Data optimization in multicloud storage services employing store sim raises security and privacy concerns

NAVANEETHA KIRSHNAN M,
Head of the Department,
Department of Computer Science and Engineering
Ammie Kavya. J, Student of Computer Science and Engineering
Harini. G, Student of Computer Science and Engineering
St. Joseph College of Engineering, Sriperumbudur, Chennai.

Abstract:

Provable Multi files are files that can be proven to be true. Data that changes over time In cloud computing, possession refers to the transfer of stored data to a cloud server in a dynamic manner. The term "multi files" refers to data that must be duplicated to various servers. When a project owner uploads data to a cloud server, the data is automatically split into numerous files, which are subsequently stored on multiple servers. If you upload your data to many servers, you can avoid data loss due to hacking and server failure. We introduced a new technology called Fully Homomorphic Encryption (FHE) in this project for taking multiple files of data, file security, and data corruption. We will use the FHE technique to safeguard the data in this project. These are keygen, copygen, and taggen, respectively. The technique described above was carried out in an existing system using a single dynamic file.

KEYWORDS – On Demand, Self Service, Grid Management, Grid Computing, Subscription Computing.

Introduction:

Compatibility for different requested tasks is difficult to guarantee for some electronic devices, which are composed of dedicated hardware equipments, such as field programmable gate array (FPGA), digital signal processor (DSP), and integrated circuit (IC), and systems will become more complicated as the number of requested tasks increases. The underpinnings of cloud computing are software defined networking (SDN) and virtualization technology, which offer a promising and flexible method to resource distribution [1], [2], [3]. Depending on demand and supply, cloud service providers can assign available resources associated to service nodes to the needed activities. When a task has numerous subtasks, these subtasks can be deployed on many service nodes to form a service chain, which is a data flow through the service nodes in a sequential order that can be represented as a directed acyclic graph (DAG) [4]. Physical resources for the central processing unit (CPU), memory, or graphics processing unit are required for each sub-task (GPU). Furthermore, data transit between service nodes incurs bandwidth expenses. For example, data transmission has five sub-tasks, and the service chain for these sub-tasks is: network receiving! capture! tracking! synchronisation! decoding, where each functional module is accomplished by software programming and can be executed on a common computer system. Cloud computing may significantly lower a system's complexity and development costs while simultaneously increasing its flexibility and scalability. However, a new hurdle in cloud computing is determining how to effectively distribute available resources associated to service nodes to the desired activities, which is a combinatorial optimization problem [5], [6].

Objectives:

We presented a new technology called Fully Homomorphic Encryption (FHE) for multi-file data, file security, and data corruption in this research.

Literature Survey:

[1] Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. 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. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.

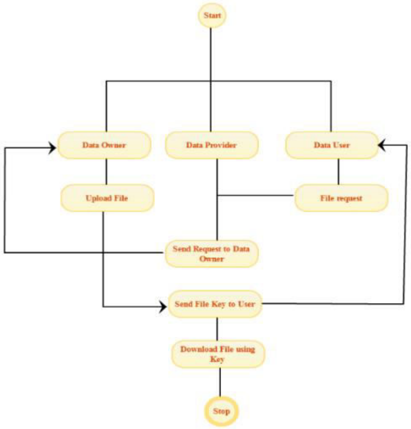
[2] VABKS: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data **.**Qingji Zheng, Shouhuai Xu, and Giuseppe Ateniese. It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This 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? Motivated by these questions, we propose a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS). The solution allows a data user, whose credentials satisfy a data owner’s access control policy, to (i) search over the data owner’s outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations.

[3] Multi-User Private Keyword Search for Cloud Computing. Yanjiang Yang, Haibing Lu, and Jian Weng. Enterprises 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. The above setting of enterprise outsourcing database to the cloud requires multi-user searchable encryption, whereas virtually all of the existing schemes consider the single-user setting. To bridge this gap, we are motivated to propose a practical multi-user searchable encryption scheme, which has a number of advantages over the known approaches. The associated model and security

requirements are also formulated. We further discuss to extend our scheme in several ways so as to achieve different search capabilities.

System Design:

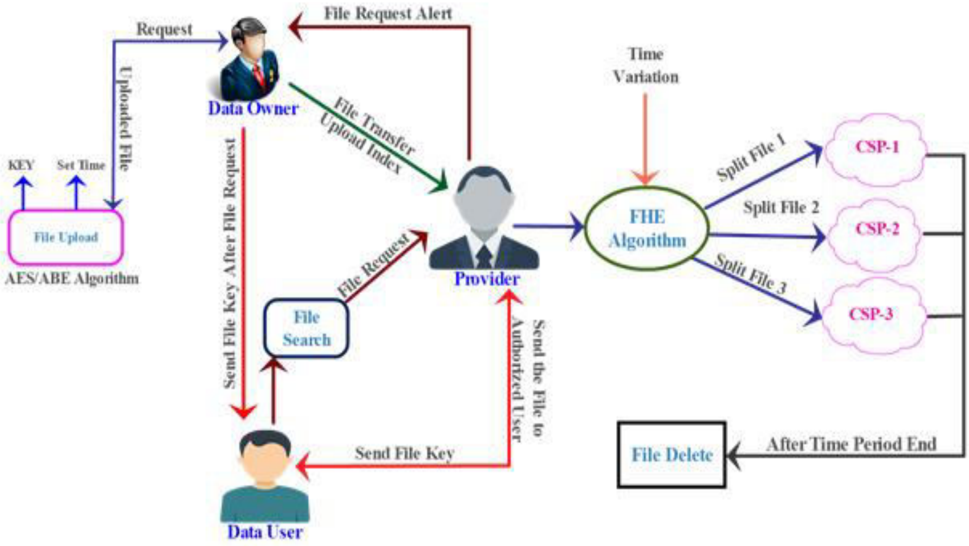
This project's suggested solution stores uploaded data in several servers (Multi files). FHE algorithms are employed in one of the proposed schemes. If the owner uploads data, three files are automatically created and kept in three servers. This is done for security and to minimise server overload. That copy is also encrypted, so the data can't be hacked by the cloud service provider or anybody else. When users submit data, the server converts it to zip format automatically.



As a result, the server automatically reduces the file size. The file was shared with an authorised user by the owner. After that, the authorised user sends a file request to the cloud server, which then sends encrypted data to the authorised user. The decrypt key is obtained from the data owner by the authorised user.

Implementation:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.



Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user and so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. The final stage is to document the entire system which provides components and the operating procedures of the system.

Conclusion and Future Enhancement:

We suggested a hybrid system that combines public key encryption and homomorphic encryption in a semi-homomorphic manner. Because it has a small bandwidth demand, requires little storage, and facilitates efficient computing on encrypted data, the proposed technique is well suited for cloud computing environments. Our approach strikes a balance between the size of sent ciphertexts and conversion expenses. PKE has a bigger ciphertext expansion than AES, but it may be homomorphically evaluated with a SHE with a much smaller multiplicative depth. When the message space of the underlying FHE is ZN, the parameters of our hybrid system are very big. We need a way to evaluate mod N arithmetic using an FHE whose message space is ZM for tiny for an efficient implementation.

Future Enhancement:

In this have to add extra features in future like

1. Send Alert Notification details to send via send SMS.

2. In future in this concept to in android app.

References:

- R. Barbulescu, P. Gaudry, A. Joux, and E. Thom´e. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. IACR Cryptology ePrint Archive, 2014.
- J. Cheon, J.-S. Coron, J. Kim, M. Lee, T. Lepoint, M. Tibouchi, and A. Yun. Batch fully homomorphic encryption over the integers. In T. Johansson and P. Nguyen, editors, Advances in Cryptology - EUROCRYPT 2013, volume 7881 of Lecture Notes in Computer Science, pages 315–335. Springer Berlin Heidelberg, 2013.
- A. Joux. A new index calculus algorithm with complexity L(1/4+o(1)) in very small characteristic. IACR Cryptology ePrint Archive, 2014.
- S. Goldwasser and S. Micali. Probabilistic encryption. J. Comput. Syst. Sci., 28(2):270–299, 2015.
- J. Fan and F. Vercauteren. Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012:144, 2015.
- W. Li, K. Xue, Y. Xue and J. Hong, “TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage,” IEEE Trans. Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484-1496, 2015
- J. Li, H. Wang, Y. Zhang and J. Shen, “Ciphertext-policy at-tribute-based 5/encryption with hidden access policy and testing, ” KSII Transactions on Internet and Information Systems, vol. 10, no. 7, pp. 3339-3352, 2016.
- Z. J. Fu, K. Ren, J. G. Shu, X. M. Sun, and F. X. Huang, “Enabling personalized search over encrypted outsourced data with efficiency improvement,” IEEE

Transactions on Parallel and Distributed Systems, , vol. 27, no. 9, pp. 2546–2559, 2016.

. Dr.M.Navaneethakrishnan M.E., PhD is a Head of the Department in the Department of Computer Science and Engineering at St. Joseph College of Engineering, Sriperumbudur, Chennai, Tamil Nadu. He has completed his Ph.D, in Cyber Security - Computer Science and Engineering in 2017 from Manonmaniam Sundaranar University (MSU) Tirunelveli, Tamilnadu. He has done his M.E, CSE in Anna University Chennai in the year 2008. Dr.M.Navaneethakrishnan has 15 years of teaching experience and has 58 publications in International Journals and Conferences. His research interests include network security, Computer Networks, data science and Machine Learning. He is an active member of ISTE, CSI, IEANG and IEI

Ms.Ammie Kavya.J B.E.,Student of Computer Science and Engineering at St.Joseph College of Engineering, Sriperumbudur, Chennai,TamilNadu.I had attended some International Conference, Workshops and Seminars in the area of Data Science Organizations, Python ,Machine Learning And Java Respectively.

Ms.Harini.G B.E.,Student of Computer Science and Engineering at St.Joseph College of Engineering, Sriperumbudur, Chennai,TamilNadu.I had attended International Conference and Seminars in the area of Data Science Organizations, Python ,Machine Learning And Deep learning Respectively. I got Placed in Reputed Companies like Wipro and TCS respectively.