



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: III Month of publication: March 2021

DOI: <https://doi.org/10.22214/ijraset.2021.33513>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage

V. S. Sureshkumar¹, B. Balakumaran², K. G. Hari Krishna³, S. Kishore⁴, B. Prasanth⁵

¹Assistant Professor, ^{2,3,4,5}UG Students – Final Year, , Department of Computer Science and Engineering, Nandha College of Technology, Perundurai, Tamilnadu, India

Abstract: People endorse the good power of cloud computing, but cannot fully trust the cloud suppliers to host privacy-sensitive info, as a results of the absence of user-to-cloud controllability. To verify confidentiality, info householders supply encrypted info rather than plaintexts. To share the encrypted files with various users, Cipher text-Policy Attribute-based writing (CP-ABE) might even be used to conduct fine-grained and owner-centric access management. But this doesn't sufficiently become secure against various attacks. Many previous schemes did not grant the cloud provides the flexibility to verify whether or not or not a downloader can decipher. Therefore, these files need to be getable to everyone accessible to the cloud storage. A malicious wrongdoer can transfer thousands of files to launch Economic Denial of property (EDoS) attacks, that's in a very position to principally consume the cloud resource. The money dealer of the cloud service bears the expense. Besides, the cloud provider serves every as a results of the controller and together the recipient of resource consumption fee, lacking the transparency to info householders. These concerns need to be resolved in real-world public cloud storage. Throughout this paper, we have a tendency to tend to propose an answer to secure encrypted cloud storages from EDoS attacks and supply resource consumption answerableness. It uses CP-ABE schemes in associate extraordinarily black-box manner and complies with capricious access policy of CP-ABE. We have a tendency to tend to gift two protocols for various settings, followed by performance and security analysis.

Keywords: Ciphertext-Policy Attribute-based Encryption (CP-ABE), access control, public cloud storage, accounting, privacy preserving.

I. INTRODUCTION

Cloud storage has several edges, like always-online, pay-as-you-go, and cheap. Throughout these years, additional information square measure outsourced to public cloud for persistent storage, together with personal and business documents. It brings a security concern to information homeowners the ultimate public cloud isn't trusty, and therefore the outsourced information shouldn't be leaked to the cloud supplier while not the permission from information homeowners. Several storage systems use server dominated access management, like password-based and certificate-based authentication. They to a fault trust the cloud supplier to safeguard their sensitive information. The cloud suppliers and their staff will scan any document in spite of information owners' access policy. Besides, the cloud supplier will exaggerate the resource consumption of the file storage and charge the payers additional while not providing verifiable records, since we tend to lack a system for verifiable computation of the resource usage.

II. PROBLEM STATEMENT

In this paper, we have a tendency to mix the cloud-side access management and therefore the existing knowledge owner-side CP-ABE based mostly access management, to resolve the same security issues in privacy protective cloud storage. Our methodology will stop the EDoS attacks by providing the cloud server with the power to ascertain whether or not the user is permitted in CP-ABE based mostly theme, while not unseaworthy different info. For our cloud-side access management, we have a tendency to use CP-ABE encryption/ coding game as challenge-response. Whereas transfer Associate in nursing encrypted file, the info owner first off generates some random challenge plaintexts and therefore the corresponding cipher texts. The cipher texts square measure associated with constant access policy with the precise file. For Associate in nursing incoming knowledge user, the cloud server asks him/her to rewrite every which way selected challenge cipher text. If the user shows an accurate result, which implies he/she is permitted in CP-ABE, the cloud-side access management permits the file transfer.

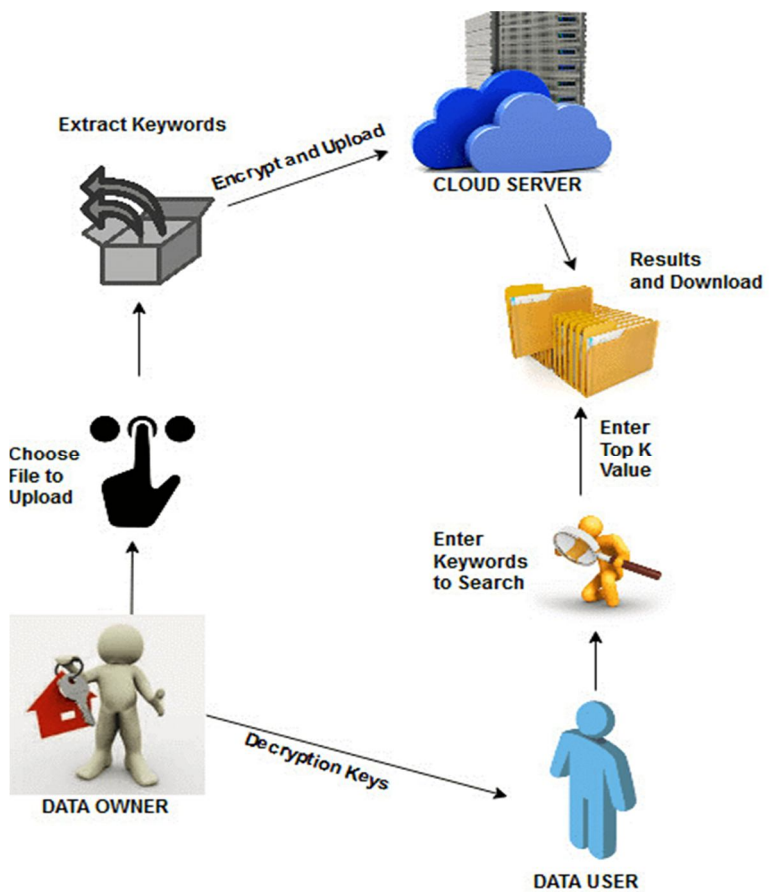


Figure 1 System Architecture

III. LITERATURE SURVEY

O'Pass is economical and reasonable compared with the standard internet authentication mechanisms. Generalized digital certificate for user authentication and key institution for secure communications Public-key digital certificate has been wide used in public-key infrastructure (PKI) to provide user public key authentication. However, the public-key digital certificate itself can't be used as a security factor to manifest user. Throughout this paper, we propose the conception of generalized digital certificate (GDC) which will be used to give user authentication and key agreement. A GDC contains user's public information, just like the data of user's digital licence, the data of a digital credentials, etc., and a digital signature of the final public information signed by a trustworthy certificate authority (CA). However, the GDC doesn't contain any user's public key. Since the user doesn't have any personal and public key try, key management in mistreatment GDC is much simpler than mistreatment public-key digital certificate. The digital signature of the GDC is utilized as a secret token of each user which will ne'er be disclosed to any verifier. Instead, the owner proves to the champion that he has the data of the signature by responding to the verifier's challenge. Supported this concept, we propose each distinct power (DL)-based and integer resolving (IF)-based protocols which will accomplish user authentication and secret key institution. To thwart parole stealing and parole recycle attacks. O Pass solely needs everycollaborating website possesses a singular sign, and involves a telecommunication service supplier in registration and recovery phases. Through o Pass, users solely have to remember a long parole for login on all websites. When evaluating the o Pass paradigm, we believe o Pass is economical and cheap compared with the normal net authentication mechanisms. Generalized digital certificate for user authentication and key institution for secure communications Public-key digital certificate has been wide utilised in public-key infrastructure (PKI) to supply user public key authentication. However, the public-key digital certificate itself can't be used as a security factor to certify user. Throughout this paper, we propose the idea of generalized digital certificate (GDC) which will be accustomed give user authentication and key agreement. A GDC contains user's public information, just like the information of user's digital licence, the information of a digital credentials, etc., and a digital signature of the final public information signed by a trusty certificate authority (CA). However, the GDC doesn't contain any user's public key.

Since the user doesn't have any personal and public key try, key management in mistreatment GDC is much simpler than mistreatment public-key digital certificate. The digital signature of the GDC is utilized as a secret token of each user which will ne'er be unconcealed to any verifier. Instead, the owner proves to the supporter that he has the information of the signature by responding to the verifier's challenge. Supported this concept, we propose each separate exponent (DL)-based and integer resolution (IF)-based protocols which will come through user authentication and secret key institution.

IV. ALGORITHM

Algorithm: Existing algorithm: Symmetric encryption algorithm Our CECS system utilizes symmetric encryption, public key encryption, digital signature, and PEKS to comprehend the function and security goals. During this section, we briefly review these cryptographic primitives. Symmetric encryption (SE) may be a cryptographic primitive that encrypts data or decrypts cipher texts with the identical secret key. Symmetric encryption may be a style of encryption where only 1 key (a secret key) is employed to both encrypt and decrypt electronic information. By using symmetric encryption algorithms, data is converted to a form that can't be understood by anyone who doesn't possess the key to decrypt it. Proposed algorithm: Digital signature algorithm A digital signature (DS) may be a cryptographic primitive for identifying digital information supported public-key encryption technology. The signer uses his private key to sign a message and publishes his public key. The verifier can prove that the signature belongs to the signer with the signer's public key. CP-ABE: Ciphertext-Policy Attribute-based-Encryption CP-ABE could be a public key coding theme with fine grained access management. In CP-ABE, each user has some attributes and information homeowners encode their files with AN access policy over attributes. Users in the system hold their own secret keys associated with their attribute sets. If and providing the user satisfies the access policy, the user will decipher. Some helpful definitions in CP-ABE as follows: Attributes: Attributes depict the party's properties relevant to access management. For example, students in technology at Berkeley could have attribute set and students in atomic number 55 at USTC could have attribute set. Policy: A policy could be a predicate over the attributes. as an example, the policy (EE CS) allows those students higher than to access, but none of them satisfy the policy (CS Berkeley). Syntax: CP-ABE for security parameter λ N and messages $m \in \mathbb{G}$ consists of PPT (probabilistic polynomial time) algorithms $\text{ABE} = (\text{Setup}, \text{KeyGen}, \text{Enc}, \text{Dec})$ as follows: • $(\text{mpk}, \text{msk}) \leftarrow \text{Setup}$ generates a master public key mpk and a passkey msk. • $\text{ski} \leftarrow \text{KeyGen}(\text{msk}, A_i)$. It takes the master secret key msk and therefore the user's attribute set A_i because the input and generates a secret key ski related to the attribute set A_i . • $\text{ct} \leftarrow \text{Enc}(\text{mpk}, m, A)$. It takes the master public key mpk, the message m, and therefore the access policy A because the input. It outputs the ciphertext ct. • $m = \text{Dec}(\text{ski}, \text{ct})$. It takes the ciphertext ct (encrypted with access policy A) and therefore the secret key ski as input. If the attribute set A_i satisfies the access policy A, it outputs the message m. Otherwise, outputs. Correctness, Security and therefore the Construction: The definitions and formal proofs of correctness and security, and CP-ABE achieve indistinguishability below chosen-plaintext attacks.

V. MODULE

A. Module Description

- 1) *Cloud Storage*: Cloud storage has many benefits, like always-online, pay-as-you-go, and cheap. During these years, more data are outsourced to public cloud for persistent storage, including personal and business documents. It brings a security concern to data owners the general public cloud isn't trusted, and therefore the outsourced data mustn't be leaked to the cloud provider without the permission from data owners. Many storage systems use server-dominated access control, like password-based and certificate-based authentication. They overly trust the cloud provider to shield their sensitive data. The cloud providers and their employees can read any document irrespective of data owners' access policy. Besides, the cloud provider can exaggerate the resource consumption of the file storage and charge the payers more without providing verifiable records, since we lack a system for verifiable computation of the resource usage.
- 2) *Attribute Based Encryption*: Data owners who store files on cloud servers still want to regulate the access on their own hands and keep the info confidential against the cloud provider and malicious users. Encryption isn't sufficient. To feature the confidentiality guarantee, data owners can encrypt the files and set an access policy in order that only qualified users can decrypt the document. With Cipher text-Policy Attribute-based Encryption (CP-ABE), we will have both fine-grained access control and robust confidentiality. However, this access control is simply available for data owners, which seems to be insufficient. If the cloud provider cannot authenticate users before downloading, like in many existing CP-ABE cloud storage systems, the cloud has got to allow everyone to download to confirm availability. This makes the storage system liable to the resource-exhaustion attacks. If we resolve this problem by having data owners authenticate the downloaders before allowing them to download, we lose the flexibleness of access control from CP-ABE.

- 3) *Resource Consumption Accountability*: In the pay-as-you-go model, users pay money to the cloud provider for storage services. The fee is set by resource usage. However, CP-ABE based schemes for cloud storage access control doesn't make online confirmations to the info owner before downloads. It's needed for the cloud service provider to convince the payers about the particular resource usage. Otherwise, the cloud provider can charge more without being discovered.
- 4) *Distributed Denial of Services*: The cryptography-driven access control doesn't protect the cloud provider against many other attacks. Since the cloud provider doesn't conduct the access control, it cannot stop those unauthorized users. One attack that's originated from this limitation is Distributed Denial of Services (DDoS). The ability of DDoS attacks has been showed to incur significant resource consumption in CPU, memory, I/O, and network. The attacks can exist publicly clouds. In, the limitation of cloud-side static resource allocation model is analysed, including the chance of Economic Denial of Sustainability (EDoS) attacks, which is that the case of DDoS attacks within the cloud setting in, or the Fraudulent Resource Consumption (FRC) attack. These attacks are intended to interrupt the budget of public cloud customers. Some existing works attempt to mitigate EDoS attacks. In, the authors proposed a mitigation technique by verifying whether a call for participation comes from a cloud user or is generated by bots.

VI. CONCLUSION

In this paper, we propose a combined the cloud-side and data owner-side access control in encrypted cloud storage, which is proof against DDoS/EDoS attacks and provides resource consumption accounting. Our system supports arbitrary CP-ABE constructions. The development is secure against malicious data users and a covert cloud provider. We relax the safety requirement of the cloud provider to covert adversaries, which may be a more practical and relaxed notion than that with semi-honest adversaries. To form use of the covert security, we use bloom filter and probabilistic sign on the resource consumption accounting to cut back the overhead. Performance analysis shows that the overhead of our construction is little over existing systems.

VII. FUTURE WORK

Use of the covert security, we have a tendency to use bloom filter and probabilistic sign in the resource consumption accounting to scale back the overhead. Performance analysis shows that the overhead of our construction is tiny over existing systems.

REFERENCES

- [1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.
- [2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, no. 1, pp. 69–73, 2012.
- [3] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," *Computers & Security*, vol. 69, pp. 84–96, 2017.
- [4] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," *IEEE Transactions on Image Processing*, vol. 25, no. 7, pp. 3411–3425, 2016.
- [5] H.-M. Sun, Y.-H. Chen and Y.-H. Lin, "o Pass: A user authentication protocol resistant to password stealing and password reuse attacks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 651–663, 2012.
- [6] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2372–2379, 2011.
- [7] V. Sekar and P. Maniatis, "Verifiable resource accounting for cloud computing services," in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*. ACM, 2011, pp. 21–26.
- [8] C. Chen, P. Maniatis, A. Perrig, A. Vasudevan, and V. Sekar, "Towards verifiable resource accounting for outsourced computation," in *ACM SIGPLAN Notices*, vol. 48, no. 7. ACM, 2013, pp. 167–178.
- [9] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 2007, pp. 321–334.
- [10] B. Waters, "Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography– PKC 2011*. Springer, 2011, pp. 53–70.
- [11] Nandagopal S, Arunachalam VP, Karthik S, "A Novel Approach for Mining Inter-Transaction Itemsets", *European Scientific Journal*, Vol.8, pp.14-22, 2012.
- [12] Gokulraj P and Kiruthikadevi K, "Revocation and security based ownership deduplication of convergent key creating in cloud", *International Journal of Innovative Research in Science, Engineering and technology*. Vol. 3, Issue 10, ISSN: 2319-8753, October 2014.
- [13] E. Prabhakar, V. S. Sureshkumar, Dr. S. Nandagopal, C. R. Dhivyaa, Mining Better Advertisement Tool for Government Schemes Using Machine learning " , *International Journal of Psychosocial Rehabilitation*, Vol.23, Issue.4, pp. 1122-1135, 2019
- [14] Vijayakumar M, Prakash s, "An Improved Sensitive Association Rule Mining using Fuzzy Partition Algorithm", *Asian Journal of Research in Social Sciences and Humanities*, Vol.6, Issue.6, pp.969-981, 2016.
- [15] Prakash S, Vijayakumar M, " Risk assessment in cancer treatment using association rule mining techniques", *Asian Journal of Research in Social Sciences and Humanities*, Vol.6, Issue.10, pp.1031-1037, 2016.



- [16] Prabhakar E, “ Enhanced adaboost algorithm with modified weighting scheme for imbalanced problems, The SIJ transaction on Computer science & its application, Vol.6, Issue.4, pp.22-26, 2018.
- [17] Nandagopal S, Malathi T, “Enhanced Slicing Technique for Improving Accuracy in Crowd Sourcing Database”, International Journal of Innovative Research in Science, Engineering and Technology, Vol.3, Issue.1, pp.278-284, 2014
- [18] Prabhakar E, Santhosh M, Hari Krishnan A, Kumar T, Sudhakar R,” Sentiment Analysis of US Airline Twitter Data using New Adaboost Approach” ,International Journal of Engineering Research & Technology (IJERT), Vol.7, Issue.1, pp.1-6, 2019
- [19] Dr.C.R. Dhivyaa, R. Sudhakar, K. Nithya and E. Prabhakar “Performance Analysis of Convolutional Neural Network for Retinal Image Classification”, International Journal of Psychosocial Rehabilitation, Vol. 23, no.4, pp.1149-1159, November 2019.
- [20] S Nandagopal, S Karthik, VP Arunachalam,” Mining of meteorological data using modified apriori algorithm”, European Journal of Scientific Research , Vol. 47, no.2, pp. 295-308, 2010.
- [21] P Gokulraj, K Kiruthika-Devi,” Revocation and security based ownership deduplication of convergent key creating in cloud”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, no.10, pp16527-16533, October 2014.
- [22] Karthik.S. Nandagopal.S, Arunachalam.V.P.,” Mining of Datasets with Enhanced Apriori Algorithm”, Journal of Computer Science, Vol. 8, no.4, pp599-605, 2012.
- [23] Nandagopal.S. Malathi.T.,” Enhanced Slicing Technique for Improving Accuracy in Crowd Sourcing Database”, International Journal of Innovative Research in Science, Engineering and Technology) , Vol. 3, no.1, pp278-284,2014.
- [24] V Dharani S Thiruvenkatasamy, P Akhila, V Arjitha, K Bhavadharani,” A MD5 Algorithm Approach to Monitor Village Using Mobile Application”, South Asian Journal of Engineering and Technology, Vol. 8, no.s1, 2019.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)