Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2023 4(1), 1075–1082

SECURE MULTI CLOUD STORAGE APPROACH FOR MULTICLOUD ENVIRONMENTS USING FOG COMPUTING

R Janaki [1], Prathap S [2], Raman R [2], Tony Wilson I [2], Yuvaraj J [2]

[1] Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Mallasamudram, Namakkal-637503, Tamilnadu, India
[2] UG Student, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Mallasamudram, Namakkal-637503, Tamilnadu, India

ABSTRACT

The use of cloud computing is rapidly increasing in many organizations. Cloud computing offers many advantages in terms of easy access to data at low cost. In a cloud computing environment, ensuring the security of cloud computing is a key element. Users typically store sensitive information on cloud storage providers, which may be unreliable. Since a single point of attack cannot expose all information, distributing data across different cloud storage providers (CSPs) automatically provides users with a level of control over data exfiltration. The study focuses on how to make key renewals as transparent as possible to customers, using key renewal outsourcing and a method called cloud storage auditing, which verifies it according to the Protection Security Algorithm (PSA). The propose system minimizes the burden of rekeying on the client side securely outsourced to the authorized party. a client uploads a new file to the cloud, it only needs to download the encryption private key from the TPA. In addition, our design also provides the user side with the ability to further verify the validity of the encryption private key provided by the PSA. All of these notable features have been carefully designed to make the entire audit process as transparent as possible to clients with significant risk resistance. Cloud computing formalizes this paradigm's definition and security model. Good safety performance simulations demonstrate that the detailed design instantiation is safe and efficient.

Keywords: Fog Computing, Protection Security Algorithm (PSA), Data Sharing Privacy Multi Cloud Environments

Corresponding Author

R Janaki, janakir@mahendra.info

DOI
10.29121/shodhkosh.v4.i1.2023.2928

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

New business models that facilitate pay-per-use, on-demand, and online economies of scale are made possible by cloud computing. With virtualized data centers at its core, the Internet cloud functions as a service factory. Hardware, software, networks, and data sets are virtualized and configured to create cloud platforms dynamically. The goal is to use virtual server clusters in data centers to shift desktop computing to a platform that is service-oriented. Nonetheless, the general acceptance of cloud computing as an outsourced computing service is being hampered by the lack of trust between cloud customers and suppliers. In order to support multi-tenancy, your cloud ecosystem needs to be dependable and safe. In actuality, trust is a social problem as much as a technical one. Nonetheless, I think that technology can improve Internet

applications' reputation, assurance, fairness, and trustworthiness. Cloud service providers (CSPs) must first build security and confidence, as well as allay consumer worries, in order to spur the uptake of web and cloud services. Users of cloud services are concerned that proprietors of data centers may misuse their systems, access private data sets arbitrarily, or divulge confidential information to unapproved parties.

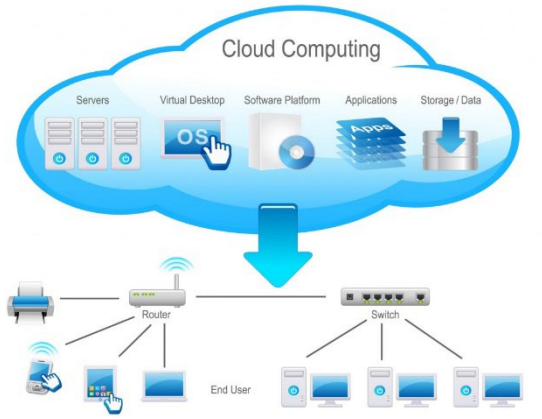

Figure 1 Cloud Services

Show fig 1 The Cloud Security Group has identified a number of issues critical to reliable cloud computing, and several recent studies have addressed common cloud security and privacy issues. Public and private clouds require different levels of security measures. Different service level agreements (SLAs) can be distinguished based on security considerations, including data integrity, user confidentiality, and trust between service providers, individual users, and user groups. These three information security needs must be separated from the three cloud service models described below. The infrastructure service model is the internal implementation layer and when extended it forms the PaaS (Platform as a Service) layer. Adding OS and middleware support. Passport further extends the software-as-a-service (SaaS) model by using specific APIs to build applications from data, content and metadata. This means that SaaS requires all security features at all levels. Cloud security has been introduced to provide comprehensive protection between the data owner and the service provider. To solve these problems, reputation-based trust management system is used, enhanced by data coloring and software watermarking. Data integrity is the cloud service provider's ability to protect data from unauthorized persons and hackers. Confidentiality is primarily a cloud service provider's way of ensuring that your data is protected from unauthorized access. Means used by cloud service providers to ensure that this is physical separation and encryption. Because cloud computing is a public network, it presents complex challenges for vendors to isolate customers.

1.1. CONTRIBUTION

- Cloud computing is an important aspect of computer services used for both private and business purposes.
- It helps to provide storage, database, software, analysis, network and intelligence through the Internet or the cloud where backup is stored.
- It also promotes resilient resources and economies of scale.
- There are pay-per-use and free services depending on the purpose of the service.

2. RELATED WORK

Cloud computing has been used as a platform for conventional business enterprise 3-tier networks and a few video processing programs to lessen price and growth deployment flexibility. Typically, those styles of programs are noticeably self-knowledge and feature easy overall performance necessities [1]. These are precise via way of means of provider stage agreements (SLAs) among the software and the cloud platform. Furthermore, new allotted cloud systems allow extra deployment fashions to guide greater overall performance-orientated programs [2]. Due to low latency necessities, positive recreation factors gain from being deployed nearer to (on-the-go) stop users. This paintings indicates the want to guide greater complicated overall performance necessities thru of his use cases: electricity metering and control, and public safety [3]. They speak approximately a software control device known as Abstract Service Manager. This device is designed to allow expression of overall performance necessities in automatic deployment of allotted cloud-local programs [4]. Our answer, which helps the maximum urgent wishes and complicated cloud

deployments, consists of a device known as Abstract Service Manager. It solves the overall performance constraints of the man or woman additives of the provider and leverages an allotted cloud orchestration supervisor to installation the provider [5].

The novelty of this answer lies with inside the kind of combos to be had with inside the introduction and deployment of devices, pushed via way of means of guide and decentralized cloud configurations. This complexity calls for automatic tools [6] as compared to current practices with trendy specifications. Compared to answers that require specialized platform software program or middleware to implement real-time guarantees, ASM assumes a high-stage overall performance description of the provider and makes use of those estimates to manual the cloud orchestration supervisor to usually installation to gently loaded servers. And networks [7]. Network connections have latency and bandwidth limitations, and require pre-configured community access, inclusive of that to be had from a business enterprise VPN [8]. This technique is regular with the general cloud philosophy of making use of standardized hardware and software program additives as a great deal as feasible to limit costs. The aggregate of automatic high-stage control and bendy allotted clouds can correctly update paintings-in depth fixed-dimensional installations. Determine [9]. Cloud computing is starting to play a large function in clinical and technical computing. However, there are nevertheless a few demanding situations that want to be addressed earlier than data-in depth clinical programs may be migrated to the cloud [10].

Adopting the Distributed Shared Memory (DSM) programming paradigm thru the usage of Partitioned Global Address Space (PGAS) languages may be one manner to ease the transition [11].In this study explore preliminary results using a representative private cloud-integrated parallel programming language based on Eucalyptus. The upload and download processes are basically transparent to the user [12]. Coincident upload and download performance by distributing subsets of files across multiple cloud providers as appropriate based on policy. Reliability is another important characteristic of his DISC [13]. To improve reliability, they proposed a solution to replicate the same subset of files between different vendors. This is useful if one provider is unresponsive and you can retrieve material from another provider that has the same subset. Security is critical when dealing with consumer data [14]. Increased reliability essentially increases security. Archives are distributed using subsets, so no single provider has a complete archive [15]. In our experiments observed performance improvements in archive delivery and retrieval compared to standard methods [16]. The results were encouraging, with processing time saved over 8 seconds [17]. As more cloud service providers expand, results are expected to improve [18]. Supporting mission-critical business use cases at a reasonable cost requires precise limits on compute, storage, and network resources [19]. When used with a distributed cloud orchestration system, it automatically reduces the complexity of building and deploying performance-intensive applications in a distributed cloud [20].

3. IMPLEMENTATION OF PROPOSED SYSTEM

Multi-cloud systems increase security when transferring data from one to another. It is possible that an attacker could decrypt messages during communication between her two users. Encryption is performed to avoid this theft. Use this technology to convert the original message to other formats. At the receiving end, it is decrypted and the original data is retrieved. Migration from a single cloud or on-premises cloud to multi cloud makes sense and is important for a variety of reasons. Outages of a single cloud service are still occurring.

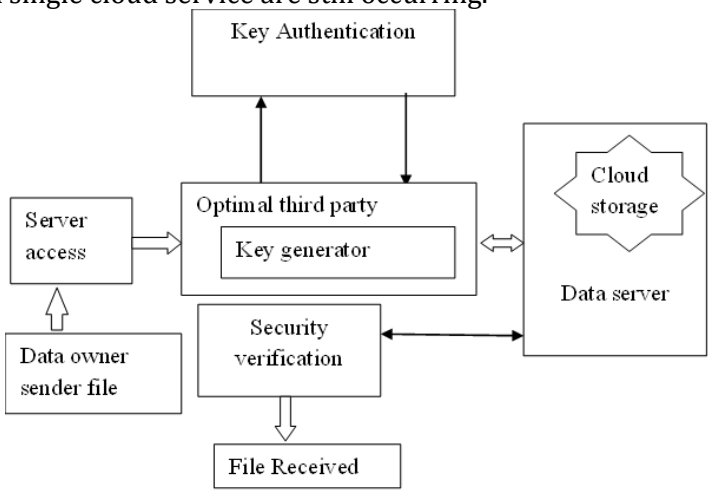

Figure 2 Implementation Diagram

Fig show 2 Data owners can configure their access control cloud policies based on user attributes and apply those policies to shared data. Accurate user-attribute-based recall can be achieved by proxy encryption using selective key distribution from the ABE attribute. All users have authorized, auditable, and flexible access to data in cloud computing. Agent cryptographic properties during distributed Chipper text encryption. Therefore, the privacy of sensitive personal data has become a primary focus for many data owners. Cloud service providers can also monitor users' personal data.

Here, d is the dimension of Cloud data. This amounts to finding W and b so that

$$y_i(W.x_i + b) > 0, i = l \dots N \quad (1)$$

In this rescale of W and b, that

$$min_{;<j<N}^{y_i(W.x_i+b)>0, i=l\dots N} \quad (2)$$

So the close-set point equation (1) hyperplanes of distance

$$y_i(W.x_i + b) > l \quad (3)$$

Here, find the optimal separating hyperplane and closed set of distance w

$$\frac{1}{||W||} = \frac{1}{4}||W||^2 \quad (4)$$

Where minimizing amount is under constraints || 〖W||〗 ^2 is under linear constraints equations (2) achieved with the multipliers. Denote by α=(α_1…α_N) the N non-negative multiplier associated, and extract the data from

$$W(\alpha) = \sum_{i=0}^{N} \alpha_i - \frac{1}{4} \sum_{i=0}^{N} \alpha_i, \alpha_j, y_i, y_j x_i . x_j \quad (5)$$

Here $\sum_{i=0}^{N} y_i \alpha_i$is achieved by the PSA Method. denote the $\alpha^0 = (\alpha^0{}_1 \dots \alpha^0{}_N)$i is solution for the maximum problem (5) found. Here(W^0, b^0), the following expression is

$$W_0 = \sum_{i=0}^{N} \alpha^0 y_i x_i \quad (6)$$

There are many encryption algorithms, and each algorithm differs based on the application and security metrics. In addition to the algorithm, an encryption key is also required. Using a key and an appropriate encryption algorithm, plaintext is converted into encrypted data, also known as cipher text. Instead of sending clear text to the recipient, encrypted text is sent over an insecure connection differential channel, which increases the number of key rounds and increases the security level.

The PSA are points for which $\alpha_i > 0$satisfies the equation (2) with equality.

From equation (6), the decision plane is to be written as

$$f(x) = sgn[\sum_{i=0}^{N} \alpha^0 y_i x_i \, W + b^0] \quad (7)$$

The input is mapped. The non-linear high-dimensional feature has been selected here

Replace x is storage selection $\Phi(x), taken\ equation(5)$ combined here.

$$W(\alpha) = \sum_{i=0}^{N} \alpha_i - \frac{1}{2} \sum_{i=0}^{N} \alpha_i, \alpha_j, y_i, y_j \Phi x_i . \Phi x_j \quad (8)$$

here k = $\Phi x_i . \Phi x_j is\ training\ algorithm\ of\ mapping\ \Phi$. symmetric

Position kernel K(x,y) is mapped with existing Mercer's theorem

Mapping σ shows that

$$K(x, y) = \sigma\, x . \sigma\, y \quad (9)$$

Kernel K filling Mercer's complaint has been selected, and the training algorithm contains reducing

$W(\alpha) = \sum_{i=0}^{N} \alpha_i - \frac{1}{4} \mathrm{W} \sum_{i=0}^{N} \alpha_i, \alpha_j, y_i, y_j K(x_i, y_i)$ (10)

For personal storage systems, develop a modified attribute-based cipher text policy encryption system using flexible and expressive access policies from the public domain. Our solution supports multiple permission scenarios, where permissions operate independently without the need for a certification authority discuss suggested technologies use the mobile cloud. An attribute-based encryption system (ABE) is used to secure cloud storage when multiple users are reading the same file stored in the mobile cloud.

PSA Algorithm Steps

```
 function PSAencrypt(plaintext, key) {
  blocks := splitIntoBlocks(plaintext);
 roundKeys = catchRoundKeys(key)
 for (block in blocks) {
  //start round
  addRoundKey(roundKeys[0], block);
  // rounds contine
  for (9, 13 or 20 rounds) {
   Bytes(block);
   moveRows(block);
   blendColumns(block);
   addRoundKey(roundKeys[..], block);
  }
  // round process
  Bytes(block);
  moveRows(block);
  add RoundKey(round Keys[numRounds - 1], block);
 }
 ciphertext := collect(blocks);
 return ciphertext;
}
```

PSA-based data encryption is a common and effective security method and choice for protecting an organization's data. However, there are several different types of encryption methods. The data that needs to be encrypted is called plain text. The plaintext has to be sent through some encryption algorithm, which is essentially a mathematical calculation on the original message.

4. RESULT AND DISCUSSION

The main goal of the transition to Interlude is expected to improve the capabilities of a single cloud by sharing reliability, trustworthiness and security across multiple cloud providers. In addition, reliable distributed storage using a subset of PSA technologies across multiple clouds is recommended. Recent work in this area has created cloud-to-cloud protocols. Attribute encryption is more appropriate as an encryption primitive because it can solve the PSA security algorithm of data access control and can effectively solve the above problems. Although the existing electronic health attribute encryption algorithm has achieving several research results, it still faces new challenges in access control, such as privacy leakage, dynamic policy updates, illegal policy changes, etc. Specifically, clear-text access policies can expose private information within the access policies.

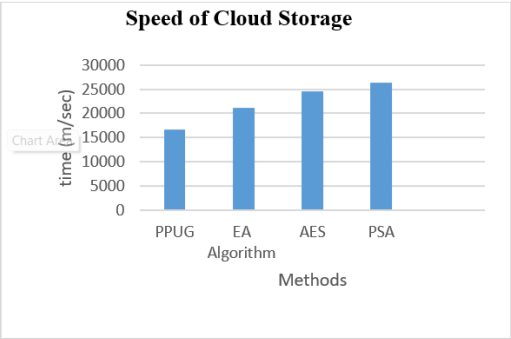

Figure 3 speed for comparing the various algorithms

Figure.3 compare the storage speed and speed for the PPUG algorithm, 16000 per second, and the EA algorithm, 21000 per second. The speed for the AES algorithm is 24000 per second, and the speed for the PSA algorithm is 26000 per second. Our using various algorithms use cloud security compared. The PPUG algorithm, EA algorithm, and AES are compared to be better for PSA algorithm.

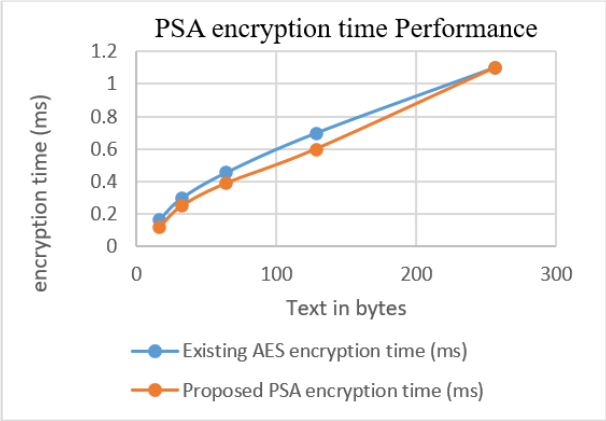

Figure 4 PSA Encryption performances

Figure.4 compares the encryption performance for the PPUG algorithm, 84.5%, and the EA algorithm performance is 85.2 %. The speed for the AES algorithm performance is 86.1 %, and the performance for the PSA algorithm is 92.5%.

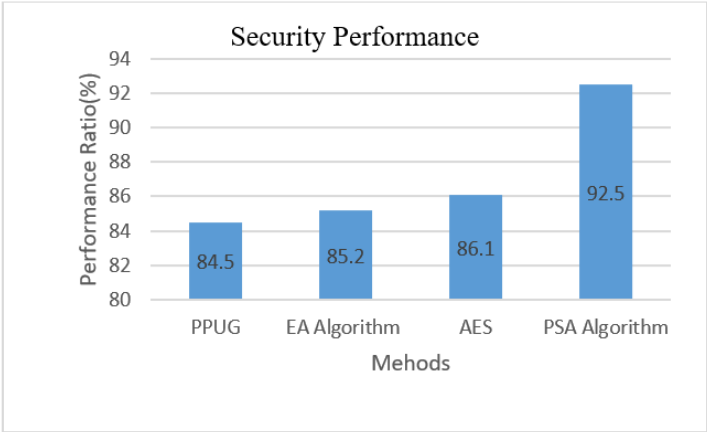

Figure 5 PSA Security performances

Figure.5 compares the security performance for the PPUG algorithm, 84.5%, and the EA algorithm security performance is 85.2 %. The speed for the AES algorithm security performance is 86.1 %, and the performance for the security PSA algorithm is 92.5%.

5. CONCLUSION

Cloud computing provides an economical and efficient solution for sharing group resources. Sharing data with multiple owners while maintaining data and identity privacy from an untrusted cloud remains a challenging data plays important role in our life and it is used in various applications in our daily life. Therefore, you must ensure the integrity and

confidentiality of the data you transmit. When users upload their data to the cloud, they leave it in a place where they have no control over monitoring. Will discuss some cloud computing technologies that play a key role in data transmission. In this study, investigate some important cryptographic algorithms of the past few decades. Conduct thorough research and analysis of these cloud computing methods to improve their performance. Each technology has unique capabilities that make it suitable for many uses. Traditional cloud computing techniques are fast, secure, and have a high level of security, as new technologies continue to be developed every day. This study provides a method for designing and inventing PSA algorithms and comparing them with existing algorithms.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

J. Chen, C. W. Sung and T. H. Chan, "Heterogeneity Shifts the Storage-Computation Tradeoff in Secure Multi-Cloud Systems," in IEEE Transactions on Information Theory, vol. 69, no. 2, pp. 1015-1036, Feb. 2023, doi: 10.1109/TIT.2022.3206868.

X. Liu, G. Yang, W. Susilo, J. Tonien, R. Chen and X. Lv, "Message-Locked Searchable Encryption: A New Versatile Tool for Secure Cloud Storage," in IEEE Transactions on Services Computing, vol. 15, no. 3, pp. 1664-1677, 1 May-June 2022, doi: 10.1109/TSC.2020.3006532.

Y. Fu, N. Xiao, T. Chen and J. Wang, "Fog-to-MultiCloud Cooperative Ehealth Data Management With Application-Aware Secure Deduplication," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3136-3148, 1 Sept.-Oct. 2022, doi: 10.1109/TDSC.2021.3086089.

J. Ren, J. Li, T. Li and M. W. Mutka, "Feasible Region of Secure and Distributed Data Storage in Adversarial Networks," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8980-8988, 1 June1, 2022, doi: 10.1109/JIOT.2021.3119031.

K. Kontodimas et al., "Secure Distributed Storage Orchestration on Heterogeneous Cloud-Edge Infrastructures," in IEEE Transactions on Cloud Computing, vol. 11, no. 4, pp. 3407-3425, Oct.-Dec. 2023, doi: 10.1109/TCC.2023.3287653.

K. Zhang, M. Wen, R. Lu and K. Chen, "Multi-Client Sub-Linear Boolean Keyword Searching for Encrypted Cloud Storage with Owner-Enforced Authorization," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 2875-2887, 1 Nov.-Dec. 2021, doi: 10.1109/TDSC.2020.2968425.

G. Hu, H. Li, G. Xu and X. Ma, "Enabling Simultaneous Content Regulation and Privacy Protection for Cloud Storage Image," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 111-127, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3081564.

R. Maher and O. A. Nasr, "DropStore: A Secure Backup System Using Multi-Cloud and Fog Computing," in IEEE Access, vol. 9, pp. 71318-71327, 2021, doi: 10.1109/ACCESS.2021.3078887.

J. Li, J. Ma, Y. Miao, R. Yang, X. Liu and K. -K. R. Choo, "Practical Multi-Keyword Ranked Search With Access Control Over Encrypted Cloud Data," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 2005-2019, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3024226.

C. Hahn, H. Yoon and J. Hur, "Multi-Key Similar Data Search on Encrypted Storage With Secure Pay-Per-Query," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1169-1181, 2023, doi: 10.1109/TIFS.2023.3236178.

T. Parbat and A. Chatterjee, "Authorized Update in Multi-User Homomorphic Encrypted Cloud Database," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 8, pp. 7796-7808, 1 Aug. 2023, doi: 10.1109/TKDE.2022.3221148.

C. Wang, D. Wang, Y. Duan and X. Tao, "Secure and Lightweight User Authentication Scheme for Cloud-Assisted Internet of Things," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2961-2976, 2023, doi: 10.1109/TIFS.2023.3272772.

S. Gao, Y. Chen, J. Zhu, Z. Sui, R. Zhang and X. Ma, "BPMS: Blockchain-Based Privacy-Preserving Multi-Keyword Search in Multi-Owner Setting," in IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2260-2272, 1 July-Sept. 2023, doi: 10.1109/TCC.2022.3196712.

F. Li, J. Ma, Y. Miao, Q. Jiang, X. Liu and K. -K. R. Choo, "Verifiable and Dynamic Multi-Keyword Search Over Encrypted Cloud Data Using Bitmap," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 336-348, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3093304.

K. He, J. Chen, Q. Yuan, S. Ji, D. He and R. Du, "Dynamic Group-Oriented Provable Data Possession in the Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1394-1408, 1 May-June 2021, doi: 10.1109/TDSC.2019.2925800.

Q. Huang, Z. Zhang and Y. Yang, "Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing," in IEEE Transactions on Mobile Computing, vol. 20, no. 5, pp. 1951-1964, 1 May 2021, doi: 10.1109/TMC.2020.2970705.

Y. Chen, W. Li, F. Gao, Q. Wen, H. Zhang and H. Wang, "Practical Attribute-Based Multi-Keyword Ranked Search Scheme in Cloud Computing," in IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 724-735, 1 March-April 2022, doi: 10.1109/TSC.2019.2959306.

Y. Zhang, H. Geng, L. Su and L. Lu, "A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage," in IEEE Access, vol. 10, pp. 105920-105929, 2022, doi: 10.1109/ACCESS.2022.3211391.

X. Li et al., "VRFMS: Verifiable Ranked Fuzzy Multi-Keyword Search Over Encrypted Data," in IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 698-710, 1 Jan.-Feb. 2023, doi: 10.1109/TSC.2021.3140092.

B. Gong et al., "SLIM: A Secure and Lightweight Multi-Authority Attribute-Based Signcryption Scheme for IoT," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1299-1312, 2024, doi: 10.1109/TIFS.2023.3331566.