8th International Conference on Multidisciplinary Research
Osmania University Centre for International Program, Osmania University Campus, Hyderabad (India)
Conference World
6th-7th September 2019 www.conferenceworld.in ISBN : 978-81-941721-5-4

Two Cloud Secure Database For Privacy preserving Using Elliptic Crypto

[1]K Sruthi , [2]Dr. C. Shobha Bindu, [3]Dr. P. Dileep Kumar Reddy

[1]M.Tech(CS) JNTU Anantapur, India,

[2] Professor of CSE, JNTU, Anantapur,india

[3]Associate Professor of CSE ,SV College of Engineering,Tirupathi,india

ABSTRACT:

In the present scenario privacy palce a vitol role in cloud computing,for providing better security for SQL queries so many secure database schemes are introduced. These schemes does not support various numeric related sql range queries like sum and also does not provide privacy preservation to the private data where keys are having very less size ,so here we are going to introduce the two secure cloud architecture by using elliptic crypto algorithm. Elliptic crypto is one of the public key cryptography, it is efficient for smaller keysize values and support the various numeric related SQL range queries.

Keywords:Cloudcomputing,cryptosystems,ellipticcrypto,sql

I.INTRODUCTION:

Now a days we can treat as cloud public as well as private. Private clouds are restricted to only few persons but not all the person's private cloud does not give permission to all public. Finally we can say cloud is a combination of both saas's as well as utility computing software. Security place a major role in cloud computing. Cloud clients are going to provide security to the cloud for both insides as well as outside. The major problem occurred here is we will get the information from server side. In order to hide this security information which is present in the server it will majorly follow some famous security methods. As said the cloud server is treated as semi-trusted Elliptic-curve [5], the algorithm that gives privacy to the applications it mainly uses database administration. Elliptic crypto permits to perform operations on SQL related queries, similarly the SQL's is using set of operators performs the functions on data. Elliptic-curve is going to provide confidentiality to the private information (e.g., health books, financial articulations, individual data) with the help of DBMS server and using some important tools it provides security to the private data. One of the algorithm Order preserving encryption (OPE)[11][12] is generally involved in databases to perform operations on Questions related to SQL on information. Order preserving encryption may leak private information to the external world it may support only few SQL related range queries not all . for providing better security to the encrypted data order preserving encryption mainly

uses one cloud is for data storing and key which is related to data. finally a secure database service system is utilizing two clouds in which the information and query are distributed in between two clouds. Henceforth, a single cloud does not provided better functionality to the private data .incase of two clouds it uses the intersection of protocols these protocols may support SQL related range queries.

II .LITERATURE SURVEY

R.A.Popa,C.Redfieldet.al, N.Zeldovichet.al and H.Balakrishnanet.al proposed novel based encryption system,by applying this method on numeric related range queries it takes more time to complete the process,while comparing to Elliptic crypto with novel based encryption elliptic crypto takes less time to complete the process.In terms of time elliptic crypto is best algorithm in cryptographic systems.

RakeshAgrawalet.al, Jerry Kiernanet.al, Ramakrishnan Srikantet.al, Yirong Xuet.al proposed Order Preserving Encryption for Numeric Data[11] .This encryption mainly uses the single cloud so it does not provide privacy to the private information.While comparing OPE with many algorithms like novel based algorithms ,multicloud architecture.Novel based architecture is best one while comparing with OPE,it will provides better security ,less time to complete the process.novel based algorithms uses the various intersection of protocols for providing privacy.Interms of privacy novel based algorithm is best one.By comparing OPE with multicloud architecture interms of cost and security OPE is best algorithms because providing a security to the single cloud is easy.

Raluca Ada Popaet.al, Frank H. Liet.al, Nickolai Zeldovichet.al, proposed "An Ideal-Security Protocol for Order-Preserving Encoding", which accomplishes perfect security. Considering key size and effective protocols elliptic crypto provides better functionality.

J.-M.Bohliet.al, N.Gruschkaet.al, M.Jensenet.al, L.L.Iaconoet.al,and N.arnauet.al, introduced the Security and privacy-enhancing multicloud architectures.This architecture mainly usesthe Homomorphic encryption.Homomorphic encryption does not provide security to the privacy preservation of private data.This encryption technique include protocols like multiparty calculation protocols,this protocols does not provide better security to the processed data,while comparing elliptic crypto with multicloud architecture interms of security elliptic crypto provides better security.

III. Kaiping Xue et.al scheme

In OPE, the client and IT enterprise want to store their database valuable and sensitive information into the cloud. The information is like transaction records, account information, disease information etc . Due to the assumption that cloud provider for his own benefit he is trying to get private information from the cloud,In this process there may be operational risk involved in this although for getting profit he may disclose that private information to the business competitors.This is the major problem occurred here.OPE did not give any solutions to this type of problems,in case of privacy it should not perform properly,the main reason that it should not consider cryptographic tools it mainly associated with larger keys.OPE stores the information and key values in single cloud, third party may get information easily because both data

and keys are stored in single cloud. Especially, order preserving encryption is applied on numeric related range query processes. In this functionality OPE does not provide privacy to the leakage data it shold not be performed well due to single cloud and when we applied cryptdb on numeric related range queries it should be well performed but not guarantee the privacy. However, since OPE does not provide sufficient privacy assurance.

- Single cloud does not guarantee the privacy to the private information.
- OPE does not support numeric related range queries like sum function. It may support larger key values so it does not provide proper security to private data.

IV. PROPOSED SCHEME

In this scheme, we are going to consider two cloud architecture,the first cloud can store the information regarding the encrypted data, and the second cloud may store the information regarding keys which is related to encrypted data.This two cloud architecture mainly uses the intersection of protocols by using this protocols it may support privacy preservation to the data and numeric related range queries(based on relational operators).Both the clouds does not have an idea about what the individual clouds store the information.

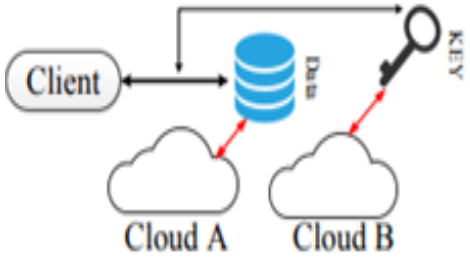

Fig1: two cloud architecture

If a client has to give a query to the cloud server the query may be spiltted into two parts like data as well as query hence this query logic will be distributed in between two clouds after combining the both the clouds they may analyse the data as well as key information finally they give the response to the cloud. In this way we are going to consider the two cloud architecture as well as elliptic crypto algorithm .kaiping xue scheme it mainly uses the ope and cryptdb in this it does not hold true for functionalities on numeric related range queries so here we are going to use elliptic crypto to support numeric related range queries mainly on functions like sum.

In this scheme we are using elliptic crypto ,elliptic crypto may guarantee the privacy preservation to the private data ,the main reason is that it may consider smaller key values .The two cloud architecture associated with elliptic crypto algorithm by using mathematical cubic function,it may operate on user given query.If the user give a query to the web ,the query consists of any relational operations including sum ,OPE does not support relational operations but elliptic crypto gives better performance incase of relational operations and gives privacy to the preservation of data.

ELLIPTIC CRYPTO:

Elliptic crypto is also a trapdoor function.It is similar to RSA based application but here it mainly uses the elliptic curves and will provide equal security for the smaller keys. Elliptic curves are defined by mathematical cubic functions.

$$y^2 = x^3 + ax + b$$

ISBN : 978-81-941721-5-4

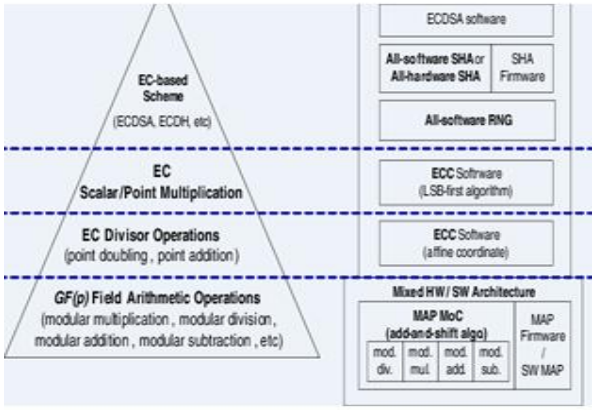

Fig2: elliptic crypto architecture

By using elliptic crypto we are going to perform so many operations like point doubling and point addition modular multiplication etc The major protocols present in this algorithm is ECDSA ECDH these both mainly support the addition operation by using this two protocols elliptic crypto mainly provides the privacy preservation to the data and also support the numeric related range operation especially sum operation,by using so many cubic curves it may combine the queries the given to the cloud server so finally it will give the result to the client .some of the important levels present in the elliptic crypto these levels are given below.

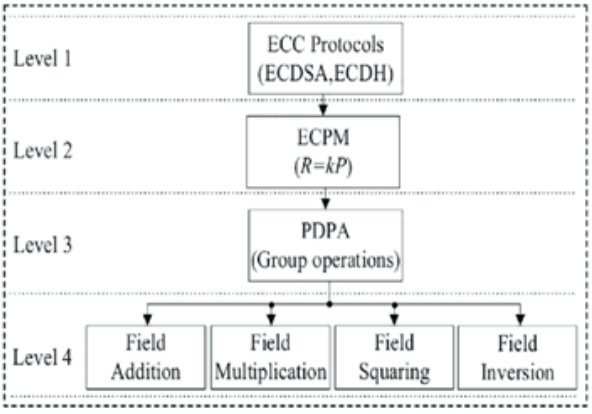

Fig3: levels present in elliptic crypto

V. PERFORMANCE ANALYSIS

The performance analysis can be identified by using computational cost Here we are going to compare the compuatational cost of different algorithms and also the key value sizes.

Time to break in MIPS	**ECC**	**OPE**	**ECC/OPE**
10^4	106	512	5:1
10^9	132	768	6:1
10^{11}	160	1024	7:1
10^{20}	210	2048	10:1
10^{79}	600	21000	35:1

Table1: comparison of keysize between ECC and OPE

In ECC a 106-bit keysize is smaller compared to the OPE 512-bit keysize,generally smaller keys provides better security as compared to larger key, based on this property ECC reduces computational cost or processing cost.ECC was proposed by Miller and Koblitz [1].

Key size		**Security Level(bits)**	**Ratio of Cost**
OPE	**ECC**		
1034	160	80	3:1
2148	234	122	7:1
3172	266	138	11:1
7580	374	182	33:1

Table2: comparison of cost

While comparing to the larger key with

the smaller keys, smaller keys will be more effective ,it provides less Computationalcost, runningtime and reduces transmission time, less memory for storage.The graph compares the time taken by the both algorithms.The ECC can take take lesser time as compared to OPE if the database having equal size in case of both the algorithms, but compared to OPE ,ECE takes less time.OPE takes 25MIPS and ECC takes 19IMPS.

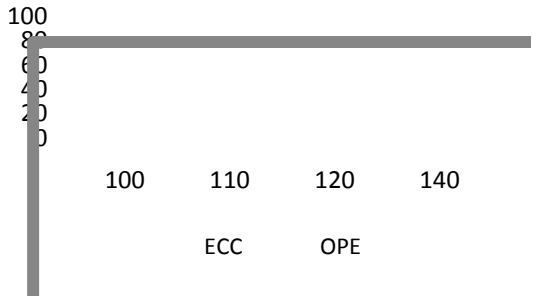

Fig4: comparison of time in between OPE and ECC Where x-axis: database size, y-axis: time

ECC is the best approach for finding solutions to numeric related range queries,in case of cost elliptic crypto requires very less as compared to the OPE.The given graph shows the what is the cost required for ECC and OPE,for equal database size of OPE and ECC they have different costs.By comparing both in terms of time and cost ecc is the best one it requires less time and cost.

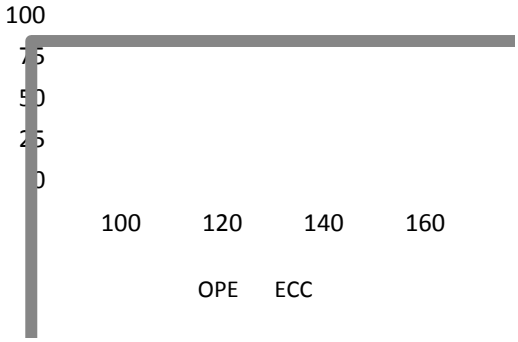

Fig5: comparison of computational cost in between OPE and ECC where x-axis: database size, y-axis:cost

VI. CONCLUSION

The Proposed system presents the elliptic crypto algorithm along with the two secure cloud architecture these both systems may hold true for functionalities like sum/avg functions. The proposed scheme is efficient for smaller key values. With the help of ESDH protocols it will provide privacy preservation to the private data. The future work of this paper is enhanced to support non numeric related range queries, privacy preservation to the larger keys.

REFERENCE

[1] Kaiping Xue, Shaohua Li, Jianan Hong, Yingjie Xue,Nenghai Yu, and Peilin Hong "Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving", IEEE Transactions on Information Forensics and Security ,2017

2[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., "A view of cloud computing", Communications of the ACM, vol. 53, no. 4, pp. 50–58,2010.

[3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou,"Toward secure and dependable storage services in cloud computing", IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[4] D. Zissis and D. Lekkas,"Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

[5] R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "Elliptic-curve : protecting confidentiality with encrypted query processing," in

ISBN : 978-81-941721-5-4

Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, pp. 85–100, 2011.

[6] D. Boneh, D. Gupta, I. Mironov, and A. Sahai, "Hosting services on an untrusted cloud," in Advances in CryptologyEUROCRYPT 2015. Springer, pp. 404–436, 2015.

[7] R. A. Popa, F. H. Li, and N. Zeldovich, "An ideal-security protocol for order-preserving encoding," in Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP'13). IEEE, pp. 463–477, 2013.

[8] J.-M. Bofhli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau,"Security and privacy-enhancing
multicloud architectures," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 212–224, 2013.

[9] F. Hao, J. Daugman, and P. Zielinski, "A fast search algorithm for a large fuzzy database," IEEE Transactions on
Information Forensics and Security, vol. 3, no. 2, pp. 203– 212, 2008.

[10] Y. Yang, H. Li, M. Wen, H. Luo, and R. Lu, "Achieving ranked range query in smart grid auction market," in 2014 IEEE International Conference on Communications (ICC2014). IEEE, Vol.2, No.4,April 2014

[11] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of
the 2004 ACM SIGMOD International Conference on Management of Data. ACM, pp.563–574, 2004.

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