iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6109

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

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

Arati Kale[1], Sarika Kajale[2], Mansi Raj[3], Aishwarya Thakare[4]
[1, 2, 3, 4]*DR. D. Y. Patil College Of Engineering Ambi, Maharashtra*

Abstract: ***People endorse the great power of cloud computing, but cannot entirely trust the cloud suppliers to host privacy-sensitive information, because of the absence of user-to-cloud controllability. to form certain confidentiality, information owners supply encrypted information instead of plaintexts. To share the encrypted files with different users, Ciphertext-Policy Attribute-based secret writing (CP-ABE) is also accustomed conduct fine-grained and owner-centric access management. but this does not sufficiently become secure against different attacks. many previous schemes did not grant the cloud provider the ability to verify whether or not or not a downloader can decipher. Therefore, these files have to be compelled to get on the market to everyone accessible to the cloud storage. A malicious wrongdoer can transfer thousands of files to launch Economic Denial of property (EDoS) attacks, that is ready to principally consume the cloud resource. The money dealer of the cloud service bears the expense. Besides, the cloud provider serves every as a result of the capitalist and conjointly the recipient of resource consumption fee, lacking the transparency to information owners. These issues have to be compelled to be resolved in real-world public cloud storage. throughout this paper, we tend to tend to propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption answerability. It uses CP-ABE schemes in associate degree passing black-box manner and complies with impulsive access policy of CP-ABE. we tend to tend to gift two protocols for varied 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 many edges, like always-online, pay-as-you-go, and low price. Throughout these years, a great deal of data unit of measurement outsourced to public cloud for persistent storage, additionally as personal and business documents. It brings a security concern to info householders the overall public cloud is not trustworthy , and so the outsourced info mustn't be leaked to the cloud provider whereas not the permission from info householders. many storage systems use server-dominated access management, like password-based and certificate-based authentication. They too trust the cloud provider to safeguard their sensitive info. The cloud suppliers and their employees can browse any document despite info owners' access policy. Besides, the cloud provider can exaggerate the resource consumption of the file storage and charge the payers a great deal of whereas not providing verifiable records, since we've got an inclination to lack a system for verifiable computation of the resource usage wanting forward to this server-dominated access management is not secure. info householders UN agency store files on cloud servers still got to manage the access on their own hands and keep the information confidential against the cloud provider and malicious users. secret writing is not comfy. to feature the confidentiality guarantee, info householders can write in code the files associate degreed set AN access policy therefore only qualified users can decipher the document. With Ciphertext-Policy Attribute-based secret writing (CP-ABE) we have a tendency to square measure able to have every fine-grained access management and strong confidentiality. However, this access management is just out there for info householders, that appears to be short. If the cloud provider cannot proof users before downloading, like in many existing CP-ABE cloud storage systems, the cloud has to allow everyone to transfer to create positive convenience. This makes the storage system at risk of the resource-exhaustion attacks. If we've got an inclination to resolve this disadvantage by having info householders proof the transferer's before allowing them to transfer, we've got an inclination to lose the plasticity of access management from CP-ABE. Here lists the two problems got to be addressed in our work.

II. MOTIVATION OF THE PROJECT

Some data sharing protocols have been proven and analyzed for security but some of them can only be applied to the key agreement between two entities and need a large amount of resources to perform calculations. Motivated by the above observation, the key agreement protocol is applicable to support data sharing in cloud computing. The generation of a common conference key is performed in a public channel, which is suitable for cloud computing environments.

III. PROPOSED SYSTEM

In this project, we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE. We present two protocols for different settings, followed by performance and security analysis

IV. LITERATURE SURVEY

1) *Paper Name:* Efficient k-NN Query over Encrypted Data in Cloud with Limited Key-disclosure and Offline Data Owner
a) *Author Name:* Lu Zhouc, Youwen Zhua,b,*, Aniello Castiglioned
b) *Description:* In this paper, we propose a new scheme to perform k-NN query over encrypted data in cloud while protecting the privacy of both data owner and query users from cloud. Our new method just reveals limited information about data owner's key to query users, and has no need of an online data owner. For gaining the properties, we present a new scalar product protocol, then the new protocol and some other transformation approaches are merged into our secure k-NN query system. Additionally, we confirm our security and efficiency through theoretical analysis and extensive simulation experiments.

2) *Paper Name:* oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks
a) Author Name: Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin
b) *Description:* Text password is the most popular form of user authentication on websites due to its convenience and simplicity. However, users' passwords are prone to be stolen and compromised under different threats and vulnerabilities. Firstly, users often select weak passwords and reuse the same passwords across different websites. Routinely reusing passwords causes a domino effect; when an adversary compromises one password, she will exploit it to gain access to more websites. Second, typing passwords into untrusted computers suffers password thief threat. An adversary can launch several password stealing attacks to snatch passwords, such as phishing, keyloggers and malware. In this paper, we design a user authentication protocol named oPass which leverages a user's cellphone and short message service to thwart password stealing and password reuse attacks. oPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through oPass, users only need to remember a long-term password for login on all websites. After evaluating the oPass prototype, we believe oPass is efficient and affordable compared with the conventional web authentication mechanisms.

3) *Paper Name:* Securing SIFT: Privacy-preserving Outsourcing Computation of Feature Extractions over Encrypted Image Data
a) *Author Name:* Shengshan Hu, Qian Wang, Jingjun Wang, Zhan Qin, and Kui Ren,
b) *Description:* This observation has recently aroused new research interest on privacy-preserving computations over outsourced multimedia data. In this paper, we propose an effective and practical privacy-preserving computation outsourcing protocol for the prevailing scale-invariant feature transform (SIFT) over massive encrypted image data. We first show that previous solutions to this problem have either efficiency/security or practicality issues, and none can well preserve the important characteristics of the original SIFT in terms of distinctiveness and robustness. We then present a new scheme design that achieves efficiency and security requirements simultaneously with the preservation of its key characteristics, by randomly splitting the original image data, designing two novel efficient protocols for secure multiplication and comparison, and carefully distributing the feature extraction computations onto two independent cloud servers. We both carefully analyze and extensively evaluate the security and effectiveness of our design. The results show that our solution is practically secure, outperforms the state-of-theart, and performs comparably to the original SIFT in terms of various characteristics, including rotation invariance, image scale invariance, robust matching across affine distortion, addition of noise and change in 3D viewpoint and illumination

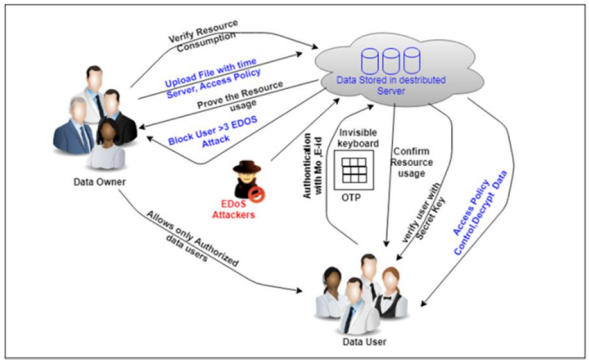
4) *Paper Name:* Security Challenges for the Public Cloud
a) *Author Name:* Kui Ren, Cong Wang, and Qian Wang
b) *Description:* Cloud computing represents today's most exciting computing paradigm shift in information technology. However, security and privacy are perceived as primary obstacles to its wide adoption. Here, the authors outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment.

5) Paper Name: Verifiable Resource Accounting for Cloud Computing Services

a) Author Name: Vyas Sekar

b) Description: In this multiplexing may cause providers to incorrectly attribute resource consumption to customers or implicitly bear additional costs thereby reducing their cost-effectiveness. Our position in this paper is that for cloud computing as a paradigm to be sustainable in the long term, we need a systematic approach for verifiable resource accounting. Verifiability here means that cloud customers can be assured that (a) their applications indeed physically consumed the resources they were charged for and (b) that this consumption was justified based on an agreed policy. As a first step toward this vision, in this paper we articulate the challenges and opportunities for realizing such a framework.

V. ARCHITECTURE DIAGRAM

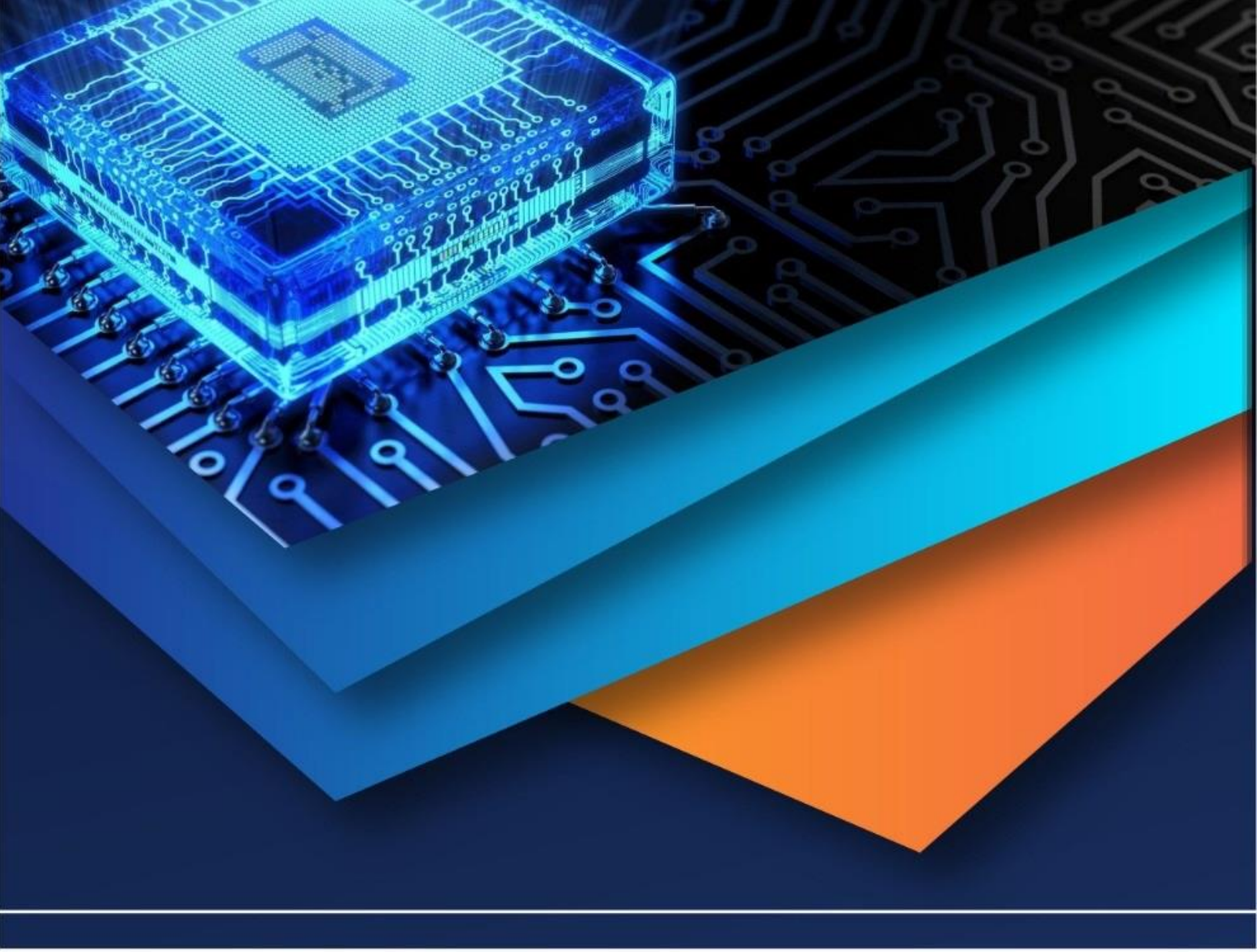


VI. CONCLUSION

In this paper, we have a tendency to tend to propose a combined the cloud-side and knowledge owner-side access management in encrypted cloud storage, that is proof against DDoS/EDoS attacks and provides resource consumption accounting. Our system supports absolute CP-ABE constructions. the event is secure against malicious information users and a covert cloud provider. we have a tendency to tend to relax the protection demand of the cloud provider to covert adversaries, which can be a extra wise and relaxed notion than that with semi-honest adversaries. to make use of the covert security, we have a tendency to use bloom filter and probabilistic register the resource consumption accounting to chop back the overhead. Performance analysis shows that the overhead of our construction is no 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, "oPass: 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, "Ciphertext-policy attributebased encryption," in 2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, 2007, pp. 321–334.
[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography– PKC 2011. Springer, 2011, pp. 53–70.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY