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

FRAMEWORK OF HOMOMORPHIC ENCRYPTION FOR CLOUD SECURITY

A.Karthiga
MPhil scholar, PRIST University,
Thanjavur
H.ParveenBegam M. Sc., M. Phil.,
Asst. Prof. in CSE,
Prist Deemed To Be University
Email: karthigasivasu99@gmail.com

Abstract :

Fully Homomorphic Encryption is used to increase the security of untrusted systems and applications that deal with sensitive data. Homomorphic encryption is a kind of encryption that enables computation to be performed on encrypted data without the need for decryption. When data is stored in the public cloud, homomorphic encryption is utilized to prevent it from being shared inside the cloud service. The encryption technique employed in Partially Homomorphic Encryption may execute either an additive or a multiplicative operation, but not both at the same time. In the case of Fully Homomorphic Encryption, on the other hand, both methods may be accomplished at the same time. In this paper, we first illustrate the challenge of transforming algorithms that can function on unencrypted or regular data to algorithms that can work on encrypted data. In this work, we show that, although FHE provides the ability to do any computations, its full usefulness can only be realized if they allow the execution of arbitrary algorithms over encrypted data. This model uses it to conduct FHE operations on encrypted data using the Enhanced Data Encryption Technique, and the encrypted data is utilized to perform sorting operations.

Keyword: Homomorphic Encryption, FHE, Decryption, security.

1.Introduction

It is also a concern for many professionals. The first step was to focus on security, which is the number one concern of organizations considering a shift to the cloud. The second step was to focus on accessibility. The use of cloud computing provides a significant number of advantages, including lower prices, easier maintenance and provisioning of assets, and more flexibility. The firm Amazon Web Services made the first actual application of the concept of cloud computing in 2002, when it leased its assets to companies on a request basis during off-seasons (when the organization's IT was not in peak demand).

Every day, a large number of people use the cloud without even realizing it. As an example, all variants of email (Gmail or Webmail) and access to applications that are not physically installed on the nearby PC, such as Excel and Microsoft Word, are made possible through the Internet; however, clients may be unaware of the location of the servers that are storing their messages and facilitating the source code of the applications that they use, as is the case with Gmail. The administrations provided by Cloud Computing providers are sourced from enormous, cutting-edge facilities known as Datacenters, which use virtualization methods to provide their services.

When the information is sent to the Cloud, we use conventional encryption mechanisms to ensure that the tasks and data storage are protected. The most important concept was to encrypt the information before transferring it to the Cloud service provider. However, the final one will be responsible for decrypting information at each action. The data owner must provide the server (Cloud provider) with the private key in order for the server to decrypt the information before performing the necessary calculations, which may have an impact on the secrecy and privacy of the information stored in the Cloud. In this research, we propose the employment of a technique to perform actions on encrypted information without decrypting it, which would result in an output that is indistinguishable from the one obtained if we had worked exclusively on the raw information, based on estimates.

Customers are the primary holders of the secret key in Homomorphic Encryption frameworks, which allow them to execute operations on encrypted material without having access to or knowledge of the private key (without decrypting). In the case of decrypting the aftereffect of any task, we are doing the same estimate as if we were working with unencrypted raw data. [9] Defined as follows: An encryption is homomorphic if and only if it is possible to figure out Enc (f (a, b)) from Enc(a) and Enc(b), where f may be any of the following: +, -, or -, and without using the private key. We recognise three types of homomorphic encryption based on the tasks that allow us to survey raw information: the added substance Homomorphic encryption (which only includes options of the raw information), the multiplicative Homomorphic encryption (which only includes items on the raw information), and the multiplicative Homomorphic encryption (which only includes items on the raw information).

II.RELATED WORK

Here is a list of relevant studies and approaches that have been utilised in the past in research papers. Researchers have released a paper named "SHIELD: Scalable homomorphic Implementation of Encrypted Data-Classifiers" by Alhassan Khedir and his colleagues. Ring Learning with Errors (RLWE) was shown using a variant of the HE framework that was recently proposed by Gentry, Sahai, and Waters in this paper (GSW). Across spite of the fact that this framework was often thought to be less productive than its partners, they displayed extraordinary contrary behaviour in a broad variety of application classes and domains. In order to obtain considerable speedups over cutting-edge HE use, such as the IBM homomorphic encryption library, they first emphasise and meticulously employ the mathematical aspects of the framework (HElib).

A comprehensive description of Cloud Computing is provided in this study, which draws on the primary qualities commonly associated with this paradigm as found in the literature to arrive at a comprehensive understanding of the Cloud. We investigated more than twenty different definitions in order to come up with a consensus definition as well as a minimal definition that had the fundamental elements. This study devotes considerable emphasis to the Grid paradigm, which is sometimes misunderstood with cloud computing technologies. We also describe the linkages and contrasts that exist between the Grid and Cloud methods in more detail than ever before.

Online interactions in social networks are often based on real-world relationships, and as a result, they may be used to infer a degree of trust among members. We suggest that we take use of these ties to construct a dynamic "Social Cloud," which will allow users to share diverse resources within the framework of a social network environment. A cloud-based framework for long term sharing may be enabled by using the inherent socially correcting processes (incentives and disincentives) of the cloud, which has reduced privacy issues and security overheads than typical cloud settings. It is recommended that a social market place be established to regulate sharing in the Social Cloud due to the unique nature of the cloud itself. The social market is innovative in that it facilitates trade by using both social and economic conventions. This article describes Social Cloud computing, outlines several characteristics of Social Clouds, and then exhibits the technique by using a Facebook-based social storage cloud implementation to showcase the concept.

MIT computer science pioneer John McCarthy predicted in 1961 that "Computing may one day be structured as a public utility, in the same way that the telephone system is organised as a public utility. Even if we aren't there yet, cloud computing is helping us get closer. Among the many advantages of cloud computing are its flexibility, adaptability, transparency, and low overall costs. Many benefits come with difficult security and privacy issues to contend with. A simple summary of computer history from the 1960s is as follows: As a continuous march toward ever more specialisation and dispersion of computer resources, When we had mainframes, security was rather simple. When minicomputers, desktop and laptop computers, and client-server models were introduced, things became even more complicated. N-tier and grid computing as well as other types of virtualization were all spawned by these principles. Distributing software and data got more complex as hardware infrastructures became more complicated and dispersed. There seemed to be no end to the amount of security vulnerabilities that emerged as a result of people dividing up their computer resources in so many different ways. The challenge has been compounded by the fact that just when one computing paradigm looked to be settling, another, more enticing one, arrived on the horizon.

III.FORWARD-SECURE CRYPTOSYSTEMS

Because of the private key's trade-off for the current day and age, it is necessary to divide the lifetime of a private key into T distinct periods in order to prevent an opponent from supplying legitimate marks for prior eras. This is accomplished by dividing the lifetime of a private key into T different periods. This resulted in the development of Bellare and Miner of unambiguous definitions of the forward-secure mark, as well as a set of practical instructions for use with forward-secure trademarks. Since then, other forward-stable mark proposals have been developed, and the debate is still ongoing. It was Canetti, Halevi, and Katz who first proposed open key cryptography in 2000, and it was put into practise in forward-secure open key cryptography a year later. Their work is very significant since they began by developing a twofold tree encryption, which they then changed into a forward-secure encryption with shown security in the arbitrary prophet presentation. In accordance with the Canetti et alapproach, Yao et al. employed two unique tiers of IBE plans to produce a forward-secure progressive IBE; Nieto et al. proposed a forward-secure progressive IBE employing two different tiered IBE plans. One of the authors came up with the idea of a forward-secured multiple-level predicate encryption technique. Specifically, through partnering with Boldyreva and others on various projects. CRYPTO 2012 saw the presentation of a non-specific improvement of presumably revocable storage quality-based encryption that increases both client disavowal and ciphertext renewal while at the same time reducing the need for more storage capacity. Several approaches, including the repudiation technique and the notion of forward security, which was previously defined, were investigated. Finally, they grow in a way that is both forward- and backward-looking in their perspective. It should be noted that the ciphertext refresh mechanism utilised in this study only necessitates the use of publically available data, which should be stressed. Unscrambling is the result of a collaborative endeavour between the private key and the refresh key, and as a result, none of their developments can be considered immune to its implementation.

IV.MODEL

The following security goals must be met if we are to survive the threats to our security and maintain command of the cloud's mutual information transformation:

For the cloud server to remain secure, it is necessary to guarantee that only authorised clients may access the plaintext of mutual information stored on the server. On top of that, cloud servers, which are supposed to be simple but yet curious, must not be able to get their hands on the plaintext of common information.

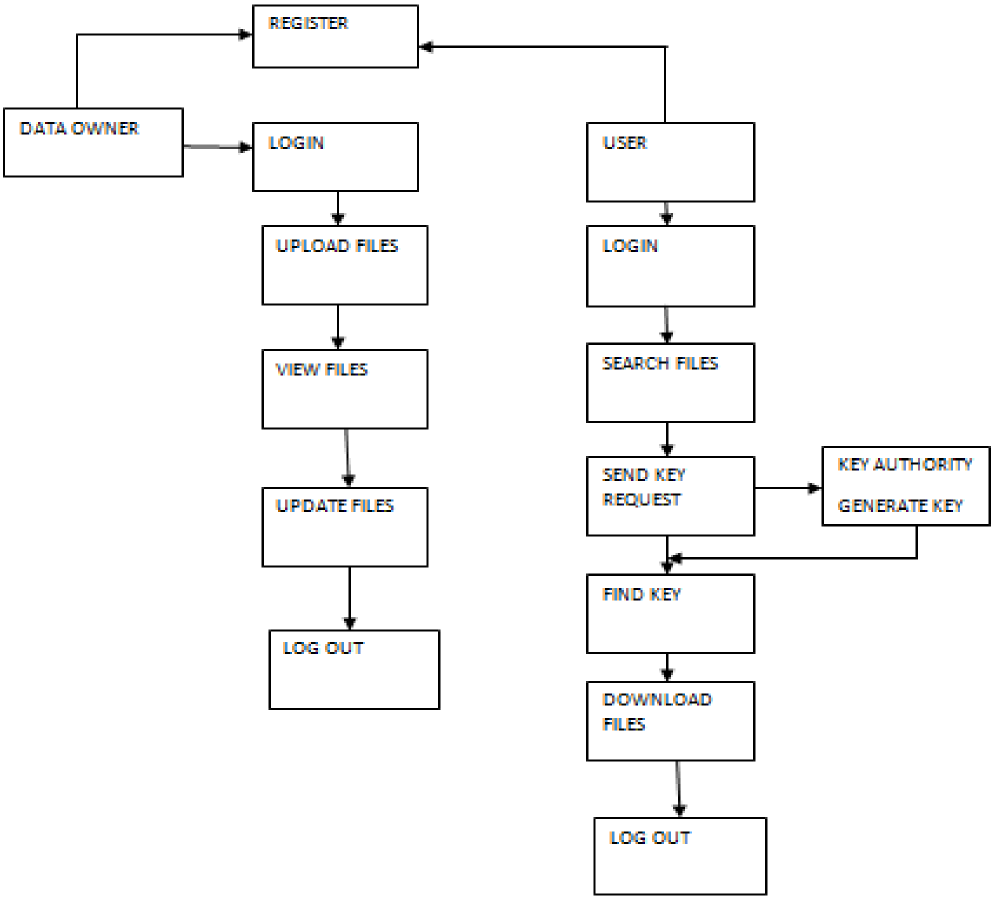
You should deny a client access to the plaintext of any information you have provided with him or her while it is still encrypted in his or her character's name when his or her authorization is revoked or threatened.

- The mystery that lies ahead: Clients should be restricted from accessing the plaintext of common information that can already be accessible by them if their power has expired or if their mystery key is in peril, according to Forward Mystery's recommendations.

V. PROPOSED METHODOLOGY

Combining techniques as often as necessary is conceivable in order to improve the tradeoff between local and remote encryption handling and to improve the overall performance. When it comes to material homomorphic applications, pre-computing, as well as customised encryption and decryption, are important advancements to make. The development of a model application that supports additional encryption computations with homomorphic features, as well as efficient and privacy-friendly confront acknowledgment and highlight extraction techniques, is planned in the near future in order to demonstrate the technology's potential for commercial application. Also planned is an in-depth investigation of facial recognition algorithms that might be utilised by the general population.

DATA FLOW DIAGRAM



VI.CONCLUSION

The RS-IBE proposal is a cost-effective and secure information sharing architecture for cloud computing. It allows both character renunciation and ciphertext refresh at the same time to prevent a repudiated client from accessing previously shared or new information. Also, the RS-IBE looks to be advancing rapidly. The standard model's RS-IBE plot is adaptive and secure using the decisional l-DBHE assumption. Our method clearly has benefits in terms of productivity and utility, making it more suitable for real-world applications.

REFERENCES

[1] Alexandra Boldyreva (Georgia institute of technology, Atlanta, GA, USA), Vipul Goyal (university of California at Los Angeles, CA, USA) and Virendra Kumar (Georgia institute of technology, Atlanta, GA, USA) “Identity-based encryption with efficient revocation” 2008.

[2] Chul Sur Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea, Youngho Park (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, SouthKorea), Sang UK Shin (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea) Kyung Hyune Rhee (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea) “Certificate-Based Proxy Reencryption for Public Cloud Storage 2013”.

[3] Mohan, Prakash, and Ravichandran Thangavel. "Resource Selection in Grid Environment Based on Trust Evaluation using Feedback and Performance." American Journal of Applied Sciences 10.8 (2013): 924.

[4] Prakash, M., and T. Ravichandran. "An Efficient Resource Selection and Binding Model for Job Scheduling in Grid." European Journal of Scientific Research 81.4 (2012): 450-458. [5] Jin Li (School of Computer Science, Guangzhou University, Guangzhou, China),Wenjing Lou (Virginia Polytechnic Institute and State University, Blacksburg) “Identity based encryption with outsourced revocation in cloud computing” 2015.

[6] Prakash, M., R. Farah Sayeed, S. Princey, and S. Priyanka. "Deployment of MultiCloud Environment with Avoidance of DDOS Attack and Secured Data Privacy." International Journal of Applied Engineering Research 10, no. 9 (2015): 8121-8124.

[7] Annamalai, R., J. Srikanth, and M. Prakash. "Integrity and Privacy Sustenance of Shared Large Scale Images in the Cloud by Ring Signature." International Journal of Computer Applications 114.12 (2015).

[8] Mohan Prakash, Chelliah Saravanakumar. “An Authentication Technique for Accessing De-Duplicated Data from Private Cloud using One Time Password”, International Journal of Information Security and Privacy, 11(2), 1-10, 2017.

[9] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy preserving public auditing for secure cloud storage,”2013.

[10] G. Anthes, “Security in the cloud,” Communications of the ACM, 2010.

[11] S. Ruj, M. Stojmenovic, and A. Nayak, s“Decentralized access control with anonymous authentication of data stored in clouds” 2014

[12] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, “Cost-effective authentic and anonymous data sharing with forward security” 2014.

[13] C. Gentry, “Certificate-based encryption and the certificate revocation problem,” 2003.

[14] V. Goyal, “Certificate revocation using fine grained certificate space partitioning,” 2007.

[15] J. M. G. Nieto, M. Manulis, and D. Sun, “Forward-secure hierarchical predicate encryption,”2013.

[16] 11. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, “An efficient cloud based revocable identity-based proxy reencryption scheme for public clouds data sharing,” 2014.

[17] 12. D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, “Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts,” 2013.

[18] 13. M. Abdalla and L. Reyzin, “A new forward-secure digital signature scheme,” 2000.