International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT18386

Secure Virtualisation Using Hash Key Authentication

D. Jegalakshmi Princy[1*], M. Shobana [2]

[1]ME Scholar, Department of Computer Science, Dhanalakshmi Srinivasan College of Engineering, Perambalur, Tamil Nadu, India

[2]Associate Professor, Department of Computer Science, Dhanalakshmi Srinivasan College of Engineering, Perambalur, Tamil Nadu, India

ABSTRACT

In the current scenario, cloud computing is new kind of computing paradigm which enables sharing of computing assets over the net. The cloud characteristics are on-call for self-service, vicinity unbiased community get right of entry to, ubiquitous community get right of entry to and usage based totally pay. Due to this charming capabilities personal and public enterprise are outsourcing their large quantity of records on cloud storage. Organizations are encouraged to migrate their facts from nearby web site to central industrial public cloud server. By outsourcing statistics on cloud customers gets alleviation from storage preservation. Although there are numerous blessings to migrate facts on cloud garage it brings many safety problems. Therefore the records owners hesitate to emigrate their sensitive data. The current technique makes use of Virtual Machines and Hypervisor Intrusion Detection System, in detecting and stopping the hypervisor attacks inside the virtualized cloud surroundings. In this work, we proposed a model which searches and get access to files which are uploaded in a network. Elliptical Curve Cryptography and Attribute Based Encryption method are implemented for secured data communication. The proposed method is implemented in real time and the results prove that the proposed method is efficient than the existing methods.

Keywords : ABE, ECC, Access, Hypervisor, IDS.

I. INTRODUCTION

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. There are different categories of threats. There are natural threats, occurrences such as floods, earthquakes, and storms. There are also unintentional threats that are the result of accidents and stupidity. Finally, there are intentional threats that are the result of malicious intent. Each type of threat can be deadly to a network. Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat. Design flaws in hardware or software can render systems vulnerable to attack or affect the availability of systems. For example, the send mail flaw in earlier versions of UNIX enabled hackers to gain privileged access to systems. Disks, tapes and other media can be stolen, lost, or damaged. Information can be copied and removed from an organization's facilities without detection. Accordingly, companies need to ensure the safety of all media that contains or stores vital information assets. Signal emissions from electrical equipment can be remotely intercepted and monitored using sophisticated devices in a process sometimes referred to as van Eck monitoring. Organizations also need to be concerned about the interception of most forms of

communication. Communication is the sharing of information on a medium. As such, it is inherently vulnerable to interception, monitoring, forgery, alteration and interruption. Human stupidity, carelessness, laziness, greed, and anger represent the greatest threats to networks and systems and will do more damage than the rest of the others combined. Moreover, human vulnerabilities and the risks associated with them are the most difficult to defend against. It is important to keep in mind that every network or system designed, configured or implemented has vulnerabilities. There is no such thing as a totally secure network or system. It does not exist. Identification is simply the process of identifying one's self to another entity or determining the identity of the individual or entity with whom you are communicating.

Authentication serves as proof that you are who you say you are or what you claim to be. Authentication is critical if there is to be any trust between parties. Authentication is required when communicating over a network or logging onto a network. Access Control refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. Your level of authorization basically determines what you're allowed to do once you are authenticated and allowed access to a network, system, or some other resource such as data or information. Access control is the determination of the level of authorization to a system, network, or information. Availability refers to whether the network, system, hardware, and software are reliable and can recover quickly and completely in the event of an interruption in service. Ideally, these elements should not be susceptible to denial of service attacks. Confidentiality can also be called privacy or secrecy and refers to the protection of information from unauthorized disclosure. Usually achieved either by restricting access to the information or by encrypting the information so that it is not meaningful to unauthorized individuals or entities. Integrity can be thought of as accuracy. This refers to the ability to protect information, data or transmissions from unauthorized, uncontrolled, or accidental alterations. The term integrity can also be used in reference to the functioning of a network, system, or application. Data integrity is achieved by preventing unauthorized or improper changes to data, ensuring internal and external consistency, and ensuring that other data attributes (such as timeliness and completeness) are consistent with requirements. Integrity can be used in reference to the proper functioning of a network, system or application. Accountability refers to the ability to track or audit what an individual or entity is doing on a network or system. Nonrepudiation is the ability to prevent individuals or entities from denying (repudiating) that information, data or files were sent or received or that information or files were accessed or altered, when in fact they were. This capability is crucial to e-commerce. Without it an individual or entity can deny that he, she, or it is responsible for a transaction and that he, she, or it is, therefore not financially liable.

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

Advocates claim that cloud computing allows companies to avoid up-front infrastructure costs (e.g., purchasing servers). As well, it enables organizations to focus on their core businesses instead of spending time and money on computer infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables Information technology (IT) teams to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This will lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model

Cloud computing is the result of the evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users focus on their core business instead of being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. Autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors. Users routinely face difficult business problems. Cloud computing adopts concepts from Service-oriented Architecture (SOA) that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way.

Cloud computing also leverages concepts from utility computing to provide metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models. In addition, measured services are an essential part of the feedback loops in autonomic computing, allowing services to scale on-demand and to perform automatic failure recovery. Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques. Though service-oriented architecture advocates "everything as a service" (with the acronyms EaaS or XaaS), cloud-computing providers offer their "services" according to different models, of which the three standard models per NIST are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models offer increasing abstraction; they are thus often portrayed as layers in a stack: infrastructure-, platform- and software-as-a-service, but these need not be related. For example, one can provide SaaS implemented on physical machines (bare metal), without using underlying PaaS or IaaS layers, and conversely one can run a program on IaaS and access it directly, without wrapping it as SaaS.

II. RELATED WORK

Wang et al., proposes a privacy-preserving public auditing system for data storage security in Cloud

Computing. We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage [1].Curtmola et al., formally define SSE in the multi-user setting and present an efficient construction that achieves better performance than simply using access control mechanisms. Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years.Our multi-user construction is very efficient on the server side: when given a trapdoor, the server only needs to evaluate a pseudo-random permutation in order to determine if the user is revoked. If access control mechanisms were used instead for this step, a "heavier" authentication protocol would be required [2].Golle et al., propose a second scheme whose communication cost is on the order of the number of keyword fields and whose security relies on a new hardness assumption. We've presented two protocols for conjunctive search for which it is provably hard for the server to distinguish between the encrypted keywords of documents of its own choosing. Our protocols allow secure conjunctive search with small capabilities. Our work only partially solves the problem of secure Boolean search on encrypted data. It would be interesting to explore solutions for the secure search problem that also protect keyword fields [3].Ballard et al., presents two provably secure and efficient schemes for performing conjunctive keyword searches over symmetrically encrypted data. Our first scheme is based on Shamir Secret Sharing and provides the most efficient search technique in this context to date. Although the size of its trapdoors is linear in the number of documents being searched, we empirically show that this overhead remains reasonable in practice. Nonetheless, to address this limitation we provide an alternative based on bilinear pairings that yields constant size trapdoors. This latter construction is not only asymptotically more efficient than previous secure conjunctive keyword search schemes in the symmetric setting, but incurs significantly less storage overhead [4].Lou et al., defines and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE) [5].Wang et al., establishes a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi keyword semantics, we choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to capture the relevance of data documents to the search query. 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. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given[6].Kang et al., proposes a novel approach, called MKQE, to address these issues. Only minor changes in the dictionary structure have to be done when extra keywords are introduced. We also introduce new trapdoor generation and scoring

algorithms to make in-order query results. Furthermore, the keyword access frequency is considered so as to select an adequate matching file set [7].Cao et al., defines and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Specifically, we explore the statistical measure approach, i.e., relevance score, from information retrieval to build a secure searchable index and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information [8].Jung et al., presents an anonymous privilege control scheme AnonyControl to address not only the data privacy problem in cloud storage, but also the user identity privacy issues in existing access control schemes. Our security proof and performance analysis shows that AnonyControl is both secure and efficient for cloud computing environment. Using multiple authorities in the cloud computing system, our proposed scheme achieves not only fine-grained privilege control, but also anonymity while conducting privilege control based on users' identity information [9].Sun et al., present a verifiable privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, we propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. To improve the search efficiency, we propose a tree-based index structure and various adaptive methods for multi-dimensional (MD) algorithm so that the practical search efficiency is much better than that of linear search. [10].

III. IMPLEMENTATION

Implementation is the process of executing the security file sharing in a in-secure network environment. In proposed work intrusion detection will be considered to avoid the data theft. In below proposed work of the intrusion detection mechanism was explained.

With the advent of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data have motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner. Instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM).

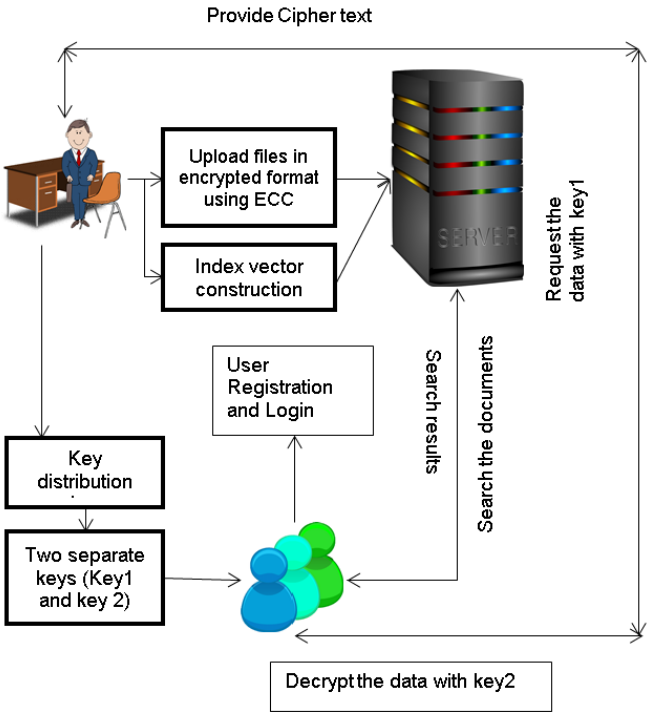

Fig 3.1: Proposed system work flow diagram

To enable cloud servers to perform secure search without knowing the actual data of both keywords

and trapdoors, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol.

There are three types of persons involved in this project. They are: Server, Owner and User. Server manages the list of owners and users. Owners have to register with the server. Authentication will be done. Users have to register under a specified owner. These users will be authenticated and will be given permission to access the files uploaded by their respective owner only. The owner to upload the file in an encrypted format using ECC algorithm. This ensures the files to be protected from unauthorized users. Data owner after logging into system adds the data which is stored in an organized structure. The data will be large so that it should be stored in the proper structure. Index is created as a list of mappings which correspond to each keyword. File ids, Term frequency, Length, Number of files that has the particular keyword are the fields for index table creation. Using these fields only, the ranking will be done. Ensures the user to search the files that are searched frequently using rank search. Once the documents are stored and indexed, the next important function is to rank them. Using the available details the user retrieves the top "k" most relevant documents. Calculate a numeric score for each file. When the user request for the data, ranking is done on requested data using coordinate matching principle. After ranking, user gets the expected results of the query. To search for a file, the user should send a request to the owner. If the owner accepts the request, user can access to the file. In the access process, the user who wants to access the file is asked for the attributes as per the access policy defined by the owner. If the attributes of the user matches the access policy, the system performs first decryption using access policy with the help of proxy server. This will partially decrypt the file. Now the proxy server asks for the key from the user. If the key is correct then the second decryption is performed and the fully decrypted file and key is sent to the user.If the key doesn't match, the following details will be mailed to the user. IP Address, MAC Address, Latitude, Longitude are the details that will be mailed. The MAC Address details will be stored in a database for the intruders. This will be helpful for the prevention of intruders in the future.

To enable privacy preserving ranked multi-keyword search in the multi-owner and multi-user cloud environment, the system design should simultaneously satisfy security and performance goals. Ranked Multi-keyword Search over Multiowner: The proposed scheme should allow multi-keyword search over encrypted files which would be encrypted with different keys for different data owners. It also needs to allow the cloud server to rank the search results among different data owners and return the top-k results.

Data owner scalability: The proposed scheme should allow new data owners to enter this system without affecting other data owners or data users, i.e., the scheme should support data owner scalability in a plug-and-play model.

Data user revocation: The proposed scheme should ensure that only authenticated data users can perform correct searches. Moreover, once a data user is revoked, he can no longer perform correct searches over the encrypted cloud data.

Security Goals: The proposed scheme should achieve the following security goals: Keyword Semantic Security. We will prove that PRMSM achieves

semantic security against the chosen keyword attack. Since the adversary A can know whether an encrypted keyword matches a trapdoor, we use the weaker security goal (i.e., secrecy), that is, we should ensure that the probability for the adversary A to infer the actual value of a keyword is negligibly more than randomly guessing. Relevance score secrecy. We should ensure that the cloud server cannot infer the actual value of the encoded relevance scores.

Nowadays, the organizations are emphasizing on the security and resilient aspect of the cloud computing to protect the privacy and confidentiality of their data information. However, the hypervisor attack remains a hot issue by the cloud user even though enormous research has accomplished to inhibit the vulnerabilities in the virtualized cloud environment. Therefore, we have proposed the Virtual Machines and Hypervisor Intrusion Detection System, VMHIDS as our technique in detecting and preventing the hypervisor attacks in the virtualized cloud environment. The VMHIDS has adopted several features from the other techniques by inspecting the tasks frequently which then prevent suspicious event occur. Through the VMHIDS, the hypervisor attack is mitigated. Virtual Machines and Hypervisor Intrusion Detection System (VMHIDS) are proposed in protecting from the hypervisor attacks. Beforehand, this paper has illustrated the concept of the hypervisor and hypervisor attack in the virtualized cloud environment in details. It is understand that the hypervisor attack is categorized in the cloud infrastructure and external attack. In order to further understand the hypervisor attack, this paper also provides an overview of the attacks that related with cloud infrastructure. Consequently, there are five exiting approaches such as virtual firewall, Intrusion Detection and Prevention Systems (IDPS), Network based IDS, Hosted-based IDS and Hypervisor-based IDS are used to compare along with their strength and weakness. Indeed, these approaches emphasizes on defending the cloud computing instead of hypervisor attack. Therefore, Virtual Machines Hypervisor Intrusion Detection System is proposed to conquer the weakness found in the existing systems.

IV. EXPERIMENTAL RESULTS

Experimental results explain the overall implementation process. Below mentioned screenshots shows the intrusion detection process. Proposed implementation provides efficient file sharing and intrusion detection process in cloud.

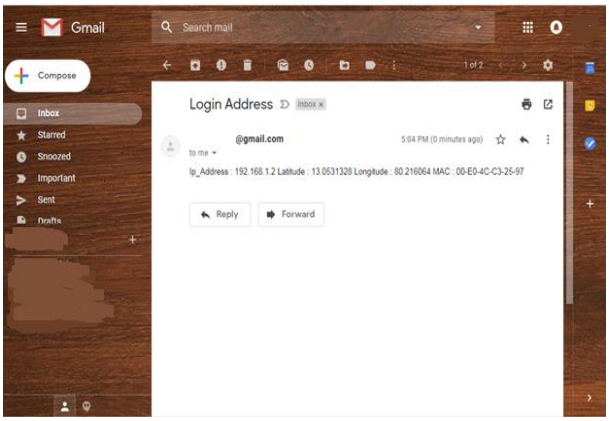

Fig 4.1 : Data Decryption

The above figure shows that an email will be sent to the user with the IP Address, MAC Address, Latitude and Longitude of the intruder. This will be received only when a wrong key is entered for decryption.

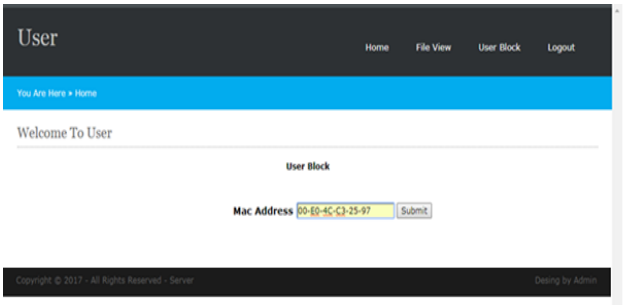

Fig 4.2: Intrusion Detection

This figure explains how a user can block the intruder. The intruder can be blocked using the MAC address.

V. CONCLUSION

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. Elliptical Curve Cryptography and Attribute Based Encryption are used in this work for secured data communication. If an intruder tries to gain access with incorrect details, the intruder's IP address and MAC address along with latitude and longitude of the intruder will be mailed to the user. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel function. Moreover, we show that our approach is computationally efficient, even for large data and keyword sets. As our future work, we will consider the problem of secure fuzzy keyword search in a multi-owner paradigm. On the other hand, we plan to implement our scheme on the commercial clouds

VI. REFERENCES

[1]. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, 2013, pp. 362-375.

[2]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS'06, VA, USA, Oct. 2006, pp. 79-88.

[3]. P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Applied Cryptography and Network Security (ACNS'04), Yellow Mountain, China, Jun. 2004, pp. 31-45.

[4]. L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. Information and Communications Security (ICICS'05), Beijing, China, Dec. 2005, pp. 414-426.

[5]. C. Wang, N. Cao, J. Li, K. Ren and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun. 2010, pp. 253-262.

[6]. N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy preserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM'11, Shanghai, China, Apr. 2011, pp. 829-837.

[7]. Z. Xu, W. Kang, R. Li, K. Yow and C. Xu, "Efficient multi keyword ranked query on encrypted data in the cloud," in Proc. IEEE Parallel and Distributed Systems (ICPADS'12), Singapore, Dec. 2012, pp. 244-251.

[8]. C. Wang, N. Cao, K. Ren and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, 2012,pp. 1467-1479.

[9]. T. Jung, X. Y. Li, Z. Wan and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proc. IEEE INFOCOM' 13, Turin, Italy, Apr. 2013, pp. 2625-2633.

[10]. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," Parallel and Distributed

Systems, IEEE Transactions on, 2014,vol. 25, no. 11, pp. 3025-3035.