JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhancing Cost-Effective Anonymous Data Sharing through Improved Authentication

Manthan Kasle[1], Raju Kamble[2], Ganesh Kandakure[3], Kushal Kolambe[4],
Department of E&TC, SKNCOE, SPPU, Pune
[1]manthankaslemk@gmail.com, [2]rdkambleiitb@gmail.com
[3]kandakureganesh@gmail.com [4]kushalkolambe22@gmail.com

ABSTRACT : Cloud computing, commonly referred to as "the cloud," provides users with instant access to remote servers, networks, and data centers, enabling the analysis of data in a way that is beneficial to society and individuals. However, sharing data with multiple parties can present problems related to efficiency, data integrity, and owner privacy. One potential solution is the use of ring signatures to create an anonymous and trustworthy data-sharing system. For cloud-based analytics, this enables data owners to verify their data anonymously. Identity-based (ID) ring signatures are gaining popularity as an alternative to traditional public-key encryption (PKI), as the time and cost of verifying certificates is a bottleneck in PKI. The research found that encrypting ID-based ring signatures with a variant of SHA-384 and adding forward security significantly increases their security. The padding technique in newer versions of SHA divides the input text into 512-byte blocks and appends the length as a 48-bit number at the end of the hash, which ensures that signatures created with a compromised secret key are still valid. This feature is crucial for large-scale data sharing systems, as it is difficult to require all data owners to re-verify their data if a single user's secret key is compromised. The paper describes a practical and effective implementation of this method, validates its security, and provides a proof of concept. The upgraded SHA-384 approach has proven to be safer for anonymous data exchange in the cloud.

1. **Keywords -** Cloud computing, Remote servers, SHA-384, Forward security, Anonymous data exchange, Valid signatures.

I. INTRODUCTION :

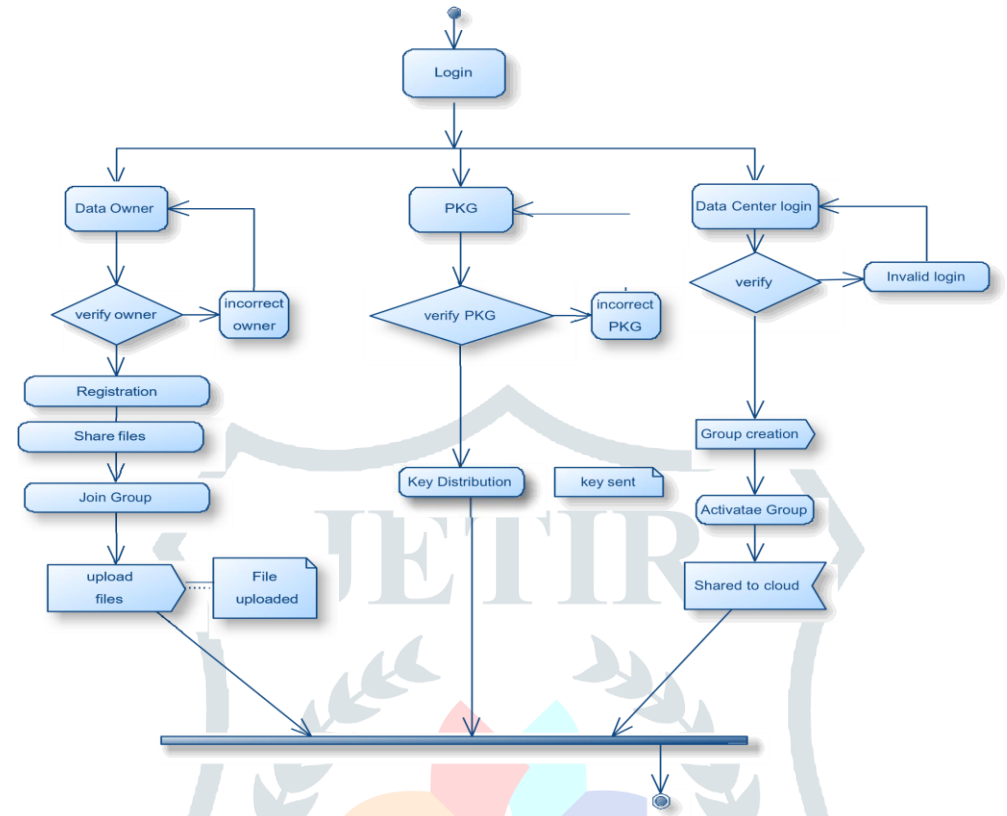
Cloud computing has revolutionized the way data is stored and processed in today's world. It provides users with instant access to a network of remote servers, networks, and data centers, making it easier to analyze large amounts of data in a way that benefits society and individuals. However, sharing data with many people can pose significant challenges, such as data integrity, efficiency, and owner privacy. Ring signatures are emerging as a potential solution to these challenges, as they enable the creation of a trustworthy and anonymous data-sharing system for cloud-based analytics. Identity-based (ID) ring signatures have gained popularity as an alternative to traditional PKI-based public-key encryption.

In a public key infrastructure (PKI), the process of verifying certificates can be time-consuming and expensive, making it a bottleneck for large-scale data sharing. ID-based ring signatures can shorten the time required for certificate verification. This research focuses on improving the security of ID-based ring signatures through the encryption of a variant of SHA-384 and the addition of forward security. Forward security is a critical feature for a large-scale data sharing system since it ensures that even if a user's secret key is compromised, any signatures that used that user's key before the compromise remain valid.

In this paper, we describe a practical and effective implementation of our method, validate its security, and provide proof of concept. Our upgraded SHA-384 approach has proven to be a safer solution for anonymous data exchange in the cloud.

II. Methodology

ID-based ring signatures offer a significant advantage over conventional public key-based ring signatures in large-scale scenarios, as they do not require the authentication of certificates for every user, thereby reducing the time and computational resources required for verification. Overall, ID-based cryptography and ring signatures offer a powerful tool for anonymous authentication and secure communication.



Ring signatures can be used in energy data sharing scenarios to ensure both the anonymity of the data source and the veracity of the data. In this scenario, the energy data owner (Bob) selects a group of users to form a ring based on their public identifying information. Bob then uploads his personal information along with a ring signature and the identification information of all ring members. By validating the ring signature, anyone can verify that the data was provided by a legitimate resident among the ring members without being able to identify the resident. This verification process is efficient and does not require certificate verification

III. Result and Discussion

With inputs from system design, the system is first developed in small programs called units, which are integrated with the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing. Figure a represents the user registration form and Figure c represents the Data Owner Login Page.

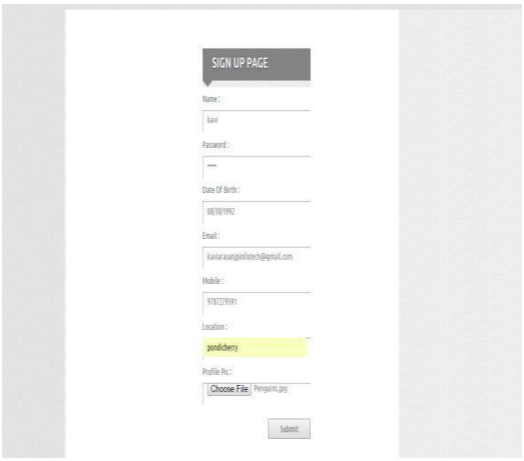


Figure: (a) User Registration and (b) Data Owner Login

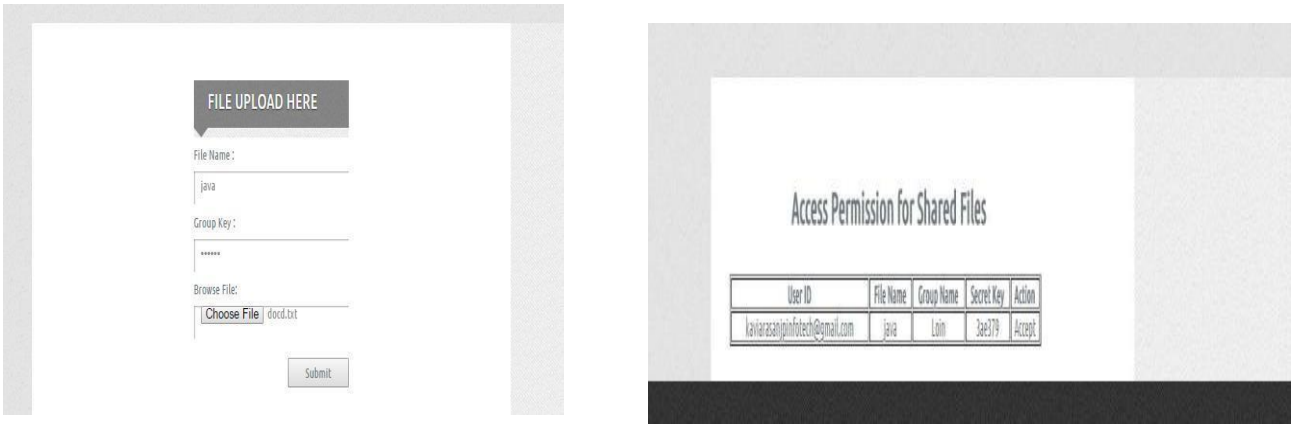


Figure: (c) File Upload (d) Access Permission for shared file

IV. CONCLUSION

The proposed attribute-based data sharing approach allows for fine-grained data access control, strengthening data security and privacy in cloud systems against various threats. To solve the key escrow issue, a secure two-party computation is used to produce secret user keys, which also makes the key authority and cloud service provider semi-trusted. The addition of weighted attributes enhances the expression of the attribute and reduces access structure complexity, ultimately reducing encryption and storage costs for encrypted data. This proposed work effectively controls data access in the sharing system, and securely manages user data in a dynamic and scalable manner. Experimental results show that the proposed method is more efficient and secure, requiring less encryption time and less storage space from the cloud service provider. Future iterations may include attribute-based data sharing with proxy re-encryption and searchable attribute-based encryption, which are being researched to facilitate data exchange using various techniques.

V. ACKNOWLEDGEMENT

We are pleased to present the initial project report on Enhancing Cost-Effective Anonymous Data Sharing through Improved Authentication. We would like to express our gratitude to our internal guide, Mr R. D. Kamble, for providing us with all the necessary assistance and guidance. Their helpful suggestions were very much appreciated. We would also like to thank Dr. S.K.Jagtap, Head of Electronics and Telecommunications Engineering Department, SKNCOE, for her invaluable support and suggestions. We are grateful to our Principal, Dr. A.V. Deshpande, for his constant support and motivation, which greatly contributed to the success of this project

VI. REFERENCES

[1] R. Loh and V. L. L. Thing, “Data Privacy in Multi-Cloud: An Enhanced Data Fragmentation Framework,” 2021 18th Int. Conf. Privacy, Secur. Trust. PST 2021, 2021, doi: 10.1109/PST52912.2021.9647746.

[2] H. Yan and W. Gui, “Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage with User Privacy Preserving,” IEEE Access, vol. 9, pp. 45822–45831, 2021, doi: 10.1109/ACCESS.2021.3066497.

[3] I. El Ghoubach, R. Ben Abbou, and F. Mrabti, “A secure and efficient remote data auditing scheme for cloud storage,” J. King Saud Univ.-Comput. Inf. Sci., vol. 33, no. 5, pp. 593–599, Jun. 2021, doi: 10.1016/J.JKSUCI.2019.02.011.

[4] S. Uthayashangar, P. Dhamini, M. Mahalakshmi, and V. Mangayarkarasi, “Efficient group data sharing in cloud environment using honey encryption,” 2019 IEEE Int. Conf. Syst. Comput. Autom. Networking, ICSCAN 2019, Mar. 2019, doi: 10.1109/ICSCAN.2019.8878759.

[5] S. Li, J. Liu, G. Yang, and J. Han, “A Blockchain-Based Public Auditing Scheme for Cloud Storage Environment without Trusted Auditors,” Wirel. Commun. Mob. Comput., vol. 2020, 2020, doi: 10.1155/2020/8841711.

[6] M. S. Salek et al., “A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications,” IEEE Internet Things J., vol. 9, no. 11, pp. 8250– 8268, Jun. 2022, doi: 10.1109/JIOT.2022.3152477.

[7] R. Leszczyna, "Standards on cyber security assessment of smart grid," Int. J. Crit. Infrastruct. Prot., vol. 22, pp. 70–89, Sep. 2018, doi: 10.1016/J.IJCIP.2018.05.006.

[8] "Microsoft Hohm Helps Consumers Save Money and Energy -Landis+Gyr." https://www.landisgyr.eu/news/microsoft-hohm-helps-consumers-save-money-andenergy/ (accessed Jul. 10, 2022).

[9] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 196 LNCS, pp. 47–53, 1985, doi: 10.1007/3-540-39568-7_5/COVER/.

[10] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2248, pp. 552–565, 2001, doi: 10.1007/3-540-45682-1_32/COVER/.

[11] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad- 33 | P a g e hoc groups," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2442, pp. 465–480, 2002, doi: 10.1007/3-540-45708- 9_30/COVER/.

[12] X. Wu, H. Ling, H. Liu, and F. Yu, "A privacy-preserving and efficient byzantine consensus through multi-signature with ring," Peer-to-Peer Netw. Appl. 2022 153, vol. 15, no. 3, pp. 1669–1684, Mar. 2022, doi: 10.1007/S12083-022-01317-4.

[13] S. Chow and S. Yiu, Efficient Identity Based Ring Signature, vol. 2004. 2004.

[14] X. Huang et al., "Cost-effective authentic and anonymous data sharing with forward security," IEEE Trans. Comput., vol. 64, no. 4, pp. 971–983, 2015, doi: 10.1109/TC.2014.2315619.

[15] X. Peng, K. Gu, Z. Liu, and W. Zhang, "Traceable Identity-Based Ring Signature for Protecting Mobile IoT Devices," 2021, pp. 158–166.

[16] S. Badrinarayanan, D. Masny, and P. Mukherjee, "Efficient and Tight Oblivious Transfer from PKE with Tight Multi-user Security," 2022, pp. 626–642.

[17] N. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, and K. Sakurai, "A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity,"