International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 07 | July 2018 www.irjet.net p-ISSN: 2395-0072

Publicly Verifiable Boolean Query over Outsourced Encrypted Data

Dr. T. Buvaneswari[1], M.Vigenesh[2], V. Karthika[3]

[1, 2]*Assistant Professor, Department of Computer Science Engineering, Annapoorana Engineering College, Salem*
[3]*P. G Scholar Department of Computer Science Engineering, Annapoorana Engineering College, Salem*

Abstract - *Outsourcing storage and computation to the cloud has become a common practice for businesses and individuals. As the cloud is semi-trusted or susceptible to attacks, many researchers suggest that the outsourced data should be encrypted and then retrieved by using searchable symmetric encryption (SSE) schemes. Since the cloud is not fully trusted, we doubt whether it would always process queries correctly or not. Therefore, there is a need for users to verify their query results. Motivated by this, in this paper, we propose a publicly verifiable dynamic searchable symmetric encryption scheme based on the accumulation tree. We first construct an accumulation tree based on encrypted data and then outsource both of them to the cloud. Next, during the search operation, the cloud generates the corresponding proof according to the query result by mapping Boolean query operations to set operations, while keeping privacy-preservation and achieving the verification requirements: freshness, authenticity, and completeness. Finally, we extend our scheme by dividing the accumulation tree into different small accumulation trees to make our scheme scalable. The security analysis and performance evaluation show that the proposed scheme is secure and practical.*

EXISTING SYSTEM:

Outsourcing data in cloud environment is a common mechanism and more number of issues has been arising like security, exact data retrieval from a cloud environment, data loss. However the cloud could not be fully trusted and it subjected to many attacks. In existing one of the common methods to secure and to search data is searchable symmetric encryption (SSE). Due to its large storage nature it leads to a suspecting like whether it processes the queried exactly or not. Therefore there is a need for every user to confirm their query results.

DISADVANTAGES:

- Cloud is semi-trusted and susceptible to many attacks.
- Retrieval of exact data with respect to query is difficult.
- Each user wants to confirm whether the retrieved query result is related to his/her search.

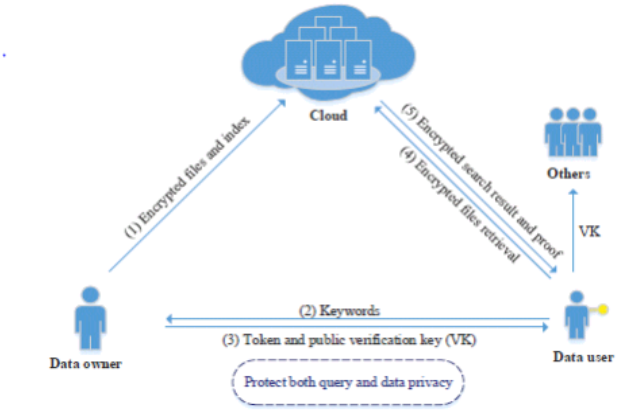
PROPOSED SYSTEM:

The issues that are discussed above could be overcome by our proposed approach. Instead of SSE here it proposes a new searchable and encryption approach names publicly verifiable dynamic searchable symmetric encryption. Here dynamic searchable on the encrypted and outsourced data has been done through accumulation tree. An accumulation tree is constructed based on encrypted data and then outsource both of them to the cloud. The encrypted data has been obtained as result through search operation is obtained by query results by mapping Boolean query operation to set operations. To confirm the exact retrieval of data cloud generates a respective proof according to the query. During data retrieval privacy has been preserved through verification requirements like freshness, authenticity and completeness.

ADVANTAGES:

- Searching required data has been done in dynamic way by publicly verifiable dynamic searchable symmetric encryption.
- Accumulation tree is constructed to ensure exact retrieval of data.
- An efficient and effective searching result has been done.
- Security and privacy is ensured by freshness, authenticity and completeness.

SYSTEM ARCHITECTURE:



ALGORITHM:

The construction of an accumulation tree AT.

Require: all e*i*, *s*, *h*(·).

1: **for** Each keyword *wi* ∈ W**do**

2: **for** All encryption document indices e*i* ∈ *wi* **do**

3: Set *acc*(*wi*)=*g*Π(e*i*+*s*).

4: **end for**

5: **end for**

6: Data owner picks a constant _, where 0 <_ <1.

7: *DO* constructs tree AT according to stag(*wi*) that has *l* = _1/__

levels and *m* leaves, where *m* is the number of W.

8: **for** Each node *v* of AT **do**

9: **if** *v* is a leaf corresponding to keyword *wi* **then**

10: *DO* sets *d*(*v*) = *acc*(*wi*)(*i*+*s*).

11: **else**

12: Compute *d*(*v*) = *g*_*v*∈*N*(*v*)(*h*(*d*(*v*)+*s*)) where *N*(*v*) denotes

the set consisted by children nodes of *v*.

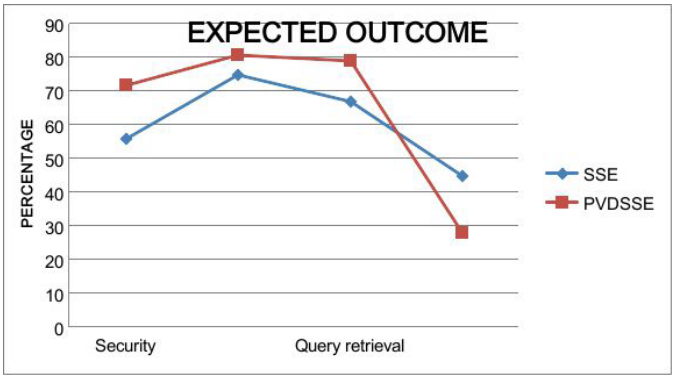
13: **end if**

14: **end for**

15: *DO* sets *d*0=*d*(*r*) where *r* is the root of AT and keeps it.

16: Finally, *DO* outsource AT with encrypted DB to the cloud.

EXPECTED OUTCOME IN GRAPH:



CONCLUSION:

The problem of verifying the freshness, authenticity, and completeness of the Boolean query result over the outsourced encrypted data has been studied. Based on the issues it proposes a publicly verifiable scheme by constructing the accumulation tree to achieve the query integrity verification while keeping privacypreserving and efficiently practical. The security analysis shows that without protecting the access pattern, our scheme can keep the privacy-preserving of private information retrieval. The performance demonstrates our scheme is scalable.

REFERENCES:

[1] S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner , "Outsourced symmetr ic pr ivate information retr ieval,"in *Proceedings of the 2013 ACM SIGSACconference on Computer & communications security* . ACM, 2013, pp. 875–888.

[2] S. Kamara,C. Papamanthou, and T. Roeder , "Dynamic searchable symmetr ic encryption," in *Proceedings of the 2012 ACM conference on Computer and communications security* . ACM, 2012, pp. 965–976.

[3] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner , "Highly-scalable searchable symmetr ic encryption with suppor t for boolean queries,"in *Advances in Cryptology-CRYPTO2013*.Spr inger, 2013, pp. 353–373.

[4] M. Naveed,M. Prabhakaran, and C. A. Gunter , "Dynamic searchable encryption via blind storage."in *Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA,May*, 2014.

[5] E. Stefanov, C. Papamanthou, and E. Shi, "Practical dynamic searchable encryption with small leakage."*IACR Cryptology ePrint Archive*, vol. 2013, p. 832, 2013.

[6] http:/ / www.wired.com/ 2009/ 01/magnolia-suffer / .

[7] http:/ / mashable.com/ 2011/ 02/ 27/ gmail-glitch/ .

[8] S. Nath and R. Venkatesan, "Publicly ver ifiable grouped aggregation queries on outsourced data streams,"in *Proceedings of the 29th International Conference on Data Engineering (ICDE)*. IEEE, 2013, pp. 517–528.

[9] H. Pang, j. Zhang, and k. Mouratidis, "Scalable ver ification for outsourced dynamic databases,"*Proceedings of the VLDBEndowment* , vol. 2, no. 1, pp. 802–813, 2009.

[10] F. Li, M. Hadjielefther iou, k. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in *Proceedings of the 2006 ACM SIGMOD international conference on* Management of data. ACM, 2006, pp. 121–132.