International Journal of Science Engineering and Advance Technology

Ensuring Semantic Security in Keyword Search using Searchable Public-Key Ciphertexts with Hidden Structures

P Gnana Iswarya[1], P Sunitha[2]
[1]M.Tech (CSE), Dhanekula Institute of Engineering & Technology, A.P., India.
[2]Asst.Professor, Dept. of Computer Science & Engineering,
Dhanekula Institute of Engineering & Technology, A.P., India.

Abstract — This paper propose searchable public key ciphertexts with inconspicuous structure for catchphrase investigate as quick as doable lacking giving up semantic security of the scrambled watchwords. In SPCHS, each one watchword searchable ciphertext are arranged by inconspicuous relative, and with the pursuit trapdoor consequent to a catchphrase, the littlest sum in succession of the relations is identify with a search for calculation as the supervision to find all comparing ciphertext capably. In SPCHS (Searchable Public-Key Ciphertexts with Hidden Structures), all catchphrase searchable ciphertexts are organized by concealed relations, and with the inquiry trapdoor relating to a watchword, the base data of the relations is revealed to a hunt calculation as the direction to locate all coordinating ciphertexts proficiently. The inquiry intricacy of our plan is reliant on the genuine number of the ciphertexts containing the questioned catchphrase, instead of the quantity of all ciphertexts. At long last, we introduce a non specific SPCHS development from mysterious character based encryption and crash free full-personality moldable Identity-Based Key Encapsulation Mechanism (IBKEM) with secrecy. We outline two impact free full-character pliant IBKEM examples, which are semantically secure and unknown, individually.

Keywords — **Public-key searchable encryption, semantic security, identity-based key encapsulation mechanism, identity based encryption**

I. INTRODUCTION

Information encryption techniques will keep the generally utilized question operation on classified information. The catchphrase seek gets to be troublesome when information are encoded. In 2004, Boneh et al. [1] proposed the primary open key encryption plan with watchword seek (PEKS) to manage the issue of looking on secret information. Open KEY encryption with catchphrase seek (PEKS), presented by Boneh et al. in [1], has the preferred standpoint that any individual who knows the beneficiary's open key can transfer watchword searchable ciphertexts to a server. The beneficiary can appoint the catchphrase inquiry to the server. All the more particularly, every sender independently scrambles a record and its separated watchwords and sends the subsequent ciphertexts to a server; when the collector needs to recover the documents containing a particular catchphrase, he appoints a watchword look trapdoor to the server; the server finds the encoded documents containing the questioned watchword without knowing the first documents or the watchword itself, and returns the relating scrambled records to the recipient; at long last, the beneficiary unscrambles these scrambled files1.

As the interest of cloud administrations is expanding, increasingly touchy information and classified data is being put away over cloud servers. Messages, individual wellbeing records, private recordings and photographs, budgetary information, government archives, military data and so forth are put away on cloud servers. In this way, information encryption turns out to be exceptionally fundamental for securing information protection and for avoiding unapproved access to private information. In this way, for security reasons cloud information is encoded before outsourcing for end-to-end information secrecy. In any case, productive inquiry of scrambled information turns out to be exceptionally troublesome and testing undertaking, in light of the fact that there could be huge measure of outsourced information records.

Notwithstanding this, on cloud servers a lot of information is outsourced for an expansive quantities of clients. Be that as it may, amid a specific session a client might be keen on recovering a particular document of his advantage as it were. It should be possible utilizing watchword based inquiry technique. Watchword based hunt procedure is exceptionally mainstream in plaintext look situations; in which client can specifically seek records of his enthusiasm utilizing the catchphrase. Be that as it may, unfortunately, when information is in scrambled structure client can't perform catchphrase based inquiry questions. Further, watchword security is additionally required at cloud server for scrambled information records.

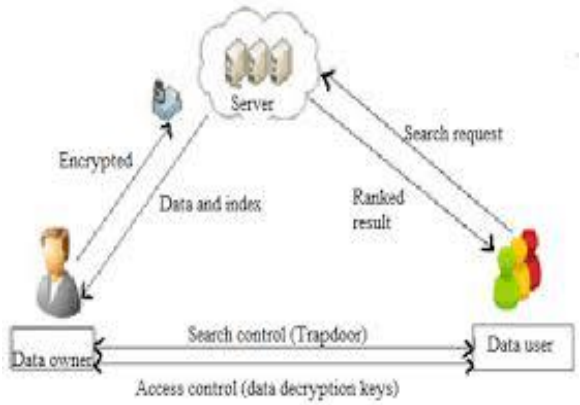

Figure 1: Architectural Diagram

The above architectural diagram is clarified as takes after. To start with, every sender independently scrambles a document and its extricated catchphrases and sends the subsequent ciphertexts to the server. At the point when the beneficiary needs to recover the records containing a particular watchword, he endows a catchphrase look trapdoor to it and finds the comparing encoded documents containing the questioned catchphrase. It additionally ensures that the first documents or the catchphrase itself is not known and after that profits the comparing encoded records to the collector. At last, the recipient unscrambles these encoded documents.

In this idea of Searchable Public-key Ciphertexts with Hidden Structures (SPCHS), the shrouded structures alongside the catchphrase searchable ciphertexts are created in an open key setting. The incomplete relations can be made known not all the coordinating ciphertexts with the assistance of a watchword trapdoor. It is additionally significant that the semantic security is characterized for both the catchphrases and the concealed structures. Contrasting with the current PEKS plan, it doesn't contain any sort of shrouded structure among the PEKS ciphertexts and in addition its semantic security is characterized for the catchphrases. In this way, the inquiry execution depends just on the genuine number of ciphertexts as opposed to all the ciphertexts which enhances the time many-sided quality and at last the execution.

II. LITERATURE STUDY OF VARIOUS SEARCH SCHEMES

A) Fuzzy logic based search:

A straightforward method is to build a similarity keyword set that incorporates not only the exact keywords but also those that differ by up to edit distance d. Also, the search would require a trapdoor for each similar word to the query keyword. However, this incurs high storage and computation overhead at the server side due to the large number of possible similar keywords.

Ranked search over encrypted data:

Ranking of search results is very important for efficient utilization of search methodology. Inverted index structures are very useful for ranked keyword search. At first, when user generates a query using search keyword, relationship between terms is identified using index values of terms. After that operations (like matching or sorting etc) are performed on retrieved data to generate ranks. For example a mathematical function is given for calculating relevance score of words and files to calculate ranks:

$Score(t, Fd) = 1\,|Fd| \cdot (1 + \ln fd,t)$

Where t is the search keyword (term), fd,t denotes the term frequency (TF) of keyword t in file Fd, and $|Fd|$ is the number of indexed keywords info.

Symmetric Searchable Encryption:

Secure searchable encryption (SSE) is a deterministic encryption scheme generally based on symmetric key of cloud owner and data user. Curtmola et al. proposed SSE [8], which uses inverted index scheme and also some basics of permutation and pseudorandom functions. This method of searching is quite efficient. Roughly speaking, the index consists of blinded keywords $fk(wi)$ and lists of FIDs containing wi keywords, where f () is a pseudorandom function and k is the secret key. The search trapdoor is also in the same form so that the server can perform matching. However, it only supports single-keyword exact query.

III. PROPOSED MODEL FOR SPCHS

Use defining the thought of Searchable Public-key Cipher texts with secret Structures and its linguistics security. During this new conception, keyword searchable cipher texts with their unidentified structures are often generated within the public key location. With a keyword seek for trapdoor, partial relations are often divulge heart's contents to show the novelty of all connected cipher texts. Linguistics security is definite for each the keywords and therefore the unknown structures. The system is established semantically safe supported the Decisional linear Diffie- playwright (DBDH) hypothesis within the Ro model. Also are being attentive in providing a regular SPCHS building to provide keyword-searchable ciphertexts with a secret starlike construction. Our normal SPCHS is excited by many exciting rationalization on Identity-Based Key Encapsulation Mechanism (IBKEM). In IBKEM, a sender encapsulates a key K to an intentional receiver ID. Of course, receiver ID will decapsulate and come through

K, and therefore the sender recognize that receiver ID can come through K conversely, a non-intended receiver ID0 may try and decapsulate and come through K0. Observe that, (1) it's usually the case that K and K0 are self-determining of each different from the read of the receivers, and (2) in some IBKEM the sender may recognize K0 obtained by receiver ID0. Discuss with the previous merchandise as conflict freeness and to the latter as full-identity plasticity. An IBKEM theme is alleged to be collision free full identity susceptible if it possesses each properties. Build a generic SPCHS construction with Identity-Based cryptography and collision free full-identity malleable IBKEM. Above diagram contains four models:

- Data Owner: Data Owner first of all login and so it upload a file into the information server. Then that files are with success hold on by the information server. It transfers the files with searchable keyword.
- Data Server: Data server is hold on server files. Data server additionally sight the assaulter and attacker's entry are hold on by the information server within the information. All transactions record also is hold on by the information server. Information server provides the key to the top user. It additionally provides the file to the top user for transfer.
- End User: End user first of all login subsequently it'll be send the cipher text to the information server. After that information server passes a public key. Then users are providing the file name to the information server. If the file name gift within the information server with revered keyword then and so solely that file area unit transfer otherwise not. It provides file with t here magnitude relation and delay.
- Verifier: Verifier is to check the entry of the each information owner and user. If the entry area unit gift within the information then and so solely information owner and user area unit login with success otherwise it rejected by the verifier.

The Proposed Generic SPCHS Construction

Let keyword space $W \subset IDI_{BKEM} = ID_{IBE}$. Our generic SPCHS construction from the collision-free full-identity malleable IBKEM and IBE is as follows.
Structure Initialization (*PK*): Take as input *PK*, arbitrarily pick a keyword $W \in W$ and a random value *u*, generate an IBKEM encapsulated key and its encapsulation $(K,C) = Encaps_{IBKEM}(PK_{IBKEM},W,u)$, and initialize a hidden structure by outputting a pair of private-and-public parts (*Pri* = (*u*); *Pub* = *C)*. Note that *Pri* here is a variable list formed as $(u,\{(W, Pt[u,W] | W \in W\})$, which is initialized as *(u*).

IV. RELATED WORK

Search on encrypted data has been extensively investigated in recent years. From a cryptographic perspective, the existing works fall into two categories, i.e., symmetric searchable encryption [14] and public-key searchable encryption.

Symmetric searchable encryption is occasionally referred to as symmetric-key encryption with keyword search (SEKS). This primitive was introduced by Song et al. in [15]. Their instantiated scheme takes search time linear with the size of the database. A number of efforts [6], [7], [8], [9], [10] follow this research line and refine Song et al.'s original work. The SEKS scheme due to Curtmola et al. [14] has been proven to be semantically secure against an adaptive adversary. It allows the search to be processed in logarithmic time, although the keyword search trapdoor has length linear with the size of the database. In addition to the above efforts devoted to either provable security or better search performance, attention has recently been paid to achieving versatile SEKS schemes as follows. The works in [14], [3] extend SEKS to a multi-sender scenario. The work in [4] realizes fuzzy keyword search in the SEKS setting. The work in [5] shows practical applications of SEKS and employs it to realize secure and searchable audit logs. Chase et al. [4] proposed to encrypt structured data and a secure method to search these data. To support the dynamic update of the encrypted data, Kamara et al. proposed the dynamic searchable symmetric encryption in [5] and further enhanced its security in [6] at the cost of large index. The very recent work [7] due to Cash et al. simultaneously achieves strong security and high efficiency. Following the seminal work on PEKS, Abdalla et al. [8] fills some gaps w.r.t. consistency for PEKS and deals with the transformations among primitives related to PEKS. Some efforts have also been devoted to make PEKS versatile. The work of this kind includes conjunctive search [10], [11], [12], [13], [14], [15], range search [5], [7], subset search, time-scope search [8],[3], similarity search [9], authorized search equality test between heterogeneous ciphertexts [1], and fuzzy keyword search [2]. In addition, Arriaga et al. [3] proposed a PEKS scheme to keep the privacy of keyword search trapdoors. In the above PEKS schemes, the search complexity takes time linear with the number of all ciphertexts. In [4], an oblivious generation of keyword search trapdoor is to maintain the privacy of the keyword against a curious trapdoor generation. A chain-like structure is described to speed up the search on encrypted keywords. One may note that the chain in [40] cannot be fully hidden to the server and leaks the frequency of the keywords (see Supplemental Materials A for details). To realize an efficient keyword search, Bellare et al. [2] introduced deterministic public key

encryption (PKE) and formalized a security notion "as strong as possible" (stronger than onewayness but weaker than semantic security). A deterministic searchable encryption scheme allows efficient keyword search as if the keywords were not encrypted. Bellare et al. [2] also presented a deterministic PKE scheme (i.e., RSADOAEP) and a generic transformation from a randomized PKE to a deterministic PKE in the random oracle model. Subsequently, deterministic PKE schemes secure in the standard model were independently proposed by Bellare et al. [1] and Boldyreva et al. [2]. The former uses general complexity assumptions and the construction is generic, while the latter exploits concrete complexity assumptions and has better efficiency. Brakerski et al. [3] proposed the deterministic PKE schemes with better security, although these schemes are still not semantically secure. So far, deterministic PEKS schemes can guarantee semantic security only if the keyword space has a high min-entropy. Otherwise, an adversary can extract the encrypted keyword by a simple encrypt-and-test attack. Hence, deterministic PEKS schemes are applicable to applications where the keyword space is of a high min-entropy.

V. CONCLUSION

This paper investigated as-fast-as-possible search in PEKS with semantic security. We proposed the concept of SPCHS as a variant of PEKS. The new concept allows keyword-searchable ciphertexts to be generated with a hidden structure. Given a keyword search trapdoor, the search algorithm of SPCHS can disclose part of this hidden structure for guidance on finding out the ciphertexts of the queried keyword. Semantic security of SPCHS captures the privacy of the keywords and the invisibility of the hidden structures. We proposed an SPCHS scheme from scratch with semantic security in the RO model. The scheme generates keyword-searchable ciphertexts with a hidden star-like structure. It has search complexity mainly linear with the exact number of the ciphertexts containing the queried keyword. It outperforms existing PEKS schemes with semantic security, whose search complexity is linear with the number of all ciphertexts. We identified several interesting properties, i.e., collision-freeness and full-identity malleability in some IBKEM instances, and formalized these properties to build a generic SPCHS construction. We illustrated two collision-free full-identity malleable IBKEM instances, which are respectively secure in the RO and standard models. SPCHS seems a promising tool to solve some challenging problems in public-key searchable encryption. One application may be to achieve retrieval completeness verification which, to the best of our knowledge, has not been achieved in existing PEKS schemes. Specifically, by forming a hidden ring-like structure, i.e., letting the last hidden pointer always point to the head, one can obtain PEKS allowing checking the completeness of the retrieved ciphertexts by checking whether the pointers of the returned ciphertexts form a ring. Another application may be to realize public key encryption with content search, a similar functionality realized by symmetric searchable encryption. Such kind of content searchable encryption is useful in practice, e.g., to filter the encrypted spam's. Specially, by forming a hidden treelike structure between the sequentially encrypted words in one file, one can obtain public-key searchable encryption allowing content search (e.g., to find whether there are specific contents in an encrypted file). The search complexity is linear with the size of the queried content.

REFERENCES

[1] Boneh D., Crescenzo G. D., Ostrovsky R., Persiano G.: Public Key Encryption with Keyword Search. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506-522. Springer, Heidelberg (2004).

[2] Bellare M., Boldyreva A., O'Neill A.: Deterministic and Efficiently Searchable Encryption. In: Menezes A. (ed.) CRYPTO 2007. LNCS vol. 4622, pp. 535-552. Springer, Heidelberg (2007)

[3] Boneh D., Boyen X.: Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223-238. Springer, Heidelberg (2004)

[4] Boyen X., Waters B. R.: Anonymous Hierarchical Identity-Based
Encryption (Without Random Oracles). In: Dwork C. (ed.) CRYPTO
2006. LNCS, vol. 4117, pp. 290-307. Springer, Heidelberg (2006)

5] Gentry C.: Practical Identity-Based Encyrption Without Random
Oracles. In: Vaudenay S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp.445-464. Springer, Heidelberg (2006)

[6] Ateniese G., Gasti P.: Universally Anonymous IBE Based on the
Quadratic Residuosity Assumption. In: Fischlin M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 32-47. Springer, Heidelberg (2009)

[7] Ducas L.: Anonymity from Asymmetry: New Constructions for Anonymous HIBE. In: Pieprzyk J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 148-164. Springer, Heidelberg (2010)

[8] Abdalla M., Catalano D., Fiore D.: Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions. Journal of Cryptology, 27(3), pp. 544-593 (2013)

[9] Freire E.S.V., Hofheinz D., Paterson K.G., Striecks C.: Programmable Hash Functions in the Multilinear Setting. In: Canetti R., Garay J.A. (eds.) Advances in Cryptology - CRYPTO 2013. LNCS, vol. 8042, pp. 513-530. Springer, Heidelberg (2013)

[10] Garg S., Gentry C., Halevi S.: Candidate Multilinear Maps from Ideal Lattices. In: Johansson T., Nguyen P. (eds.) Advances in Cryptology - EUROCRYPT 2013. LNCS, vol. 7881, pp. 1-17. Springer, Heidelberg (2013)

[11] Boneh D., Franklin M.: Identity-Based Encryption from the Weil Pairing. In: Kilian J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213-239. Springer, Heidelberg (2001)

[12] Barth A., Boneh D., Waters B.: Privacy in Encrypted Content Distribution Using Private Broadcast Encryption. In: Di Crescenzo G., Rubin A.(eds.) FC 2006. LNCS, vol. 4107, pp. 52-64. Springer, Heidelberg (2006)

[13] Libert B., Paterson K. G., Quaglia E. A.: Anonymous Broadcast
Encryption: Adaptive Security and Efficient Constructions in the Standard Model. In: Fischlin M., Buchmann J., Manulis M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 206-224. Springer, Heidelberg (2012)

[14] Curtmola R., Garay J., Kamara S., Ostrovsky R.: Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. In: ACM CCS 2006, pp. 79-88. ACM (2006)

[15] Song D. X., Wagner D., Perrig A.: Practical techniques for searches on encrypted data. In: IEEE S&P 2000, pp. 44-55. IEEE (2000)

Ms P Sunitha is presently working as Assistant professor in CSE department. Dhanekula Institute of Engineering & Technology, Ganguru, Vijayawada. She has obtained B.Tech., degree from JNTU, Hyderabad and M.Tech., degree from JNTU, Kakinada. She is presently doing Ph.D., Kakinada in the research area of Cloud Computing. She has published several research papers in various national and international Journals.

Ms P Gnana Iswarya is a student of Dhanekula Institute of Engineering & Technology, Ganguru, Vijayawada. She is presently pursuing her M.Tech., degree from Dhanekula Institute of Engineering & Technology Affiliated to JNTU, Kakinada. She has obtained B.Tech., degree from Dhanekula Institute of Engineering & Technology Affiliated to JNTU, Kakinada in the year 2014.