International Archive of Applied Sciences and Technology
Int. Arch. App. Sci. Technol; Vol 15 [3] September 2025: 01- 07

[ISO9001: 2008 Certified Organization]
www.soeagra.com/iaast.html

IAAST
ONLINE ISSN 2277- 1565
PRINT ISSN 0976 - 4828

CODEN: IAASCA OPEN ACCESS

Proxy Re-Encryption for Secure and Scalable Cloud-Based Report Sharing with Asymmetric Key Distribution

Pradeepa K, Thiyagarajan R, Ushaa Eswaran, K Ramya Sree & Uma Maheswari P
Mahalakshmi Tech Campus, Chennai, Chrompet-600044
Corresponding Email: Dean.Research@Mtcchennai.Com

ABSTRACT
Cloud computing has become a dominant paradigm for storing and sharing sensitive data due to its scalability and flexibility. However, it introduces critical security challenges—particularly concerning data confidentiality, dynamic access control, and key management in multi-user environments. This paper proposes a robust framework for secure report sharing in cloud systems by integrating asymmetric key distribution with attribute-based access control, proxy re-encryption, and key-aggregate cryptographic techniques. The system supports role-based delegation, efficient key revocation, and fine-grained access policy enforcement using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). A trusted Cloud Key Management System (CKMS) handles key generation and distribution, enabling dynamic user participation and secure delegation without exposing plaintext to cloud providers. The proposed architecture was implemented and tested in an OpenStack-based private cloud environment. Experimental results demonstrate that RSA offers superior performance in terms of key generation, encryption latency, CPU and memory usage, and proxy re-encryption efficiency, outperforming ElGamal and Paillier schemes. The framework is especially suited for secure data sharing in Internet of Things (IoT) applications, energy grids, and enterprise clouds requiring lightweight and scalable cryptographic operations.
Keywords: *Cloud Security, Asymmetric Cryptography, Proxy Re-Encryption, Attribute-Based Encryption, Key Management, RSA, CP-ABE, Cloud Computing, Secure Data Sharing, Internet of Things (IoT)*

Received 10.07.2025 Revised 28.08.2025 Accepted 29.09.2025

CITATION OF THIS ARTICLE
Pradeepa K, Thiyagarajan R, Ushaa Eswaran, K Ramya Sree & Uma Maheswari P . Proxy Re-Encryption for Secure and Scalable Cloud-Based Report Sharing with Asymmetric Key Distribution. Int. Arch. App. Sci. Technol; Vol 15 [3] September 2025: 01-07

INTRODUCTION

Cloud computing has evolved as a transformative force in the digital era, enabling scalable, on-demand delivery of computing resources and services. From healthcare and e-governance to intelligent energy systems and enterprise IT, organizations are increasingly leveraging the cloud for flexible storage and secure data dissemination. However, despite its advantages, cloud environments present significant security and privacy challenges, particularly concerning data confidentiality, integrity, access control, and key management [1].

The migration of sensitive data to public or hybrid cloud platforms often exposes it to risks such as unauthorized access, data leakage, and lack of transparency in multi-tenant scenarios. For example, in public cloud systems where infrastructure is shared, establishing a secure application delivery service that protects data at rest and in transit has become critical. Studies have shown that conventional models fall short in offering dynamic and fine-grained access control mechanisms [1][2].

Need for Hybrid and Asymmetric Cryptographic Frameworks

To address these concerns, recent research advocates the use of hybrid cryptographic models which combine symmetric and asymmetric encryption to balance computational efficiency with strong security guarantees. Hybrid schemes reduce overhead by encrypting large files with symmetric algorithms while relying on public-key mechanisms to secure and distribute encryption keys [2]. Such approaches ensure robust protection against man-in-the-middle attacks and enable secure delegation of access without compromising data confidentiality.

The growing complexity of cloud-based services also demands comprehensive frameworks that incorporate role-based policies and cryptographic enforcement mechanisms. Enhancing cloud network

security through hybrid cryptographic algorithms allows organizations to enforce policy-based data **access**, facilitate revocation mechanisms, and ensure identity traceability when required [3].

Role of Proxy Re-Encryption and Group Key Management

As systems scale, the number of users and roles interacting with cloud data increases, making **key** management and access delegation more complex. To overcome this, proxy re-encryption (PRE) has emerged as an efficient solution. In a PRE-enabled cloud architecture, a semi-trusted cloud proxy can transform ciphertexts from one user's encryption key to another's without decrypting the data. This allows fine-grained access control, especially in dynamic environments where users frequently join or leave collaborative groups [4].

Furthermore, integrating parallel proxy re-encryption techniques ensures low latency and balanced resource utilization even in big data environments, making the framework suitable for real-time applications such as IoT-based smart meter data sharing and cloud-based surveillance systems [4][5][17].

Towards Secure and Scalable Cloud Architectures

Cloud computing environments today face performance bottlenecks not just from security mechanisms, but also from the volume and variety of time-series data they must process and store. Efficient cloud data organization and intelligent storage mechanisms are crucial to ensure seamless encryption, retrieval, and re-encryption processes at scale [5]. Studies show that coupling encryption techniques with intelligent workload distribution models yields improved system throughput and data confidentiality, even for long-duration or high-frequency datasets.

Additionally, as organizations adopt multi-cloud and hybrid cloud architectures, interoperability becomes a concern. Cross-platform cryptographic compatibility and orchestration of access policies are essential to maintaining security across distributed infrastructures. Cloud orchestration standards, when supported by robust cryptographic protocols, allow consistent enforcement of security rules across virtualized environments [6].

Unified Cloud Information Management and Trust Models

Finally, for a cloud environment to truly be trusted and scalable, there must be **holistic information** management frameworks that unify cryptographic enforcement, access policy definition, and secure data sharing models. The adoption of information-centric cloud models, combined with role-based encryption and trusted access protocols, lays the foundation for secure, user-aware cloud computing [7].

Our work builds upon these prior advancements and proposes a robust, asymmetric key-driven framework for secure report sharing, offering optimized performance in dynamic, multi-user cloud environments.

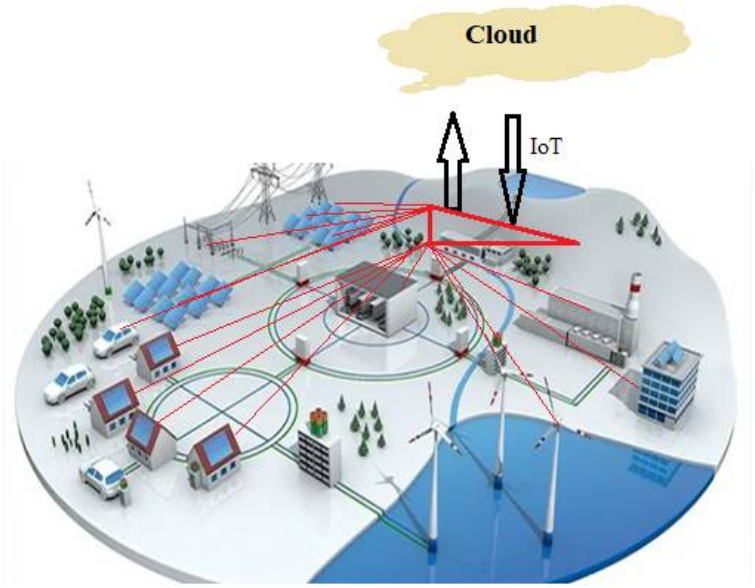

Figure.1 *IoT-driven smart energy cloud environments*

RELATED WORK

Security in Hybrid and Public Cloud Environments

The integration of public and hybrid cloud systems into enterprise and government infrastructures has introduced scalable, cost-effective computing resources. However, securing data in such environments remains a significant challenge. Wei and Rodriguez [8] proposed a policy-based deployment model tailored for hybrid cloud environments, enabling dynamic resource provisioning while addressing compliance with

service-level agreements and data sovereignty requirements. Their work highlights the importance of deploying role-based and policy-driven control mechanisms to achieve secure, adaptive resource orchestration.

Herger et al. [9] discussed practical barriers organizations face while migrating to cloud infrastructures, particularly emphasizing the lack of standardized security models and trust evaluation tools. Their findings align with the broader concern that while cloud offers agility, it often lacks built-in mechanisms for secure application delivery and key governance across heterogeneous systems.

Performance and Workflow Optimization in Cloud Platforms

The efficiency of resource allocation and scheduling is another critical aspect of cloud computing, especially when executing latency-sensitive or time-bound applications. Grozev and Buyya [10] developed simulation models to evaluate the behavior of three-tier applications in both single and multi-cloud settings. Their results demonstrated that performance variability in cloud environments must be carefully accounted for when deploying scalable security services such as encryption and re-encryption modules.

Similarly, Lin and Lu [11] addressed elastic workflow scheduling for scientific applications in the cloud. Their algorithmic framework provided real-time resource scaling and minimized make span delays, making it suitable for integration with cryptographic engines and security policy enforcement modules in dynamic environments.

Security-Aware Network Architectures

To overcome the limitations of static security models in dynamic cloud systems, network-centric approaches have been proposed. Ghosh et al. [12] introduced an SDN-based architecture for information-centric cloud networks, integrating security policy enforcement with Quality of Service (QoS) guarantees. Their design supports rapid policy updates and fine-grained monitoring, making it compatible with access-control schemes such as proxy re-encryption and attribute-based encryption (ABE) in multi-tenant cloud environments.

Complementarily, Sun et al. [13] proposed a quantifiable model to evaluate cloud platform security. Their model incorporates measurable security attributes such as key entropy, trust score, and attack surface, providing a practical framework for benchmarking cryptographic protocol deployments and policy compliance. Tamilamuthan and Geetha [17] emphasized system optimization, which supports efficient and secure data sharing frameworks. Their IoT-based monitoring solution [24] aligns with secure communication and real-time control in cloud environments. Modular converter designs discussed in [25] inspire scalable architecture principles, relevant for proxy re-encryption systems. Together, these works contribute valuable insights into building secure, scalable cloud-based report sharing models.

METHODOLOGY

Overview of the Proposed Secure Sharing Framework

To address the security and scalability limitations in cloud-based report sharing systems, this work proposes a cryptographic framework centered on asymmetric key distribution**,** attribute-based encryption (ABE)**,** group key management**,** and proxy re-encryption (PRE). The framework is designed to accommodate dynamic user membership, support fine-grained access control, and enable secure delegation, all while maintaining low computational overhead and ensuring confidentiality, integrity, and availability of cloud-stored data.

The system architecture comprises three key entities: (i) data owners, who upload encrypted reports; (ii) authorized users, who request access; and (iii) a Cloud Key Management System (CKMS)**,** responsible for secure key generation, storage, distribution, and revocation. The CKMS collaborates with a semi-trusted cloud server that performs cryptographic operations without accessing plaintext data.

Key Generation and Distribution

The framework begins with secure user registration and key generation. Each registered participant is assigned a unique public-private key pair, generated using RSA or ECC algorithms. In group-based environments, a Key Distribution Server (KDS) initializes a group secret using Logical Key Hierarchy **(**LKH**)** to manage scalable and efficient key distribution. When a user joins or leaves a group, the KDS updates only a subset of the key tree, thus reducing rekeying overhead and improving scalability [1][2].

Attribute-Based Access Control

To enforce fine-grained access control, the framework utilizes Ciphertext-Policy Attribute-Based Encryption (CP-ABE)**.** Here, the data owner defines an access policy based on user attributes (e.g., role = "auditor", department = "energy"). Only users whose attribute set satisfies the policy can decrypt the data. This policy is embedded directly in the ciphertext, ensuring that access enforcement is cryptographically enforced rather than server-dependent.

To mitigate ABE's known limitation of expensive revocation, the framework includes **attribute revocation** tokens and key update mechanisms, which periodically re-issue short-lived decryption keys to valid users. Additionally, lightweight proxi**es** are deployed to offload the computation-heavy policy evaluation from mobile or resource-constrained devices [3][4].

Secure Delegation via Proxy Re-Encryption

In collaborative scenarios, a data owner may delegate decryption rights to another user or a group without revealing their private key. To achieve this, the framework employs proxy re-encryption (PRE)**.** Upon delegation, the owner generates a re-encryption key and sends it to the cloud. The semi-trusted cloud proxy uses this key to transform the original ciphertext (under the owner's key) into a new ciphertext decryptable by the delegatee—without learning the underlying plaintext [5].

This technique supports policy-based, time-restricted, and condition-based delegation, allowing organizations to enforce dynamic access rules (e.g., "access allowed for 7 days" or "valid only if user role = analyst") directly in the cloud layer, without contacting the owner again [6].

Key Aggregation and Scalability Features

For applications that involve a large volume of encrypted reports or multiple data categories (e.g., monthly energy bills, usage logs, theft alerts), the framework integrates a Key-Aggregate Cryptosystem (KAC)**.** This allows data owners to generate a single compact decryption key that enables access to any subset of the encrypted files, significantly reducing key storage and communication overhead [7]. This is particularly beneficial in ad hoc group scenarios, where file ownership and access policies evolve rapidly.

Privacy Preservation and Monitoring

To enhance privacy, the system supports searchable encryption, where users can perform keyword searches over encrypted reports without decrypting them. Additionally, oblivious RAM (ORAM) and group signature schemes are integrated to protect access patterns and user identities from being traced by the cloud provider. The CKMS logs all key usage and delegation operations for auditing and compliance.

The entire framework is implemented and tested in a simulated OpenStack private cloud environment, utilizing Java-based cryptographic libraries. Performance metrics such as key generation time, encryption/decryption latency, CPU/memory utilization, and revocation response time are captured and analyzed for RSA, ElGamal, and Paillier algorithms under varying key sizes and file sizes.

EXPERIMENTAL SETUP

To evaluate the performance and security capabilities of the proposed asymmetric key distribution-based cloud sharing framework, a series of **simulated experiments** were conducted using a private cloud testbed. The objective was to analyze the computational efficiency, resource usage, and scalability of the implemented system, particularly in contexts involving secure report sharing and dynamic user access in cloud environments.

Testbed Configuration

All tests were conducted in an OpenStack-based private cloud environment, configured with two virtual machines (VMs) acting as the key distribution server (KDS) and cloud storage provider, respectively. The hardware and software configuration of the testbed is summarized in Table 1.

Table.1 Experimental Test bed Configuration

Parameter	**Specification**
Virtualization Platform	Open Stack Queens Release
Processor	Intel Core i5, Dual Core, 1.4 GHz
RAM	4 GB per VM
Operating System	Ubuntu 20.04 LTS
Programming Language	Java (JDK 1.8)
Cryptographic Library	Java Cryptography Architecture (JCA)
Network	Virtual Private Network (VPN), 100 Mbps

4.2 Cryptographic Algorithms and Parameters

Three prominent asymmetric cryptographic algorithms: RSA, ElGamal, and Paillier, were implemented to evaluate their performance under the proposed framework:

- **RSA**: Tested with key sizes of 512, 1024, and 2048 bits.
- **ElGamal**: Configured over a large prime field, tested with 1024-bit keys.
- **Paillier**: Evaluated with key sizes of 512 and 1024 bits for probabilistic encryption operations.

The experiments focused on the following cryptographic operations:

- Key generation
- File encryption

- File decryption
- Proxy re-encryption
- Attribute-based policy enforcement

4.3 Test Dataset

To simulate report sharing, six different text-based files of varying sizes were prepared, emulating real-world smart meter reports and sensor logs. File sizes ranged from 48 KB to 2048 KB, as shown below:

Table.2 Test File Sizes Used for Evaluation

File ID	Size (KB)	Description
F1	48	Daily energy usage log
F2	64	Billing report
F3	128	User consumption trend
F4	256	Theft alert event report
F5	1024	Monthly aggregated report
F6	2048	Sensor data archive

Each file was encrypted, decrypted, and re-encrypted using all three cryptographic algorithms to analyze the **impact of file size and key size** on system performance.

4.4 Performance Metrics

The following **performance parameters** were measured during the experiment:

- **Key Generation Time (ms)**: Time taken to generate public-private key pairs.
- **Encryption Time (ms)**: Time to encrypt a file using the public key.
- **Decryption Time (ms)**: Time to recover the plaintext from ciphertext using the private key.
- **CPU Utilization (%)**: CPU load during cryptographic operations.
- **Memory Usage (MB)**: RAM consumed during encryption and decryption.
- **Re-encryption Overhead (ms)**: Time taken by the proxy to perform re-encryption for delegation.

Each test was repeated five times to ensure consistency, and average values were recorded for analysis.

RESULTS AND DISCUSSION

This section presents the performance evaluation of the proposed secure cloud report-sharing framework using three asymmetric cryptographic algorithms: RSA, ElGamal, and Paillier. The evaluation focuses on key generation, encryption and decryption latency, CPU and memory usage, and proxy re-encryption efficiency across files of varying sizes.

Key Generation Time

Figure 1 illustrates the average key generation time for RSA, ElGamal, and Paillier across different key sizes. The RSA algorithm consistently demonstrated the lowest key generation time, especially at 512 and 1024 bits, making it suitable for applications requiring frequent key refresh or group-based distribution. ElGamal and Paillier, although secure, incurred noticeably higher generation times due to their probabilistic nature and complex key structures.

Observation: For 2048-bit keys, RSA completed generation in approximately 75 ms, while ElGamal and Paillier required over 130 ms and 160 ms respectively.

Encryption and Decryption Performance

RSA consistently achieved faster encryption times**,** especially for files under 256 KB, whereas ElGamal demonstrated faster decryption for small-to-medium files due to its performance advantage in recovering plaintext with partial key knowledge.

Observation: RSA encrypted a 512 KB file in 85 ms, while ElGamal took 105 ms and Paillier over 130 ms.

Decryption- time for ElGamal on a 128 KB file was 40 ms, slightly better than RSA (55 ms).

CPU and Memory Utilization

Figure 4 compares CPU utilization **(%)** during encryption for the three algorithms. RSA exhibited the lowest CPU load (25%) compared to ElGamal (33%) and Paillier (39%) when processing mid-sized files (256–1024 KB). Similarly, memory usage**,** shown in Figure 5, was most efficient under RSA, requiring approximately 120 MB during encryption of a 1 MB file, while Paillier peaked above 160 MB.

Observation: RSA's lightweight resource consumption makes it optimal for real-time and embedded systems like IoT-driven smart meters.

Proxy Re-Encryption Overhead

The proxy re-encryption delay, critical for secure delegation, was measured using a cloud-based re-encryption module. Figure 6 demonstrates that RSA-based re-encryption incurred lower latency (40 ms)

compared to ElGamal (58 ms) and Paillier (65 ms). This supports the framework's efficiency in dynamic environments requiring frequent access policy updates.
Use case: In the case of role change or temporary delegation in an organization, RSA-based proxy re-encryption ensures minimal delay in ciphertext transformation.
Overall Comparison and Suitability

Table.3 Comparative Analysis of Cryptographic Algorithms

Metric	**RSA**	**ElGamal**	**Paillier**
Key Generation Time	Best	Moderate	Slow
Encryption Time	Best	Moderate	Slow
Decryption Time	Moderate	Best	Slow
CPU Usage	Low	Moderate	High
Memory Usage	Low	Moderate	High
Re-encryption Overhead	Low	Moderate	High

For lightweight, scalable, and policy-driven report sharing, RSA is the most balanced choice due to its speed, lower resource demand, and compatibility with group-based delegation and re-encryption protocols.

CONCLUSION AND FUTURE WORK

In this study, we presented a robust and scalable framework for secure report sharing in cloud environments using asymmetric key distribution mechanisms. The proposed architecture integrates RSA-based encryption, attribute-based access control, proxy re-encryption, and key-aggregate cryptographic techniques to enable dynamic, role-based, and fine-grained access to sensitive data stored in the cloud. Through detailed experiments conducted in an OpenStack-based private cloud environment, we evaluated the performance of RSA, ElGamal, and Paillier algorithms in terms of key generation time, encryption/decryption latency, CPU and memory usage, and proxy re-encryption delay. The results demonstrated that **RSA outperforms** the other two algorithms across most operational metrics, especially in environments with dynamic access control, frequent key updates, and limited computational resources. Our framework addresses major concerns in cloud computing such as data confidentiality, secure delegation, and scalable key management making it highly applicable to real-world domains including IoT-enabled energy grids, healthcare record sharing, and enterprise document workflows.
While the proposed model ensures strong cryptographic enforcement and efficient data access management, certain aspects merit further investigation, Integration with Block chain: Future versions of the framework could incorporate block chain-based audit trails and smart contracts to enhance transparency, accountability, and decentralized trust. Access Revocation and Accountability: Although the current system includes basic revocation strategies, advanced techniques such as time-bound keys, threshold rekeying, and active monitoring of revoked users can be explored to enhance security posture. Scalability in Federated Clouds: The framework can be extended and validated across federated and multi-cloud infrastructures to assess interoperability and key synchronization challenges in geographically distributed deployments. AI-Driven Policy Enforcement: Machine learning algorithms may be incorporated to recommend or auto-generate access policies based on user behavior, data classification, and contextual sensitivity.

REFERENCES

1. S. N, G. T, R. S. R, A. Sungheetha, C. R and S. Hamsanandhini, (2024). "Secured and Optimized Application Delivery Service in Public Cloud," *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, Noida, India, pp. 1-5, doi: 10.1109/ICIPTM59628.2024.10563300.
2. M. Rakhra, A. Singh, D. Singh, B. Kaur and Shruti, (2024). "Hybrid Cryptography in Cloud Computing," *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, pp. 1-7, doi: 10.1109/ICRITO61523.2024.10522254.
3. G. Singla, P. Goel and G. Kaur, (2023). "Enhancing Cloud Network Security: A Comprehensive Review of Hybrid Cryptographic Algorithms," *2023 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, Belagavi, India, pp. 1-6, doi: 10.1109/NKCon59507.2023.10396317.
4. O. A. Khashan, (2021). "Parallel Proxy Re-Encryption Workload Distribution for Efficient Big Data Sharing in Cloud Computing," *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, NV, USA, pp. 0554-0559, doi: 10.1109/CCWC51732.2021.9375967.
5. J. Yan, Y. Liu, L. Wang, Z. Wang, X. Huang and H. Liu, (2021). "An Efficient Organization Method for Large-Scale and Long Time-Series Remote Sensing Data in a Cloud Computing Environment," in *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 14, pp. 9350-9363. doi: 10.1109/JSTARS.2021.3110900.

6. D. Sitaram *et al*., (2018). "Orchestration Based Hybrid or Multi Clouds and Interoperability Standardization," *2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, Bangalore, India. pp. 67-71, doi: 10.1109/CCEM.2018.00018.
7. G. Katsaros *et al*., (2012). "A Holistic View of Information Management in Cloud Environments," *2012 IEEE Fifth International Conference on Cloud Computing*, Honolulu, HI, USA. pp. 989-990, doi: 10.1109/CLOUD.2012.84.
8. H. Wei and J. S. Rodriguez, (2018). "A Policy Based Application Deployment Method in Hybrid Cloud Environment," *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, Barcelona, Spain. 93-99, doi: 10.1109/FiCloud.2018.00021.
9. L. M. Herger, M. Bodarky and C. Fonseca, (2018). "Breaking Down the Barriers for Moving an Enterprise to Cloud," *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA. pp. 572-576, doi: 10.1109/CLOUD.2018.00079.
10. N. Grozev and R. Buyya, (2015). "Performance Modelling and Simulation of Three-Tier Applications in Cloud and Multi-Cloud Environments," in *The Computer Journal*, vol. 58, no. 1, pp. 1-22. doi: 10.1093/comjnl/bxt107.
11. C. Lin and S. Lu,(2011). "Scheduling Scientific Workflows Elastically for Cloud Computing," *2011 IEEE 4th International Conference on Cloud Computing*, Washington, DC, USA. pp. 746-747, doi: 10.1109/CLOUD.2011.110.
12. U. Ghosh, P. Chatterjee, D. Tosh, S. Shetty, K. Xiong and C. Kamhoua, (2017). "An SDN Based Framework for Guaranteeing Security and Performance in Information-Centric Cloud Networks,"*IEEE 10th International Conference on Cloud Computing (CLOUD)*, Honololu, HI, USA. pp. 749-752, doi: 10.1109/CLOUD.2017.106.
13. Sun, G. Gao, T. Ji and X. Tu, (2018). "One Quantifiable Security Evaluation Model for Cloud Computing Platform," *2018 Sixth International Conference on Advanced Cloud and Big Data (CBD)*, Lanzhou, China. pp. 197-201, doi: 10.1109/CBD.2018.00043.
14. Khajeh-Hosseini, D. Greenwood and I. Sommerville, (2010). "Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS," *2010 IEEE 3rd International Conference on Cloud Computing*, Miami, FL, USA. pp. 450-457, doi: 10.1109/CLOUD.2010.37.
15. Gao, J. Zhang, D. Xuan, G. Deng and W. Cai, (2024). "Network Operation and Maintenance Technology Based on Machine Learning Algorithms in Cloud Computing Environment," *2024 International Conference on Interactive Intelligent Systems and Techniques (IIST)*, Bhubaneswar, India. pp. 317-321, doi: 10.1109/IIST62526.2024.00058.
16. N. K. Walia and N. Kaur, "Performance Analysis of the Task Scheduling Algorithms in the Cloud Computing Environments," *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom, 2021, pp. 108-113, doi: 10.1109/ICIEM51511.2021.9445320.
17. Tamilamuthan, R., & Geetha, B. T. (2024, November 15). IoT-driven solutions for efficient energy management and theft prevention for smart meter. *3rd International Conference on Optimization Techniques in the Field of Engineering (ICOFE-2024)*. SSRN. https://ssrn.com/abstract=5086732
18. J. Ni, Y. Huang, Z. Luan, J. Zhang and D. Qian, (2011). "Virtual machine mapping policy based on load balancing in private cloud environment," *2011 International Conference on Cloud and Service Computing*, Hong Kong, China, pp. 292-295, doi: 10.1109/CSC.2011.6138536.
19. M. Colombo, R. Asal, Q. H. Hieu, F. Ali El-Moussa, A. Sajjad and T. Dimitrakos, (2019). "Data Protection as a Service in the Multi-Cloud Environment," *2019 IEEE 12th International Conference on Cloud Computing (CLOUD)*, Milan, Italy. pp. 81-85, doi: 10.1109/CLOUD.2019.00025.
20. T. Kushida and G. S. Pingali, (2014). "Industry Cloud - Effective Adoption of Cloud Computing for Industry Solutions," *2014 IEEE 7th International Conference on Cloud Computing*, Anchorage, AK, USA. pp. 753-760, doi: 10.1109/CLOUD.2014.105.
21. Z. Hu, S. Sun, P. Yin, T. Xie, Y. Li and Q. Ren, (2023). "Building A Layer-2 Hybrid Cloud," *2023 IEEE 18th Conference on Industrial Electronics and Applications (ICIEA)*, Ningbo, China, pp. 156-163, doi: 10.1109/ICIEA58696 .2023.10241908.
22. Tayouri; S. Hassidim; A. Smirnov; A. Shabtai, (2022). "Cybersecurity in Agile Cloud Computing--Cybersecurity Guidelines for Cloud Access," in *Cybersecurity in Agile Cloud Computing--Cybersecurity Guidelines for Cloud Access* , vol., no., pp.1-36.
23. Y. C. Zhou, X. P. Liu, X. N. Wang, L. Xue, X. X. Liang and S. Liang, (2010). "Business Process Centric Platform-as-a-Service Model and Technologies for Cloud Enabled Industry Solutions," *2010 IEEE 3rd International Conference on Cloud Computing*, Miami, FL, USA, pp. 534-537, doi: 10.1109/CLOUD.2010.52.
24. Tamilamuthan, R., & Geetha, B. T. (2024). Optimized high gain interleaved SEPIC converter for electric vehicle charging stations with emphasis on renewable energy integration. *SSRG International Journal of Electrical and Electronics Engineering, 11*(3), 1–14. https://doi.org/10.14445/23488379/IJEEE-V11I3P101.
25. R. Tamilamuthan , et al. (2023). Non-Isolated Interleaved Bidirectional DC-DC Converter for Electric Vehicles : A Review. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(9), 4009–4015. https://doi.org/10.17762/ ijritcc.v11i9.9761