IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

Advanced Access Controls and Deduplication for Privacy in Multimedia Cloud Computing

Chrisel Goveas[1], Gaanashree S[2], Indushree M[3]
Students, B.E. Department of Information Science and Engineering[1,2]
Assistant Professor, Department of Information Science and Engineering[3]
Global Academy of Technology, Bengaluru, India

Abstract: *This work provides a privacy-preserving multi-dimensional media sharing system, SMACD, for portable cloud computing scenarios within the context of widespread media sharing enabled by cloud computing and devices. Attribute-based encryption is used to jumble each media layer, ensuring media privacy and granular access control. To reduce the complexity of the get-to arrangement and adapt to the properties of multi-dimensional media, a multi-level get-to arrangement development with a secret-sharing plot is presented. For both intra-server and inter-server deduplication, decentralized key servers are offered. With cloud computing, databases and application software are moved to sizable data centers, where data and service management may not be entirely reliable. However, this special feature brings up a number of new, poorly understood security challenges. Due to the fact that both user data and applications are on provider premises, cloud computing raises data security problems as neither is entirely contained on the user's machine. Although clouds often have a single architecture, they can have numerous customers with various needs. The solution provided by all cloud providers is to use encryption methods to encrypt the data. To solve every issue, there's also a potential that the cloud service is unreliable.*

Keywords: Multi-dimensional media, scalable access control, secure deduplication.

I. INTRODUCTION

The provision and sharing of high-definition video services on popular mobile devices has been made possible by cloud services like Google Cloud and Microsoft Sky Blue. Although these stages promote comfort, security worries persist, especially when it comes to putting your trust in cloud media centers. Because coordination control is relinquished once content is posted, media wholesalers—who may even have security settings—may be hesitant to fully believe these stages, raising the possibility of a media security vulnerability.

In order to preserve media confidentiality and guarantee authorized access in the context of mobile cloud computing, this worry has led researchers to investigate cryptographic methods. Although both broadcast encryption and identity-based encryption (IBE) have been used, their suitability for large-scale media sharing is called into question because of the widespread distribution of content. ABE (attribute-based encryption), and more especially CP-ABE (ciphertext-policy ABE), appears to be a potential way to address this problem. Media distributors can provide expressive access privileges to media material by enforcing fine-grained access controls based on attributes thanks to CP-ABE.

People's methods of connecting and communicating have evolved as a result of the rapid advancement of portable computing innovation and the wide range of social contact available via portable devices. Multifunctional devices have become indispensable in this context, enabling individuals to obtain information from service providers and easily communicate information with related clients. The dissemination and consumption of media content, particularly videos, via platforms such as YouTube and Netflix is becoming increasingly popular due to the rise of flexible services and the dominance of cloud computing.

A shared pool of reconfigurable computer resources, such as networks, servers, storage, and so forth, can be accessed conveniently and instantly through the use of the cloud computing architecture. Cloud storage was one of the first services provided by the cloud and is still a common solution. A form of networked internet storage known as "cloud storage" stores data in virtualized storage pools that are typically hosted by outside parties. Mobile phones, desktop PCs, and other Internet-connected devices can temporarily cache data stored remotely thanks to cloud storage. In Fig.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

1:System architecture shows the flow of the project .The two most important considerations in this industry are security and pricing, which might differ significantly depending on the vendor selected.

1.1 SYSTEM ARCHITECTURE

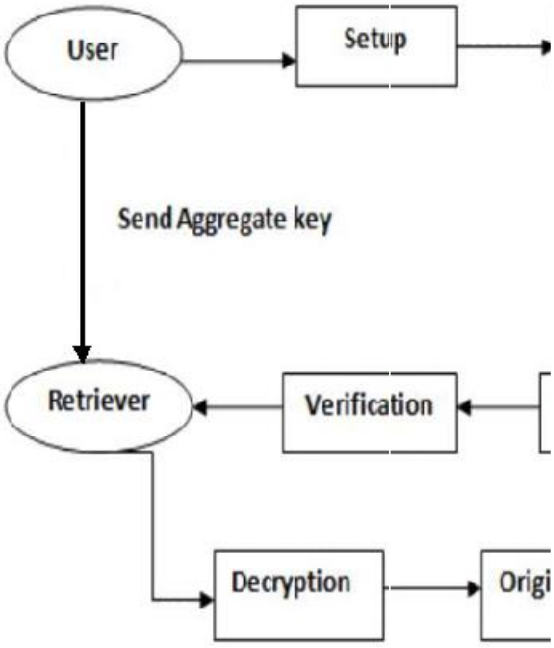

Fig. 1: System a

II. LITERATURE SURVEY

2.1 Scalable Media Encryption

Users of the services are able to post media content. However, the consumer loses control when they upload media from their device to the media center, which leads to privacy concerns . Liu et al. [14] social media sharing strategy with privacy scheme encrypts media data using image-based key whitening and chaotic mapping before compression, keeping the media data unaltered. However, this media encryption algorithm's end-to-end decryption key distribution isn't appropriate for a big number of social users, nor can it handle the fine-grained assignment of data access permissions. Using the video compression standard, media content can be encoded into various levels for flexible adaptability, which can be thought of as multi-layered data [25].

2.2 Scalable Media Access Control

Ma et al. [16] distributed the access keys in a scalable manner based on CP-ABE, thereby proposing a scalable access control system for media sharing in cloud computing. By removing the same characteristics of different access restrictions, this technique can lower the cost of key management while protecting the structure of two-dimensional media material. Ma et al. [17] then suggested an enhanced scalable media access control mechanism, SCP ABE, for arbitrary dimensional scalable media streams in the expanded version of [8]. This approach created a single access tree that was organized by several access policies. As a result, by decrypting various secrets from the tree, different degrees of access rights could be imposed. This design reduces the number of access trees in CP-ABE [20] ,when compared to the conventional access tree.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.3 Secure Media Deduplication

Secure deduplication techniques have been presented as a way to preserve cloud storage capacity in response to the exponential development of media contents. The convergent encryption system, which encrypts a message using a key obtained from the message, was initially presented by Douceur et al. [18]. Thus, the same ciphertexts are generated from the same plaintexts. Message-locked encryption (MLE) is a proposal by Bellare et al. [19] that provides comprehensive security definitions and subsumes convergent encryption. The security concepts of MLE were reinforced by Abadi et al. [21], who took into account the plaintext distributions that are dependent on the public parameters. Nevertheless, MLE is vulnerable to brute-force attacks. For the purpose of deduplication, Bellare et al. [22] suggested a server-aided encryption technique called DupLESS, in which messages are encrypted using message-based keys that are received from a central key server.

This technique has a single point of failure even if it deters brute-force attacks. A decentralized server-aided encryption technique for deduplication with several key servers was presented by Shin et al. [23] in order to overcome the drawbacks of a centralized setup of a single key server. The first secure deduplication method for multi-dimensional media using server-assisted encryption and public keys was presented by Zheng et al. [24]. The settings of decentralized agency servers were also taken into account in this system.

2.4 Privacy-Preserving Media Sharing, Secure Deduplication in Mobile Cloud Computing

A vast amount of media assets, including videos, are shared in mobile networks thanks to cloud computing and mobile devices. While flexible adaptability can be achieved through the use of scalable video coding, media privacy is seriously threatened by cloud computing. In this research, we present SMACD, a multi-dimensional privacy-preserving media sharing technique in mobile cloud calculating. First, attribute-based encryption access policies are used to encrypt every media layer, ensuring both fine-grained access control and media secrecy. We then go over how to design a multi-level access policy with a secret sharing mechanism. It makes sure that mobile users who acquire a media layer at a higher access level are required to meet the requirements of its child layers' access trees at a lower access level, which is less complicated for access policies and in line with the features of multi-dimensional media. Furthermore, we associate distinct access restrictions with the same encrypted media through the introduction of decentralized key servers, which enable both intra-server and inter-server deduplication. Lastly, using real-world datasets, we do an experimental evaluation on a cloud platform and mobile device. The findings show that SMACD reduces processing and storage costs while protecting media privacy from unauthorized parties and cloud media centers.

Advantage- Enhanced Privacy Protection

- SMACD provides granular control over access to media content through attribute-based encryption and multi-level access policies, effectively safeguarding against unauthorized access and enhancing privacy.

Disadvantage- Complexity of Implementation and Management

- Implementing and managing SMACD involves integrating multiple complex components like attribute-based encryption and decentralized key servers, which can increase development and maintenance costs and pose challenges in scalability and operational management.

2.5 Privacy-preserving Cloud Computing on Sensitive Data: a Survey of Method Products and Challenges

It is becoming more and more important to use the cloud to process data on cloud premises in addition to storing it, due to the number of sensitive and personal data that data controllers are collecting. However, security worries about frequent data breaches combined with recently updated legal standards for data protection (such as the General Data Protection Regulation of the European Union) caution against sending sensitive data that isn't protected to public clouds. This survey addresses technologies that enable the privacy-aware outsourcing of sensitive data processing and storage to public clouds in order to address this issue. In particular, and in a novel way, we examine anonymization and data splitting-based masking techniques for outsourced data in addition to the cryptographic techniques discussed in prior surveys. Next, we evaluate different approaches in terms of overhead, influence on data administration, accuracy preservation, and supported operations on the masked outsourced data. Additionally, We provide a list of numerous

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

ongoing studies and products that have made some of the solutions from the poll a reality. Lastly, we list the most important research problems.

Advantage-

Anonymized data offers ease of processing compared to encrypted data and data splitting. With anonymization, masking occurs only at the storage stage, enabling transparent queries without additional overhead for processing. Retrieval and calculations don't require unmasking, eliminating the need for local proxies beyond storage and key management.

Disadvantage-

Anonymized data has drawbacks, including the tendency for calculations to yield approximations rather than precise conclusions. Additionally, keyword searches on anonymized attributes are not feasible. Anonymization is suitable for aggregate computations like statistics but not for queries on individual data, as it alters values while aiming to preserve overall dataset utility. Maintaining aggregate data like variance or mean is possible with certain anonymization techniques, but drawing conclusions about specific individuals from anonymized data would compromise privacy.

2.6 Survey on Privacy-Preserving Methods for Storage in Cloud Computing

The paper addresses the growing reliance on online storage services for data backup and real-time access, highlighting the associated security and privacy concerns due to data being stored off-premises. It focuses on cloud computing as the infrastructure for such services, which offers cost reduction through resource sharing and on-demand provisioning. However, without adequate security and privacy solutions, cloud computing could face significant challenges. The paper specifically discusses privacy issues and analyzes ongoing research aimed at addressing these concerns to ensure the privacy of outsourced data on cloud storage platforms.

Advantage

The paper provides a thorough examination of privacy concerns in cloud storage, offering insights into the evolving landscape of cloud computing and proposing potential solutions. It raises awareness of the importance of privacy in this context and stimulates discussion on privacy-preserving measures.

Disadvantage

While comprehensive, the paper may lack depth in analyzing specific privacy-preserving techniques and practical implementation strategies. Concrete examples or case studies illustrating real-world challenges and solutions could enhance the paper's applicability and effectiveness.

2.7 Secure Data Sharing in Cloud Storage with Key Aggregate Cryptosystem

Emphasizes the benefits of data sharing enabled by cloud systems and highlights the importance of efficient encryption schemes for secure sharing. It discusses the concept of Key-Aggregate Cryptosystem (KAC), which allows for selective and confidential data sharing with minimal ciphertext expansion. Cryptography plays a crucial role in ensuring data confidentiality, integrity, and accuracy. The passage underscores the challenge of effectively sharing encrypted data in cloud storage while maintaining its value, advocating for the ability to grant access rights for direct server access.

Advantage

Cloud systems facilitate convenient and flexible data sharing, enhancing accessibility and collaboration. Encryption schemes like KAC ensure secure sharing while maintaining confidentiality.

Disadvantage

Despite encryption measures, cloud storage introduces security and privacy concerns, including the risk of unauthorized access and data breaches. Challenges may arise in managing access rights and maintaining control over data stored with third-party providers.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.8 Share Your Data Carefree: An Efficient, Scalable and Privacy-Preserving Data Sharing Service in Cloud Computing

Cloud services' strong processing and storage capacities, data sharing has become ingrained in a wide range of applications, such as social networks, e-health, and crowdsourcing transportation systems. It makes sense that sending data to an unreliable cloud would cause privacy violations. One way to mitigate this is by taking use of Secure data sharing using Broadcast Based Searchable Encryption (BBSE). However, there are still issues with the most recent suggested BBSE's efficiency or security. Our research presents ESPD, a method for sharing data over encrypted cloud datasets that is efficient, scalable, and privacy-preserving. Unlike earlier studies, ESPD maintains a fixed ciphertext length regardless of changes in the number of system users and allows sharing of target data to numerous users with different secret keys.

Advantage

EPD offers a scalable, effective, and private-maintaining cloud data exchange platform. It improves search performance and scalability by enabling the dissemination of target data to several users with different secret keys while preserving a constant ciphertext length. The efficacy of the architecture in maintaining file privacy, keyword privacy, and trapdoor privacy is demonstrated by its security analysis.

Disadvantage

ESPD may have trouble being adopted and implemented despite its benefits. Putting the framework into practice and making sure it works with different cloud settings and apps could take a lot of time and experience. Furthermore, even if ESPD increases the scalability and efficiency of searches, there might still be trade-offs in terms of resource usage and computational overhead, especially in large-scale deployments.

2.9 Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network

The growing prevalence of mobile social networks (MSNs) and the difficulties in profile matching—especially with regard to privacy and computational overhead—are covered in the study. The private data of users may be compromised by the high processing needs of current profile-matching techniques. To overcome these issues, the authors suggest a unique cloud-assisted privacy-preserving profile-matching technique. By utilizing cloud computing, the plan seeks to lessen processing load while maintaining data privacy. Personal profiles are encrypted and sent to cloud servers for matching, all while maintaining security protocols to prevent privacy breaches. Based on the honest-but-curious (HBC) model and the assumption of no collaboration between cloud servers, the system is meant to be secure.

Advantage

The proposed cloud-assisted privacy-preserving profile-matching scheme offers an efficient solution to the high computational overhead and privacy concerns associated with current profile-matching schemes. By leveraging cloud computing, the scheme reduces the computational burden on users while ensuring data privacy. It allows users to encrypt their personal profiles and send them to cloud servers for matching, providing scalability and cost-effectiveness.

Disadvantage

Despite its advantages, the scheme introduces reliance on cloud servers, raising concerns about data privacy and security. Users must trust that the cloud servers will not collude to compromise their privacy. Additionally, the effectiveness of the scheme may be contingent on the availability and reliability of cloud services, which could impact its usability and performance in practice.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.10 An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing

The paper presents a novel privacy-preserving approach for efficient and secure data storage and retrieval in cloud environments. By leveraging probabilistic public key encryption techniques, the proposed scheme minimizes computational overhead during encryption and decryption processes while ensuring the confidentiality of the plaintext. Additionally, the incorporation of ranked keyword search functionality enables the cloud server to identify specific keywords and their relevance scores within encrypted files without accessing the plaintext content, thereby reducing communication overhead during file retrieval and facilitating data integrity verification. Security analysis demonstrates the scheme's resilience against various attacks, while performance evaluations confirm its efficiency and superiority over existing approaches. Overall, the proposed approach offers a comprehensive solution to address key challenges in cloud data management, including privacy preservation, communication efficiency, and data integrity verification.

Advantage

The proposed approach offers efficient and secure privacy-preserving data storage and retrieval in cloud environments. By utilizing probabilistic public key encryption techniques, it reduces computational overhead during encryption and decryption processes while ensuring confidentiality. Additionally, the incorporation of ranked keyword search functionality enhances communication efficiency during file retrieval and enables data integrity verification without compromising data privacy.

Disadvantage

Despite its advantages, the approach may require specialized expertise for implementation and integration into existing cloud systems. Additionally, while the scheme enhances privacy and security, there may be trade-offs in terms of computational complexity and performance, particularly in large-scale deployments. Users must also consider potential limitations in the scalability and interoperability of the proposed approach with different cloud environments and applications.

2.11 Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing

The paper introduces a novel framework of Hierarchical Predicate-Conditioned Attribute-Based Encryption (HP-CP-ABE) with efficient authority identification, focusing on data confidentiality and user privacy protection. The key contributions include proposing the HP-CP-ABE framework, which emphasizes efficient authority identification for enhanced security. Additionally, an authority identification method is designed to streamline decryption computations, enabling users to verify their authorization status efficiently. The scheme achieves a constant private key size, reducing transmission and storage costs, and provides a compact security analysis demonstrating anonymity, addressing a gap in existing works

Advantage

The proposed HP-CP-ABE framework with efficient authority identification enhances data confidentiality and user privacy protection, addressing key concerns in secure data sharing.

The constant private key size achieved by the scheme reduces transmission and storage costs, enhancing efficiency in data management.

Disadvantage

Implementing and integrating the proposed framework may require specialized expertise and resources, potentially posing challenges for practical deployment.

While the scheme offers enhanced security and efficiency, its effectiveness may vary depending on the specific use case and environment, necessitating careful consideration of implementation factors.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.12 Data-Matching-Based Privacy-Preserving Statistics and Its Applications in Digital Publishing Industry

As digital media technology advances quickly, more and more individuals are choosing to read e-books instead of print versions of articles.

The digital publishing platform has the capacity to gather and examine vast quantities of reader reading data. The statistical evaluation. The platform's digital assets, which it uses to charge consumers for services, can be thought of as outcomes. Three privacy concerns, however, include readers' reading data, users' statistical choices, and the digital assets of the site. This paper suggests a privacy-preserving statistical approach based on data matching. In order to achieve an effective match between users' statistical preferences and the corresponding reading information of massive readers, as well as statistical analysis of the matching results, the proposed solution combines bloom filters, secret sharing, and perturbing technologies without jeopardizing the privacy of various parties.

Advantage

The article proposes a data-matching-based privacy-preserving statistic scheme, DMSA, tailored for the digital publishing industry. DMSA enables personalized statistical analysis services while safeguarding the privacy of all participants. The scheme facilitates accurate ordering strategies and business plans for service requesters based on the platform's responses. DMSA achieves privacy-preserving data-matching and aggregation through perturbing technology, Bloom filters, and threshold secret sharing. It introduces Mirror Secret Shares and Buddy Edge Devices to enhance system robustness and collusion resistance.

Disadvantage

However, while DMSA offers significant advantages in privacy preservation and robustness, it may require specialized expertise for implementation and could potentially introduce complexities in system management and maintenance. Additionally, the scheme's effectiveness may be contingent on factors such as data volume and user engagement, which could impact its practical utility.

2.13 Privacy Preserving in Image processing on Cloud

The past ten years have seen a sharp increase in cybercrime. Cyberattacks can be carried out on a variety of platforms, with data servers being one of the easiest targets. Users' private documents and other sensitive information were exposed as a result of these assaults. Researchers are concentrating on safe and private image transmission systems as a result of this issue. These systems transfer encrypted photos to cloud servers, avoiding issues with privacy linkage in cloud services. Cloud IaaS, PaaS, and SaaS offer various service kinds, and each one requires a reliable and secure way to protect user data. This survey study compares and discusses the various privacy-preserving techniques used in Image Cloud. Over the past ten years, many techniques Several strategies have been presented in the past ten years; a few are discussed in this survey. Few techniques are centered on maintaining privacy; the majority are concerned with data security. Talk about the main concerns regarding cloud privacy as well. Homomorphism Encryption (HE), Virtual Machine Servers (VMS), Privacy Preservation, IaaS, PaaS, SaaS, and Swift formula.

Advantage

The paper discusses privacy-preserving techniques in image processing on cloud platforms, emphasizing the importance of protecting individual privacy while ensuring data confidentiality. It highlights the limitations of conventional security systems and encryption methods due to key sharing drawbacks and trust violations. The paper proposes image encryption techniques to convert original images into encrypted ones, ensuring confidentiality between users. However, while encryption safeguards data, decryption requires authorized access with a secret key, limiting accessibility. The advantage lies in enhanced data confidentiality and privacy protection through encryption.

Disadvantage

The reliance on secret keys for decryption poses a challenge in managing access and potential key sharing vulnerabilities. Overall, the paper contributes to addressing privacy concerns in image processing on cloud platforms but also highlights the complexities in balancing data security and accessibility.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.14 Privacy preserving data sharing method for social media platforms

To begin with, the program protects the privacy of authorised users by guaranteeing that their identities are hidden when communicating. Users' confidence and privacy within the system are increased as a result. Second, the technique enables effective user revocation without requiring the cloud server to discover the details of the encrypted data or the identities of the revoked users. Data privacy is protected even when user revocation procedures are carried out thanks to this functionality. Fine-grained data access control is another feature of the suggested cryptosystem that permits selective data exchange with specific recipients while safeguarding the identities of authorized recipients.

Advantage

The suggested methodology has a lot to offer identity-based broadcast encryption systems looking to protect user anonymity and data privacy. Legitimate subscribers' privacy is adequately preserved, protecting their identities during communication operations.

Disadvantage

Dependence on cryptographic presumptions such as the random oracle model and the BDHP computational assumption could result in theoretical flaws that could be used in real-world scenarios. During integration, ensuring compatibility and interoperability with current systems and protocols may present difficulties.

2.15 Towards differential access control and privacy-preserving for secure media data sharing in the cloud

In order to improve safe data exchange in cloud contexts, the study presents TFPRE-OT, a new cryptographic primitive. It uses an oblivious transfer protocol to protect requester anonymity and lightweight one-time type keys to streamline access control. The technique achieves differential access control and privacy preservation by fusing TFPRE-OT with watermarking technology. The process resolves conflicts between various security criteria for requesters and data owners, ensuring efficiency and security.

Advantage

The suggested approach introduces TFPRE-OT, which lowers computing overheads and preserves requester privacy through effective key management, streamlining safe data sharing in cloud contexts. Through the incorporation of watermarking technology, it guarantees strong access control and privacy maintenance, thereby satisfying a variety of security needs.

Disadvantage

The methodology's implementation may result in resource demands and complexity, necessitating careful integration and optimization work. Although it improves security and privacy, it might present interoperability and scalability issues, requiring careful assessment and modification for realistic implementation.

2.16 Privacy-Preserving Image Retrieval and Sharing in Social Multimedia Applications

For social multimedia applications, the suggested methodology presents a content-based image retrieval and sharing system that protects privacy. It allows picture owners to safely upload their photos to a public cloud server and gives a social service provider access to a secure index. The strategy functions under a more realistic danger model than earlier models, in which the social service provider is not totally trustworthy and has restricted access to user data, including encryption keys. The methodology's streamlined key management and access control procedures within multi-user social apps is one of its main features. To improve user autonomy and privacy, users with similar photos can submit retrieval queries and decode the results individually. The system also includes a secure index that is intended to retrieve photos from enormous databases in an efficient manner.

Advantage

The approach allows for improved user autonomy and privacy when it comes to content-based picture sharing and retrieval for social multimedia apps. By using a secure index maintained by a social service provider and providing

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

secure image outsourcing to a public cloud server, it improves data privacy and retrieval effectiveness. Users are empowered by streamlined access controls, and massive dataset retrieval is made efficient by dynamic updates that guarantee scalability and constant lookup times.

Disadvantage

Despite the social service provider's limited access, trust issues might still exist, which would undermine user confidence. There may be difficulties with integration and implementation complexity, especially with relation to scalability and secure indexing techniques. With the growth of user bases and picture repositories, continuous optimization efforts might be needed to preserve retrieval efficiency. Therefore, it is necessary to carefully evaluate trust and scalability challenges while boosting privacy and user autonomy.

2.17 Disclose More and Risk Less: Privacy Preserving Online Social Network Data Sharing

Through three primary contributions, the methodology described in this research aims to address privacy problems in social network data sharing. First, the self-disclosure rate is introduced as a metric to measure the leaking of user secrets in the published network. The authors employ a social-attribute network model to characterize both the social network data and the attacker's knowledge. Second, they define a privacy-preserving social network data sharing issue that balances privacy guarantees with user self-disclosure value to thwart inference assaults. This optimization issue allows for variable self-disclosure evaluation to meet a variety of demands and scenarios while taking into account a variety of user concerns.

Advantage

The approach provides a thorough framework for handling privacy issues with social network data sharing. In order to measure and reduce user secret leakage while increasing user self-disclosure value with privacy guarantees, it presents new metrics and formulations. Experiments on real datasets confirm the flexibility and efficiency of the distinct sharing mechanisms proposed.

Disadvantage

Disadvantage of the methodology is that it might need a lot of computer power and experience to implement. It may be difficult to strike a balance between user value and privacy goals, and there may be little room for generalization from studies using real-world datasets. Though it seems promising, thorough verification and practical limitations must be taken into account.

2.18 A Selective Privacy-Preserving Approach for Multimedia Data

The methodology outlined in the paper addresses resource and time-delay constraints in multimedia systems by transforming them into concrete mathematical expressions for simplified theoretical analysis. A single objective optimization problem is formulated, integrating constraints of time delay and resources to determine the maximum total privacy weights from a set of variables, including data package types, privacy weights for each package, and operation times for encrypted and non-encrypted data. Additionally, the paper proposes a data-split-based encryption method to safeguard against malicious cloud activities. This approach ensures efficient resource allocation and timely processing while prioritizing privacy concerns in multimedia systems, offering a systematic solution to optimize performance and security simultaneously.

Advantage- The methodology provides multimedia systems with a methodical way to handle resource and time-delay restrictions. By streamlining theoretical analysis and facilitating effective resource allocation, privacy concerns are prioritized through optimization. Security against malevolent cloud operations is improved by the suggested data-split-based encryption technique.

Disadvantage- Major resources and experience may be needed for implementation. Theoretical discoveries may prove difficult to apply in practice, and the complexity of encryption and optimization may drive up expenses. For deployment to be effective, integration with current systems may provide difficulties that need to be carefully considered.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

III. RESEARCH GAP AND FUTURE DIRECTIONS

- Develop and deploy end-to-end encryption techniques to ensure privacy of the shared media content.
- Implement secure deduplication methods, considering the multi dimensional nature of media and attempt to reduce cloud storage.
- The media is first encoded into multiple layers with the SVC standard, and each layer is then encrypted with advanced SHA-512algorithm.
- The consumer can decrypt the encrypted media layers by satisfying their access policies and decode them into media content .

3.1 FUTURE DIRECTIONS

- Advanced Encryption Techniques: To strengthen media content privacy beyond SHA-512, investigate homomorphic encryption or lattice-based cryptography.
- Tailored Deduplication Techniques: To reduce the amount of cloud storage needed, create content-based deduplication algorithms that are designed for multi-dimensional media.
- Scalability and Performance Optimization: To increase efficiency and scalability, make use of distributed computing and cloud-native technologies.
- Continuous Security Assessments: To address new threats and weaknesses, evaluate and upgrade encryption methods and security protocols on a regular basis.

By taking these actions, the goals of guaranteeing media privacy, safe deduplication, and effective sharing in cloud environments will be advanced

IV. CONCLUSION

After multi-dimensional extension, shared media information in setting is typically encoded into multiple layers with varying quality. Greater difficulties arise for maintaining data confidentiality and enforcing owner-enforced access control. Additionally, we accomplish attribute-based ciphertext deduplication within and between servers, allowing for the possibility of assigning distinct access restrictions to the same encrypted media layer. According to the experimental evaluation, our technique is more practicable for private media sharing in cloud computing because it has lower computational, communication, and storage overhead than comparable schemes.

REFERENCES

[1]. 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. keywords: {Media;Cloud computing;Videos;Privacy;Access control;Encryption;Multi-dimensional media;scalable access control;secure deduplication;mobile cloud computing},

[2]. Z. Zhang, F. Zhou, S. Qin, Q. Jia and Z. Xu, "Privacy-Preserving Image Retrieval and Sharing in Social Multimedia Applications," in IEEE Access, vol. 8, pp. 66828-66838, 2020, doi: 10.1109/ACCESS.2020.2984916. keywords: {Cryptography;Image retrieval;Access control;Feature extraction;Indexes;Privacy;Cloud computing;Image retrieval;image sharing;multimedia;privacy-preserving},

[3]. L. Xu, T. Bao, L. Zhu and Y. Zhang, "Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks," in IEEE Transactions on Multimedia, vol. 21, no. 3, pp. 591-602, March 2019, doi: 10.1109/TMM.2018.2887019. keywords: {Privacy;Social network services;Access control;Loss measurement;Face;Simulation;Tuning;Social trust;anonymization;privacy preserving;photo sharing;online social networks},

[4]. S. Badsha, I. Khalil, X. Yi and M. Atiquzzaman, "Designing Privacy-Preserving Protocols for Content Sharing and Aggregation in Content Centric Networking," in IEEE Access, vol. 6, pp. 42119-42130, 2018, doi: 10.1109/ACCESS.2018.2856299. keywords: {Privacy;Cryptography;Routing protocols;Cryptographic protocols;Access control;Statistical analysis;CCN;privacy;publishers;consumers;content},

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

[5]. D. Yang, B. Qu and P. Cudré-Mauroux, "Privacy-Preserving Social Media Data Publishing for Personalized Ranking-Based Recommendation," in IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 3, pp. 507-520, 1 March 2019, doi: 10.1109/TKDE.2018.2840974. keywords: {Data privacy;Social network services;Publishing;Distortion;Privacy;Engines;Loss measurement;Privacy-preserving data publishing;customized privacy protection;personalization;ranking-based recommendation;social media;location based social networks},

[6]. W. Tang, J. Ren and Y. Zhang, "Enabling Trusted and Privacy-Preserving Healthcare Services in Social Media Health Networks," in IEEE Transactions on Multimedia, vol. 21, no. 3, pp. 579-590, March 2019, doi: 10.1109/TMM.2018.2889934. keywords: {Medical services;Social network services;Privacy;Resists;Collaboration;Servers;Social media healthcare networks;trust;privacy preservation;bloom filter;collaborative filtering;sybil attack},

[7]. J. Chen, J. He, L. Cai and J. Pan, "Disclose More and Risk Less: Privacy Preserving Online Social Network Data Sharing," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 6, pp. 1173-1187, 1 Nov.-Dec. 2020, doi: 10.1109/TDSC.2018.2861403. keywords: {Privacy;Data privacy;Authorization;Servers;Feature extraction;Social networking (online);Risk management;Inference attack;online social network;privacy;data sharing},

[8]. C. Ma, Z. Yan, and C. W. Chen, "Attribute-based multi-dimensionscalable access control for social media sharing," in 2016 IEEEInternational Conference on Multimedia and Expo (ICME), 2016, pp.1–6.

[9]. Y. Qu, S. Yu, W. Zhou, S. Chen and J. Wu, "Customizable Reliable Privacy-Preserving Data Sharing in Cyber-Physical Social Networks," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 1, pp. 269-281, 1 Jan.-March 2021, doi: 10.1109/TNSE.2020.3036855. keywords: {Privacy;Differential privacy;Diseases;Human factors;Social networking (online);Cyber-physical social network;customizable privacy protection;differential privacy;attack-proof.},

[10]. Q. Li, Y. Tian, Y. Zhang, L. Shen and J. Guo, "Efficient Privacy-Preserving Access Control of Mobile Multimedia Data in Cloud Computing," in IEEE Access, vol. 7, pp. 131534-131542, 2019, doi: 10.1109/ACCESS.2019.2939299. keywords: {Encryption;Cloud computing;Mobile handsets;Access control;Privacy;Mobile multimedia data;access control;CP-ABE;partially hidden policy;online/offline encryption;efficient decryption},

[11]. L. Lyu, S. C. -K. Chau, N. Wang and Y. Zheng, "Cloud-Based Privacy-Preserving Collaborative Consumption for Sharing Economy," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1647-1660, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3010235. keywords: {Cloud computing;Privacy;Protocols;Collaboration;Cryptography;Data privacy;Data aggregation;Cloud-based privacy-preserving;collaborative consumption;sharing economy;homomorphic cryptosystems},

[12]. J. H. Abawajy, M. I. H. Ninggal and T. Herawan, "Privacy Preserving Social Network Data Publication," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1974-1997, thirdquarter 2016, doi: 10.1109/COMST.2016.2533668. keywords: {Social network services;Data privacy;Publishing;Privacy;Media;Joining processes;Electronic mail;Social network data;Privacy attacks;Anonymized graphs;Privacy preserving;data privacy},

[13]. J. Shen, H. Yang, P. Vijayakumar and N. Kumar, "A Privacy-Preserving and Untraceable Group Data Sharing Scheme in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2198-2210, 1 July-Aug. 2022, doi: 10.1109/TDSC.2021.3050517. keywords: {Servers;Cloud computing;Security;Distributed databases;Data privacy;Protocols;Data models;Data sharing;oblivious random access memory;cloud computing;multiple users},

[14]. H. Li, K. Wang, X. Liu, Y. Sun and S. Guo, "A Selective Privacy-Preserving Approach for Multimedia Data," in IEEE MultiMedia, vol. 24, no. 4, pp. 14-25, October-December 2017, doi: 10.1109/MMUL.2017.4031322. keywords: {Encryption;Data privacy;Streaming media;Data models;Data analysis;Computer crime;Big data;Resource management;Handheld devices;Computer security;multimedia data;security levels;privacy weights;time constraints;resource constraints;security;big data;data analysis;cybercrime}.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

[15]. K. Liu, M. Li, and X. Li, "Hiding Media Data via Shaders: EnablingPrivate Sharing in the Clouds," in 2015 IEEE 8th InternationalConference on Cloud Computing, 2015, pp. 122–129.

[16]. 16 .C. Ma and C. W. Chen, "Secure media sharing in the cloud:Two-dimensional-scalable access control and comprehensive key management," in 2014 IEEE International Conference on Multimedia and Expo (ICME), 2014, pp. 1–6.

[17]. C. Ma, Z. Yan, and C. W. Chen, "Scalable Access Control For Privacy-Aware Media Sharing," IEEE Transactions on Multimedia,vol. 21, no. 1, pp. 173–183, Jan. 2019.

[18]. J. R. Douceur, A. Adya, W. J. Bolosky, P. Simon, and M. Theimer,"Reclaiming space from duplicate files in a serverless distributed file system," in Proceedings 22nd International Conference on Distributed Computing Systems, 2002, pp. 617–624.

[19]. M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-Locked Encryption and Secure Deduplication," in Advances in Cryptology EUROCRYPT 2013, 2013, pp. 296–312.

[20]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in 2007 IEEE Symposium on Security and Privacy (SP '07), 2007, pp. 321–334.

[21]. M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev,"Message-Locked Encryption for Lock-Dependent Messages," in Advances in Cryptology CRYPTO 2013, 2013, pp. 374–391.

[22]. M. Bellare, S. Keelveedhi, and T. Ristenpart, "DupLESS: Serveraided Encryption for Deduplicated Storage," in Proceedings of the 22nd USENIX Conference on Security, 2013, pp. 179–194.

[23]. Y. Shin, D. Koo, J. Yun, and J. Hur, "Decentralized Server-aided Encryption for Secure Deduplication in Cloud Storage," IEEETransactions on Services Computing, pp. 1–1, 2018.

[24]. Y. Zheng, X. Yuan, X. Wang, J. Jiang, C. Wang, and X. Gui, "Toward Encrypted Cloud Media Center With Secure Deduplication," IEEE Transactions on Multimedia, vol. 19, no. 2, pp. 251–265, Feb. 2017.

[25]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data,"in Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98

[26]. M. Ambrosin, C. Busold, M. Conti, A.-R. Sadeghi, and M. Schunter, "Updaticator: Updating Billions of Devices by an efficient, Scalable and Secure Software Update Distribution over Untrusted Cache-enabled Networks," in Computer Security - ESORICS 2014, 2014, pp. 76–93.

[27]. "Vimeo Case Study," https://cloud.google.com/customers/vimeo.

[28]. J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan,"Secure sharing and searching for real-time video data in mobile cloud," IEEE Network, vol. 29, no. 2, pp. 46–50, Mar. 2015.

[29]. Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing," IEEE Access, vol. 6, pp. 36 584–36 594, 2018.

[30]. Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. 2011. Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems, IEEE Trans. on, 22(5), 847-859