IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 12-18
International Conference on Management Practices, Innovations & Research 2019

A Survey on Privacy-Preserving Mining of Association Rules from Transaction Databases

[1]Rani Mankar, [2]Jayant Adhikari,3 Jiwan Dehankar

[1]M.Tech Student, Department of Computer Science & Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, Maharashtra, India.

[2,3]Assistant Professor, Department of Computer Science & Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, Maharashtra, India.

Abstract— *Database Outsourcing is a promising data organization system in which Data-proprietor stores the private information at the untouchable organization supplier's site. The organization provider directs and deals with the database and benefits the readymade organizations to the data proprietor and their clients to make, update, eradicate and get to the database. Regardless of the way that database security is required in light of the way that more organization providers are not reliability. The genuine necessities for getting security in outsourced databases are mystery, assurance, trustworthiness, and freshness if there ought to be an event of component redesigns, get to control in multi-customer condition, availability and request approval and confirmation. To achieve these all necessities distinctive security frameworks like get to control based strategy, ask for ensuring encryption based technique, hardware based encryption approach, fake tuple based philosophy, secret sharing system, checked data structure approach, qualities based procedure, united intermittence and encryption based procedure, have been progressed till date. In this paper diverse security segments separated and their basics given in this review paper.*

Keywords— *Access Control, Confidentiality, Freshness, Integrity, Outsourced Databases, Query Authentication, Security mechanisms*

I. Introduction

"Assurance Preservation" in data mining suggests the Confidential or basic data must be jam or secure by the unapproved individual or attacker. The issue of security ensuring data mining has ended up being more indispensable starting late because of the growing ability to store singular data about customers, and corporate data of private foundation with the ultimate objective of outsourcing and an extensive variety of various purposes. Starting late, the security of outsourced databases is a pervasive examination subject. The untouchable gives a framework to allow their customers to make, store and get to their databases at provider end. Using outsourced database can help affiliation diminish gear equipment cost, system building, furthermore diminish cost of the work constrain division. Regardless, when the all of data be placed in outsourced database organization provider, the provider is not trusted, sensitive data may have spilled crisis. Thusly, the shielding insurance of database ends up being basic issues [6]. The expression "Database as a Service" (DBaaS) appeared in [7]. DBaaS is the breakaway advancement of the late period. The data proprietor of the affiliation stores their data at the pariah organization supplier's site and delegates the obligation of administering and managing the data to the organization provider. This perspective diminishes the need of presenting data organization programming and gear, utilizing administrative and data organization group (work drive) at the association's site. Along these lines, the affiliation can concentrate on their middle business justification rather than on the tedious control of data organization provoking the saving in data organization cost. Cloud subterranean insect, Amazon Dynamo DB, Hosted MongoDB are a couple instances of database organization providers.

Ensuring the security of the outsourced databases is a phenomenal test in the present situation. As the data is secured at the organization supplier's site, the truths may affirm that organization provider is wary to the extent revealing and mishandling the data. For this circumstance, security of the database can be hampered essentially. In the occasion that fitting security is not approved, then there are chances of data bursts and hacking the data in an unapproved way. Data breaking suggests disclosing the fragile data intentionally or coincidentally. According to the audit taken by Trust wave Global Security [1], out of 450 data burst tests, 63% of examinations were related to the association of outcast organization providers. As demonstrated by the data break examination done by Trust wave in 2012, 76% of security needs were made by the outcast organization provider [2]. Thusly, it is to a great degree principal for the associations to think about security finishing in their outsourced databases to keep the data private and in this way taking after the organization gauges and controls. Mystery, respectability in setting of satisfaction and precision, authenticity, duty, et cetera is considered as the foundation of security organizations. Along these lines, completing them in a proficient way is basic from the security point of view. Distinctive systems are used for understanding the security as a piece of database outsourcing. These frameworks fuse encryption, checked data structures; ask for shielding encryption, signature arrangements, et cetera. In this paper, we have given the entire examination of security systems nearby their points of interest and weaknesses.

The objective of this paper is to focus generally on various security techniques for outsourced trade datasets. Whatever is left of the piece of the paper is made like this Section II demonstrates the speculative establishment of this paper. Region III presents comparable review/examination of different security techniques and section IV shuts the paper with framework and future heading.

II. Literature Review

A. Access Control Based Approach [13]

Data arrangement, respectability, and security of the clients' information are guaranteed by this system. Among various organizations of circulated registering, engaging secure access to outsourced data builds up a solid structure for information organization and distinctive operations. In any case, more research attempts are required to finish versatile get to control to tremendous scale dynamic data. In this condition, the data can be redesigned just by the principal proprietor. Meanwhile, end customers with different get to rights need to scrutinize the information in a gainful and secure way. Both data and customer components must be properly dealt with to spare the execution and prosperity of the outsourced stockpiling structure.

In[13]"Secure and Efficient Access to Outsourced Data", Weichao Wang, Zhiwei Li,Rodney Owens, Bharat Bhargava proposed their techniques that consolidate:- (1)The proposed approach gives fine grained get to control to outsourced data with versatile and beneficial organization. The data proprietor needs to keep up only several favoured bits of knowledge for key acceptance. (2)It does not need to get to the limit server except for data updates. They propose finish frameworks to deal with stream in customer get to rights and overhauls to outsourced data.

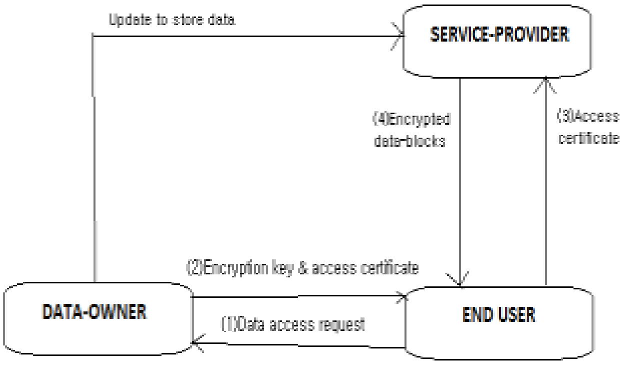

Figure.6 Illustration of the application situation [13]

Along these lines, the proposed strategy is solid against scheming attacks if the hash limit is seen as ensured. Examination shows that the key assurance framework in perspective of hash limits will exhibit to a great degree obliged overhead. They propose to use over-encryption and additionally indifferent revocation to keep denied customers from getting to updated data pieces. The essential preferred standpoint of this procedure is amazingly limited overhead, keep up a vital separation from tricky ambushes. The check plan of PKI is used for keeping up the uprightness data get to and the correspondence achieved for resource sharing. The duty is in like manner supported in this procedure by taking after the customer interest for data using the timestamp. The drawback of this system does not have the quality with respect to master recovery. The technique does not support the flexibility for acquiring broad number of clients.

B. Quality Based Access Control Approach[14]

To achieve Confidentiality, Accountability, Access Control Attribute based get to control system is used as a piece of which the passage structure is related to the game plan of characteristics of the customer. In[14]"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", Shucheng Yu, Cong Wang, KuiRen, and Wenjing Louaddress the open issue and propose an ensured and versatile fine-grained data get to control anticipate circulated registering. They proposed arrange in which each data record can be associated with a course of action of characteristics which are essential as to interest. The passage structure of each customer can accordingly be portrayed as a fascinating cognizant expression over these credits to reflect the degree of data records that the customer is allowed to get to. As the genuine expression can address any desired data record set, fine-graininess of data get to control is refined. To maintain these passageway structures, they describe an open key part for each attribute. Data archives are encoded using open key parts identifying with their attributes. Customer riddle keys are portrayed to reflect their passage structures so that a customer can interpret a figure content if and just if the data report properties satisfy his passageway structure. Here fulfilled these all Security essential:

1. Fine-graininess of Access Control
2. Client Access Privilege Confidentiality
3. Client Secret Key Accountability
4. Information Confidentiality

The advantage of this strategy is that calculation and correspondence cost brought about for denial is less. It experiences one shortcoming. The characteristics connected with the clients are put in Attribute Authority. The denied client can degenerate this power by overhauling their own particular mystery key likewise the mystery key of non-repudiated clients.

C. Fake Tuple Insertion Based Approach [15][16][17][18]

Fake tuple based strategy is generally used as a piece of outsourcing trade database for the essential question is to dumbfound the organization provider which may be attacker besides the security organizations get a kick out of the chance to reliability and insurance. Because of the fake tuple organization provider can't find the main sponsorship of the things in the dataset. The expansion of fake tuple based approach is gotten in [15], [16] and [17] to give the uprightness organizations. It dominatingly joins two strategies as probabilistic approach and deterministic strategy. In probabilistic system [15]"Integrity assessing of outsourced data", M. Xie, H. Wang, J. Yin, and X. Meng proposed the fake tuples are made and implanted into the database. For affirming the question genuineness, the request is given up against the database server which contains both the honest to goodness and fake tuples as the predicates. The server gives back the request comes to fruition. These results are affirmed by the client who knows all the fake tuples in the database. The client evaluates the fake tuples returned by server through outcome and the tuples managed by him. In case tuples from server and from client are found to show up as something else, then the server is considered as misleading and it is articulated that the data has been modified; else if tuples from both client and server are same, then it can be ensured that satisfaction is refined i.e. respectability of the data is kept up. Starting at now determined, the client should think about the fake tuples. The client needs to keep up the copy generally tuples. On the off chance that there ought to emerge an event of broad databases, a close-by database of fake tuples must be kept up which causes extra limit overhead on client and it is against outsourcing. Freshness is guaranteed by using the fake upgrade operation. The client eradicates and inserts the fake tuples and separate the results got by the server and surveys the freshness. In [16] "Giving freshness confirmations to outsourced databases, "M. Xie, H. Wang, J. Yin, and Meng proposed the deterministic philosophy facilitates the need to save the fake tuples. The deterministic limits are used to repeat the fake tuples. These made fake tuples have prominent illustration and it can be viably noted by the software engineer. Thusly, an encryption is associated on the bona fide and fake tuples.

In [17] "Information Integrity Evaluation in Cloud Database-as-a-Service", P. Ghazizadeh, R. Mukkamala S. Olariucreates the tuples with no discernable case using uniform spread and from this time forward removes the need of scrambling the tuples.

D. Equipment level Encryption based approach [19] [20]

For the security advantage the data assurance, one of a kind encryption gear for IBM DB2 has been used as a piece of [7]. Here each one of the lines of the database is mixed all things considered using DES (Data Encryption Standard) count. The question execution time in gear level encryption is significantly less when appeared differently in relation to the item level encryption. In [19]"SHAROES: A Data Sharing Platform for Outsourced Enterprise Storage Environments", Aameek Singh,Ling Liu propose a phase called SHAROES that gives data sharing capacity over such outsourced stockpiling circumstances. SHAROES give rich *nix-like data sharing semantics over SSP set away data, without trusting the SSP for data mystery or get to control. SHAROES is stand-out in its ability in decreasing client commitment in the midst of setup and operation utilizing as a part of band key organization and grants a nearby steady move of existing stockpiling circumstances to the new model. It is additionally predominant in execution by limiting the usage of exorbitant open key cryptography in metadata organization. In [20]"Trusted DB: A Trusted Hardware based Database with Privacy and Data Confidentiality", Summit Bajaj, Radu Sion proposed server side encouraged and generous prototyping gear. It gives privacy and data characterization playing out the question streamlining and reinforces any sort of request let conflict with database.

The benefit of this procedure is gives security, mystery and get to control. In any case, due to in-created hardware treatment of query.it encounters cost overhead and it has some execution confinements. It is useful for little databases. In the event of limitless databases, encryption and unscrambling causes additional overhead on the structure inciting degradation in framework execution and profitability. Encryption based systems experience the ill effects of key organization overheads.

E. Verified information structure based approach[21]

Confirmed data structure based philosophy is used for generally Authentication and Integrity organizations in the outsourced trade database show. For Authenticated data structure approach a couple of techniques are used as a piece of is one-way hash limit, cryptographic check approach, merkle hash tree, Bloom channels, Elliptic curve cryptography. In [21]"Scalable Verification for Outsourced Dynamic Databases", HweeHwa Pang Jilian Zhang KyriakosMouratidis concentrate the issue of checking the validity, satisfaction and freshness of question answers from as regularly as conceivable overhauled databases that are encouraged on untrusted servers. They introduce a tradition, based upon stamp add up to, for checking the precision of question answers. Their strategy has the fundamental property of allowing new data to be scattered speedily, while ensuring that out-dated qualities past a pre-set age can be recognized. They furthermore create check instruments for the B+-tree and standard social overseers that are sensible for component databases. The favourable position is finishing fundamentally higher trade throughput. The disservice is correspondence incurred significant damage for trading the page-level data is furthermore more. For executing the automated mark arrange, immense limit and exchange speed is required.

F. Mystery Share Distribution based approach[22]

In spite of the fact that the encryption makes the information private for safety, it makes additional overhead of encryption and decryption on the framework and corrupts the execution of database. So to ensure the information, mystery offer appropriation based approach best suits in the framework where encryption is not connected. As opposed to performing encryption on information, information is dispersed on different servers, called as shares.

To accomplished privacy, respectability, accuracy in [22]"Privacy-Preserving Computation and Verification of Aggregate Queries on Outsourced Databases”, Brian Thompson, Stuart Haber, William G. Horne, Tomas Sander, Danfeng Yao present an answer in which administration suppliers can cooperatively figure total inquiries without picking up information of transitional results, and clients can confirm the outcomes of their questions, depending just on their trust of the information proprietor. Our conventions are secure under sensible cryptographic suspicions, and are powerful to intrigue among k unscrupulous administration suppliers. They concentrated on processing total inquiries incorporating SUM and AVERAGE with SELECT provisos. The main objective of PDAS is to anticipate miniaturized scale information (i.e., singular information sections) from being got to by clients or any of the outsider administration suppliers who are assigned by the information proprietor to answer questions. They presented two primary procedures: - A dispersed engineering is presented for outsourcing databases utilizing numerous administration suppliers. They stretched out limit mystery sharing plans to bolster complex collection operations by utilizing the added substance property of polynomials over a field. - A check convention is created for the client to confirm that the outsourced calculation is to be sure figured effectively, without releasing any microdata. They gave security investigation that our convention achieves secrecy, uprightness, accuracy, and plot resistance properties. They likewise talked about conceivable variations. The advantage of this methodology is Encryption is not required so overhead is not happens. The drawback of this methodology is that it just backings the numeric information. It doesn't bolster total questions.

G. Request Preserving Encryption based approach[23]

To increased better security in [23]"Order Preserving Encryption for Numeric Data", Rakesh Agrawal , Jerry Kiernan, Ramakrishnan Srikant, YirongXu present a request protecting encryption plan for numeric information that permits any examination operation to be specifically connected on encoded information. Question comes about delivered are sound (no false hits) and finish (no false drops). It permits standard database files to be worked over encoded tables and can without much of a stretch be coordinated with existing database frameworks. The proposed plan has been intended to be conveyed in application situations in which the gate crasher can access the scrambled database, however does not have earlier space data, for example, the circulation of qualities and can't encode or decode self-assertive estimations of his decision. The encryption is strong against estimation of the genuine quality in such situations. While encoding a given database P, OPES makes utilization of all the plaintext values as of now present P, furthermore utilizes a database of tested qualities from the objective dispersion. Just the encoded database C is put away on plate. In the meantime, OPES additionally makes some helper data K, which the database framework uses to unscramble encoded values or scramble new values. Consequently K serves the capacity of the encryption key. This assistant data is kept scrambled utilizing routine encryption procedures. OPES works in three phases: 1. Model: The information and target dispersions are demonstrated as piece-wise direct splines. 2. Straighten: The plaintext database P is changed into a "level" database with the end goal that the qualities in F are consistently conveyed. 3. Change:

The level database F is changed into the figure database C with the end goal that the qualities in C are appropriated by target circulation.

The primary preferred standpoint of encryption is that it makes the information muddled and conspire handles upgrades smoothly and new values can be included without requiring changes in the encryption of different qualities. It is valuable for little databases. The downside is that this methodology bolsters just the reach inquiries and experiences plain-message picked assaults and the extent of encryption key is twice as vast as the quantity of extraordinary qualities in the database.

H. Discontinuity based approach [24]

To grabbed mystery of the necessities and rightness and satisfaction in [24]"Horizontal Fragmentation for Data Outsourcing with Formula-Based Confidentiality Constraints", Lena Wiese exhibits level irregularity in which lines of tables are detached (as opposed to segments for vertical crack). They give a condition based significance of grouping objectives and a proposal based importance of level crack precision. By then they apply the interest technique to pick this precision property and present a figuring that procedures a correct level irregularity. In their procedure for vertical break, just projection onto fragments is maintained and thusly the claimed "privacy necessities" are just described as sets of properties of the database design. To expand the "vertical irregularity simply" approach they make the going with responsibilities:- – They propose to use vertical and also level break. In particular, their hope to filter through characterized lines to be securely secured at the proprietor site. Whatever is left of the lines can safely be outsourced to the server. - They intensify expressiveness of the "order prerequisites" by using first demand conditions instead of sets of trademark names. This recommends vertical break can be data subordinate as in only a couple of cells of a section must be secured. – They unequivocally allow a full database mapping with a couple of relations pictures and a game plan of database conditions. With these conditions they familiarize the probability of inductions with the brokenness point and give an estimation to keep up a vital separation from such conclusions. In their level intermittence approach pieces are sets of columns as opposed to sets of sections. The parts (the lines in the server and the proprietor piece) must be merged again by recently taking the union U of the areas. The upside of this technique is encryption not require here so extra overhead not occur here. The drawback is that how to adaptively update the data and structure is gotten the opportunity to bewilder.

I. Joined discontinuity and encryption based approach[25]

To achieve information classification and protection in [25]" Adaptive, Secure, and Scalable Distributed Data Outsourcing: A Vision Paper" Li Xiong, Slawomir Goryczka, Vaidy Sunderam made a structure in which they consolidate information apportioning, encryption, and information decrease, for example, packed or factual information outsourcing to guarantee information secrecy and security while minimizing the expense for information transportation and calculation. Every asset supplier may store parts of the information in unique, scrambled, or lessened structure. Calculations can be produced to permit clients to pre-process their information for secure outsourcing on appropriated asset suppliers that efficiently adjust the prerequisites on classification and protection, versatility, and scientific utility of the information for a given workload. Versatile outsourcing plan that permit clients to progressively arrangement their outsourcing needs with information upgrades and changing question workload. Control-hypothesis based instruments can be created to viably model and gauge the changing inquiry workload and changing information for powerfully conforming the outsourcing plan. An essential building piece of their structure is encryption and apportioning (or discontinuity) procedures. Encryption comprises in encoding every one of the estimations of a quality, in this way making them indiscernible to unapproved clients. Discontinuity comprises in dividing information records (level apportioning) or qualities (vertical parceling) in subsets with the end goal that exclusive records or properties in the same part are noticeable together.

The benefit of this systems techniques that make different types of cloud and local platforms compatible, host practical manifestations of remote databases, and perform at optimal levels in order to make the technology eminently usable. The drawback is that how to adaptively update the data in the cloud while balancing the computational overhead and accuracy of the synopsis is a challenge. However, updating the deployed data too often increases the amount of noise that need to be added to the synopsis. Careful privacy budget management needs to be performed.

III. Requirements of a PPDM Algorithm

J. Accuracy

The Accuracy is almost related to the information misfortune coming to fruition due to the concealing method: the less is the information misfortune; the better is the data quality. PPDM calculation has needed to keep up high accuracy to diminish information loss [1].

K. Completeness and Consistency

Completeness surveys the level of missed data in the sanitized database. Insufficient data hugy affects data mining comes to fruition and debilitates the data mining estimations from giving a careful representation of the hidden data.

L. Scalability

It is another basic point of view to study the execution of a PPDM calculation. In particular, versatility portrays the capability designs when data sizes increase.

M. Data quality

It is a fundamental piece of PPDM. Brilliant data that has been masterminded especially for data mining assignments will realize important data mining models and yield. Then again, low quality data has a significant negative impact on the utility of data mining results.

N. Security

It is the level of protection against mischief, loss of information, and wrongdoing. There are two rule techniques concerning how to deal with the issues of security that rise today. The essential is a legitimate and plan approach whereby affiliations are compelled by the way they store and use data centered on assurance law and open technique. It normally satisfies desires by surveying circumstances and picking if the security crack achieved by using the data inside a given way is upheld or not. The second approach is inventive, and gives approved assurance guarantees through cryptographic means. This approach has the limit of engaging the data to be used while deflecting assurance bursts.

IV. Conclusions

The Database as a Service is a late database organization game plan which is creating well known well-ordered on account of its helpfulness. In this paper, we have discussed the possibility of DBaaS, its building and its advantages. The watchful examination of general security necessities for the outsourced databases is done in this paper. We have fundamentally based on how the security associated in outsourced databases and separated the frameworks with their handiness for the same. The quick and dirty talk of fulfilling the mystery, reliability, culmination, Correctness, get to control and duty in single and multi-customer condition is given. The summed up security structure can be delivered to such a degree, to the point that it supports an extensive variety of databases and each one of the sorts of request. Here sketched out all the unmistakable security procedures with their preferences and burdens in table. The future change can similarly base on offering security to outsourced trade database nearby reducing the correspondence, figuring cost and streamlining of request get ready time.

References

[1]. http://www.computerweekly.com/news/2240178104/Badoutsourcingdecisions-cause-63ofdatabreaches.

[2]. http://www.networkworld.com/news/2012/020712-data- breach-255782.html

[3]. www.oracle.com/technetwork/topics/.../oes-refarch-dbaas508111.pdf

[4]. http://dbaas.wordpress.com/2008/05/14/whatexactly-is-database-as-a-service/

[5]. https://451research.com/reportshort?entityId=78105&referrer=marketing

[6]. Yung-Wang Lin, Li-Cheng Yang, Luon-Chang Lin, and Yeong-Chin Chen, Preserving Privacy in Outsourced Database, International Journal of Computer and Communication Engineering, Vol. 3, No. 5, September 2014.

[7]. H. Hacigumus, B. Iyer and S. Mehrotra, Providing database as a service, in Proc. of IEEE 18th ICDE, 2002, pp. 29-38.

[8]. E. Mykletun, M. Narasimha, and G. Tsudik,Authentication and integrity in outsourced databases, In Proc. of ACM Trans. On Storage, vol. 2, 2006, pp. 107-138.

[9]. M. Xie, H. Wang, J. Yin, and X. Meng, Integrity auditing of outsourced data,"VLDB 2007, pp. 782-793.

[10]. Zheng-Fei Wang, Ai-Guo Tang,Implementation of Encrypted Data for Outsourced Database, In Proc. of Second International Conference on Computational Intelligence and Natural Computing (CINC), IEEE, 2010, pp. 150-153.

[11]. Li Feifei, Marios H, George K, Dynamic Authenticated Index Structures for Outsourced Database, In Proc. of ACM SIGMOD"06. Chicago, Illinois, 2006, pp. 121-132.

[12]. SomchartFugkeaw, Achieving Privacy and Security in Multi- Owner Data Outsourcing, In Proc. of IEEE Transactions 2012, pp.239-244.

[13]. Weichao Wang, ZhiweiLi,Rodney Owens, Bharat Bhargava,Secure and Efficient Access to Outsourced Data, CCSW'09, November 13, 2009, Chicago, Illinois, USA ACM 978-1-60558-784-4/09/11.

[14]. Shucheng Yu, Cong Wang, KuiRen, and WenjingLou,Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, IEEE INFOCOM 2010.

[15]. M. Xie, H. Wang, J. Yin, and X. Meng, Integrity auditing of outsourced data, VLDB 2007, pp. 782-793.

[16]. M. Xie, H. Wang, J. Yin, and Meng, Providing freshness guarantees for outsourced databases, in Proceedings of the 11th international conference on Extending database technology: Advances in database technology, ser. EDBT "08. New York, NY, USA: ACM, 2008, pp.323–332.

[17]. P. Ghazizadeh, R. Mukkamala S. Olariu, Data Integrity Evaluation in Cloud Database-as-a-Service", In Proceedings of IEEE Ninth World Congress on Services, 2013, pp. 280-285.

[18]. FoscaGiannotti, Laks V. S. Lakshmanan, Anna Monreale, Dino Pedreschi, and Hui (Wendy) Wang, Privacy-Preserving Mining of Association Rules From Outsourced Transaction. Databases, IEEE SYSTEMS JOURNAL, VOL. 7, NO. 3, SEPTEMBER 2012.

[19]. AameekSingh,Ling Liu, SHAROES: A Data Sharing Platform for Outsourced Enterprise Storage Environments,Data engineering, IEEE 2008.

[20]. Sumeet Bajaj, RaduSion, TrustedDB: A Trusted Hardware based Database with Privacy and Data Confidentiality, In Proc. of IEEE Transactions on Knowledge and Data Engineering, 2013.

[21]. HweeHwa Pang Jilian Zhang KyriakosMouratidis,Scalable Verification for Outsourced Dynamic Databases, ACM.VLDB „09, August 2428, 2009, Lyon, France Copyright 2009.

[22]. Brian Thompson, Stuart Haber, William G. Horne, Tomas Sander, Danfeng Yao, Privacy-Preserving Computation and Verification of Aggregate Queries on Outsourced Databases, HP Laboratories HPL-2009-119, published by Springer Aug-2009.

[23]. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, Order pre-serving encryption for numeric data, In Proceedings of the 2004 ACM SIGMOD international conference on Manage-ment of data,SIGMOD "04, pages 563–574, 2004.

[24]. Lena Wiese,Horizontal Fragmentation for Data Outsourcing with Formula-Based Confidentiality Constraints, Advance in information and computer security, Springer 2010.

[25]. Li Xiong, SlawomirGoryczka, VaidySunderam, Adaptive, Secure, and Scalable Distributed Data Outsourcing: A Vision Paper,3DAPAS"11, June 8, 2011, San Jose, California, USA. Copyright 2011 ACM 978-1-4503-0705-5/11/06.