Role Based Access Control with Homomorphic Encryption for secure data exchange in the cloud

Abinaya P1, Aakash T2, Jerry J A Roshan2

Department of Computer Science and Engineering, Assistant Professor (Sl. Grade), Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India

Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India

***Abstract*—In today's digital landscape, when a myriad of products are widely available online, the critical necessity for authenticity, anonymity, and security above accessibility highlights the importance of encryption with access management. This research paper proposes an advanced encryption approach designed to improve the security of overall resource admissions. In contrast to traditional techniques, our proposed solution makes use of an Enhanced Homomorphic Encryption-based approach combined with Role-Based Access Control (RBAC) and eXtensible Access Connectivity Markup Language (XACML). This novel technology enables secure data storage within internet computers by utilizing cryptographic principles and a fast admission management mechanism. The suggested encryption approach combines classic homomorphic encryption procedures with a dynamic information distribution strategy, resulting in a strong barrier for sensitive data. Users gain the advantage of obtaining information in a secure and privacy-preserving manner by using this hybrid encryption technology. Notably, when compared to existing encryption approaches, the overall execution of our suggested solution is significantly faster. This study adds to the expanding landscape of secure information storage and retrieval by seamlessly merging homomorphic encryption with RBAC, providing a more efficient and protective paradigm for managing online resources and protecting sensitive data.**

***Index Terms*—** **homomorphic encryption, Role-Based Access Control (RBAC), eXtensible Access Connectivity Markup Language (XACML)**

# I. INTRODUCTION

Because of the pervasiveness of web technology, clients can now access information globally via the World Wide Web. While the internet makes it easy to get information, cloud computing expands these capabilities by providing users with shared resources such as memory, networks, and processing power. Cloud signatures entail storing private keys and performing data signing directly on the server. To enable the use of secure cloud signatures, issues such as strong client authentication and safe private key storage must be addressed.

Virtual droplet platforms, whether managed in-house or by

third-party vendors, are becoming increasingly important in the domain of personal computing. The global internet provides computer resource availability, while collaborative networks allow many enterprises to collaborate on shared resources. Hybrid cloud architectures combine several internet technologies to provide information mobility via standards and

proprietary technologies.

Robust access mechanisms are critical in the context of internet technology for preventing illegal access and preserving data integrity. Recent enhancements have included support for cryptographic algorithms, allowing for the creation of safe static WEB clients with high security needs.

Access control strategies such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC) are critical components of information security. RBAC, which involves grouping clients based on allocated responsibilities, is very relevant. Given these considerations, the primary goal of this article is to assure efficient and safe information storage. A novel solution is proposed that combines RBAC with an extended connectivity management modeling vocabulary and makes use of homomorphic encryption to enable safe data retrieval with minimal delay.

In today's linked world, the importance of cloud security cannot be emphasized. When sensitive data is kept in the cloud, strong security measures are required to prevent unwanted access and preserve data integrity. The suggested hybrid cryptography-based encryption solution, which combines RBAC and homomorphic encryption, offers a viable route for improving the efficiency and security of information storage in cloud environments.

## III. PROPOSED WORK

In the ever-changing world of cloud computing, the need to protect sensitive data from unwanted access has fuelled a continuing search for sophisticated security solutions. Using the revolutionary integration of homomorphic encryption and eXtensible Access Control Markup Language (XACML), this research aims to improve cloud security by building on the fundamental concepts of secrecy, accessibility, efficiency, and durability.

This study will initially investigate the incorporation of homomorphic encryption algorithms into cloud infrastructure. Homomorphic encryption permits computations on encrypted data without the need for decryption, protecting sensitive information's confidentiality. The study's goal is to investigate the influence of homomorphic encryption on data processing efficiency and its suitability in a cloud setting. In parallel, the study will look into the use of XACML for fine-grained access control policies. XACML is a standardized access control system that, when paired with homomorphic encryption, promises to give a strong mechanism for regulating and enforcing permissions on encrypted data. The goal is to create customized XACML policies that address the unique issues given by homomorphically encrypted data. In addition to these efforts, the research will concentrate on the Java cryptography architecture, taking use of its popularity to broaden the library of cryptographic algorithms compatible with homomorphic encryption. The project intends to provide a versatile and secure framework for implementing homomorphic encryption methods while adhering to industry standards by improving Java's cryptographic capabilities. Improved data confidentiality through homomorphic encryption, fine-grained access control enabled by XACML, safe data processing in cloud contexts, and developments in the Java cryptography architecture are among the predicted consequences. The study has a lot of promise in terms of tackling fundamental security concerns in cloud computing and helping to the establishment of robust and privacy-preserving data management techniques.

**Role based access control with XACML**

**Admission-Based Security and RBAC Integration**:

Admission-based security measures are critical in the field of internet technology for preventing unauthorized users from getting access to a network. The major purpose is to create a secure environment in which users are not permitted to make unwanted changes. This is accomplished by assigning login credentials to roles in a Role-Based Access Control (RBAC) system, where permissions are assigned to certain tasks and then assigned to individuals. However, while RBAC authenticates a user's identify, it falls short of measuring user trustworthiness to prevent unauthorized access. RBAC is seamlessly coupled with the extended access control markup language (XACML) to alleviate this problem.

**Attribute-Based Access Control with XACML:**

XACML, a well-known attribute-based access control technology, becomes an important component in improving RBAC. Attributes are important data points for the subject attempting to access a resource, the resource itself, and the context in which the access attempt occurs. This attribute-centric approach serves as the primary evaluation criterion for evaluating whether access should be granted or refused. XACML not only provides attribute-based access control, but it also makes role-based access control easier to build, resulting in a versatile and complete security architecture.

Policy Framework and XACML Components:

The suggested solution uses XACML to incorporate RBAC rules, presenting an authorization framework with separate components. The Policy Decision Point is in charge of assessing access decisions, the Policy Administration Point is in charge of policy creation and management, the Policy Information Point is in charge of storing policy information, the Policy Enforcement Point is in charge of executing authorization requests, and the Policy Retrieval Point is in charge of storing policies for reference. Figure 2 depicts a cohesive and effective Role-Based Access Control with XACML system made up of these components.

Digital Signatures and Workflow Integration:

Going beyond access control, enterprises can strengthen their security architecture by incorporating digital signatures or stamps into workflows. Digital signatures are used by system integrators in both existing and new document management systems. Organizations must carefully assess and select the Digital Signature Standard (DSS) solution that best meets their project requirements. This decision takes into account regulatory constraints, the size of the organization, and different case-specific circumstances. This comprehensive strategy ensures that the integrated security measures address the organization's digital environment's various and developing needs.

**Homomorphic Encryption**

Homomorphic encryption is a game-changing development in the world of cryptography, providing a novel solution to the problem of safely processing data while it is encrypted. In contrast to typical encryption approaches, homomorphic encryption allows computations to be done directly on encrypted data, avoiding the requirement for decryption before processing. This breakthrough has major ramifications for privacy-preserving computing since it allows for secure data processing outsourcing to third-party entities without disclosing the underlying sensitive information. At its core, homomorphic encryption is based on mathematical approaches that allow computations on ciphertexts to generate results that are compatible with the outcomes of the same computations performed on plaintext when decrypted. This is accomplished using mathematical operations that maintain the link between encrypted and decrypted data. There are numerous types of homomorphic encryption methods, such as partially homomorphic and fully homomorphic encryption, each with a varying level of computing capability while ensuring data security.

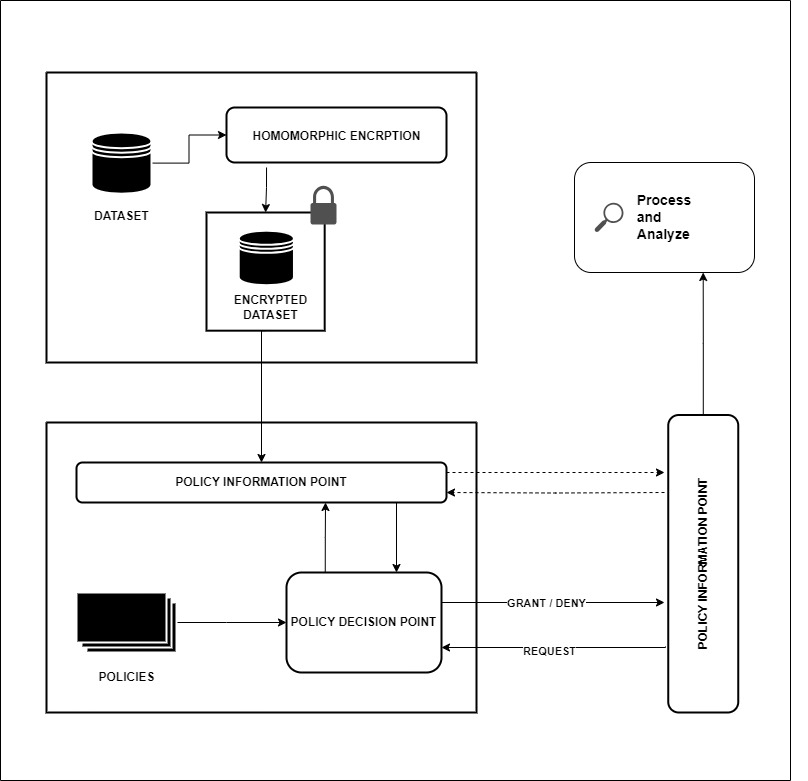
**Integration of Homomorphic Encryption and Role-Based Access Control with XACML**

Homomorphic encryption is essential for protecting the secrecy of sensitive data. It establishes a strong privacy-preserving layer by allowing computations on encrypted data without the requirement for decryption. This cryptographic approach enables safe data processing while limiting the dangers of data exposure during the calculation and storage phases. Concurrently, RBAC provides a standardized framework for managing system access privileges. Users are assigned roles, and their access to certain resources is determined by the permissions associated with those roles. This RBAC approach works in tandem with XACML, an attribute-based access control system. XACML adds a dynamic and flexible layer to RBAC, allowing attribute-driven access decisions depending on a user's role, the resource being accessed, and the surrounding environment.

XACML introduces attribute-based access control, which bases access choices on specific properties associated with the user and the resources in issue. Key components of the integration include Policy Decision Points (PDP), Policy Administration Points (PAP), and Policy Enforcement Points (PEP). The PDP compares access requests to specified policies, the PAP oversees policy formulation and administration, and the PEP enforces access decisions in real time. Within this collaborative framework, homomorphic encryption integrates neatly into the data processing pipeline. Homomorphic operations are conducted on encrypted data, allowing computations to be performed without exposing the raw data. The encrypted data remains confidential throughout the calculation, in accordance with the security principles of RBAC and XACML.

This integration's overall impact extends to the broader area of cloud computing. The combination of homomorphic encryption, RBAC, and XACML creates a privacy-preserving environment in which data confidentiality and access control coexist. This not only improves the system's security posture, but also helps with regulatory compliance and the construction of a safe and trustworthy cloud infrastructure.

This system provides a strong defense against unauthorized access and maintains the privacy of sensitive information in cloud computing settings by combining the strengths of cryptographic confidentiality, role-based access control, and attribute-driven access decisions.



## III. RELATED WORKS

### Kousalya A. et al. (2023) [[1]](#_Kousalya,_A.,_&) proposed a paper with the objective of enhancing cloud security and effectiveness through an improved RSA-based Role-Based Access Control (RBAC) with eXtensible Access Control Markup Language (XACML) technique. The new design incorporates a stronger encryption strategy to safeguard resource access. The enhanced RSA-based RBAC with XACML ensures both information encryption and privilege maintenance. This is accomplished through the use of a hybrid encryption technique that combines homogeneous encryption with insecure information distribution. The proposed work is faster to execute than other encryption methods, which contributes to the advancement of secure and efficient cloud computing practices.

### Sepczuk M. et al. (2018) [[2]](#_Sepczuk,_M.,_&) proposed a risk-based authentication management model leveraging contextual data, with the goal of enhancing user satisfaction without compromising security. The model includes a detailed risk analysis procedure for selecting a multi-step authentication process that balances user satisfaction (Quality of Experience, QoE) and security (Quality of Protection, QoP). This approach seeks to provide a strong authentication system that not only ensures security but also prioritizes a positive user experience, thus aligning with the dual goals of increased security and increased user satisfaction.

### Batra G. et al. (2019) [[3]](#_Batra,_G.,_Atluri,) proposed a solution for the commercial viability of Attribute-Based Access Control (ABAC) by integrating ABAC policies into Role-Based Access Control (RBAC) and Temporal RBAC (TRBAC) systems. Despite ABAC's longer evaluation time compared to RBAC/TRBAC, the approach aims to enhance flexibility and portability. The paper examines management costs and suggests mitigation strategies, as well as practical advice on optimizing access control systems. Jiao K. et al. (2020) [[4]](#_Jiao,_K.,_Ye,) proposed an image encryption scheme employing a generalized Arnold map and the RSA algorithm. The RSA algorithm is used to generate the Arnold map parameters. The scheme conceals image data using XOR diffusion and cyclic confusion, with an additive mode diffusion operation incorporated for third-layer hiding. The encryption scheme, which relies on the RSA algorithm, demonstrates strong anti-attack capabilities and key sensitivity, ensuring high-security measures in image protection. Rao K. R. et al. (2021) [[5]](#_Rao,_K._R.,) proposed a role recommendation model for Role-Based Access Control (RBAC) systems, optimizing user-role assignments by revoking and refurbishing based on user access behavior. The model, which was implemented as Role-Assignment-as-a-Service in the cloud to reduce costs, exhibits a 50% higher efficiency in experimental results when compared to state-of-the-art approaches, demonstrating its effectiveness in enhancing user-role assignments within RBAC systems.

### Saraswathy K. S. et al. (2023) [[6]](#_Saraswathy,_K._S.,) proposed a trapdoor-based NDSGA-II AC for secure cloud data storage, using a stream cipher algorithm to encrypt parameters. This results in significant reductions in energy consumption, resource usage, and access time. When NTRU cryptosystem, CP-ABE, and RBAC are used, the encryption time is reduced by 11%, 16%, and 23%, respectively, when compared to the current method. Access time is also reduced by 8% and 15% when compared to CP-ABE and RBAC, demonstrating the proposed approach's efficacy in improving both security and operational efficiency in cloud environments.

### S Uthayashangar. et al. (2020) [[7]](#S. Uthayashangar, J. Abinaya, V. Harshini and R. Jayavardhani, "Image And Text Encrypted Data With Authorized Deduplication In Cloud," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020, pp.) proposed a privacy-centric system employing role re-encryption to prevent data leakage and deduplication. Authorized users are identified using a proof of ownership mechanism, and personal images and text files are encrypted. The system's primary goal is to eliminate text and image data duplication while emphasizing robust privacy measures within a concise framework.

### Riad. et al. (2021) [[8]](#_Riad,_Khaled_&) proposed a paper addressing access control in distributed IoT environments through the utilization of XACML. The paper identifies a flaw in common XACML schemes, which frequently overlook authentication parameters and are vulnerable to attacks. In response, the paper proposes an adaptive XACML scheme that integrates access code generation and verification seamlessly. This novel approach considers authentication parameters and protects against Masquerade and Man-in-the-Middle (MITM) attacks. The proposed adaptive XACML validates the efficacy, efficiency, compatibility, and performance, providing a comprehensive solution for enhanced access control in distributed IoT settings.

### Deng. et al. (2019) [[9]](#Deng, Fan & Zhang, Liyong & Zhang, Changyu & Ban, Hao & Wan, Chang & Shi, Minghao & Chen, Chao & Zhang, Enti. (2019). Establishment of rule dictionary for efficient XACML policy management. Knowledge-Based Systems. https://doi.org/175. 26-35. 10.1016/j.kn) proposed XDPMOE, a novel XACML policy management optimization scheme designed to enhance efficiency. This novel approach improves evaluation efficiency by utilizing bitmap storage and HashMap, establishing a rule dictionary based on an array sequential storage structure. The use of bitmaps to store the policy set helps to reduce space complexity. The experimental results validate XDPMOE's improved efficiency in comparison to other engines, demonstrating its effectiveness in optimizing XACML policy management for improved performance.

### Nagendran K. et al. (2018) [[10]](#_Nagendran,_K_&) proposed a novel public cloud security technique, the paper introduces Hybrid Elliptic Curve Cryptography (HECC) as a cornerstone. A Lightweight Edwards curve is used for key generation, and private keys are modified using Identity-Based Encryption. The use of a key reduction technique improves the AES encryption process's efficiency. A comparative analysis shows that the proposed method outperforms existing models in terms of key generation and encryption time. The achieved throughput of 693.10 kB/s demonstrates the effectiveness of the proposed approach in enhancing public cloud security via efficient cryptographic mechanisms.

### MAmeur Y. et al. (2023) [[11]](#_MAmeur,_Y.,_Bouzefrane,) proposed a multi-cloud platform to enhance data privacy and availability, the paper introduces the utilization of homomorphic encryption, enabling data processing and manipulation while maintaining encryption. The study explores existing security solutions in the realm of multi-cloud environments employing homomorphic encryption. Additionally, it identifies open issues and opportunities for further enhancement in the pursuit of bolstering data security across diverse cloud platforms.

### M Louk. et al. (2015) [[12]](#_M._Louk_and) proposed a paper delves into the security aspects of mobile multi-cloud computing (MMC), with a focus on data security using homomorphic encryption. It goes on to investigate the implementation and evaluation of homomorphic encryption in the context of mobile cloud computing, providing insights into its effectiveness in improving data security in MMC environments.

### K Zkik. et al. (2016) [[13]](#K. Zkik, G. Orhanou and S. El Hajji, "Secure scheme on mobile multi cloud computing based on homomorphic encryption," 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 2016, pp. 1-6, doi: https://doi.org/10.1109/ICEMIS.2016.774) proposed a secure authentication mechanism based on homomorphic encryption in the context of mobile cloud computing, enabling users to fully leverage mobile technologies. The increasing mobile traffic, combined with security challenges, necessitates novel solutions. The proposed mechanism is not just theoretical; it has been implemented and simulated, demonstrating its robustness and reliability as an effective countermeasure in ensuring secure authentication in the evolving landscape of mobile cloud computing.

### Deshmukh. et al. (2021) [[14]](#_Deshmukh,_Jyoti_&) proposed a structured ciphertext-policy attributes model designed to address security threats and challenges posed by cloud computing in data protection. . The novel approach entails completely removing the database server to prevent unauthorized data access. Notably, the proposed mechanism not only improves security but also reduces processing time, providing a comprehensive solution for data protection in the cloud computing environment.

### Goswami. et al. (2020) [[15]](#_Goswami,_Radha._(2020).) proposed an improved honeypot cryptographic scheme aiming at predictive efficacy in cloud security. The paper defines key terms such as cloud security, honeypot algorithm, cryptography, feature extraction, classification, attack prediction, and key generation. Preprocessing a raw Intrusion Detection System (IDS) dataset (KDD cup), addressing missing values, and removing duplicates are all part of the research. In addition, the study calls for the use of sample size reduction methods and feature selection techniques to improve the overall effectiveness of the enhanced honeypot cryptographic scheme for robust predictive capabilities in cloud security.

Kumar. et al. (2022) [[16]](#Kumar, Manish. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. Array. https://doi.org/15. 100242. 10.1016/j.array.2022.100242.Saraswathy, K. S., & Sujatha, S. S. (2023). Secure data storage and access for fish monit) proposed a paper discussing the design, development, and standardization of quantum-safe cryptography algorithms. It addresses the serious threats posed by quantum computers to cybersecurity and existing cryptographic methods by conducting a performance analysis of potential quantum-safe algorithms. To effectively fortify cryptographic systems, the transition to quantum computers necessitates the use of quantum-safe cryptography algorithms, which may necessitate more CPU cycles, more memory, and larger key sizes.  
  
Shivaramakrishna D. et al. (2023) [[17]](#Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control. Alexandria Engineering Journal, 84,) proposed a hybrid cryptographic framework designed for secure data storage in cloud computing. To improve data confidentiality and integrity, this novel approach combines time-limited access control, adaptive key management, RSA, and AES-OTP. Thorough performance evaluations show that the framework is robust, with high accuracy, precision, recall, and F1-score values. With its comprehensive features, this framework effectively protects private information in cloud storage settings from unauthorized access, providing a dependable solution for heightened security in cloud-based data storage.

Dey K. et al. (2022) [[18]](#_Dey,_K.,_Debnath,) proposed a cryptographic paper introducing a signcryption scheme for confidentiality and unforgeability. Recognizing quantum computers as a threat to traditional cryptographic schemes, the paper investigates isogeny-based cryptography (IBC) as a post-quantum candidate. IBC has several advantages, including lower communication costs and a smaller public key size. This study presents the first IBC-based signcryption scheme, based on three difficult problems: Commutative Supersingular Isogeny Decisional Diffie-Hellman, Group Action Inverse Problem, and Commutative Supersingular Isogeny Knowledge of Exponent. The scheme meets predefined security levels and employs predefined ciphertext sizes.

Fu Xingbing. et al. (2022) [[19]](#Fu, Xingbing & Wang, Yinglun & You, Lin & Ning, Jianting & Hu, Ziquan & Li, Fagen. (2022). Offline/Online lattice-based ciphertext policy attribute-based encryption. Journal of Systems Architecture. 130. 102684. https://doi.org/10.1016/j.sysarc.2022.10268) proposed an innovative offline/online lattice-based ciphertext policy attribute-based encryption (CP-ABE) scheme. When compared to Lattice-based Learning With Errors (LWE) schemes, this approach strategically divides computations into offline and online phases, resulting in improved computational performance. This scheme, which is specifically designed for mobile devices, not only demonstrates efficiency but also resilience against potential quantum computing attacks, making it a promising solution in the realm of secure attribute-based encryption.  
  
Chen L. et al. (2023) [[20]](#_Chen,_L.,_Chen,) proposed a paper introducing a multi-party Quantum Homomorphic Encryption (QHE) based on quantum voting, presenting an enhanced scheme for anonymous broadcast. This advancement lowers the cost of delegated quantum computation while also broadening the applicability of Quantum Homomorphic Encryption in quantum networks. As a result, the proposed method advances the development of secure and efficient quantum communication protocols, particularly in scenarios involving multiple parties and quantum-based voting mechanisms.

Sathish Kumar. et al. (2023) [[21]](#Sathish Kumar, G., Premalatha, K., Uma Maheshwari, G., & Rajesh Kanna, P. (2023). No more privacy concern: A privacy-chain based homomorphic encryption scheme and statistical method for privacy preservation of user’s private and sensitive data. Expert Sys) proposed a paper introducing a privacy-chain-based homomorphic encryption scheme designed for privacy preservation. The proposed algorithm adeptly perturbs both numerical and categorical values without compromising data utility by leveraging statistical methods such as weight of evidence and information value. The algorithm's performance is compared to state-of-the-art techniques to determine its efficacy. The proposed algorithm outperforms existing techniques in the realm of privacy-preserving homomorphic encryption, according to experimental results.

### Li X. et al. (2023) [[22]](#_Li,_X.,_Li,) proposed a paper addressing multi-user collaboration in cloud computing with a focus on user privacy protection. The study introduces an improved DGHV homomorphic scheme aimed at removing ciphertext modulus constraints. In addition, a number theory-based DGHV-type Multilevel Key Homomorphic Encryption (MKHE) scheme is proposed. The addition of an extended key for ciphertext extension is part of this. The paper proves semantic security under the assumptions of error-free approximate greatest common divisor and large integer factorization difficulty. Simulation experiments show that the MKHE scheme is available and computationally efficient, making it suitable for multi-user scenarios in cloud environments.

## V. References

#### Kousalya, A., & Baik, N. (2023). Enhance cloud security and effectiveness using improved RSA-based RBAC with XACML technique. International Journal of Intelligent Networks, 4, 62–67. <https://doi.org/10.1016/j.ijin.2023.03.003>

#### Sepczuk, M., & Kotulski, Z. (2018). A new risk-based authentication management model oriented on user’s experience. Computers &amp; Security, 73, 17–33. <https://doi.org/10.1016/j.cose.2017.10.002>

#### Batra, G., Atluri, V., Vaidya, J., & Sural, S. (2019). Deploying ABAC policies using RBAC Systems. Journal of Computer Security, 27(4), 483–506. <https://doi.org/10.3233/jcs-191315>

#### Jiao, K., Ye, G., Dong, Y., Huang, X., & He, J. (2020). Image encryption scheme based on a generalized Arnold Map and RSA algorithm. Security and Communication Networks, 2020, 1–14. <https://doi.org/10.1155/2020/9721675>

#### Rao, K. R., Nayak, A., Ray, I. G., Rahulamathavan, Y., & Rajarajan, M. (2021). Role Recommender-RBAC: Optimizing user-role assignments in RBAC. Computer Communications, 166, 140–153. <https://doi.org/10.1016/j.comcom.2020.12.006>

#### Saraswathy, K. S., & Sujatha, S. S. (2023). Secure data storage and access for fish monitoring in cloud environment. Measurement: Sensors, 27, 100693. <https://doi.org/10.1016/j.measen.2023.100693>

#### S. Uthayashangar, J. Abinaya, V. Harshini and R. Jayavardhani, "Image And Text Encrypted Data With Authorized Deduplication In Cloud," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020, pp. 1-5, doi: <https://doi.org/10.1109/ICSCAN49426.2020.9262324>

#### Riad, Khaled & Cheng, Jieren. (2021). Adaptive XACML access policies for heterogeneous distributed IoT environments. Information Sciences. 548. [https://doi.org/135-152. 10.1016/j.ins.2020.09.051](https://doi.org/135-152.%2010.1016/j.ins.2020.09.051)

#### Deng, Fan & Zhang, Liyong & Zhang, Changyu & Ban, Hao & Wan, Chang & Shi, Minghao & Chen, Chao & Zhang, Enti. (2019). Establishment of rule dictionary for efficient XACML policy management. Knowledge-Based Systems. [https://doi.org/175. 26-35. 10.1016/j.knosys.2019.03.015](https://doi.org/175.%2026-35.%2010.1016/j.knosys.2019.03.015)

#### Nagendran, K & Nadesan, Thillaiarasu & Chandrika, P & Chethana, R. (2018). Hyper Elliptic Curve Cryptography (HECC) to Ensure Data Security in the Cloud. <https://doi.org/10.14419/ijet.v7i4.19.22045>

#### MAmeur, Y., Bouzefrane, S., & Thinh, L. V. (2023). Handling security issues by using homomorphic encryption in multi-cloud environment. Procedia Computer Science, 220, 390–397. <https://doi.org/10.1016/j.procs.2023.03.050>

#### M. Louk and H. Lim, "Homomorphic encryption in mobile multi cloud computing," 2015 International Conference on Information Networking (ICOIN), Cambodia, 2015, pp. 493-497, <https://doi.org/10.1109/ICOIN.2015.7057954>

#### K. Zkik, G. Orhanou and S. El Hajji, "Secure scheme on mobile multi cloud computing based on homomorphic encryption," 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 2016, pp. 1-6, doi: <https://doi.org/10.1109/ICEMIS.2016.7745297>

#### Deshmukh, Jyoti & Yadav, Santosh & Bhandari, Gayatri. (2021). Attribute-Based encryption mechanism with Privacy-Preserving approach in cloud computing. Materials Today: Proceedings. [https://doi.org/80. 10.1016/j.matpr.2021.05.609](https://doi.org/80.%2010.1016/j.matpr.2021.05.609)

#### Goswami, Radha. (2020). Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security. Microprocessors and Microsystems. 81. 103719. <https://doi.org/10.1016/j.micpro.2020.103719>

#### Kumar, Manish. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. Array. [https://doi.org/15. 100242. 10.1016/j.array.2022.100242](https://doi.org/15.%20100242.%2010.1016/j.array.2022.100242).Saraswathy, K. S., & Sujatha, S. S. (2023). Secure data storage and access for fish monitoring in cloud environment. Measurement: Sensors, 27, 100693. <https://doi.org/10.1016/j.measen.2023.100693>

#### Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control. Alexandria Engineering Journal, 84, 275–284. [https://doi.org/10.1016/j.aej.2023.10.054](https://doi.org/10.1016/j.aej.2023.10.054%20)

#### Dey, K., Debnath, S. K., Stănică, P., & Srivastava, V. (2022). A post-quantum signcryption scheme using isogeny based cryptography. Journal of Information Security and Applications, 69, 103280. [https://doi.org/10.1016/j.jisa.2022.103280](https://doi.org/10.1016/j.jisa.2022.103280%20)

#### Fu, Xingbing & Wang, Yinglun & You, Lin & Ning, Jianting & Hu, Ziquan & Li, Fagen. (2022). Offline/Online lattice-based ciphertext policy attribute-based encryption. Journal of Systems Architecture. 130. 102684. <https://doi.org/10.1016/j.sysarc.2022.102684>

#### Chen, L., Chen, L., & Li, Q. (2023). Practical multi-party quantum homomorphic encryption. Theoretical Computer Science, 971, 114067. [https://doi.org/10.1016/j.tcs.2023.114067](https://doi.org/10.1016/j.tcs.2023.114067%20)

#### Sathish Kumar, G., Premalatha, K., Uma Maheshwari, G., & Rajesh Kanna, P. (2023). No more privacy concern: A privacy-chain based homomorphic encryption scheme and statistical method for privacy preservation of user’s private and sensitive data. Expert Systems with Applications, 234, 121071. [https://doi.org/10.1016/j.eswa.2023.121071](https://doi.org/10.1016/j.eswa.2023.121071%20)

#### Li, X., Li, H., Gao, J., & Wang, R. (2023). Privacy preserving via multi-key homomorphic encryption in cloud computing. Journal of Information Security and Applications, 74, 103463. [https://doi.org/10.1016/j.jisa.2023.103463](https://doi.org/10.1016/j.jisa.2023.103463%20)