International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

Integrating Two-Cloud Database and Keys Generation technique for Privacy Preserving SQL Range Queries Over Outsourced Database

Mr. Gorakshanath. N. Handge

PG Student, Department of Computer Engineering, R.H. Sapat COE Nasik, Maharashtra, India.

Abstract – *In the most of the organizations, instead of hosting database the management system in-house, the computing industry has moved towards the most recent trends of outsourcing the database storage. The standard reason is that database is encouraged and taken care of in cloud server in order to maintain reliability and reducing overhead of server maintenance. In the database management, one of the vital necessities is to give security to the database by holding the data confidential. But if the database is in encrypted form then there exist the issue of processing queries. In addition to enhance the security while ensuring common logic and the consistent and numerical queries those plans cannot give sufficient security affirmation against probable difficulties. Also, extended number of queries will release more information to the cloud server. The SQL Queries require a couple of secure database schemes for its desired working, thus it prompts privacy preserving to the cloud server. For numerical range queries there is security threat. So we have proposed a two-cloud architecture with a protocol for outsourced database administration, which guarantees the privacy preservation of information, statistical properties and can apply query pattern for different numeric-related range queries and the aggregation operations with security. In order to acquire this we have kept the data on one cloud and processing is handled by another cloud. Range queries with encryption capacity are used for data privacy preserving. In addition we have used a key logic for user identification purpose. So that unauthenticated user can not access the data from cloud without administrator permission.*

Key Words: Cloud Architecture, Database management, Privacy preservation, Range queries.

1. INTRODUCTION

In modern era it tends to be seen that cloud has assumed the take control over the IT business and its big data [4] in different aspects. It holds the probability to change a wide bit of the IT business, making programming essentially extra fascinating as an organization. Distributed computing is suggested to as SaaS (Software as a Service) since it renders the applications as associations over the Web and the hardware and structures programming in the different server that offer those organizations. The equipment of various server and programming is known as a cloud. Private clouds are identified with the internal server farms of a business or other organizations, not made accessible to the broadly useful. Cloud enlisting along these lines can be compacted as a mix of SaaS and utility registering, booting out the various servers. Security is the primary concern of the distributed computing [1]. Cloud clients go facing security threats both from outside and inside the cloud. Shielding the information from the server itself is the primary of the standard issues related with it. The server will by depiction control the "base layer" of the item stack, which successfully circumvents most known security strategies. As said the cloud server is acknowledged as semi-trusted.

A structure that offers protection to applications that utilizes database management systems (DBMSes) is known as CryptDB[9]. It licenses to execute queries over encoded information; comparably the SQL is incredibly described the administrators and queries over encrypted data[13]. CryptDB keeps an eye on the peril of a curious database administrator (DBA) who proceeding to learn private data (for example clinical information, money related information, personal information and so on.) by keeping a consideration on the DBMS server. The DBA attempt to learn private data by utilizing various techniques and security usefulness. One of the system being the Order protecting encryption (OPE) [08][11] is commonly utilized as a piece of databases to process SQL queries over encoded information. It grants to perform request procedure on cipher text like the plaintext e.g. Information server can assemble record to execute range queries [3] and sort the encrypted data like the plaintext. Despite the security reason well, despite the fact that all that it reveals the request for the cipher text.

Thus the reason for security assurance of the outsourced information to a cloud server is created by parceling the secured data into two sections and stores them in two distinct clouds by using cryptographic techniques (RSA, AES etc.)[20] [21]. Moreover, secure database administration service is known by using two non-colluding clouds in which the data and query pattern is isolated into two clouds. So each cloud knows just its particular information and they are non-colluding so that each of them know just piece of the pattern of queries. By terminating out queries on a solitary cloud we can't be discover any private information. Other than an advancement of protocols for a customer to lead numeric related SQL queries [">", "<", "<>"] and the operations "SUM/AVG" with security assurance is also executed. It will never discover any request related data from any of the two non-colluding clouds. To discover any kind of information the client must know the access pattern and access public key also [18].

In Summary We have considered the various procedures and protocols related with the assurance

preservation of the outsourced data to the outside cloud server. The advancement in this area a bit of the works related range queries, organize protecting encryption and multi-cloud structure. The Range Queries work by executing the repeated range query can keep secrecy of keywords, verification, data integrity and query privacy. After that it combines the range queries constructively completed the encoded information utilizing a novel SQL secured encryption system. The request secured encryption is one of the tools used which enables assessment activities to be especially related on encoded information, without decoding the operands. So that as it might encryption of non-numeric data isn't possible with this tools. Afterward the two-cloud system is presented which partitions the private data and queries pattern into encrypted form in two distinct clouds which don't have known about one another. The data privacy and client authenticity also increased with a secrete key so that no any unauthorized client / user can access private data.

There are some issues in handling cloud based databases, we have tried to handle some of them in this project. They are as below:

1.1 Potential Threats and Privacy Requirements

This segment characterizes the potential threats and the security necessities when the database is outsourced to the cloud. This segment contains information and the queries forms. Despite the fact that there are numerous information encryption techniques, some of them neglect to give adequate security assurance after measurable examination. As often as possible and huge measure of inquiry forms uncover the access pattern as well as release the stored encrypted information to the unapproved client.

1.2 Queries Pattern Module

The queries pattern may contains private information, as they can uncover the customer's motivation of the query. Indeed, even not as good as such pattern can release some measurable properties. In view of the above conversation, we express that a scalable multi-dimensional range queries [12] and encrypted data have to maintain a strategic distance from the accompanying private information from being obtained by the outsourced clouds.

1.3 Privacy of Item Values Modules

The ideal system is required to make nothing of the measurable properties be spilled to the cloud. However, the protection privacy of statistical properties in a viable outsourced database cloud is unavoidable, as restoring a piece of information as opposed to worldwide requires information for sifting [17]. For instance, if the customer needs to recover an information from the outsourced database, a cloud server with no information on the range request can restore all information of the database to the customer, which is unusable.

1.4 Multi-Clouds Architecture

Rather than utilizing Clouds A and Cloud B to play out the comparative solicitation over and over, we can utilize another pragmatic methodology that comprises of the one cloud provider watch the usage of the other cloud provider. For instance, Cloud A gives transitional aftereffects of its calculations to a watching procedure which run at Cloud B [16]. With the goal that Cloud B can check that Cloud A makes figuring and do the calculation planned by the cloud client. Besides Cloud B may run a model director administration that changes the execution way which is utilized by Cloud A.

2. REVIEW OF LITERATURE

F. Hao et al [5] have proposed a fast search algorithm for a huge fuzzy database that stores iris codes or information with a relative paired structure. The vague idea of iris codes and their high dimensionality is constrained by the novel procedure, Beacon Guided Search, which does as such by scattering countless "beacons" in the clear search. BGS is considerably quicker than the current ES with an insignificant loss of exactness. It takes extensively less recollections and it doesn't rely upon reserving information away, along these lines killing the need for composite storing the executives. The preprocessing is basic and speedy. It holds up to 30% mistakes in the inquiry and furthermore up to seven cyclic pivots. The lot of memory put is little and quickly moderate.

R. A. Popa et al proposed CryptDB [9], a structure to shield the private data in databases from right off the bat the curious cloud server itself and besides the application server's understandings. Crypt DB fundamentally contains utilizing the assortment queries beneficially finished the encoded data utilizing a unique SQL-mindful encryption framework. It limits the information presented to the untrusted database management server [6]. Not with remaining of generous the task of wellbeing defending, still a couple of data is revealed in the methodology. J.M. Bofhli et al proposed the Security and protection improving multi-cloud architectures [1]. This paper fills in as an outline paper where makers talked about the security in open cloud and different cloud. Additionally the high potential for security gauges in distributed computing have been contended. Homomorphic encryption and secure multiparty estimation rules to be strikingly boosting concerning both specialized security and administrative consistence. Despite the fact that there is no single ideal approach to manage develop both security and lawful consistence in a relevant manner. The imprisonments of these practices simply start from their compelled appropriateness and high multifaceted nature being utilized.

B. Hore et al proposed database outsourcing is a rising data administration model [3] which has the conceivable to change over the IT tasks of enterprises. The protection dangers in database re-appropriating plan where trust on the specialist organization is constrained. Especially,

investigate the information apportioning strategy and algorithmically extend this procedure to manufacture security insurance record on touchy fields of a social table. Such file empower semi-believed server to evaluate hazy range inquiries with least information spillage. In light of the work proposed by Dan Boneh et al. in [15], an open key based methodology called Hidden Vector Encryption (HVE). It bolsters correspondence and request look over scrambled information. In any case, the multifaceted nature of range search per information thing is straight in the range size, which can be an excess of costly regarding execution time when the range size is huge. Additionally, the proposed strategy doesn't utilize any type of ordering to lessen get to unpredictability that may be amazingly costly when managing huge datasets.

Yin Yang et al proposed a ranked range query (RRQ) plot [10], which can bolster both range inquiry and positioned search. Relies upon the Homomorphic Paillier crypto framework, we utilize two super-expanding arrangement to add up to multidimensional catchphrases. The first is utilized to entire one buyer's for the multidimensional watchwords to a gathered number. The subsequent one is connected to make an outline number by expanding the aggregated measures all things considered. Security request uncovers that RRQ can accomplish classification of watchwords, affirmation, data unwavering quality and question mystery. Meanwhile increasingly convoluted pre-sifting rules for example "also, "or", "not" will be not wrapped up by RRQ system.

Rakesh Agrawal et al proposed Order Preserving Encryption for Numeric Data [14] that allows any correlation activity to be legitimately associated on encoded data. Inquiry outcomes delivered are far reaching (no bogus hits) and complete (no bogus drops). OPES (Order Preserving Encryption Scheme) permits correlation activities to be explicitly related on scrambled data, without decoding the operands. Consequently, equalization and range questions and furthermore the MAX, MIN, and COUNT , GROUP BY and ORDER BY inquiries can be absolutely arranged over encoded information. OPES results are right and don't contain bogus positives , an incentive in a segment can be altered or another worth can be embedded in a section without requiring changes in the encryption of different qualities and it tends to be easily joined with present database systems. Encryption of non-numeric data, for instance, factor length strings aren't finished by OPES. Likewise while applying SUM or AVG to a gathering the qualities must be decoded.

Raluca Ada Popa et al proposed an Ideal-Security Protocol for Order-Preserving Encoding [8], which accomplishes perfect security. The essential procedure utilized is variable/alterable figure messages, which recommends, the figure messages for not many plaintext values change and its approved that fleeting figure writings are fundamental for immaculate security. Sulk is better than anything OPE conspire by 1-2 solicitations of degree. The equivalent time OPE security (sTOPE) performs with the end goal that lone the request for things present in the database is known. Sulk and stOPE use Merkle hashing to ensured customers against a pernicious server. So produce the request data of the information in plaintext. Other than the model concerns just a single query at a time, where all the more fine grain requesting is conceivable.

M. A. AlZain et al proposed the Cloud computing security from single to multi-clouds; It indicates security in single cloud and numerous clouds [7]. Moreover decides some limitation and focal points in security in distributed computing. Single cloud take a shot at three stages SaaS, PaaS, IaaS. Customers and business associations don't lose their held information as a result of noxious assailant in the cloud. It has a high ability to debilitate security risks that influence the distributed computing customer. Find attainable to possible imprisonment. All things considered the office accessibility is as yet a discontent and furthermore there is a mischief of organization comfort. J. Vaishnavi et al proposed the Latent Information towards Various Numerical Related SQL Queries [24] in which they determined that by using a multi cloud with a series of dealing proprieties and it not only secures the confidentiality of standing data, but also addresses latent privacy preserving in numerical properties or after large number of query fired [22]. They used RSA algorithm for key generation and AES algorithm for encryption and decryption of data.

3. SYSTEM ARCHITECURE / SYSTEM OVERVIEW

Our work is based on work of Kaiping Xue et al based on two-cloud computing, along with key generation our proposed system gives a way to deal with queries of numeric related information with security assurance. We have considered the procedures and protocols related with the assurance preservation of the outsourced data to the outside cloud server. The Range Queries work by executing the repeated range query can keep secrecy of keywords, verification, data integrity and query privacy. After that system combines the range queries constructively completed the encoded information utilizing a novel SQL secured encryption system. The request secured encryption is one of the tools used which enables assessment activities to be especially related on encoded information, without decoding the operands. So that as it might encryption of non-numeric data isn't possible with this tools. Afterward the two-cloud system is presented which partitions the private data and queries pattern into encrypted form in two distinct clouds which don't have known about one another. The data privacy and client authenticity also increased with a secrete key so that no any unauthorized client / user can access private data.

As mentioned earlier we have the customer can recapture the necessary information from the cloud, when the query contain logical operators like ">", "<" and "<>" and the operations like "SUM / AVG" for one segment, or in different condition more than one sections. Assume, the customer

needs to recover information from the table, whose segment T_i ought to be ">" than a steady x (i.e., SELECT *FROM table WHERE T_i > x). In our system, it is settled by figuring the indication of each estimation of (T_i(k) - x), in which k crosses all columns of the whole table. On the off chance that the outcome is "> 0" at that point the important information fulfills the query logic. These operations are executed on the encoded fields, with the goal that the security is vigorously saved. For this at the hour of putting away information in to cloud A, every section name T_i must be encrypted. As needs be, on the off chance that the administrator is "<" at that point the predicate becomes "T_i < x" and the relating activity is (x - T_i(k)). The remaining stages are same as the above cases. For the instance of "< >" i.e "Among x AND y", the outcome is the crossing point of T_i > x and T_i < y.

The project framework can keep up the security of information and query demands against every one of the two clouds. Especially, Cloud A solitary realizes the query demand style and the last record, yet because of copy information, Cloud A can't precisely comprehend the at long last satisfied list set for each single solicitation. For Cloud B, it realizes the fulfilled records of each single solicitation, yet after the proposed tasks, it doesn't have a clue about the connection of the relating information. Also, Cloud B can barely separate whether two got sections are created from at least one segments in the novel database.

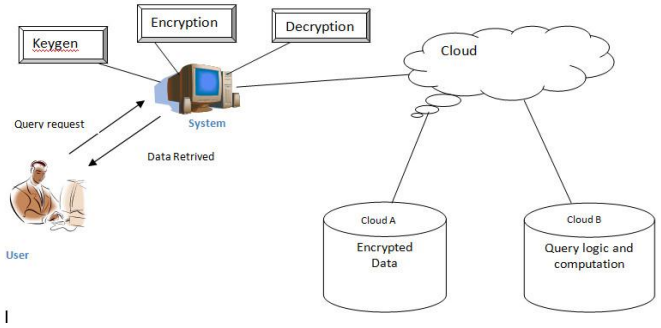

Fig -1: System Architecture

A. System Admin

Our proposed system architecture incorporates a database manager, and two cooperating clouds. In this system, the database manager can be executed on a client side from the point of view of cloud administration. The two clouds (Cloud A and Cloud B), at the server's side and provide necessary calculations to the administrator.

B. System User

He is approved client who access information from cloud database. The two clouds work together to react each queries demand from the approved clients (accessibility).

C. System Interface

In our system, data are converted into encrypted form and stored on cloud A and the private keys are stored on Cloud B with query computational logic. So for each query, the corresponding knowledge includes the data contents and the relative processing logic.

D. Security Policy

We proposed to use CryptDB and encryption algorithm to encrypt block of data. This algorithm is used for Key-expansion and Data Encryption purpose.

Algorithm

1. Start
2. Allocate Cloud A and Cloud B
3. Use key for user authentication.
4. Encrypt Data Using CryptDB and encryption algorithm.
5. Data in encrypted form is stored on Cloud A.
6. Store private keys with query computing logic on Cloud B.
7. Use request secured encryption tools to enable encoded data access activities, without decoding the operands using range queries.
8. End

4. METHOD OF EXPERIMENTATION

To lessening the hazard for information just as applications in a outsourced cloud is the simultaneous utilization of different clouds. A few methodologies are advanced as of late by this technique. Cryptographic techniques and security levels are the two main things of secured mobile cloud computing [2]. This contains a usage on these various protections and security assurance on numeric related SQL queries by utilizing two-cloud approaches. These created two-cloud designs permit to classify the accessible framework and to investigate them as indicated by their improved security benefits. We propose protection and security on SQL range queries just as scientific tasks over outsource cloud database. By utilizing that Two-cloud design we propose a two level encryption and decryption technique which gives high security to cloud client's information. The simulation results according to proposed algorithm are noted for data insertion and data selection. The average rate for insert is noted for data insertion and query response time is noted for data selection process as a performance measure.

5. RESULT ANALYSIS

The result of insertion of queries and accessing system by number of users is shown in following figures.

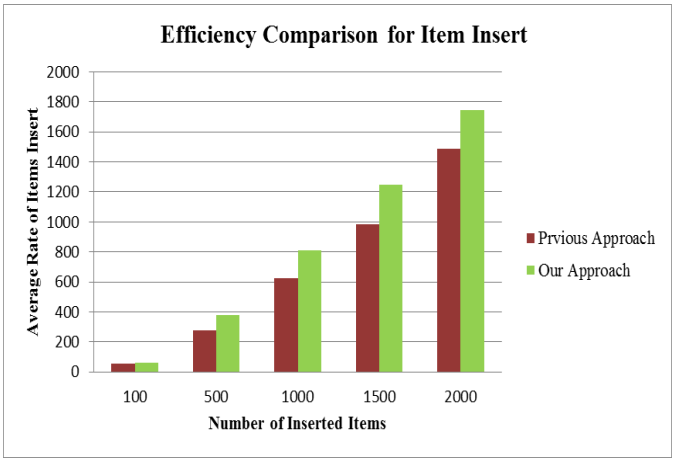

Fig -1: Diagram showing comparison of average rate of insertion for Item Insertion Process with existing technique and proposed technique Item.

The efficiency of insertion process comparison for the previous and proposed approach is shown in above Figure 1. It shows that with proposed approach, we achieve higher query insertion rate, because while inserting the data on one cloud, we used encryption technique along with a key logic on another cloud, so no need to do any overhead computation on the same cloud.

The efficiency calculation for item select in terms of delay calculation between previous and proposed system is shown in Figure -2. It can be stated that proposed approach performs better because all computational work needed for accessing database will done in between client and query processing cloud and data is on another cloud. Also cloud computing is built upon number of servers with multi-kernel CPUs, which provides parallel property to cooperatively complete a given task. i.e. more no of user can access system in parallel.

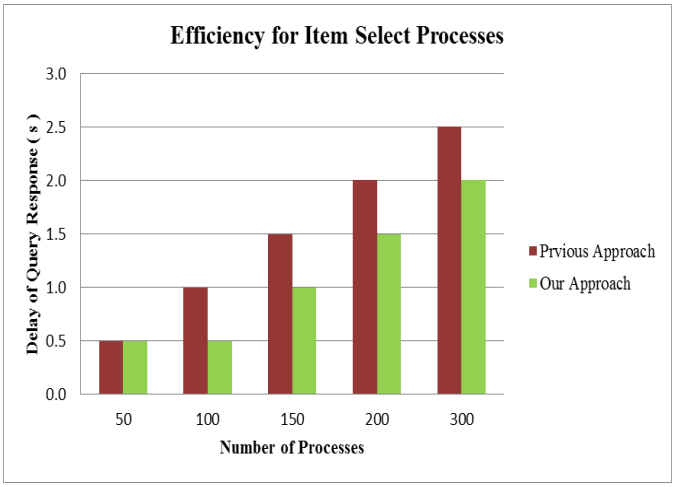

Fig -2: Diagram showing comparison of delay in query respond in Seconds for Item Selection Process with existing technique and proposed technique.

6. CONCLUSION AND FUTURE SCOPE

We have considered the various procedures and protocols related with the assurance preservation of the outsourced data to the outside cloud server. The advancement in this area a bit of the works related range queries, organize protecting encryption and multi-cloud structure. The Range Queries work by executing the repeated range query can keep secrecy of keywords, verification, data integrity and query privacy. After that it combines the range queries constructively completed the encoded information utilizing a novel SQL secured encryption system. The request secured encryption is one of the tools used which enables assessment activities to be especially related on encoded information, without decoding the operands. So that as it might encryption of non-numeric data isn't possible with this tools. Afterward the two-cloud system is presented which partitions the private data and queries pattern into encrypted form in two distinct clouds which don't have known about one another. The data privacy and client authenticity also increased with a secrete key so that no any unauthorized client / user can access private data. In our future work, with security we can speedup data processing by using parallel algorithms using technologies like GPU / CUDA.

REFERENCES

[1] J.M. Bofhli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multi-cloud architectures," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 212224, 2013.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches" Wireless Communications and Mobile Computing, vol.13, no.18, pp.15871611, 2013.

[3] B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-Preserving Index for Range Queries," Proc. 30th Intl Conf. Very Large Data Bases (VLDB04), pp. 720-731, Aug. 2004.

[4] X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, "Data mining with big data" IEEE Trans- actions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 97107,2014.

[5] 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.

[6] E. Damiani, di S. D. C. Vimercati, M. Finetti, S. Para-boschi, P. Samarati, and S. Jajodia . Implementation of a storage mechanism for untrusted dbmss. In 2nd Inter-national IEEE Security in Storage Workshop (SISW 2003), Information Assurance, The Storage Security Perspective, 31 October 2003, Washington, DC, USA, pages 3846, 2003.

[7] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud computing security: from single to multi-clouds," in Proceedings of the 45th Hawaii International Conference on System Science (HICSS2012). IEEE, pp. 54905499, 2012.

[8] 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 (SP13). IEEE, pp. 463477, 2013.

[9] R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: protecting confidentiality with encrypted query processing," in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, pp.85100, 2011.

[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] Z. Liu, X. Chen, J. Yang, C. Jia, and I. You, "New order preserving encryption model for outsourced databases in cloud environments" Journal of Network and Computer Applications, vol. 59, pp. 198207, 2016.

[12] B. Wang, Y. Hou, M. Li, H. Wang, and H. Li . Maple: scalable multi-dimensional range search over encrypted cloud data with tree-based index. In 9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS 14, Kyoto, Japan - June 03 - 06, 2014, pages 111122, 2014.

[13] E. Shi, J. Bethencourt, H. T. Chan, D. X. Song, and A. Perrig. Multi-dimensional range query over encrypted data. In [DBL 2007], pages 350364.

[14] 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.563574, 2004.

[15] D. Boneh and B. Waters . Conjunctive, subset, and range queries on encrypted data. In Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings, pages 535554, 2007.

[16] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud computing security: from single to multi-clouds," in Proceedings of the 45th Hawaii International Conference on System Science (HICSS2012). IEEE, 2012, pp. 54905499.

[17] S. R. Ganta, S. P. Kasiviswanathan, and A. Smith, "Composition attacks and auxiliary information in data privacy," in Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2008, pp. 265273.

[18] P. Paillier, "Public-key cryptosystems based on composite degree residuosityclasses," in Advances in Cryptology-EUROCRYPT99. Springer, 1999, pp. 223238.[42] ANSI, X3-135, American national standard for information systems: Database language SQL, American National Standards Institute, NY,1986.

[19] E. Stefanov and E. Shi, "Oblivistore: High performance oblivious cloud storage," in Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP13). IEEE, 2013, pp. 253267.

[20] O. Goldreich, Foundations of cryptography: volume 2, basic applications. Cambridge university press, 2009.

[21] J. Katz and Y. Lindell, Introduction to modern cryptography. CRC press, 2014.

[22] Y. Dou, K. C. Zeng, H. Li, Y. Yang, B. Gao, K. Ren, and S. Li, "P 2 -SAS: Privacy- preserving centralized dynamic spectrum access system," IEEE Journal on Selected Areas in Communications, 2016.

[23] M. AdelsonVelskii and E. M. Landis, "An algorithm for the organization of information," DTIC Document, Tech. Rep., 1963.

[24] J.Vaishnavi, Dr. Aruna Varanasi,Dr. Prasanta Kumar Sahoo " Latent Information towards Various Numerical Related SQL Queries" researchgate.net publication, April 2019.