

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Hybrid Two-Tier Framework for Enhancing Security in Cloud Environment

Prashanth Kumar J¹, Sarath Kumar M C², Srinivasan E³, Balachander K⁴

U.G[B.E] Students, Velammal Institute of Technology, Chennai, Tamil Nadu, India ^{1,2,3},

Assistant Professor, Velammal Institute of Technology, Chennai, Tamil Nadu, India ⁴

ABSTRACT: A crossover homomorphic encryption that consolidates fully homomorphic encryption (FHE) applications. In this model, messages are scrambled with an Algorithm and calculations on encoded information are completed utilizing FHE after homomorphic unscrambling. To acquire productive homomorphic unscrambling, crossover plot joins FHE Algorithm without convoluted message cushioning with FHE with an extensive number message space. A technique with lessen the level of the exponentiation circuit at the cost of extra public keys. As an autonomous intrigue to get a non-specific strategy for changing over from private-key FHE to public key FHE. The way how to transform any additively homomorphic private-key encryption scheme into a public-key homomorphic encryption scheme when the message. To apply this method, the private-key FHE needs to be compact which means that the length of a homomorphically generated encryption is independent of the number of cipher texts from which it was created. An additive homomorphic encryption is converted from private-key to public key by adding a number of encryptions of zero and one to the public key.

KEYWORDS: Fully homomorphic encryption (FHE), *Message Scrambling*, *Public Key*, *Private Key*, *Message Space*.

I. INTRODUCTION

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance. Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand. Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing. Homomorphic encryption is a form of encryption that allows computation on cipher texts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The purpose of homomorphic encryption is to allow computation on encrypted data. Cloud computing platforms can perform difficult computations on homomorphically encrypted data without ever having access to the unencrypted data. Homomorphic encryption can also be used to securely chain together different services without exposing sensitive data. Services from different companies can calculate 1) the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services. Homomorphic encryption can also be used to create other secure systems such as secure voting systems, collision-resistant hash functions, and private information retrieval schemes. We remark that our technique solves the open problem of when the FHE message space is Z for large. We convert the double modulo reduction into a depth-3 circuit, and then, we apply the technique. Our improved technique plays an important role in this method, as the parameters depend heavily on the homomorphic capacity of FHE. We also present a generic method for converting from a private-key FHE to a public key FHE using our hybrid scheme.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

II. LITERATURE REVIEW

In 2016, Ning Cao, Cong Wang, Ming Li, KuiRen, and Wenjing Lou proposed a technique. The first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. We further use “inner product similarity” to quantitatively evaluate such similarity measure.

In 2014, Qingji Zheng, Shouhuai Xu, and Giuseppe Ateniese proposed a common technique for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as: How should a data owner grant search capabilities to the data users? How can the authorized data users search over a data owner’s outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf?

In 2011 Yanjiang Yang, Haibing Lu, and JianWeng proposed how to outsourcing their databases to the cloud and authorizing multiple users for access represents a typical use scenario of cloud storage services. In such a case of database outsourcing, data encryption is a good approach enabling the data owner to retain its control over the outsourced data. Searchable encryption is a cryptographic primitive allowing for private keyword based search over the encrypted database.

In 2016, Zhihua Xia, Xiongfei Wang, Xinghua Sun, and Qijie Wang proposed. Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval.

In 2014, Wenhai Sun, Shucheng Yu, Wenjing Lou, Y Thomas Hou, and HuiLi Search had proposed over encrypted data is a critically important enabling technique in cloud computing, where encryption-before outsourcing is a fundamental solution to protecting user data privacy in the untrusted cloud server environment. Many secure search schemes have been focusing on the single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and managed by a single owner, typically based on symmetric cryptography.

III. PROPOSED SYSTEM

➤ SYSTEM DESIGN

In this approach, the cipher text expansion ratio is only two or three regardless of the message size. Moreover, the decryption circuit is very shallow when the FHE allows large integers as messages. For example, the decryption circuit over has a multiplicative depth of nine under a FHE with the message space. We can reduce the depth further by representing the secret exponent e as log binary vectors of length, which is an improvement over. Homomorphic encryption is the encryption scheme which means the operations on the encrypted data. Homomorphic encryption can be applied in any system by using various public key algorithms.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

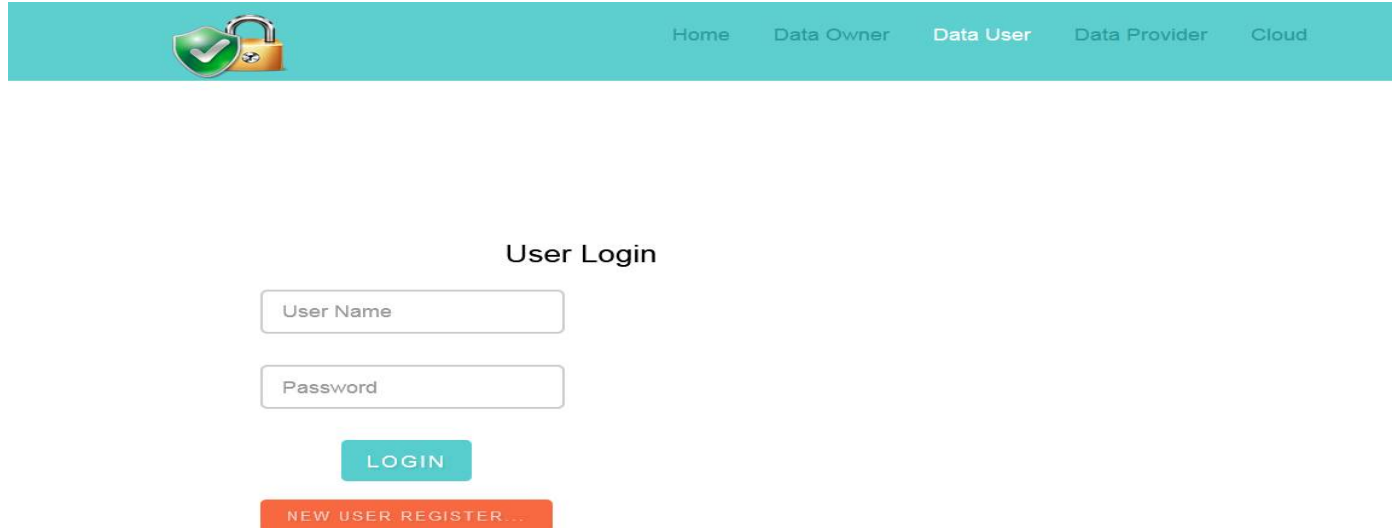
F. FILE RECOVERY

If user file may be corrupt or may be delete. So if user delete any file from server, user can recover the deleted files from file server. It is very useful to all cloud users. If user to recover the deleted file, user login and get the deleted file.

➤ PROPOSED ALGORITHM

We explore an alternative method that encrypts messages with a FHE Algorithm and converts them into FHE-cipher Texts for homomorphic computations. In this approach, the cipher Text expansion ratio is only two or three regardless of the message size. Moreover, the decryption circuit is very shallow when the FHE allows large integers as messages. For example, the decryption circuit over has a multiplicative depth of nine under a FHE with the message space. We can reduce the depth further by representing the secret exponent e as log binary vectors of length, which is an improvement over. the purpose of homomorphic encryption is to allow computation on encrypted data. Thus data can remain confidential while it is processed, enabling useful tasks to be accomplished with data residing in untrusted environments. Homomorphic encryption is the encryption scheme which means the operations on the encrypted data. Homomorphic encryption can be applied in any system by using various public key algorithms.

IV. RESULTS



The screenshot shows a web application interface with a teal header. On the left of the header is a lock icon with a green checkmark. On the right are navigation links: Home, Data Owner, Data User, Data Provider, and Cloud. Below the header is a white box titled "User Login". It contains two input fields: "User Name" and "Password". Below these fields is a teal "LOGIN" button and an orange "NEW USER REGISTER..." button.

Fig.1

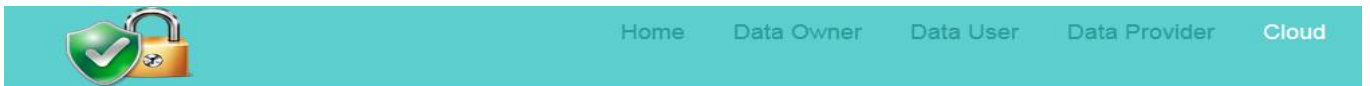
In fig.1, user will register and then login into their account. After that, they enter into the cloud and upload their files.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018



Cloud Login

Fig.2

In fig.2, Now the data owner login into cloud and verify the correct user with the key value. After that user can able to access the cloud.



File Download

Welcome !!! Arjun

File Key 2

FileID	FileName	FilePath
1	Document	Download
2	Abstract	Download
3	Old	Download
3	Old	Download
5	File1	Download

Fig.3

In fig.3, the user can able to view their file to upload into the cloud. File will be present anywhere in the system.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

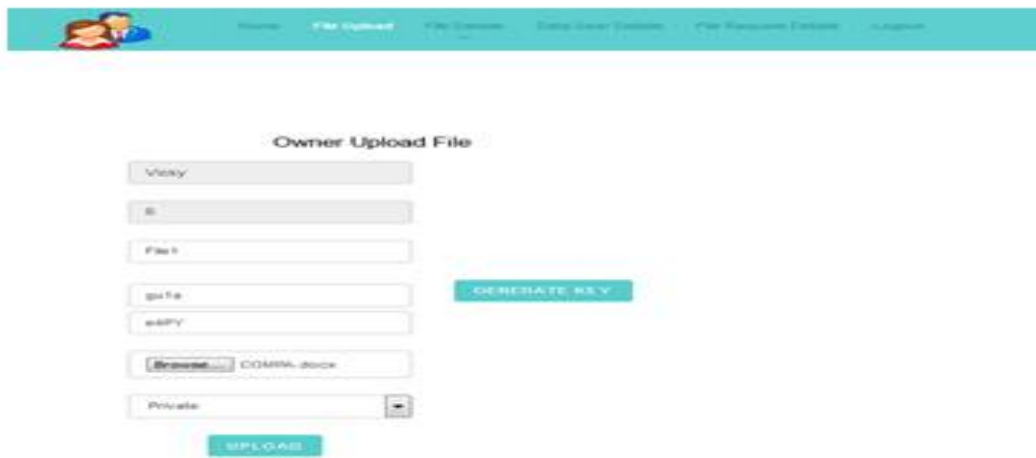


Fig.4

In fig.4, After completing all the process owner will upload the file into the cloud and then the key value will be generated and send it to the data owner.



Data Owner Details

OwnerID	Name	MobileNo	MailID	Request
1	Vicky	1234567890	vicky@gmail.com	Accept
2	Vimal	1234567891	vimal@gmail.com	Accept
3	Saravanan	9876543210	saravanan@gmail.com	Accept
4	Ram	2143658709	ram@gmail.com	Not Accept



Fig.5

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

In fig.5, Now the cloud service provider verifies the user details and then retrieve the data from the cloud and give it to the user.

V. CONCLUSION

A hybrid scheme that combines public key encryption and somewhat homomorphic encryption. The proposed scheme is suitable for cloud computing environments since it has small bandwidth, low storage requirement, and supports efficient computing on encrypted data. This solution provides a trade-off between the size of the transmitted cipher Texts and the conversion costs. While the cipher Text expansion of Fully Homomorphic Algorithm is larger than that of AES, it can be homomorphically evaluated with a FHE of much smaller multiplicative depth. The parameters of hybrid scheme are very large when the message space of the underlying FHE is Z_N . For an efficient implementation, we need a method to evaluate mod N arithmetic using an FHE whose message space is Z_M for small.

REFERENCES

- [1] S. Chee, and C. Jr, "Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center," CRC Press, Boca Raton, U.S.A, 2009.
- [2] B. Sosinsky, "Cloud Computing Bible," John Wiley & Sons, San Francisco, U.S.A, 2011.
- [3] A. Alsarhan and A. Al-Khasawneh, "Resource trading in cloud environments for utility maximisation using game theoretic modelling approach," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 31, no. 4, pp.319-333, 2016.
- [4] L. Wu, SK.Garg, S. Versteeg and R. Buyya, "SLA-based resource provisioning for hosted software as a service applications in cloud computing environments," *IEEE Transactions on services computing*, vol. 99, no.1, pp. 465-485, 2013.
- [5] J. Almeida, V. Almeida, D. Ardagna, I. Cunha, C. Francalanci, and M. Trubian, "Joint admission control and resource allocation in virtualized servers," *Journal of Parallel and Distributed Computing*, vol. 70, no. 4, pp. 344-362, 2010.
- [6] D. Kusic, JO. Kephart, JE. Hanson, N. Kandasamy, and G. Jiang, "Power and performance management of virtualized computing environments via lookaheadcontrol," *Cluster Computing*, vol.12, no 1, pp.1-15, 2009
- [7] B. Dario, "A stochastic model to investigate data center performance and QoS in IaaS cloud computing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp.560-569, 2014.
- [8] A. Alsarhan, K. Al-Sarayeh, A. Al-Ghuwairi, and Y. Kilani, "Resource trading in cloud environments for profit maximisation using an auction model," *International Journal of Advanced Intelligence Paradigms*, vol.,6, no. 3, pp. 176-190, 2014.
- [9] A. S. Prasad and S. Rao, "A Mechanism Design Approach to Resource Procurement in Cloud Computing", *IEEE Transactions on Computers*, vol. 63, no. 1, pp. 17-30., 2014.
- [10] H. Shen and G. Liu, "An Efficient and Trustworthy Resource Sharing Platform for Collaborative Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 4, pp. 862-875, 2014.
- [11] W. Chen, J. Cao and Y. Wan, "QoS-aware virtual machine scheduling for video streaming services in multi-cloud", *Tsinghua Science and Technology*, vol. 18, no. 3, pp. 308-317, 2013..
- [12] C. Papagianni, A. Leivadreas, S. Papavassiliou, V. Maglaris, C. Cervelló-Pastor and A. Monje, "On the optimal allocation of virtual resources in cloud computing networks," *IEEE Transactions on Computers*, vol. 62, no. 6, pp. 1060-1071, 2013.
- [13] B. Abraham, V. Almeida, J. Almeida, A. Zhang, D. Beyer and F. Safai, "Self-adaptive SLA-driven capacity management for Internet services.", *Proc.NOMS*, pp. 557-568, 2006.
- [14] K. Appleby, S. Fakhouri, L. Fong, G. Goldszmidt, S. Krishnakumar, D. Pazel, J. Pershing and B. Rochwerger, "Oceano—SLA-based management of a computing utility," *Proc.IEEE/IFIP*, pp. 855-868, 2001.
- [15] J. O. Fitó, I. Goiri and J. Guitart, "SLA-driven elastic cloud hosting provider," *Proc.PDP'10*, pp. 111-118, 2010.
- [16] G. Lodi, F. PanzieriD. Rossi and E. Turrini, "SLA-driven clustering of QoS-aware applications servers," *IEEE Transactions on Software Engineering*, vol. 33, no. 3, pp.186-197, 2007.
- [17] J. Ejarque, M. de Palol, I. Goiri, F. Julià, J. Guitart, R. Badia and J. Torres, "SLA-Driven semantically-enhanced dynamic resource allocator for virtualized service providers," *Proc.eScience*, pp. 8-15, 2008.
- [18] D. Mei, B. Meeuwissen and F. Phillipson, "User perceived Quality-of-Service for voice-over-IP in a heterogeneous multi-domain network environment," *Proc ICWS*, pp. 1-13, 2006.
- [19] D. Mei and H. B. Meeuwissen, "Modelling end-to-end Quality-of-Service for transaction-based services in multidomain environment," *Proc ITC19*, pp. 1109-1121, 2005.
- [20] J. Martin and A. Nilsson, "On service level agreements for IP networks," *Proc INFOCOM*, pp. 1-6, 2002.