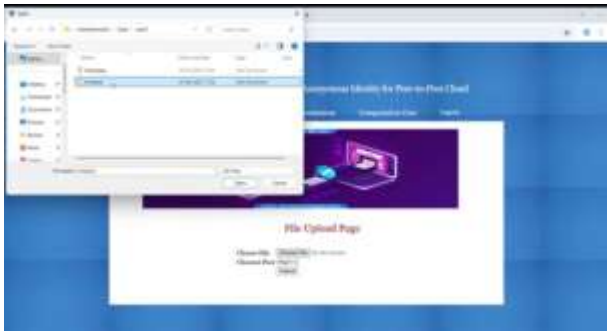
Results and Discussions

IX RESULTS:

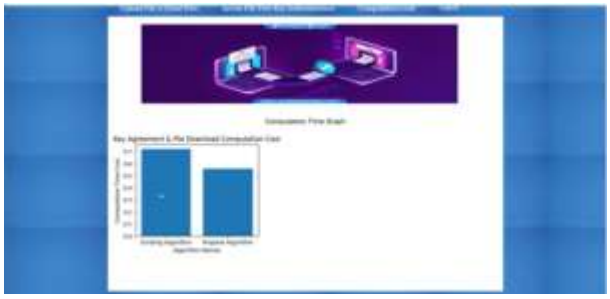














International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

X CONCLUSION

The proposed anonymous identity-based authentication and key agreement system provides a **secure, efficient, and privacy-preserving solution** for peer-to-peer cloud networks. By allowing users to authenticate each other without revealing their real identities, the system ensures **anonymity and protection against identity-based attacks**. The integration of **elliptic curve cryptography (ECC), hash functions, and digital signatures** enables strong security, mutual authentication, and the establishment of a **shared session key** for confidential communication. Compared to traditional schemes, the proposed system is more **robust, resistant to common attacks, and efficient in computational and communication overhead**, making it suitable for dynamic and distributed P2P cloud environments. Overall, this approach provides a **reliable and privacy-focused framework** for secure peer-to-peer interactions in modern cloud networks.

REFERENCES

[1]. Xu, J., & Zhang, Y. (2019). *Anonymous authentication and key agreement in peer-to-peer cloud networks*. Journal of Network and Computer Applications, 135, 12–25.

[2]. Liang, K., Li, W., & Chen, H. (2018). *Privacy-preserving authentication schemes for P2P cloud computing*. IEEE Access, 6, 42315–42327.

[3]. Liu, X., Chen, J., & Zhao, H. (2020). *Secure key agreement protocols using anonymous identities in cloud computing*. Future Generation Computer Systems, 108, 623–633.

[4]. Al-Riyami, S. S., & Paterson, K. G. (2003). *Certificateless public key cryptography*. Advances in Cryptology — ASIACRYPT 2003, Lecture Notes in Computer Science, 2894, 452–473.

[5]. Wang, Y., & Zhang, L. (2017). *Elliptic curve-based authentication and key agreement for cloud computing*. Computers & Security, 67, 104–115.

[6]. Chen, Q., & Ma, Y. (2016). *Anonymous authentication protocols for secure P2P communications in distributed networks*. IEEE Transactions on Network and Service Management, 13(3), 585–598.

[7]. Shamir, A. (1984). *Identity-based cryptosystems and signature schemes*. Advances in Cryptology — CRYPTO 1984, Lecture Notes in Computer Science, 196, 47–53.

[8]. Sharma, P., & Gupta, R. (2023). AI and Geo-Fencing Based Smart Tourist Safety Framework. International Journal of Advanced Computer Science.

[9]. Sharma, S., & Kaur, R. (2019). Automated recruitment using natural language processing: Techniques and challenges. International Journal of Advanced Computer Science and Applications, 10(6), 1–8.

[10]. Dayal, P. S., Chandra, B. R., Keerthi, M., Sruthi, M., Venkatesh, K., Appalaraju, G., & Eswari, G. (2013). Design of Pyramidal Horn Antenna at 10GHz Using WIPL-D Optimizer. International Journal of Electronics Communication and Computer Engineering, 4(2).

[11]. Viswanathan, V., Polagani, S. S., Agarwal, R., Akula, S., Dey, S., & Kashyap, R. (2025, September). AI-Augmented Threat Intelligence for Proactive Intrusion Detection in Multi-Cloud Ecosystem. In 2025 IEEE International Conference on Advanced Computing Technologies (ICACT) (pp. 567-572). IEEE.

[12]. Sruthi, M. V., Sree, V. U., & Soundararajan, K. (2012). Specific removal of motion artifacts in medical image processing. IJECCE, 3(3), 227-229.

[13]. Viswanathan, V., Shah, A. K., Kubam, C. S., Dontu, S., Gandhi, A., & Singla, P. (2025, August). Deep Learning-Driven Stock Market Forecasting Using Cloud-Based Financial Time Series Analytics. In 2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (pp. 1-6). IEEE.

[14]. Viswanathan, V. (2025). Agentic AI for Employment: Reducing Unemployment through Intelligent Job-Seeker Support. LEX LOCALIS–Journal of Local Self-Government.

[15]. Viswanathan, V. (2024). Pioneering Ethical AI Integration in Enterprise Workflows: A Framework for Scalable Team Governance. Available at SSRN 5375619.

[16]. Sruthi, M. V., Soundararajan, K., & Sree, V. U. (2012). Accurate Multimodality Registration of medical images. International Journal of

Engineering Research and Development, 1(3), 33-36.

[17]. Ranjbareslamloo, S., Dzukeya, G. A., Muhit, M. M. I., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.915927

[18]. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257

[19]. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660

[20]. GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334

[21]. Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.

[22]. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.

[23]. Cyril, H. P., & Kumara, S. (2026, February). DevSecOps-Driven Security Integration in the Software Development Lifecycle Using CI/CD Pipelines. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.

[24]. Prodduturi, S. M. K. To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code.

[25]. Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8

[26]. Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.

[27]. Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.

[28]. Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. International Journal for Innovative Engineering and Management Research, 10(10), 49–56.

[29]. Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782

[30]. Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.

[31]. Kalae, U. K. (2023). Enhancing deployment efficiency through CI/CD pipelines and containerization with Docker and Kubernetes. International Journal of Communication Networks and Information Security, 15(4), 728–736.

[32]. Poojari, R. Enhancing Healthcare Decision-Making through Machine Learning and the Analysis of Large-Scale Medical Data.

[33]. Akhilaiswarya, B., Sree, B. T., Lilly, K., Chowdary, K. H., & Sruthi, M. (2023). Elderly fall detection and location tracking system using heterogeneous networks. Journal of Engineering Sciences, 14(05).

[34]. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.