iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** III **Month of publication:** March 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Generating Content Searchable Cipher Texts with Semantic Security

Pondkule Priyanka[1], Yadav Ashwini[2], Khomane Sharmila[3], Nale Supriya[4], Prof. Kadam P.R.[5]
[1,3,5]*Department of Computer Engineering, Savitribai Phule Pune University*

Abstract— Many systems which uses various content distribution over the network requires access restriction, prevention from unauthorized access and hiding the identity of users. Current systems face problems there are some types of attacks are there on user privacy. Lot of work has been done on keyword searchable cipher text with public key encryption. In public key encryption to search keyword has advantage that anyone who knows the public key of receiver can upload file easily with encrypted cipher text. This technique is semantically secure and takes search time equal to number of cipher texts. But system face problems when we retrieve data from large databases.to tackle this problem searchable public-key cipher texts with hidden star like structures (SPCHS) provides fast keyword search with keeping semantic security of keyword which are encrypted. In this paper we focus on another different application of public key encryption in which we are going for content search. We are applying the same technique of semantic security by making the hidden tree structure. Such type of content search is useful while recognizing the spams which are encrypted. While doing this we are keeping focus on search complexity should be linear with the query content size. Finally, we present an architecture with a generic SPCHS construction which we got as output from anonymous identity-based encryption and collision-free full-identity adaptable Identity-Based Key Encapsulation Mechanism (IBKEM) with anonymity.

Keywords— Identity-Based Key Encapsulation Mechanism component, semantic security, Public-key searchable encryption.

I. INTRODUCTION

In network communication at server side it is important to make some fixed data available to certain users only. It is also important to keep identity of users secure who are accessing the content. In this simple method of data protection we are getting the problem at network communicated data receiver may want to keep data secure and receiver may want to keep it safe from administrator also. The Public key encryption technique which was introduced by Boneh D [1], gives us advantage that if anyone knows the receiver's public key can upload file and keyword to the server. The receiver gives authority to the server for keyword search. While sending the file sender sends the file in encrypted format and chosen keywords and content extracted from the file and outputted cipher text. When receiver wants any type of file having specific keyword he gives a keyword for search to the trapdoor at the server. User also gives specific content search. Server starts the process of finding and server finds the file which is in an encrypted format and contained keyword queried by client without any knowledge of original contain of file and content also and provides the file to the receiver. Receiver of the file will decrypt these file and if want this is a spam then can report to server also.

Existing system of secure public key encryption for keyword search takes search time of keyword linear with the total number of cipher texts. The system developed by Peng Xu[2], they considered deterministic encryption for keyword search in this technique they use searchable public-key cipher texts with hidden star like structures (SPCHS) for fast keyword search. By implementing this same technique we are working for the content search. Sender uploads the encrypted file containing encrypted keyword with encrypted content and receiver may download the file by giving the specific cipher text of keyword or the content to download the file and if receiver finds that this one is spam then it reports server about the spam mail and server will keep restricting such type of file from the sender.

A. Our Motivation

We are keeping our interest to work on the generating content searchable cipher text by using SPCHS without relinquishes the semantic security .We find that in many applications keeping semantic security of data is crucial while searching the keyword. So taking search time linear with the number of cipher text is difficult. Also in the same scenario we face problem at the find encrypted content search and reporting whether it is spam or not. The linear time complexity of findings looks unavoidable as sever checks each and every cipher text. Same problem is also unavoidable while working with the content also. If we go for in detail then it seems that it's still possible to work with content also with the help of SPCHS.

B. Our Work

We are working on the application of public encryption that is with content search. We are using the same technique of SPCHS

which provides semantic security. In practice we can use this content searchable encryption for filtering the encrypted spam. So by constructing the hidden tree like structures between the continuous words from single file we can apply PEKS for content also. The search complexity is linearly depends on size of content which is queried.

C. Basic Ideas

1) Hidden Tree like Structure: We use hidden star like structure to maintain the privacy of the keyword and content. Following diagram represents the hidden star like structure.

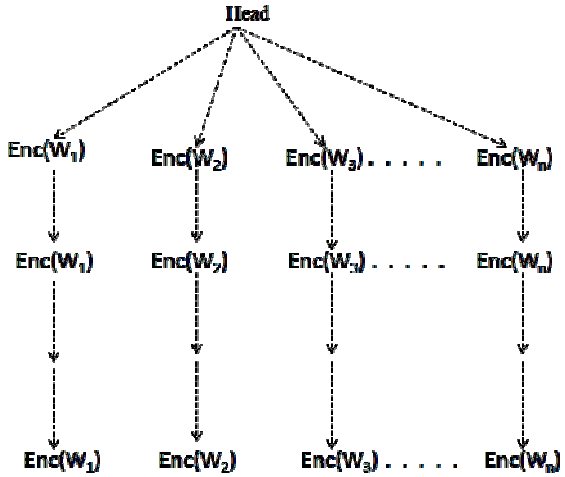


Fig1. Hidden Star like Structure

If we have this hidden tree like structure for content search like in Fig.1 then searching for specific queried content for cipher text may be increased. Suppose in our system cipher texts of the same contents will form one chain by using related hidden relations. Also there will be relation present between the Head to first cipher text of each chain. With the help of content search system and head the server pick out from the first matching content's cipher text through the relations from the head. Another relation will get communicated through the found cipher text and this will help us to find another cipher text. By following this concept we will go for searching other cipher texts. And because of this search time will depend on cipher texts of content.

2) Use Of SPCHS: We are using the technique developed in [2] of SPCHS. This technique is depending on the Identity Based Key Encapsulation Mechanism's observations. In this sender's encapsulation of key is done with receiver id. Receiver can de capsulate same and will get the key. While building SPCHS for content search we are using Identity Based Encryption (IBE) and collision-free full-identity malleable IBKEM. The result of this will get the content searchable cipher texts with the hidden tree like structure. As both IBKEM and IBE have the semantic security then resulted SPCHS is also semantically secure.

II. RELATED WORK

A. Symmetric Searchable Encryption

Symmetric key encryption for keyword search was first introduced by Song [4] with linear search time with the size of database. Another research in [5], [6], [7], [8], and [9] works on the same technique and rectifies the original work of Song. The Curtmola et al. [3] proved the semantic security of technique with adaptive adversary. In This technique search time is logarithmic time but keyword search trapdoor's length is linear with the size of database. This all techniques are developed for improving the search time and to get better performance, recently researches work for the scalability.

The technique developed in [3], [10] extended the work of SKES to multi sender model. Fuzzy keyword search is also provided by [11] in SEKs scenario. The Waters B. R in their paper [12] uses SKES for Building an Encrypted audit logs that can be Searchable. Again Chase et al. [13] proposed a technique in which they encrypts the structured data and also proposes secure method for searching the data. In the research proposed by Kamara et al. [14] dynamic updating of encrypted data is proved and they proposed symmetric encryption for dynamic searchable data. This technique is also enhancing in terms of security and large index cost in [15]. In new technique developed by Cash D. [16] they achieve very strong efficiency and security also.

B. Public Key Searchable Encryption

With following the same work on PEKS Abdalla et al. [17] Works on consistency keeping with filling some gaps of PEKS and

works with the enhancements in the primitives with the PEKS. Some extra efforts are also there to make PEKS more flexible. The work includes different searches like range serach in [24], [25], [26] conjunctive search [18], [19], [20], [21], [22], [23], Time search in [17], [27], subset search [26], authorized search in [29], [30] and similarity search in [28]. Heterogeneous cipher texts equality test [31], and fuzzy keyword search is provided in [32].Besides this, Arriaga et al. [33] proposed the PEKS technique use to keep privacy of keyword searchable trapdoors. In these techniques the search time is linear with the number of cipher texts.

In [13] new chain like structure is provided for fast searching of encrypted keyword. The chain like structure given in [35] is not fully hidden from severs and may get trapped. For efficient keyword search Bellare et al. [34] proposed deterministic public key encryption (PKE) with the formalized strongest security mechanism. Brakerski et al. [36] proposed same deterministic PKE technique but with security enhancements, still these systems are not semantically secure. Previously the semantic security is provided if keyword space with high min-entropy.

Peng Xu [2] proposed a new technique for providing a semantic security for PEKS. They use the SPCHS as search algorithm for the technique but there is a still space for applying the same concept on the content search for filtering the spams.

C. Our Observations

By studying all these techniques we come to know that research has been done on keyword search with keeping semantic security and on search time scope. There is a still scope to apply the SPCHS technique for the content search and keeping the security for the same.

III. PROPOSED SYSTEM

The proposed system architecture is shown in fig2. Let us look in detail for the architecture. While describing the system we are using different algorithms.

A. SPCHS Algorithm

We are using this algorithm from [2] for encrypting the content and generating the hidden tree like structure. While implementing this the encryption algorithm will take input as Pr if Pr:Pb is hidden structure. We can't create the hidden relations by using the Pb because it doesn't contain any about hidden structure. At last of encryption technique Pr should be updated as we created new hidden relation. With this algorithm we require to initialize Pr:Pb by using the input as master public key for initialization. This algorithm will run before creation of cipher text. With the content search algorithm the SPCHS also provides partial relations to guide the searching process of cipher text. SPCHS Contains following Five algorithms

1) System Setup: Input- 1k (Security Parameter), W (Keyword Space)
Output- pair of PK (Public Key) and SK (Secret Key)

2) Structure Initialization: Input-PK. hidden structures
Output-private and public parts Pr:Pb

3) Structured Encryption: Input- PK, Keyword W2W, and Hidden structure's Pr
Output-Content searchable cipher text c, Hidden structure

4) Trapdoor : Input- SK, W2W
Output- Content searchable Trapdoor TW

5) Structured Search: Input- PK, Pb, All content searchable cipher text

C, TW

In general SPCHS each sender has private values Pr. we are allowing sender to keep his/her Pr at the server side in encrypted form so that user can download and re encrypted his/her Pr[2]. In keeping the semantic security SPCHS choses keyword and SS-CKSA (structure Attacks).

B. SS-CKSA Security

To keep semantic security SPCHS uses SS-CKSA Security. Using this technique we will follow Different phases as follows.

1) Setup Phase: In this phase challenger will use System Setup to generate PK and SK. By using the Structure Initialization they will initialize the N hidden structures. At last challenger sends PK

2) Query Phase 1: In this phase various queries will send by challenger, like Trapdoor query (TW), Privacy query (Pb),

encryption query.at last challenger outputs the cipher text SPCSH.

3) Challenge Phase: In this phase a will send two challenge keywords to challenger and challenger will randomly picks the key and will send cipher text.

4) Query Phase 2 : This phase is same as query phase 1.

5) Guess Phase: In this phase a will send guess to challenger and if it will match then A will win.

C. Forward And Backward Security

If in case if sender's privacy of Pr gets compromised then SPCHS will provide them forward security technique. In this hidden relation of cipher texts will stays confidential as local privacy only keeps new generated cipher texts relationships only. In backward security sender can ask for initialization of new structure under Structure Initialization algorithm for newly generated cipher text as structure is independent on old texts. The local privacy which gets compromised will not give the new structure.

By using these techniques we are working for the architecture given below in Fig 2. To get more in detail we are using the SPCHS algorithm for the content searchable public key encryption technique. Sender can send any file with encrypted content and keyword also and receiver will send queried keyword from the user and server is unaware of the actual file .receiver notice that this file is spam file then receiver report the spam mail to the server and server will keep such type of file to the spam files for the further reference and after wards will report every time to the user about this type of spam files. In our system server also able to give authorities to the sender and receiver and also verifies the loins in the system.

Let us explain the whole system by sequence. In this system

Data owner will upload file and content to the server in encrypted format.

Sever will keep files from the data owner and unable to see contains of the file.

Sever will also keep the encrypted contents.

User will give keyword or content search to the trapdoor.

If keyword or content will match then user will download the file.

If required then report the spam to the server.

Server will keep spam files for further reference.

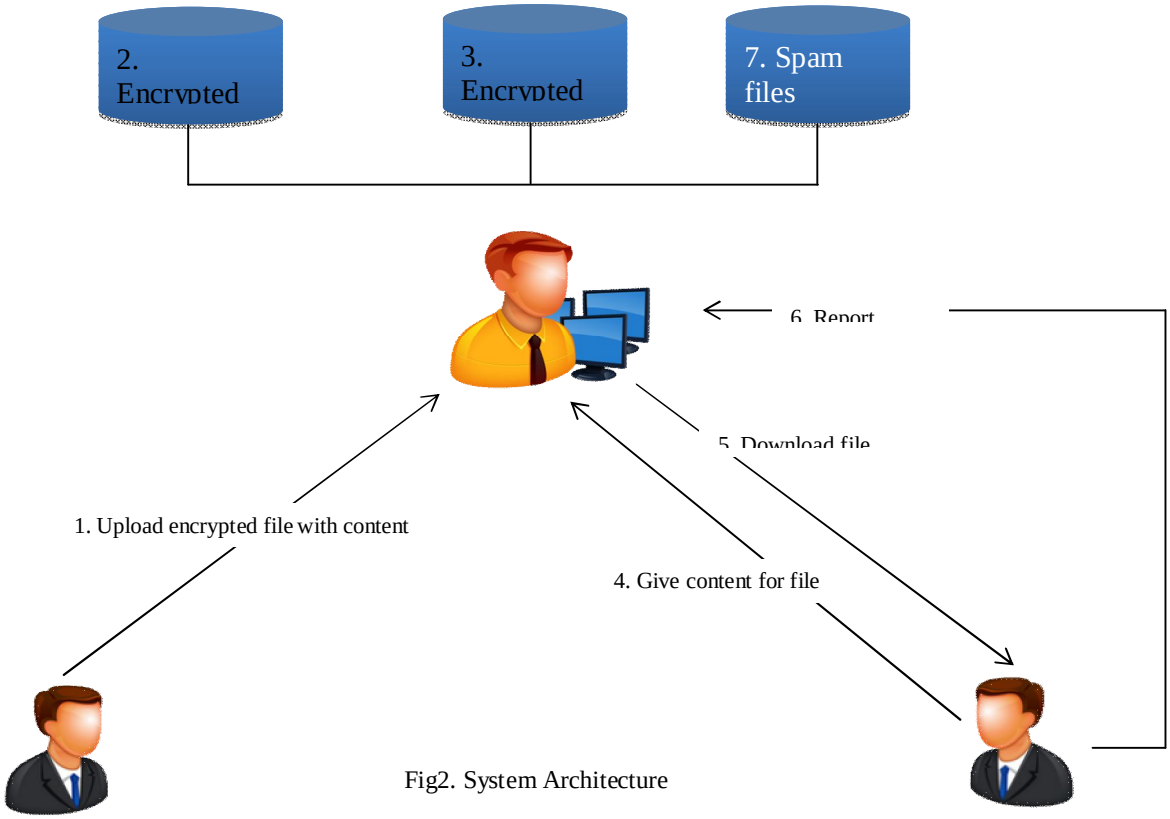


Fig2. System Architecture

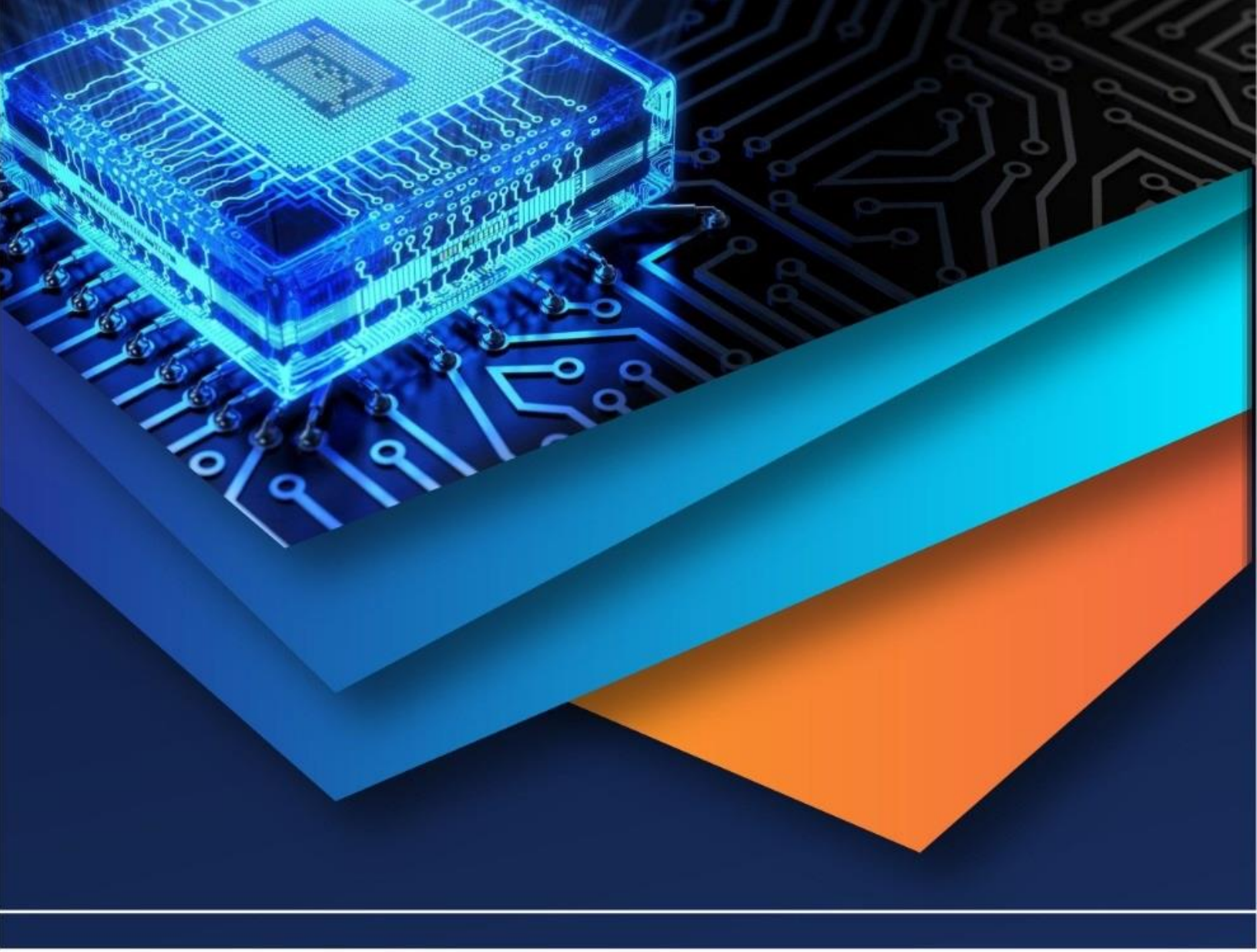
IV. CONCLUSION

This paper works with the content search in PEKS by providing semantic security. In this technique we are using SPCHS which is alternative for the PEKS and this technique allows us to generate content searchable cipher texts by generating hidden tree like structure. The trapdoor at server side uses the search algorithm is responsible for the disclosing the parts of hidden structure and guide us to find out the cipher texts. SPCHS algorithm is provided with the semantic security and provides privacy to the keyword, content and hidden structure also. Content search is useful for recognizing the spam files. The search complexity is linear with the query content size. This technique uses the existing SPCHS schemes with semantic security for content search. In future we may work for the retrieval of complete verification by generating hidden tree like structure by keeping last pointer at the head.

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] Peng Xu, Qianhong Wu, Wei Wang, Willy Susilo, Josep Domingo-Ferrer, Hai Jin, "Generating Searchable Public-Key Ciphertexts with Hidden Structures for Fast Keyword Search", IEEE Transactions on Information Forensics and Security Volume: PP Year: 2015.
[3] Curtmola R., Garay J., Kamara S., Ostrovsky R. "Searchable SymmetricEncryption: Improved Definitions and Efficient Constructions" .In: ACM CCS 2006, pp. 79-88. ACM (2006).
[4] Song D. X., Wagner D., Perrig A. "Practical techniques for searches on encrypted data". In: IEEE S&P 2000, pp. 44-55. IEEE (2000).
[5] Goh E.-J. "Secure Indexes. Cryptography ePrint Archive", Report 2003/216 (2003).
[6] Bellovin S. M., Cheswick W.R. "Privacy-Enhanced Searches Using Encrypted Bloom Filters". Cryptography ePrint Archive, Report 2004/022 (2004).
[7] Agrawal R., Kiernan J., Srikant R., Xu Y. " Order Preservin Encryption for Numeric Data". In: Proceedings of the 2004 ACM SIGMOD international conference on Management of data, pp. 563-574. ACM (2004).
[8] Chang Y.-C., Mitzenmacher M. " Privacy Preserving Keyword Searches on Remote Encrypted Data". In: Ioannidis J., Keromytis A. and Yung M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 442-455. Springer, Heidelberg (2005).
[9] Boldyreva A., Chenette N., Lee Y., O'Neill A. " Order-Preserving Symmetric Encryption". In: Joux A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 224-241. Springer, Heidelberg (2009).
[10] Bao F., Deng R. H., Ding X., Yang Y. " Private Query on Encrypted Data in Multi-User Settings". In: Chen L., Mu Y., Susilo W. (eds.) ISPEC 2008. LNCS, vol. 4991, pp. 71-85. Springer, Heidelberg (2008)
[11] Li J., Wang Q., Wang C., Cao N., Ren K., Lou W. "Fuzzy KeywordSearch over Encrypted Data in Cloud Computing". In: IEEE INFOCOM 2010, pp. 1-5. (2010).
[12] Waters B. R., Balfanz D., Durfee G., Smetters D. K. "Building an Encrypted and Searchable Audit Log". In: NDSS 2004 (2004).
[13] Chase M., Kamara S. "Structured Encryption and Controlled Disclosure". In: M. Abe (ed.) Advances in Cryptology - ASIACRYPT 2010. LNCS, vol. 6477, pp. 577-594. Springer, Heidelberg (2010).
[14] Kamara S., Papamanthou C., Roeder T. "Dynamic searchable symmetric encryption". In ACM Conference on Computer and Communications Security, pp. 965976 (2012).
[15] Kamara S., Papamanthou C. "Parallel and Dynamic Searchable Symmetric Encryption". In: Sadeghi A.-R. (ed.) FC 2013. LNCS, vol.7859, pp. 258-274. Springer, Heidelberg (2013).
[16] Cash D., Jaeger J., Jarecki S., Jutla C., Krawczyk H., Ros M.-C., Steiner M. "Dynamic Searchable Encryption in Very Large Databases: Data Structures and Implementation". In: NDSS 2014.
[17] Abdalla M., Bellare M., Catalano D., Kiltz E., Kohno T., Lange T., Malone-Lee J., Neven G., Paillier P., Shi H. "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions". In: Shoup V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205-222. Springer, Heidelberg (2005).
[18] Park D. J., Kim K., Lee P. J. "Public Key Encryption with Conjunctive Field Keyword Search". In: Lim C. H. and Yung M. (eds.) WISA 2004. LNCS, vol. 3325, pp. 73-86. Springer, Heidelberg (2004).
[19] Golle P., Staddon J., Waters B. R. "Secure Conjunctive Keyword Search over Encrypted Data". In: Jakobsson M., Yung M., Zhou J. (eds.) ACNS 2004. LNCS, vol. 3089, pp. 31-45. Springer, Heidelberg (2004).
[20] Ballard L., Kamara S., Monrose F. "Achieving Efficient Conjunctive Keyword Searches over Encrypted Data". In: Qing S. et al. (eds.) ICICS 2005. LNCS, vol. 3783, pp. 414-426. Springer, Heidelberg (2005).
[21] Hwang Y. H., Lee P. J. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System". In: Takagi T., Okamoto T., Okamoto E. and Okamoto T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 2-22. Springer, Heidelberg (2007).
[22] Ryu E.K., Takagi T. " Efficient Conjunctive Keyword-Searchable Encryption". In: 21st International Conference on Advanced Information Networking and Applications Workshops, pp. 409-414. IEEE (2007).
[23] Baek J., Safavi-Naini R., Susilo W. " Public Key Encryption with Keyword Search Revisited". In: Gervasi O. (ed.) ICCSA 2008. LNCS, vol. 5072, pp. 1249-1259. Springer, Heidelberg (2008).
[24] Bethencourt J., Chan T.-H. H., Perrig A., Shi E., Song D. "Anonymous Multi-Attribute Encryption with Range Query and Conditional Decryption". Technical Report CMU-CS-06-135 (2006)
[25] Shi E., Bethencourt J., Chan T.-H. H., Song D., Perrig A. "Multi- Dimensional Range Query over Encrypted Data". In: IEEE S&P 2007, pp. 350-364. IEEE (2007)
[26] Boneh D., Waters B. R. "Conjunctive, Subset, and Range Queries on Encrypted Data". In: Vadhan S. P. (ed.) TCC 2007. LNCS, vol. 4392,
[27] pp. 535-554. Springer, Heidelberg (2007).
[28] Davis D., Monrose F., Reiter M. K. " Time-Scoped Searching of Encrypted Audit Logs". In: Lopez J., Qing S., Okamoto E. (eds.) ICICS
[29] 2004. LNCS, vol. 3269, pp. 532-545. Springer, Heidelberg (2004).
[30] Cheung D. W., Mamoulis N., Wong W. K., Yiu S. M., Zhang Y. "Anonymous Fuzzy Identity-based Encryption for Similarity Search". In: Cheong O., Chwa K.-Y and Park K. (eds.) ISAAC 2010. LNCS,

[31] vol. 6505, pp. 61-72. Springer, Heidelberg (2010).
[32] Tang Q., Chen X. "Towards asymmetric searchable encryption with message recovery and flexible search authorization". ASIACCS 2013, pp. 253-264 (2013).
[33] Ibraimi L., Nikova S., Hartel P. H., Jonker W. "Public-Key Encryption with Delegated Search". In: Lopez J. and Tsudik G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 532-549. Springer, Heidelberg (2011).
[34] Yang G., Tan C. H., Huang Q., Wong D. S. " Probabilistic Public Key Encryption with Equality Test ". In: Pieprzyk J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 119-131. Springer, Heidelberg (2010).
[35] Xu P., Jin H., Wu Q., Wang W. " Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack". IEEE Transactions on Computers, 62(11), pp. 2266- 2277 (2013).
[36] Arriaga A., Tang Q., Ryan P. " Trapdoor Privacy in Asymmetric Searchable Encryption Schemes". In: Pointcheval D. and Vergnaud D. (eds.) AFRICACRYPT 2014. LNCS, vol. 8469, pp. 31-50. Springer, Heidelberg(2014).
[37] 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).
[38] Camenisch J., Kohlweiss M., Rial A., Sheedy C.: Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data. In: Jarecki S. and Tsudik G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 196-214. Springer, Heidelberg (2009).
[39] Brakerski Z., Segev G.: Better Security for Deterministic Public- Key Encryption: The Auxiliary-Input Setting. In: Rogaway P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 543-560. Springer, Heidelberg (2011).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY