WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhancing Data Security in Cloud Computing through the Implementation of Revocable Storage and Identity-Based Encryption

[1]S. Subash, [2]Dr. S.Subatra Devi, [3]Dr. C. Priya

[1]PG Student, Department of Computer Applications, Dr. M.G.R Educational and Research Institute, Chennai, TamilNadu, India subashbala842@gmail.com

[2]Professor, Faculty of Computer Applications, Dr. M.G.R Educational and Research Institute, Chennai, TamilNadu, India subathra.mca@drmgrdu.ac.in

[3]Associate Professor, Faculty of Computer Applications, Dr. M.G.R Educational and Research Institute, Chennai, TamilNadu, India priya.mca@drmgrdu.ac.in

DOI: https://doi.org/10.55248/gengpi.5.0524.1290

ABSTRACT

Secure data sharing in cloud computing is a pressing concern, given the rising reliance on cloud services for sensitive information storage. One potential solution involves employing revocable storage and identity-based encryption techniques. Revocable storage systems allow organizations to retract access to data, crucial for maintaining privacy in sectors like healthcare and finance. Identity-based encryption simplifies key management by using user identities as encryption keys, enhancing security and streamlining processes. Combining these methods offers a potent solution for secure cloud data sharing, reducing unauthorized access risks. This approach is particularly valuable in sectors prioritizing data privacy, such as healthcare and government. Future research may focus on refining revocable storage systems and exploring novel encryption methods. Integrating these technologies into existing cloud infrastructures could optimize data sharing experiences while upholding stringent security standards.

Keywords---revocable keys, secure file storage, encryption, ECDSA (Elliptical Curve Digital Signature Algorithm), sharing

1. INTRODUCTION

TripleTechSoft LLP is an India leader for trusted HR and related products and services. We create a positive influence on the lives of our clients, partners, and workforce through our work.We do this every day by enhancing their financial security, productivity and relationships within their own teams, and how they take on their interactions with the world. At TripleTechSoft LLP, we bring more life to people. TripleTechSoft LLP is a part of $2 billion Briley group. The Briley group has substantial interests in Aviation, Hospitality & ITES. TripleTechSoft LLP is exposed to the best international practices in each of the service businesses it offers to clients.

TripleTechSoft LLP is a pioneer in delivering trusted end-to-end HR Services in Payroll, Staffing (temping), Compliances, Search & Selections (Recruitments) and Training, we have become a vendor by choice for large MNC's, and SME's.

Our reputation has flourished over the years, becoming synonymous with excellence, dependability, and exceptional system and process quality. We take pride in our dynamic, driven team, whose relentless pursuit of excellence continually raises the bar for performance, ensuring lasting customer satisfaction.

Team TripleTechSoft LLP fosters the spirit of team work in ensuring that our clients view us as partners in their businesses. Tailored to each client's distinct requirements and business environment, our HR services strive to optimize HR expenditures while advocating for the interests of both employers and employees through unbiased expert advice. Supported by state-of-the-art technology, our offerings are customized to enhance your HR initiatives. We harness our expertise in HR and technology development to craft solutions tailored to your specific needs.

2. LITERATURE SURVEY

The cloud environment is increasingly favored by researchers, academia, government sectors, and businesses due to its minimal upfront capital investment and maximum scalability. However, despite its numerous benefits, data protection remains a primary concern in information security and cloud computing. While various solutions have been developed to address this challenge, there is a need for a comprehensive analysis of these solutions. This article presents a comparative and systematic study, offering an in-depth analysis of leading techniques for secure data sharing and protection in the cloud. Each technique is discussed, including its functioning, potential solutions, core information, achievements, scope, gaps, and future directions. Additionally, a comprehensive and comparative analysis of these techniques is provided, followed by a discussion on their applicability to meet

requirements. Finally, research gaps and future directions in the field are identified and reported.The authors believe that this article's contribution will operate as a catalyst for the potential researchers to carry out the research work in the area.

In the present national network environment, publishing is open to anyone. As an important information resource, knowledge files reflect the workload of publishers. Moreover, high-quality knowledge files can promote the progress of society. However, pirated inferior files have the opposite effect. At present, most organizations use centralized servers to centrally manage the knowledge files released by users. The inclusion of an untrusted third party to inspect and encrypt file contents results in a non-transparent process for storing file transactions,tampering with intellectual copyright, and the inability to have consistent systems of file management among institutions due to the lack of uniform standards for the same intellectual files. The aim of this paper is twofold: ensuring secure storage of knowledge files while facilitating efficient sharing of copyrighted content. To achieve this, the paper proposes a method that integrates NDN (Named Data Network) technology with a distributed blockchain and Interplanetary File System (IPFS). This blockchain-based approach utilizes NDN for file content signature and encryption, separating security from transmission processes. Additionally, it employs flexible NDN routing strategies and an IPFS private storage network to enhance data storage security. Furthermore, the method leverages consensus among participating nodes and blockchain synchronization for file sharing and traceability. The paper outlines the method's structure, principles, file upload, and transfer process, followed by performance comparison and evaluation. Finally, it summarizes the method's strengths, weaknesses, and future research directions.

We introduce Charon, a cloud-based storage system designed to securely, reliably, and efficiently store and share large datasets across multiple cloud providers and storage repositories while adhering to legal requirements for handling sensitive personal data. Charon offers three key features: (1) it operates without the need to trust any single entity, (2) it eliminates the necessity for client-managed servers, and (3) it effectively manages large file transfers across geographically dispersed storage services. Additionally, we have developed a novel Byzantine-resilient data-centric leasing protocol to prevent write-write conflicts when multiple clients access shared repositories. To assess Charon's performance, we conducted evaluations using both micro and application-based benchmarks, simulating workflows commonly encountered in bioinformatics, a significant domain for big data applications.. The results show that our unique design is not only feasible but also presents an end-to-end performance of up to 2.5×2.5× better than other cloud-backed solutions.

Sanjeev Kumar Dwivedi Priyadarshini Roy

Industry 4.0 integrates cutting-edge technologies like cloud computing, the Internet of Things (IoT), machine learning and artificial intelligence (ML/AI), and blockchain to enhance automation within industrial processes and also bridges the gap between the physical and digital worlds through the cyber-physical system. The inherent nature of IoT devices is transforming industries into smart ecosystems, known as Industrial IoT (IIoT), through data-driven decision-making policies. However, challenges such as decentralization, security and privacy vulnerabilities, single points of failure (SPOF), and trust issues persist within IoT systems. Blockchain emerges as a promising technology to address these challenges. This article investigates the integration of IoT with blockchain technology and offers an in-depth examination of blockchain-enabled IoT and IIoT systems. State-of-the-art research is categorized into techniques for data storage and management, big data and cloud computing (including finance and data auditing), and various industrial sectors (such as supply chain, energy, and healthcare). The paper also presents insightful discussions based on these categories. Specifically, it introduces IoT and IIoT, followed by a discussion on the necessity of smart contracts within these systems.Next, we concentrate on the convergence of blockchain and IoT with state-of-the-art research. Furthermore, this article outlines open avenues for future research within this domain, accompanied by noteworthy observations. The advent of cloud infrastructure has markedly diminished the expenses associated with hardware and software resources within computing infrastructure.

. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption.Nonetheless, ensuring quick search and maintaining data confidentiality poses a significant challenge for cloud service providers, as users expect prompt results without compromising data security. To address these issues, we introduce a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. Our solution not only facilitates attribute-based keyword search but also supports attribute-based data sharing concurrently, distinguishing it from existing solutions that typically offer only one of these features. Moreover, our scheme allows for keyword updates during the sharing phase without the need for interaction with the PKG. In this article, we expound on the concept of CPAB-KSDS and its security model, propose a concrete scheme, and demonstrate its resistance against chosen ciphertext and chosen keyword attacks in the random oracle model. Finally, we showcase the practicality and efficiency of our proposed construction through performance and property comparisons.

3. EXISTING SYSTEM

In the Existing System, AKE(authenticated key exchange)scheme is more efficient than others since they are only based on hash operations, but cannot provide perfect forward secrecy and untraceability, additional, these two schemes can notResist offline password guessing attack once the information stored in smart card is compromised. These schemes cannot provide perfect forward secrecy, use the server's public key and cannot achieve user's anonymity if an adversary can know the information stored in smart card. Therefore, the proposed two-factorauthentication scheme is more practical than other schemes.

4. PROPOSED SYSTEM

The proposed system focuses on improving the current work in terms of comfort maintenance and violation detection, believe in value is used to determine the colleagues balance in the group In a data sharing company, colleagues initiate data evaluation based on their belief in its value, where trust in professionalism determines the credibility of the assessment.These Proposed method ECDSA (Elliptical Curve Digital Signature Algorithm) ie., the group key agreement of two-factor data security protection mechanism for cloud storage system, in which a data sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use both his/her secret key and a security device to gain access to the data. Our solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked, the corresponding ciphertext will be updated automatically by the cloud server without any notice of the data owner. Additionally, we provided security validation and efficiency analysis for our system.

5. MODULES

LOGIN MODULE

It is the module which is used for login purpose. In this module the admin or member type their user-name and their password .If both username and password is match with what is in the database then it goes to the next module.

ADMIN AUTHENTICATION MODULE

Admin authentication is used to login the admin. It is used to verify he/she is admin. In case they are not admin they can only search but admin can also access the search engine. The admin module also have an important process of giving an approve to each image uploaded by member. Only if admin gives approve from this module the image gets stored in content module or else the image doesn't get stored in database.

REGISTRATION MODULE

Registration Module is the module which is used to upload each and every information of every member. Once the information are entered it gets stored in database. Once the member details are entered it displays the message that message has been send to mail.

SEARCHING MODULE

A module that is used to select whether the user have to search by image search or by Textual search.

SEARCHING MODULE-TEXTUAL SEARCH

A software application designed to locate and identify database items matching user-specified keywords or characters, particularly useful for locating specific websites on the Internet.

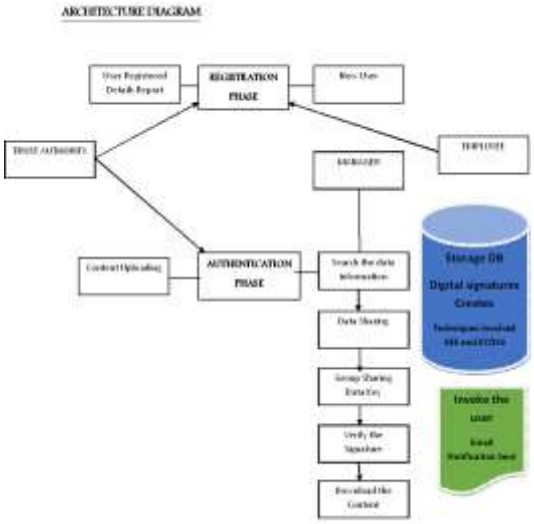
CONTENT MODULE

Content Module is one in which a both Admin, Trust Authority and Employee used to upload images to the website and they used to give tag names,its description and divide its category and etc…It is used to upload any types of image but not video files.

DATA SHARING MODULE

Trust Authority is sending the request to employee, because they wants some information to a particular employee details... If he accept their request then one OTP messages sent through their mail with respect to the receiver. If these OTP will be matched automatically the information can be download and view their details.

5. Architecture Diagram



6. FUTURE WORK

In our future work, we suggest that the best of our knowledge, we firstly present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. Combined verifiable computation and encrypt-then-mac mechanism with our ciphertext-policy attribute-based hybrid encryption, we could delegate the verifiable partial decryption paradigm to the cloud server. In addition, the proposed scheme is proven to be secure based on k-multilinear Decisional Diffie-Hellman assumption. Conversely, our scheme is implemented using integer values. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, we could apply it to ensure the data confidentiality, the fine grained access control and the verifiable delegation in cloud.

7. CONCLUSION

In this project, we evolved a new architecture, IDBAS as a basic attempt to create a traffic and energy efficient encrypted keyword search tool on to cloud storages. We began with the introduction of a basic scheme that we compared to previous encrypted search tools for cloud computing and we presented their inefficiency in a mobile cloud conditions. IDBAS is more time and energy consuming than keyword search over plain-text, but simultaneously it saves significant energy related to traditional strategies promoting a similar security level. Based on enhanced AES, this work can be expanded for more other novel implementations. We have proposed a single keyword search scheme to make encrypted data search capable. However, there are possible extensions of our present work remaining.

REFERENCES

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, “Simultaneoushardcore bits and cryptography against memory attacks,” in Proc.6th Theory Cryptography Conf., 2009, pp. 474–495.

[2] S. S. Al-Riyami and K. G. Paterson, “Certificateless public keycryptography,” in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003,pp. 452–473.

[3] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, “Certificate based(linkable) ring signature,” in Proc. Inf. Security Practice ExperienceConf., 2007, pp. 79–92.

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang,“Malicious KGC attacks in certificateless cryptography,” in Proc.2nd ACM Symp. Inf., Comput. Commun. Security, 2007, pp. 302–311.

[5] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols andatomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. CryptographicTechn., 1998, pp. 127–144.

[6] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryptionwith efficient revocation,” in Proc. ACM Conf. Comput. Commun.Security, 2008, pp. 417–426.

[7] D. Boneh, X. Ding, and G. Tsudik, “Fine-grained control of securitycapabilities,” ACM Trans. Internet Techn., vol. 4, no. 1, pp. 60–82, 2004.

[8] D. Boneh and M. Franklin, “Identity-based encryption from theWeil pairing,” in Proc. 21st Annu. Int. Cryptol. Conf., 2001, pp. 213–229.

[9] R. Canetti and S. Hohenberger, “Chosen-ciphertext secure proxyre-encryption,” in Proc. ACM Conf. Comput. Commun. Security,2007, pp. 185–194.

[10] H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang, "NCCloud: A network-coding-based storage system in a cloud-of-clouds," IEEETrans. Comput., vol. 63, no. 1, pp. 31–44, Jan. 2014.

[11] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security-mediatedcertificateless cryptography," in Proc. 9th Int. Conf. Theory PracticePublic-Key Cryptography, 2006, pp. 508–524.