PRIVATE SEARCHING ON STREAMING DATA BASED ON HOMOMORPHIC ENCRYPTION

Mrs.V.RAJALAKSHMI[1], SAHAYA AURO STINA[2], SANTHIYA.S[3]

[1]Prof., Dept. of IT, Faculty of Computing, Sathyabama University, Chennai-600119, Tamilnadu, India
[2 &3] Dept. of IT, Faculty of Computing, Faculty of Computing, Sathyabama University, Chennai-600119, Tamilnadu, India
E-mail: rajalakshmibalasubramaniyan@gmail.com, aurostina@gmail.com, santhiya.js15@gmail.com

Abstract

Theoretical In this paper the issue ought to be taking into account the completely homomorphic encryption to under lying nobility's system. In the current system quantity of time essential words ought to be utilized. It does not consider magic word recurrence. The main disadvantage of existing system is memoryless. To conquer this arrangement in the proposed work consider magic word recurrence in light of straightforward completely homomorphic encryption. The information can get to just by the client secretly. In this paper information ought to be semantically secure.

Index Terms—Gentry's Technique, Private Query, Fully Homomorphic Encryption, Keyword Frequency

I. INTRODUCTION

The issue of private seeking on spilling information was initially presented by ostrovsky and skeith. In this work to consider another private question which look for reports in view of watchward recurrence. The information ought to be assault by others. So that issue create how to keep the pursuit criteria from the enemy's hands. The looking records containing one or more pivotal words k={k1,k2….kn}. On the premise of this thought a few answer for private seeking on spilling information to be proposed. In this issue two answers for private looking on spilling information one is paillier crypto framework. It permits us to handle inquiries. In completely homomorphic encryption method to give answers for coordinating archives without crashes. Scramble the recurrence edge for every essential word diverse catchphrase may have disjunctive recurrence edges. Private limit inquiry in view of watchword, which can help us more applicable archives from spilling information. In whatever remains of this paper proceed onward the related work and conclusion for the issue. This problem has many application purpose of intelligence gathering.

II. RELATED WORK

J.Bethencourt, et al. [1] A system for private stream searching allows a client to retrieve documents matching some search criteria from a remote server while the server evaluating the request. In this paper, we give a high level outline of a new scheme for this problem. The new scheme is highly efficient in practice. John Bethencourt, et al [2]the new scheme is highly e_client in practice. We demonstrate the practical applicability of the scheme by considering its performance in the demanding scenario of providing a privacy pre-serving version of the google news alerts service. Zvika braserski et al [3] Radically new approach to fully homomorphic encryption (FHE) that dramatically improves performance and bases security. In our work is a new way of constructing leveled fully homomorphic encryption schemes (capable of evaluating arbitrary polynomial-size circuits) without gentry's bootstrapping procedure. RafilOstrovsky et al [4] private searching on streaming data, we can efficiently implement searching for documents that satisfy a secret criteria (such as presence or absence of hidden combination of hidden keywords) under various cryptographic assumptions. Result can be viewed in a verityof ways. Positive results and delegation. Ivan Damg et al [5] paillier's probabilistic open key framework, the development element is decreased and which permits to change the square length of the plan even after general society key has been _xed, without losing the homomorphic property. The speculation is securing the Paillier's unique framework and proposes a few approaches to enhance executions. We build an edge variation of the summed up plan. The zero learning

conventions to demonstrate that a given figure content encodes one of a set given plain messages, and conventions to confirm multiplicative relations on plain messages. We can demonstrate how these building squares can be utilized for applying the plan to e_client electronic voting. Taherelgamal et al [6]it it should be introduces some of the possible attacks on the signature scheme. Some of these attackers are easily shown to be equivalent to computing discrete logarithms over GF (p). It has not yet been proved that breaking the signature scheme is equivalent to computing discrete logarithms or equivalent to breaking the distribution scheme. The reader is encouraged to

Grow new assailants, or discover quick calculations to perform one of the aggressors portrayed. The assaults will be partitioned into two gatherings. Taherelgamal et al [7] two improvements to Gentry's completely homomorphic plan in light of perfect cross sections and its investigation: we give a more forceful examination of one of the hardness suspicion and we present a probabilistic decoding calculation that can be executed with a logarithmic circuit of low multiplicative degree. These enhancements likewise apply to the completely homomorphic plans of Smart and Vercauteren [PKC'2010] and van Dijk et al. [8] Inf. Michael Niedermeier and Prof. Dr. Hermann de Meer at the seat of Computer Networks and Communications, this paper covers the examination of the security ensuring limits of homomorphic cryptography in the Smart Grid concerning its imperativeness capability. The paillier computation gives the representation for homomorphic cryptography. It is used as a piece of two different structural circumstances which are familiar and after that differentiated and lopsided and symmetric cryptography as for their benefit and rational congruity [9Taking after Gennaro, Gentry and Parno (Cryptology ePrintarchieve 2009/547), we use totally homomorphic encryption to plan improved arrangements for allotting count. In such plans, a delegator out sources the revenge of an utmost F on different, proficiently picked inputs xi to a laborer in such a course, to the point that it is infeasible for the star to make the delegator perceive an outcome other than F(xi).The "online stage" of the Gennaro et al. Our _rst headway takes out the massive open key from the plan. Gennaro et al. The delegator still contributes poly (T) time in the online stage, however does not need to confer or appropriate anything. ElGamal et al [10] another mark plan is proposed, together with an execution of the Diffie-Hellman key appropriation conspire that attains to an open key cryptosystem. The security of both frameworks depends on the trouble of processing discrete logarithms over limited fields. X. Yi et al [11] Private looking for on spouting data is a technique to dispatch to an open server a framework which chases spilling wellsprings of data without revealing looking criteria and subsequently sends back a help .containing the finding The late jump forward in totally homomorphic encryption has allowed us to create subjective looking for criteria theoretically We show an improvement of the chasing criteria down private edge looking for on spilling data on the reason of the best in class totally homomorphic encryption procedures. Our tradition is semantically secure the length of the essential totally homomorphic encryption arrangement is semantically secure. Z. Brakerski et al.[12] totally homomorphic encryption arrangement that is considering the (standard) learning with breaches (LWE) assumption. Applying known the results of LWE, the security is considering most adverse plausibility. The hardness of "short vector issues" considering subjective networks. Homomorphic encryption upgrades past works in two plot: 1) we exhibit that "to a degree homomorphic" encryption can be taking into account LWE, utilizing another re-linearization method. In get, all past plans depended on many-sided quality suppositions identified with goals in different rings. 2) We digress from the "squashing ideal model" utilized as a part of all past works. We present another measurement modules diminishment procedure, which abbreviates the figure messages and diminishes the unscrambling intricacy of our plan, without presenting extra suppositions.

A. Existing System:

To perform private searching for keywords, Ostrovsky and Skeith segmented the streaming data S into streaming documents fM1; M2; . . ., each of which is composed of a number of words, and filtered one at a time. If two different matching documents are ever added to the same buffer box, a collision will occur and both copies will be lost. The existing solutions for private searching on streaming data have not considered keyword frequency, the number of times that keyword is used in a document. Search engines like Google.

Disadvantages:

- Large data couldn't maintain by the process of keyword search.
- Disjunctive threshold query based on keyword search only supported.
- The Quality of Service is low, because of Disjunctive threshold problem.

B. Proposed Work:

In this undertaking proposed an answer for quest for reports containing more than t out of n magic words, purported (t; n) edge looking. The arrangement is based on the best in class completely homomorphic encryption (FHE) method and the cradle keeps at most m coordinating archives without crashes. Hunting down records containing one or more ordered essential words like can be attained to by (1; n) limit looking. We consider another private question, which hunt down records from gushing information in view of essential word recurrence, such that various times that a catchphrase shows up in a coordinating record are not a needed to be higher or lower than a given limit. Proposed an alternate methodology for recovering coordinating archives from the support

Advantages:

- Efficient prohibition of searching a keyword in a particular frequency.
- Conjunctive threshold query based on keyword frequency.
- Conjunctive threshold query is composed of four key words: KeyGen, Filtered, Filter Exec, and Buffer Dec.
- Our conjunctive construction can be formally presented.

i. System Architecture

The overall system architecture is shown in figure1, Which consists of the following components, User Interface, Filter Generation, Threshold Queries, Public Database Management, Semantic Security

1. User Interface Design

Interface design deals with the process of developing a method for modules in a system to connect and communicate. These modules can apply for software, hardware or the interface between a user and machine. In this module mainly we are focusing the login design page with the Partial knowledge information. Application Users need to view the application they need to login through the User Interface GUI is the media to connect User and Media Database and login screen where user can input his/her username and password will check in database, if that will be valid username and password then he/she can access the database.

2. Filter Generation

You can always see the result of the mix of all these components in the one file Continuous aggregation queries over dynamic data are used for decision making and timely business intelligence. In this we consider a new queries, where a client to be notified over distributed data crosses a specified file. Any type of file user upload not creating separate database for particular files but filter generation filter one folder only maintain all the files. Also, learn about integrating features such as single sign-on and cooperative sharing information using the properties.

3. Threshold Queries

The performance comparison of our threshold query protocols can be summarized in Complexity client and Complexity server, where enc. And dec. Stand for encryption and decryption of that data. In such queries client desires to be notified whenever the ratio of two aggregates, over distributed data, crosses the specified threshold.

- Mainly two types of queries is there
- Disjunctive threshold queries. Conjunctive threshold queries

4. Public DB Management

Database systems are central to most organizations information systems strategies. At any organizational level, user can expect to have frequent contact with database systems. Therefore skills in using such system-understanding their capabilities and limitations. How to access data directly or through technically. How to effectively use the information such systems can provide, skills in designing new systems and related applications – is a distinct advantage and necessity in public DB

Administration continuously our information put

away in scramble form on the grounds that aggressors don't comprehend the information.

5. *Semantic Security*

Semantic security gives measures to anticipating, confining or minimizing impacts of semantic assaults. Conventional ways to data framework security concentrated on ensuring frameworks and the data put away, transformed and disseminated on them. The objective of this task is to create strategies to recognize irregularities or anomalies (Behavior that ruptures the standard, custom or ethical quality) in online data, distinguish false data and assess the dependability of data sources and track those sources. A semantic assault is one in which the aggressor alters electronic data in such a path, to the point that the outcome is wrong, yet looks right to causal or maybe even the mindful viewer. IRIA added to an arrangement of semantic assaults, and additionally executing a set of methods for recognizing semantic assaults.

(Examination and Reporting of Incidents and Accidents)

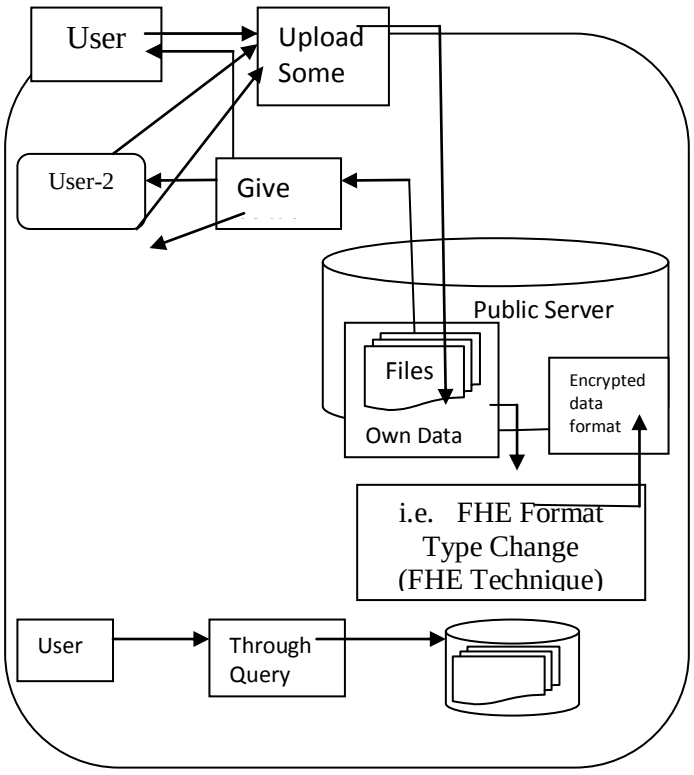

Figure1. System Architecture

Step.1 Key gen (k) Takes a security parameter k and generates a pair of public and secret key (pk,sk).

Step.2 Filter gen (D,Qk,pk) A query Qk the public key pk and generate the program F.

Step.3 Filter Exec (S,F,pk,m) S,F search for any document Qk(M) = 1 processing one document at a time and encrypt each matching document with the public key and keep up to m encrypted document in a buffer B and finally outputs an encrypted buffer B.

Step.4 Buffer Dec (B,sk) Decrypts the encrypted buffer using the privatekey.

Algorithm

III. PERFORMANCE ANALYSIS

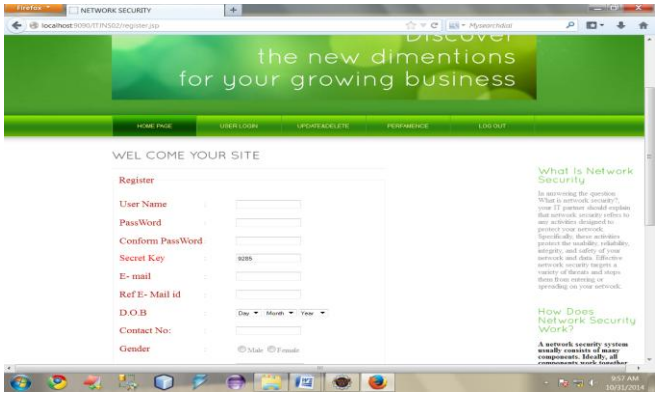

Figure2. Registration

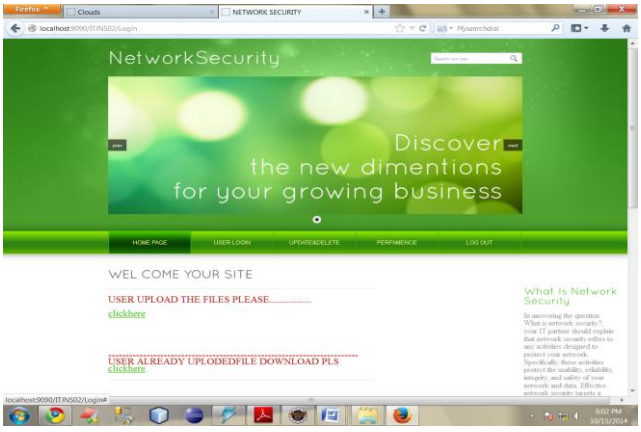

Figure3. File upload

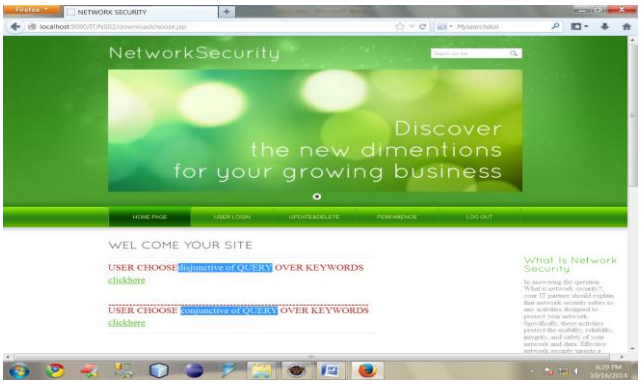

Figure4. Download file

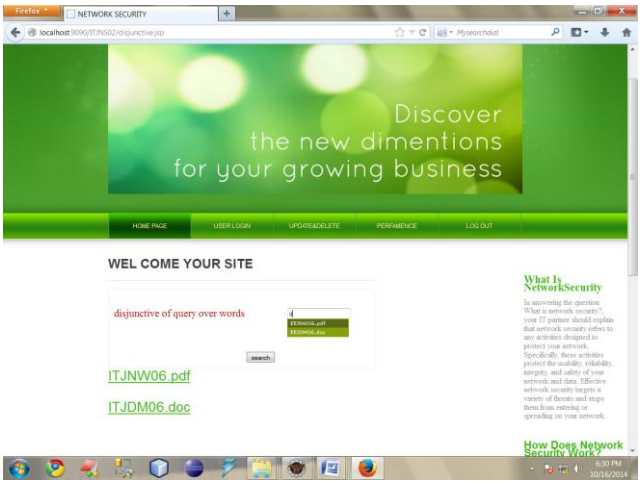

Figure 5. Disjunctive query

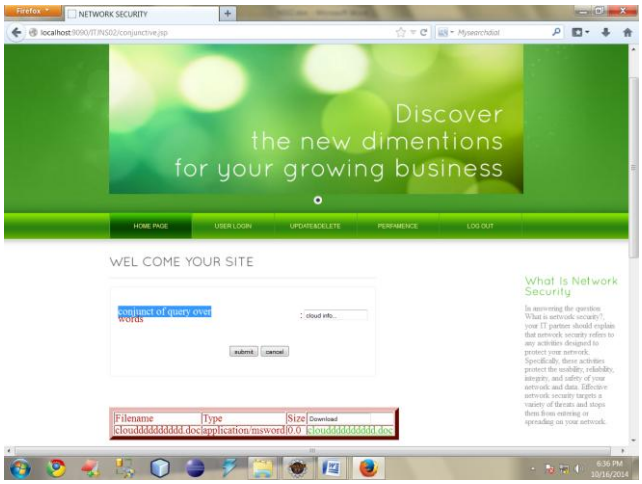

Figure 6. Conjunctive Query

In (Fig 6) An handoff is taking place where the data flow is shifting from one relay node to another because of its coverage

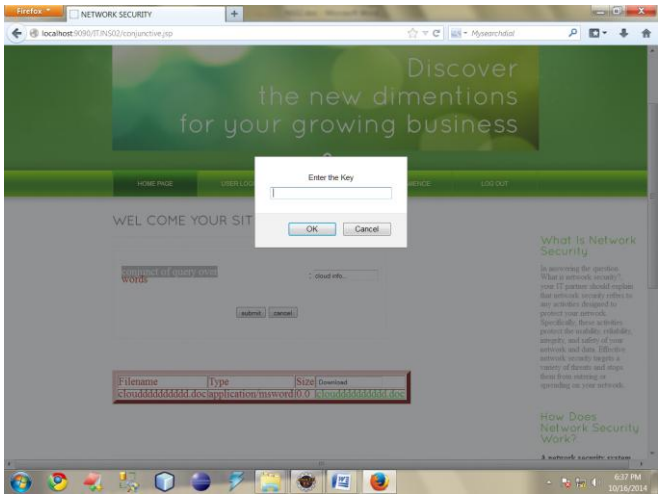

Figure7. Secret key

IV. CONCLUSION

On the premise of the best in class completely homomorphic encryption procedures, we have exhibited developments for disjunctive, conjunctive and supplement limit inquiry in view of essential word recurrence. Conventions are semantically secure the length of the basic completely homomorphic encryption plan is semantically secure. The future can reach out the length of the basic completely homomorphic encryption plan is functional, our conventions will be useful. So far completely homomorphic encryption plan are case for your put away numerous records.

Client need to know what number of records transferred and downloaded in that time client enters our name based upon the name what number of documents transferred and downloaded in table. So processing expense is diminished.

REFERENCES

[1]. J.Bethencourt, D.song and B.water & ldquo, New construction and practical applications for private searching & rdquo, proc IEEE symp. Security and privacy, 2006.

[2]. John Bethencourt, Brent Waters. New constructions and practical applications for private stream searching, 2010.

[3]. Zvika braserski, Craig Gentry Fully. Homomorphic Encryption without Bootstrapping, 2007.

[4]. Rafil and Ostrovsky, Private Searching On Streaming Data,2007

[5]. Ivan Damg_ard, MadsJurik and JesperBuus Nielsen A Generalization of Paillier's Public-Key System with Applications to Electronic ScheduliVoting.ks, 2010

[6]. Taherelgamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms , 2009

[7]. Damien Stehle, Faster Fully Homomorphic Encryption, 2007

[8]. Maximiliane Zirm, Michael Niedermeier, The Future of Homomorphic Cryptography in Smart Grid Applications, 2008

[9]. Kai-Min Chung, SalilVadhan, Improved Delegation of Computation using Fully Homomorphic Encryption , 2005

[10]. T. ElGamal, & ldquo,A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,& rdquo, *IEEE Trans. Information Theory,* vol. 31, no. 4, pp. 469-472, July 1985.

[11]. X. Yi and C.P. Xing, & ldquo, Private (t, n) Threshold Searching on Streaming Data,& rdquo, *Proc. Int',l Conf. Social Computing Privacy, Security, Risk and Trust (PASSAT ',12),* pp. 676-683, 2012.

[12]. Z. Brakerski and V. Vaikuntanathan, & ldquo, Efficient Fully Homomorphic Encryption from (Standard) LWE,&rdquo, http://eprint.iacr.org/344, 2011.