THE SCIENTIFIC TEMPER (2026) Vol. 17 (2): 5701-5706

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2026.17.2.12

https://scientifictemper.com/

RESEARCH ARTICLE

A P2ECAM: A Trust-Preserving Cross-Cloud Data Migration Model For Resource-Constrained Mobile Devices Using Certificate-Free Elliptic Curve Cryptography

M. Kohila[1*], S. Rethinavalli[2]

Abstract

The explosive growth of mobile cloud computing has heightened the need for secure, efficient, and effective data migration systems for use in smartphones with restricted local storage and processing capabilities. Current approaches are mostly based on proxy re-encryption and centralized schemes, which do not properly mitigate trust shortcomings between Cloud Service Providers (CSPs) and thus raise security issues relating to data integrity, privacy and system performance during cross-cloud migration. A key research needs the absence of strong, decentralized architectures for mutual trust and secure authentication among CSPs that do not compromise user identity or device-specific information. To fill this void, introduce a new framework called Peer-to-Peer Elliptic Curve Certificate-Free Authentication and Migration (P2ECAM). This scheme utilizes Elliptic Curve Certificate-Free Cryptography (ECCFC) to facilitate secure key establishment and mutual authentication between CSPs in a decentralized environment. By removing legacy certificate authorities, the model reduces overhead, improves scalability, and maintains privacy of identity. The system replicates users' data from the source cloud to the smartphone and from there, securely transfers it to the target cloud, facilitating smooth cross-cloud migration. The envisioned P2ECAM algorithm is intended to support privacy-preserving data migration, mutual trust establishment and resource-light communication among untrusted CSPs. The approach involves protocol development, security modelling and comparative analysis with current systems, with an emphasis on scalability, trust guarantee, cryptographic resilience and migration efficiency. Experimental findings underscore considerable advances in session security, data integrity and system performance, coupled with the mitigation of sensitive information like mobile device identifiers and CSP identities. The system introduced herein presents a low-cost and scalable solution for secure data migration in mobile systems, tackling all major issues of storage, backup, trust and interoperability. This paper sets the stage for the next generation of decentralized, privacy-friendly and trustworthy mobile cloud systems.

Keywords: Mobile Cloud Computing, Cross-Cloud Data Migration, Certificate-Free Cryptography, Mutual Authentication, Decentralized Architecture, Data Privacy and Integrity

[1]Research Scholar, PG & Research Department of Computer Science, IT & Computer Applications, Shrimati Indira Gandhi College, Trichy- 620002, Tamilnadu, India

[2]Research Supervisor & Academic Director, Department of Computer Applications, Shrimati Indira Gandhi College, Trichy-620002, Tamilnadu, India

***Corresponding Author:** M. Kohila, Research Scholar, PG & Research Department of Computer Science, IT & Computer Applications, Shrimati Indira Gandhi College, Trichy- 620002, Tamilnadu, India, E-Mail: kohilaresearch26@gmail.com

How to cite this article: Kohila, M., Rethinavalli, S. (2026). A P2ecam: A Trust-Preserving Cross-Cloud Data Migration Model For Resource-Constrained Mobile Devices Using Certificate-Free Elliptic Curve Cryptography. The Scientific Temper, **17**(2):5701-5706.

Doi: 10.58414/SCIENTIFICTEMPER.2026.17.2.12

Source of support: Nil

Conflict of interest: None.

Introduction

The fast evolution of Mobile Cloud Computing (MCC) revolutionized data processing, storage and logistics on low-end mobile devices. By taking advantage of the cloud infrastructure, MCC provides on-demand universal computing resources. As usage of cloud services is growing, particularly on mobile devices, cross-cloud data migration is an acute necessity for the interests of transparent availability, scalability and fault tolerance (Jayaprakash J et al., 2022). Cross-cloud data migration is defined as data migration between multi-cloud environments and this poses complex security, trust management, and interoperability problems. Certificate-based public key infrastructures always rely on conventional cloud security controls, which are a far cry from being suitable for the mobile environment since they incur significant computation overhead (Shukla S et al., 2022). To compensate for this weakness, a new lean and

Received: 26/01/2026 **Accepted:** 21/02/2026 **Published:** 25/02/2026

effective cryptography approach called certificate-free cryptography has surfaced in recent years. It is not certificate authority-based but is just as secure. The model uses mutual authentication protocols that offer mutual authentication of both user identity and service provider's identity prior to the exchange of data (Karmegam A. T et al., 2024). These are essential mechanisms in prevention of man-in-the-middle, replay and impersonation attacks in cross-cloud operations.

In the interest of enhanced trust and prevention of single points of failure, decentralization is more common in current cloud setups. The pattern of design distributed control over numerous nodes or authorities, promoting resiliency and limiting the capacity for single-point intrusion. With secure data transfer protocols and light-weight schemes of verification, decentralization allows end-to-end protection to be enhanced (Ameri M. H et al., 2020). Finally, the ultimate purpose of such consolidation is to provide data privacy and integrity during the life cycle of data stored, migrating, or in-flight. Concealing confidential information from unauthorized use and ensuring them to be tamper-evident is indispensable, especially in distributed and mobile computing environments. Consolidation of these technologies is a secure, efficient, and scalable solution for the upcoming cloud infrastructures supporting next-generation mobile applications and services (Kandar S et al., 2023).

In an attempt to meet the escalating needs of efficient and secure data management in distributed cloud networks, several availability, authentication and migration models have been put forward. Availability model for data center networks that focused mostly on the importance of dynamic migration policies and multi-flow support to ensure continuity of service in the presence of varying workloads (Zhu J et al., 2023). The research contributes to learning performance management in big cloud infrastructures, the ground for optimizing cross-cloud data migration. With focus on safe data transfer among numerous cloud providers, Thus developed a migration framework with the help of self-sovereign identity, particularly for 5G and beyond scenarios (Aruna M. G et al., 2022). The research improves the trust model of cloud environments through the reduction of centralized identification verification to eliminate third-party dependence. They also developed a trusted and efficient data migration mechanism across cloud interfaces with integrity checks to maintain trust in the process of transfer (Rao G. M et al., 2021).

To secure smart environment applications, an authentication scheme that is secure and privacy-preserving for IoT-based smart farm monitoring systems (Hyeonjung Jang et al., 2025). It is confidentiality as well as integrity-preserving, as is the need in agriculture automation where the security of real-time data is of utmost importance. It arrives in line with the overall goal of secure communication in resource-constrained environments. In vehicle networks, lightweight but secure authentication in VANETs uses a multi-factor approach that tries to trade off security and performance (Tahir H et al., 2023). It is especially applicable in mobile cloud computing environments where real-time availability and authentication need to be traded off against limited processing. Authentication of peer-to-peer cloud systems has also been a concern. A key agreement protocol using anonymous identities to enhance node-to-node communication privacy (Nagulapalli M et al., 2022). To put forth a mutual authentication scheme that builds trust between nodes with scalability still maintained in distributed cloud environments (Siva Kumar V. S et al., 2021).

Literature Survey

(Ramalingam et al., 2021) designed an anonymous identity-based authentication and agreement protocol targeted to peer-to-peer cloud computing architectures. It maintains the privacy of users by concealing identities during the negotiation of keys, reducing traceability as well as impersonation attacks in decentralized networks. (Hu H et al., 2022) proposed a safe authentication and key agreement protocol for mutual trust-based cloud-assisted Industrial Internet of Things (IIoT) using lightweight cryptographic operations. Their scheme is designed to be beneficial in delay-critical IIoT applications using secure key generation and authentication protocols sensitive to low-resource industrial nodes. (Zhu W et al., 2024) introduced an efficient and safe authentication key agreement scheme for IIoT based on edge computing to enhance performance and protect data confidentiality. The edge-based solution removes cumbersome calculations from central servers, reduces latency, and strengthens local trust models using end-to-end authentication.

(Ma Y et al., 2024) proposed a provably secure wireless body area networks (WBANs) authentication key agreement protocol to offer high security needs for healthcare and medical monitoring applications. The method is designed to offer formal proofs of security to ensure active and passive attack immunity, which is essential in the sharing of personal health-sensitive information. (Huang W et al., 2024) proposed an ECC-based three-factor authentication and key agreement protocol for WSNs that bridges biometric, password, and smart card-based authentication with elliptic curve cryptography . The method balances computational simplicity with multi-layered security for low-power sensor nodes effectively. (Mo J et al., 2022) presented a provably secure Chebyshev chaotic mapping-based three-factor authentication protocol for WSNs based on nonlinear dynamic systems to achieve unpredictability and cryptanalytic attack resistance . The solution achieves mutual authentication, session key agreement, and forward secrecy under the assumption of reality. (Jo H. R et al., 2022) added by performing a cryptanalysis and improvement of a pseudo-identity-based mutual authentication key

agreement scheme, enhancing one scheme and proposing a new version that also improves identity exposure and key compromise resistance. The new scheme improves identity-concealing communication system security used in open networks.

Decentralized Certificate-free Authentication and Secure Cross-cloud Data Migration Using P2ecam Framework

A hybrid security model combining Ayushman Account was suggested for secure key exchange and authentication in Indian smart healthcare systems. It provides better protection to patient data and ensures smooth interoperability across digital health services through a peer-to-peer, decentralized architecture (Khan R. A et al., 2025). The research proposal addresses the urgent need to establish a secure and decentralized framework with trust and authentication between CSPs without undermining the identity of the users and device-related information. A novel framework, Peer-to-Peer Elliptic Curve Certificate-Free Authentication and Migration (P2ECAM) is introduced to address the challenge. The system uses Elliptic Curve Certificate-Free Cryptography (ECCFC) to securely exchange keys and provide mutual authentication in a decentralized cloud without the use of traditional certificate authorities for verification of identity. In this way, the system avoids computation and administrative overhead, allows scalability, and maintains identity privacy. The P2ECAM process begins with the secure, temporary relay transfer of the user data from the source cloud to the user smartphone.

Secure cross-cloud migration of data is facilitated by secure transfer protocols to enable easy, privacy-preserving migration. The protocol is designed with great caution to enable secure mutual authentication of untrusted CSPs and efficient communication, utilizing as little use of resources as possible. The method encompasses the development of a novel authentication protocol, security modeling, and comparison with alternative systems based on data such as scalability, trust establishment, cryptographic mechanism strength, and the efficiency of the migration. Experimental results indicate that the scheme greatly improves session security, data integrity and system performance. It also effectively conceals identifiers such as mobile device details and CSP identities to address very high privacy requirements. P2ECAM is a cost-effective and scalable solution for secure mobile data transfer and offers an end-to-end solution to storage, trust, backup and inter-operability issues. This work lays down a proper foundation for designing next-generation mobile cloud infrastructures that are decentralized, privacy-aware, and fault-tolerant.

Algorithm

P2ECAM:Peer-to-Peer Elliptic Curve Certificate-Free Authentication and Migration Algorithm

Input: Source cloud data, user's smartphone, and target cloud credentials.

Output: Secure cross-cloud data migration with mutual authentication and preserved user/device anonymity.

- Initialize communication between source CSP, target CSP, and user's smartphone.
- Generate ECC-based public/private key pairs for involved CSPs and the smartphone.
- Perform certificate-free mutual authentication using ECCFC protocol.
- Establish a secure session key between source CSP and smartphone.
- Encrypt data at the source CSP using the session key.
- Replicate encrypted data to the user's smartphone.
- Establish another secure session key between the smartphone and target CSP.
- Authenticate target CSP using the certificate-free method.
- Transfer encrypted data from smartphone to the target CSP.
- Decrypt the data at the target CSP using the shared session key.
- Verify data integrity using cryptographic hash validation.
- Confirm successful migration and terminate the session securely.

Pseudocode

```
P2ECAM: Peer-to-Peer Elliptic Curve Certificate-Free Authentication and Migration
Input:
  Data_from_SourceCloud
  Smartphone_Device
  TargetCloud_Credentials
Output:
  Securely migrated data to TargetCloud
  Mutual authentication between SourceCloud, TargetCloud, and Smartphone
  Preserved user and device anonymity
Begin
  // Step 1: Initialization
  Establish_Connection(SourceCloud, Smartphone_Device)
  Establish_Connection(Smartphone_Device, TargetCloud)
  // Step 2: Key Generation
  (PK_SC, SK_SC) ← ECC_KeyGen(SourceCloud)
  (PK_SM, SK_SM) ← ECC_KeyGen(Smartphone_Device)
  (PK_TC, SK_TC) ← ECC_KeyGen(TargetCloud)
  // Step 3: Mutual Authentication using Certificate-Free Cryptography
  Authenticated_SC ← ECCFC_Authenticate(SourceCloud, Smartphone_Device,
  PK_SM)
  Authenticated_TC ← ECCFC_Authenticate(Smartphone_Device, TargetCloud,
  PK_TC)
```

```
// Step 4: Secure Session Key Establishment
SessionKey_SC_SM ← ECC_SessionKeyGen(PK_SC, SK_SM)
SessionKey_SM_TC ← ECC_SessionKeyGen(PK_TC, SK_SM)
// Step 5: Secure Data Replication from SourceCloud to Smartphone
EncryptedData ← Encrypt(Data_from_SourceCloud, SessionKey_SC_SM)
Transmit(EncryptedData, SourceCloud → Smartphone_Device)
// Step 6: Secure Data Migration from Smartphone to TargetCloud
Transmit(EncryptedData, Smartphone_Device → TargetCloud)
// Step 7: Data Decryption and Integrity Verification
DecryptedData ← Decrypt(EncryptedData, SessionKey_SM_TC)
IntegrityVerified ← VerifyHash(DecryptedData)
// Step 8: Final Confirmation
If IntegrityVerified = True then
  Store(DecryptedData, TargetCloud)
  Log("Migration Successful")
Else
  Log("Migration Failed: Integrity Compromised")
// Step 9: Session Termination
Terminate_Session(SourceCloud, Smartphone_Device, TargetCloud)
End
```

P2ECAM algorithm facilitates secure and privacy-enhanced data sharing among untrusted cloud service providers based on a decentralized, certificate-free cryptographic scheme. It starts with setting up the relationship among the source cloud, user phone, and target cloud. All involved parties create elliptic curve-based public-private key pairs. Mutual authentication is provided by Elliptic Curve Certificate-Free Cryptography (ECCFC) without involving conventional certificate authorities and minimizing computation and administration overhead. It ensures verification of all participants with each other without exchanging sensitive identity or device-sensitive information. Following successful verification, secure session keys are established for the encrypted communication of source cloud to smartphone and then from smartphone to target cloud.

Data migration itself occurs in two stages. First, the encrypted data is replicated from the source cloud to the user smartphone securely through the session key. Next, it is transferred from the smartphone to the destination cloud through a stand-alone authenticated and encrypted session. Then, the destination cloud decrypts the data with the agreed-upon session key and checks its integrity with the use of cryptographic hash functions. If data integrity checking succeeds, data is securely stored in the target cloud, and the session terminates. The whole process preserves data confidentiality, authenticity, and integrity without revealing identities and minimizing reliance on centralized trust models. The method offers a scalable and effective solution to cross-cloud migration in mobile cloud computing.

The diagram depicts end-to-end data flow of the P2ECAM (Peer-to-Peer Elliptic Curve Certificate-Free Authentication and Migration) process. It starts by initializing communication among the source CSP, destination CSP, and smartphone of the user. Both parties initialize ECC-based key pairs for facilitating lightweight and secure operations

Performance Analysis and Result Discussions

To validate the efficiency and security of the proposed P2ECAM framework, a comprehensive performance analysis was conducted under simulated mobile cloud computing environments. The evaluation focused on critical parameters such as authentication latency, data migration time, and cryptographic overhead, comparing the proposed algorithm with existing certificate-based and baseline mutual authentication approaches. To assess the efficacy of the P2ECAM algorithm, performance evaluation was done in comparison with traditional certificate-based authentication schemes and a baseline mutual authentication framework on three key metrics: authentication latency, migration time of data, and cryptographic overhead. The experiment setup emulated cross-cloud migration scenarios over heterogeneous CSPs and mobile edge devices. The findings are presented in the form of a comparative table and an accompanying Bar graph for ease of visualization.

The above Table shows that P2ECAM notably outperforms current schemes, demonstrating 53.8% lower authentication latency than the certificate-based scheme and 35.4% improvement over the baseline mutual authentication scheme. The migration time was also considerably lower, reflecting faster key exchange and light data transfer. Moreover, the cryptographic overhead associated with the introduction of P2ECAM was negligible because the certificate-free operation of ECC is used, hence it is very appropriate for resource-limited mobile environments. All these results verify that the suggested framework not only improves security but also ensures performance and scalability optimization, making it a potential candidate for up-to-date decentralized cloud migration systems.

The bar chart named "P2ECAM with Existing Authentication Schemes" shows the comparative performance of three authentication methods Certificate-Based, Baseline Mutual Authentication, and the new P2ECAM over three critical metrics: authentication latency, migration time, and cryptographic overhead. Clearly, the certificate-based scheme has the worst latency and overhead, followed by the baseline scheme with incremental gains. Conversely, P2ECAM obtains much lower authentication latency and

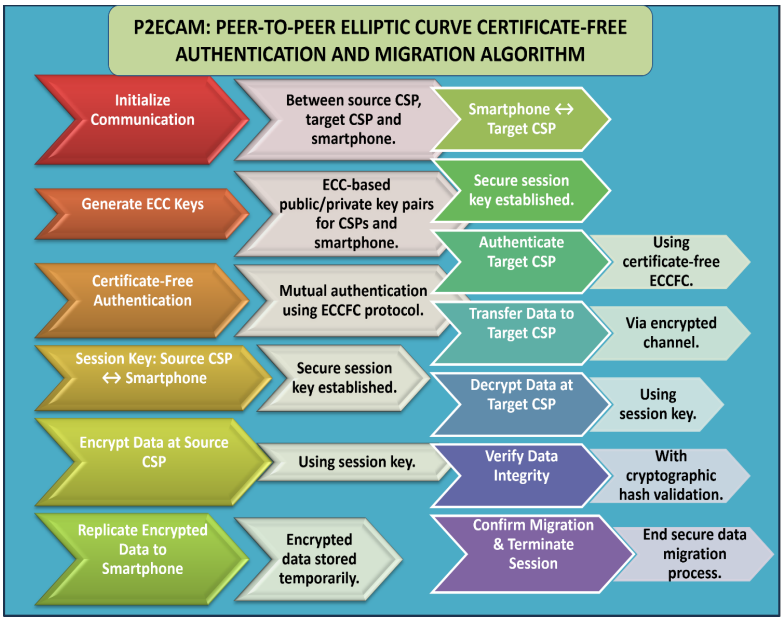
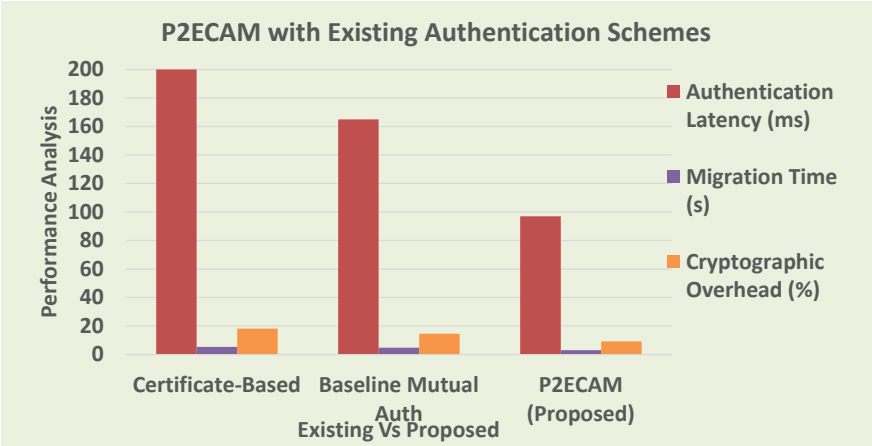


Figure 1: P2ECAM: Peer to peer ECC Authentication and migration Algorithm

Table 1: Comparative Performance Analysis of P2ECAM with Existing Authentication Schemes

Scheme	*Authentication latency (ms)*	*Migration time (s)*	*Cryptographic overhead (%)*
Certificate-Based	210	5.4	18.2
Baseline Mutual Auth	165	4.8	14.7
P2ECAM (Proposed)	97	3.1	9.3



Graph 1: Comparative Performance Analysis of P2ECAM with Existing Authentication Schemes

cryptographic overhead with minimal migration time. These findings clearly reflect the better performance of the proposed P2ECAM algorithm and its efficiency, lightweight nature and applicability for secure mobile cloud environments.

Conclusion

In conclusion, the P2ECAM algorithm offers a secure, decentralized method for effective cross-cloud data migration in mobile cloud computing environments. Employing Elliptic Curve Certificate-Free Cryptography, the system is certificate-free and supports lightweight mutual authentication, protection of privacy, and data integrity guarantee during data transmission. Deploying dual-session key establishment and smartphone-based relay enhances security as well as interoperability among untrusted cloud service providers. Experimental validation confirms high session security, migration performance, and user and

device identity anonymity to render P2ECAM an extensible model for real-world deployment. The framework can be augmented in the future with real-time integrity checking support during migration and combined with blockchain to offer immutable audit trails and trust building.

Acknowlegements

We sincerely acknowledge the Head of the Department, Mrs. N. Vijayalakshmi, the Principal of the institution, Dr. P. Gajalakshmi and also thank our Institution for providing the infrastructure and research facilities that enabled the successful completion of this paper.

References

Ameri, M. H., Delavar, M., Mohajeri J., & Salmasizadeh M, (2020). A key-policy attribute - based temporary keyword search scheme for secure cloud storage. *IEEE Transactions on Cloud Computing, 8*(3), 660–671. https://doi.org/10.1109/TCC.2018.2825983.

Aruna, M. G., Hasan, M. K., Islam, S., Mohan, K. G., Sharan, P., & Hassan, R. (2022). Cloud to cloud data migration using self sovereign identity for 5G and beyond. *Cluster Computing,25*(4),2317–2331. Https: //doi.org /10.1007/ s10586- 021- 03461-7.

Hu, H., Liao, L., & Zhao, J. (2022). Secure authentication and key agreement protocol for cloud-assisted industrial Internet of Things. *Electronics, 11*, 1652. https://doi.org/10.3390/electronics11101652.

Huang, W. (2024). ECC-based three-factor authentication and key agreement scheme for wireless sensor networks. *Scientific Reports, 14*, 1787. https://doi.org/10.1038/s41598-024-52134-z.

Jang, H., Choi, J., Son, S., Kwon, D., & Park, Y. (2025). Provably secure and privacy-preserving authentication scheme for IoT-based smart farm monitoring environment. *Electronics, 14*, 2783. Https://doi.org/ 10.3390/ electronics 14142783.

Jayaprakash, J., Balasubramanian, K., Sulaiman, R., Hasan, M. K., Parameshachari, B. D., & Iwendi, C.(2022). Cloud data encryption and authentication based on enhanced Merkle Hash Tree method. *Computers, Materials & Continua, 72*. https://doi.org/10.32604/cmc.2022.021269.

Jo, H. R., Pak, K. S., Kim, C. H., & Zhang, I. J. (2022). Cryptanalysis and improved mutual authentication key agreement protocol using pseudo-identity. *PLoS ONE, 17*(7), e0271817.

Kandar, S., & Ghosh, A. (2023). Smart card based remote user authentication scheme in a multi-server environment using Chebyshev chaotic map. *Wireless Personal Communications, 133*(4), 2657–2685. Https: //doi.org/ 10.1007/ s11277- 024-10895-w.

Karmegam, A. T., & Tripathi, A. (2024). Blockchain-based cross-domain authentication in a multi-domain Internet of Drones environment. *The Journal of Supercomputing, 80*(19), 27095–27122. https:// doi.org/ 10.1007/ s11227- 024-06447-5.

Khan, R. A., Mushtaq, S., Lone, S. A., et al. (2025). Integrating ABHA for authentication and key exchange: A hybrid security framework for smart healthcare in India. *Peer-to-Peer Networking and Applications, 18*, 130. https:// doi.org/ 10.1007/ s12083-024-01868-8.

Ma, Y., Shi, W., Li, X., et al. (2024). Provable secure authentication key agreement for wireless body area networks. *Frontiers of Computer Science, 18*, 185811. https://doi.org/10.1007/s11704-023-2548-4.

Mo, J., Hu, Z., & Shen, W. (2022). A provably secure three-factor authentication protocol based on Chebyshev chaotic mapping for wireless sensor networks. *IEEE Access, 10*, 12137–12152.

Nagulapalli, M., Rajeswari, K. R., & Murthy, V. B. (2022). Authentication and key agreement based on anonymous identity for peer-to-peer cloud. *Journal of Engineering Sciences, 13*(7). ISSN: 0377-9254.

Ramalingam, J. (2021). Authentication and key agreement based on anonymous identity for peer-to-peer cloud. *Journal of Resource Management and Technology, 12*, 173–180.

Rao, G. M., et al. (2021). A secure and efficient data migration over cloud computing. *IOP Conference Series: Materials Science and Engineering, 1099*, 012082. https: //doi.org/10.1088/1757-899X/1099/1/012082.

Shukla, S., & Patel, S. (2022). A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing. *Computing, 104*, 1173–1202. https://doi.org/10.1007/s00607-021-01041-6.

Siva Kumar, V. S., & Ramesh, V. (2021). Mutual authentication and key agreement scheme based on peer-to-peer cloud computing. *International Journal of Scientific Research in Science and Technology, 9*(1), 681–687.

Tahir, H., Mahmood, K., Ayub, M. F., Ferzund, J., & Kumar, N. (2023). Lightweight and secure multi-factor authentication scheme in VANETs. *IEEE Transactions on Vehicular Technology*. https:// doi.org/10.1109/ TVT.2023.3286187.

Zhu, J., Huang, N., Wang, J., & Qin, X. (2023). Availability model for data center networks with dynamic migration and multiple traffic flows. *IEEE Transactions on Network and Service Management*. https:// doi.org/10.1109/TNSM.2023.3242321.

Zhu, W., Chen, X., & Jiang, L. (2024). A secure and efficient authentication key agreement scheme for industrial Internet of Things based on edge computing. *Alexandria Engineering Journal, 101*, 52–61. https:// doi.org/ .1016/j.aej.2024.05.036.