OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

EnDAS: EFFICIENT ENCRYPTED DATA SEARCH AS A MOBILE CLOUD SERVICE

Ashwini Anil Pulekar[1], Dr. Archana Lomte[2]

M. E. Student, Department of Computer, JSPM's BSIOTR, Wagholi, Pune, Maharashtra, India

Assistant Professor, Department of Computer, JSPM's Bhivarabai Sawant Institute of Technology & Research, Pune, India

Abstract: Now a day's large amount of data accumulated on cloud. All information stored on cloud throughout the world. It will be unsecure unless all data encoded for the security purpose. Crumbled information arranges properly to be effectively and easily for searchable and retrievable data with no security access, especially for the versatile customer. Number of issue find out in previous studies relates to cloud data. Especially in portable cloud platform cell phone can't be connected it may cause to difficulties occurred remote systems. For example, inertness affectability, poor availability, and low transmission rates. However, it may lead risk to as data cannot be encrypted for security purpose. Especially for the mobile client encrypted form data should be accessible and retrieval without any privacy leak. Although recent research has solved many security issues, the architecture cannot applied on mobile devices directly under the mobile cloud environment. It will be forced by wireless networks, such as latency sensitivity, poor connectivity, and low transmission rates. This leads to a long search time and extra network traffic costs when using traditional search schemes. In our study we proposed Efficient Encrypted data search as mobile clod service to resolve these issues. In these propose studies we using lightweight trapdoor (Encrypted format keyword), which optimizes the data communication process by reducing the trapdoor's size for traffic efficiency.

Keywords: *Mapping Table, Compression, Ranking Search, Encrypted Search, Mobile Cloud.*

I INTRODUCTION

As cloud computing can support flexible services and cloud provide large amount of storage and lot of computational resources which will be help for rapidly increased popularities. Now a day's many data providers upload data on cloud instead of direct provide to user with the help of effective cloud. Providers can able to search document on cloud as cloud provides such important task. To protect data security users need to query certain documents, they first send keywords to the original data provider. In that case provider can generates encrypted keywords means trapdoor and these trapdoors return to the user. The user then sends these trapdoors to the cloud. Upon receiving the trapdoors, documents and index are encrypted before upload on cloud then clod use special algorithms for search specific documents. User can give trapdoor and based on the index easy to search required documents which is in encrypted format. Finally user use private key for access search encrypted data for the decryption.

This architecture, as define in Figure 1, protects data security while entitling the providers to use both the computation and storage power of the Cloud for document searches. Due to these advantages, this architecture has already been well-adopted in privacy-preserving search systems. Cell phones (e.g. cell phones and tablets) were evaluated to surpass two billion development (0.3 billion for PCs) in the year 2014, which commands the general shipment of shopper hardware gadgets. Now a days, clients intensely use cell phones to demand archive look administrations. By and large, cell phones interface with the Internet principally by means of remote systems (Wi-Fi /3G/4G/LTE), which brings about some difficulties when contrasted with conventional wired systems. These challenges include:

A. **Latency Affectability:**

This remote system may lead longer system which is not movable. For instance, in the conventional configuration appeared in Figure 1, a solitary inquiry requires three round excursions and results in remarkable latency for remote correspondence.

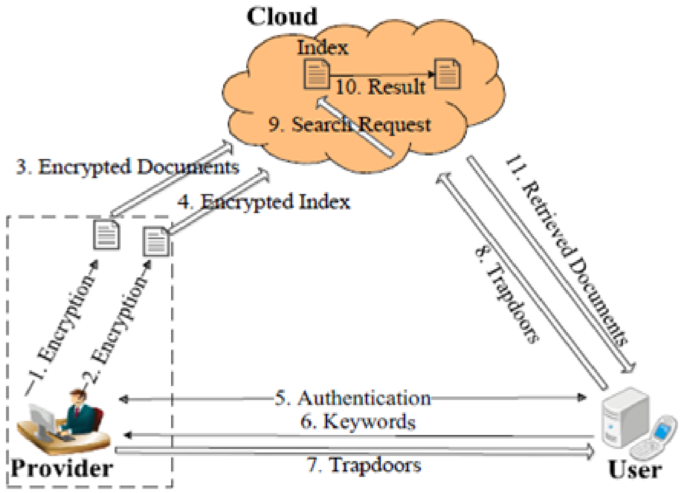


Figure 1: Traditional Encryption search system over cloud

B. **Less Availability:**

Mobile gadgets are typically unequipped for keeping up a long-running association with the Cloud, generally for vitality sparing purposes. Different inquiry solicitations could bring about various re-association operations and additional authentication costs.

C. **Less System Transmission Rate:**

Three round outings essentially force prominent hunt delay and intemperate system movement, which could be immoderate for a cell phone. As indicated by our estimation, a hunt demand in the customary framework could create trapdoors with a size up to 1.2MB. At the point when performing seek asks for, the trapdoor must be sent twice (step 7 and 8). In such case, security protecting ventures could prompt longer inquiry deferral and more data transmission utilization, which couldn't be moderate to versatile clients. This study concentrates on movement and pursuit time inefficiency issues over the portable cloud.

We promote propose a few instruments to pack trap-entryways and exhibit that our pre-processed trapdoor table has a size of 0.31MB and could be adequately put away and stacked in cell phone memory. Regarding seek time, EnDAS retrofits the inquiry calculation in the cloud. In view of the parallel tree rule, we display Ranked Serial Binary Search (RSBS) calculation, which could lessen inquiry time in the cloud. Our commitments can be compressed as takes after:

1) We inspected the customary scrambled inquiry architecture as far as system activity and hunt time. Results demonstrate that the customary methodology is not appropriate in versatile cloud situations.

2) We created EnDAS to address these difficulties. Our engineering incorporates a trapdoor pressure strategy to diminish activity costs, and a Trapdoor Mapping Table (TMT) module and RSBS calculation to decrease look time.

3) We assessed the effectiveness of EnDAS in system activity and hunt time.

II. RELATED WORK

1. "Privacy-preserving multi-keyword ranked search over encrypted cloud data" [1] From This Paper we Referred-

With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE).

We establish 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 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.

2. "**Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data"** [2] **From This Paper we Referred-**

Cloud computing economically enables the paradigm of data service outsourcing. However, to protect data privacy, sensitive cloud data have to be encrypted before outsourced to the commercial public cloud, which makes effective data utilization service a very challenging task. Although traditional searchable encryption techniques allow users to securely search over encrypted data through keywords, they support only Boolean search and are not yet sufficient to meet the effective data utilization need that is inherently demanded by large number of users and huge amount of data files in cloud. In this paper, we define 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.

3. “**Secure Ranked Keyword Search over Encrypted Cloud Data”** [3] **From This Paper we Referred-**

As Cloud Computing becomes prevalent, sensitive information are being increasingly centralized into the cloud. For the protection of data privacy, sensitive data has to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow users to securely search over encrypted data through keywords, these techniques support only boolean search, without capturing any relevance of data files. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. On the one hand, users, who do not necessarily have pre-knowledge of the encrypted cloud data, have to post process every retrieved file in order to find ones most matching their interest, On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. In this paper, for the first time we define 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.

4 “**Implementing Gentry's fully-homomorphic encryption scheme**” [4] **From This Paper we Referred-**

We describe a working implementation of a variant of Gentry's fully homomorphic encryption scheme (STOC 2009), similar to the variant used in an earlier implementation effort by Smart and Vercauteren (PKC 2010). Smart and Vercauteren implemented the underlying "somewhat homomorphic" scheme, but were not able to implement the bootstrapping functionality that is needed to get the complete scheme to work. We show a number of optimizations that allow us to implement all aspects of the scheme, including the bootstrapping functionality.

Our main optimization is a key-generation method for the underlying somewhat homomorphic encryption, that does not require full polynomial inversion. This reduces the asymptotic complexity from Õ(n2.5) to Õ(n1.5) when working with dimension-n lattices (and practically reducing the time from many hours/days to a few seconds/minutes). Other optimizations include a batching technique for encryption, a careful analysis of the degree of the decryption polynomial, and some space/time trade-offs for the fully-homomorphic scheme.

5 “Efficient and secure ranked multi-keyword search on encrypted cloud data” [5] From This Paper we Referred

Information search and document retrieval from a remote database (e.g. cloud server) requires submitting the search terms to the database holder. However, the search terms may contain sensitive information that must be kept secret from the database holder. Moreover, the privacy concerns apply to the relevant documents retrieved by the user in the later stage since they may also contain sensitive data and reveal information about sensitive search terms. A related protocol, Private Information Retrieval (PIR), provides useful cryptographic tools to hide the queried search terms and the data retrieved from the database while returning most relevant documents to the user. In this paper, we propose a practical privacy-preserving ranked keyword search scheme based on PIR that allows multi-keyword queries with ranking capability. The proposed scheme increases the security of the keyword search scheme while still satisfying efficient computation and communication requirements. To the best of our knowledge the majority of previous works are not efficient for assumed scenario where documents are large files.

III.PROPOSED ALGORITHM

1. Efficient Search Algorithm

The efficient search algorithm proposed by EnDAS relies on a binary search tree structure to accelerate indexing. In the section, we will first introduce the conventional privacy-preserving index construction procedures, including index construction.

A. **Trapdoor Generation Process:**

This area presents the outline of the EnDAS framework and retrofitted trapdoor era process in EnDAS. Contrasted the EnDAS framework and traditional system , the fundamental distinction is that network traffic is diminished by a solitary round excursion information exchange and the trapdoor pressure strategy; and the pursuit time is decreased by the RSBS calculation and the TMT module; and the processing trouble for producing trapdoors is likewise offloaded by the TMT module.

- **Input:**
  Keyword: K
  Hash function in FAH algorithm: H()
  Mapping function in FAH algorithm: G()
  Noise set: ɵ = {ε1, ε 2; : : : ε p}
- **Output:**
  Index: Compressed trapdoor
  1: Extract the term t from K.
  2: if the term t hits in the TMT module then
  3: Obtain its pure trapdoor without any noise.
  4: else

Hash it by H() and get its l-bit hash code Tt = H(t);

Map Tt to Tt = {0, 1}r by G(), which contains r bits

6: end if

7. Choose q noises from the noise set ϴ to build a subset ε = {ε1, ε 2 ….εq} and accumulate it with t to get Tt V ε

8: Calculate the location of each characteristic bit 0 in t V ε by utilizing an m-bit {0, 1} codes to record this location (r = 2m), accumulate values of locations in order $\underbrace{\{0,1\}^m \bigwedge \{0,1\}^m \bigwedge \ldots \{0,1\}^m}_{f}$, get a compressed trapdoor $\bar{T_t}' = \{0,1\}^{f \times m}$ $(f$ m (f as the number of characteristic bits).

9: return Tt.

B. **Encryption and Decryption Algorithm**

1. **Encryption:** In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text (ibid.). This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message.
2. **Decryption:** An authorized party, however, is able to decode the ciphertext using a decryption algorithm, that usually requires a secret decryption key, that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm, to randomly produce keys

C. **Mathematical Model**

Let S be the whole System,

S = {R, I, P, O}

I-input,

P-procedure,

O- Output,

R- Rules,

R = should be in encrypted format data

I = {U, F U} = No of users

U = {u1, u2, …un}

F =Files in DB

F = {DF, IF, TD}

DF = Data File.

IF = Index File.

TD = Trapdoor

TD = {IK, TV}

IK = index keyword

TV = trapdoor value

P = {P1, P2, P3 }

P1 = Upload Encrypted index and Data

P2 = Generate Trapdoor,

P3 = Search File P4 Download File

O = {EDS}

EDS = Encrypted Data Search.

IV. SYSTEM ARCHITECTURE

The proposed system introduces the design of the EnDAS system and retrofitted trapdoor generation process in EnDAS. Compared the EnDAS system with traditional system, the main difference is that

(1) Network traffic is reduced by a single round trip information exchange and the trapdoor compression method; and

(2) The search time is reduced by the RSBS algorithm and the TMT module; and

(3) The computing burden for generating trapdoors is also offloaded by the TMT module. Aforementioned performance benefits are enabled by a retrofitted trapdoor generation process and a retrofitted search algorithm.

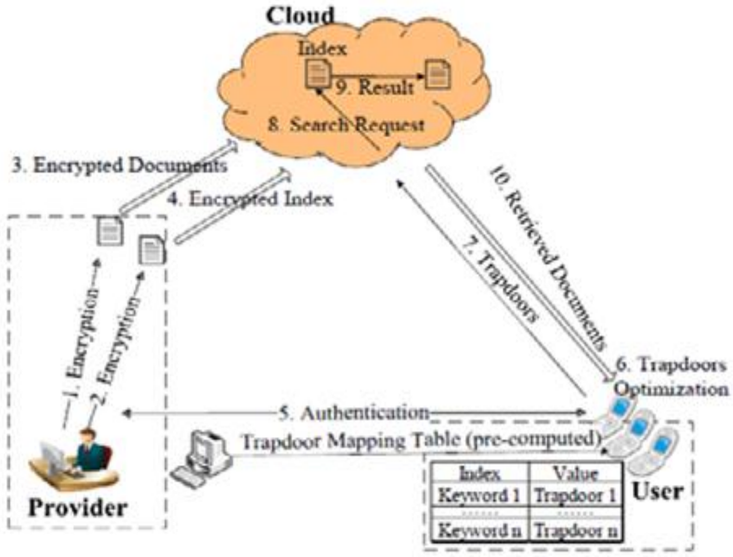
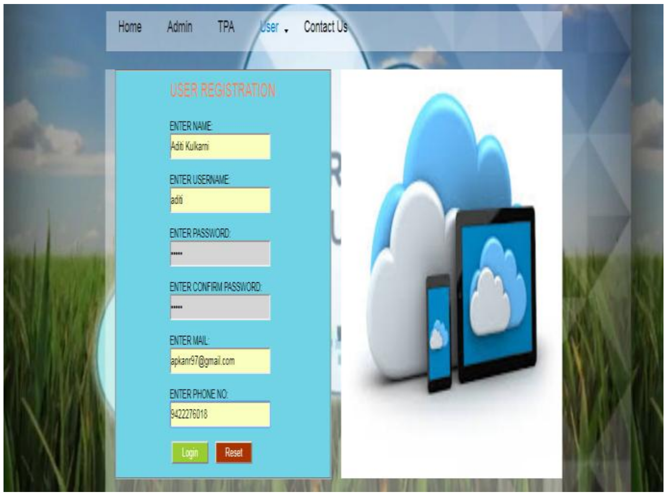


Figure 2: System Architecture

The trapdoor generation process and the cloud search algorithm are retrofitted to reduce search delay and network traffic. For trapdoor generation, EnDAS stores a precomputed Trapdoor Mapping Table (TMT) in mobile devices, which maps common English words to corresponding trapdoors. When the mobile device initiates a search request, the trapdoor is looked up from the table instead of being requested from the provider. This optimization saves one network round trip for the trapdoor generation. Furthermore, EnDAS also provides new algorithms to optimize and compress trapdoors to reduce network traffic to transmit trapdoors. For the search algorithm, EnDAS proposes to leverage a binary tree structure to reduce the lookup costs and thus improve the search responsiveness. Figure shows the search flow in EnDAS system. The retrofitted trapdoor generation process is described in this system. This process includes the trapdoor mapping table and the trapdoor compression algorithm.

V. RESULTS



ENTER NAME: Aditi Kulkarni

ENTER USERNAME: aditi

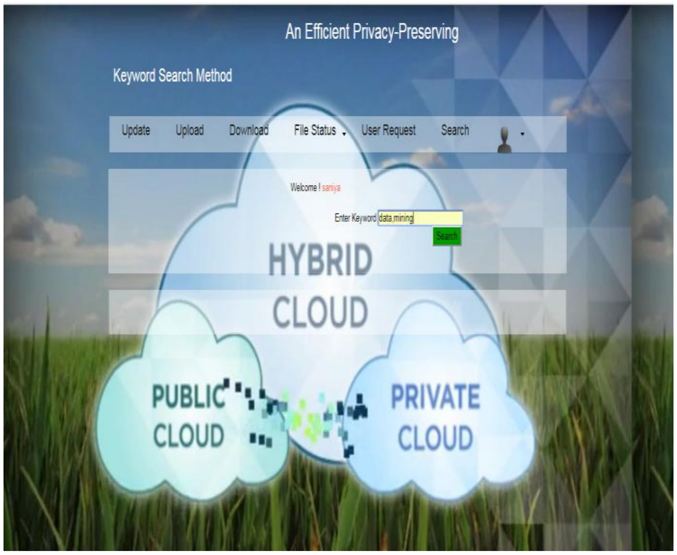
ENTER PASSWORD: •••••

ENTER CONFIRM PASSWORD: •••••

ENTER MAIL: apkanr97@gmail.com

ENTER PHONE NO: 9422276018

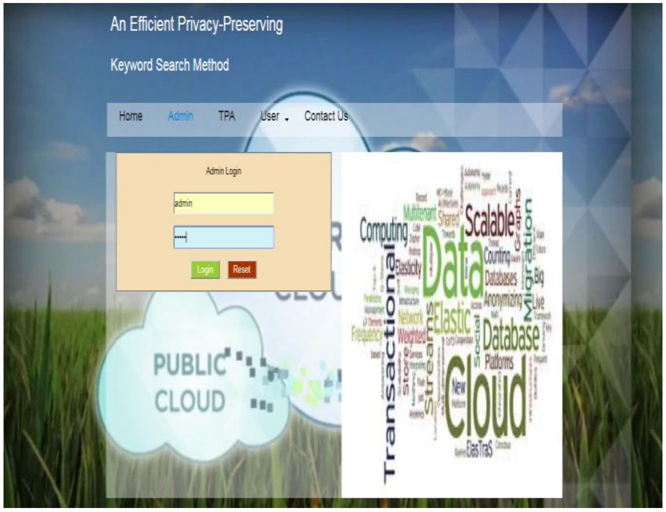
Figure 3: User Registration



Welcome ! saniya

Enter Keyword data,mining

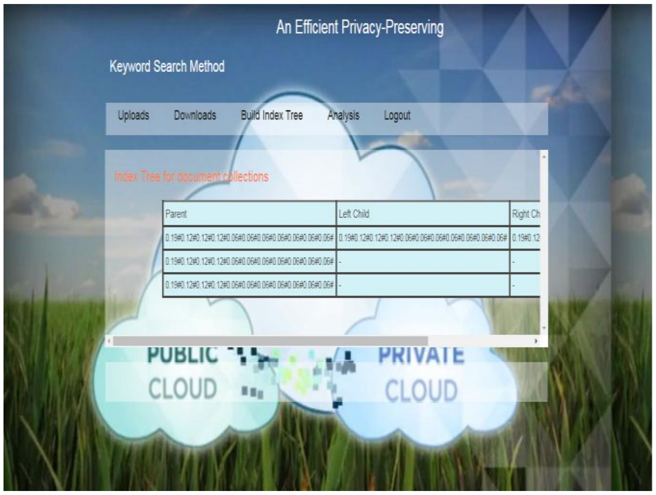
Figure 4: Keyword Search



admin

•••••

Figure 5: Admin Login



Index Tree for document collections

Parent	Left Child	Right Ch
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	0.19#0.12
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	-	-
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	-	-

Figure 6: Build Index Tree

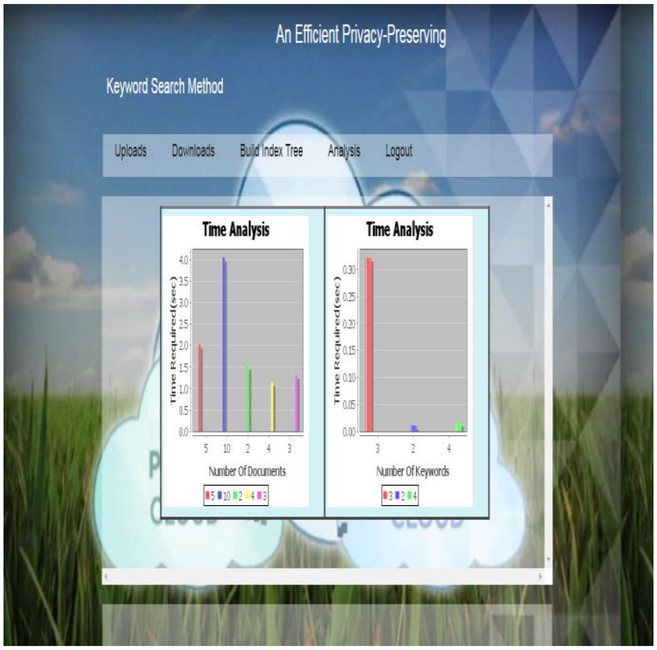


Figure 7: Performance Analysis

VI. CONCLUSION AND FUTURE WORK

In this work, we proposed a novel encrypted search system EnDAS over the mobile cloud, which improves network traffic and search time efficiency compared with the traditional system. We started with a thorough analysis of the traditional encrypted search system and analyzed its bottlenecks in the mobile cloud: network traffic and search time inefficiency. Then we developed an efficient architecture of EnDAS which is suitable for the mobile cloud to address these issues, where we utilized the TMT module and the RSBS algorithm to cope with the inefficient search time issue, while a trapdoor compression method was employed to reduce network traffic costs.

REFERENCES

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted

cloud data," in Proc. Int. Conf. Comput. Commun. (INFOCOM), Apr. 2011, pp. 829–837.

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

[3] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2010, pp. 253–262.

[4] C. Gentry and S. Halevi, "Implementing gentrys fully homomorphic encryption scheme," in Advances in Cryptology– EUROCRYPT 2011, 2011, pp. 129–148.

[5] C. Orencik and E. Savas¸, "Efficient and secure ranked multi-keyword search on encrypted cloud data," in Proc. Joint EDBT/ICDT Workshops, Mar. 2012, pp. 186–195.

[6] J. Benaloh and M. De Mare, "One-way accumulators: A decentralized alternative to digital signatures," in Advances in Cryptology EUROCRYPT 1993, 1994, pp. 274–285.

[7] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manag. Data (COMAD), Jun. 2004, pp. 563–574.

[8] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M. Wu, and D. W. Oard, "Confidentiality-preserving rank-ordered search," in Proc. ACM Workshop Storage Secur. Survivability (StorageSS), Oct. 2007, pp. 7–12.

[9] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order preserving symmetric encryption," in Advances in Cryptology EUROCRYPT 2009, 2009, pp. 224–241.

[10] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.