Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 1, January-2019, ISSN 2230-7540

Research on Distributed Database and Replication

Meenakshi[1]* Dr. Prerna Nagpal[2]

[1] Research Scholar, Sunrise University, Alwar, Rajasthan

[2] Associate Professor, Sunrise University, Alwar, Rajasthan

Abstract – As distributed database turned out to be increasingly well known, the requirement for development in distributed database management system become considerably progressively significant. The most significant issue is security that may emerge and conceivably bargain the entrance control and the integrity of the system. Right now, propose some answer for some security angles, for example, staggered get to control, confidentiality, unwavering quality, integrity and recuperation that relate to a distributed database system.

Keywords: Database, Management, Handling, Security, Development, Integrity

----------X----------

INTRODUCTION

Transparent Management of Distributed and Replicated Data

Transparency alludes to division of the more elevated level semantics of a system from lower-level usage issues. At the end of the day, a straightforward system conceals the usage subtleties from clients. The benefit of a completely straightforward DBMS is the elevated level of help that it accommodates the development of complex applications.

Reliability Through Distributed Transactions

Distributed DBMSs are expected to improve unwavering quality since they have duplicated segments and, in this way dispense with single purposes of disappointment. The disappointment of a solitary site, or the disappointment of a correspondence connect which makes at least one locales inaccessible, isn't adequate to cut down the whole system. On account of a distributed database, this implies a portion of the data might be inaccessible, however with appropriate consideration, clients might be allowed to get to different pieces of the distributed database. The correct consideration comes as help for distributed transactions and application protocols.

Improved Performance

The case for the improved performance of distributed DBMSs is normally made dependent on two focuses. Initial, a distributed DBMS parts the reasonable database, empowering data to be put away in nearness to its places of utilization (additionally called data restriction). This has two potential preferences: right off the bat, since each site handles just a bit of the database, conflict for CPU and I/O administrations isn't as serious with respect to brought together databases and besides, restriction lessens remote access postpones that are typically involved in wide area networks.

Easier System Expansion

In a distributed situation, it is a lot simpler to suit expanding database sizes. Significant system updates are only occasionally fundamental; development can for the most part be dealt with by adding preparing and capacity to the system. Clearly, it may not be conceivable to acquire a direct increment in power, since this likewise relies upon the overhead of dissemination. Be that as it may, critical upgrades are as yet conceivable.

Types of Distributed Databases

1. Homogeneous Distributed Database
2. Heterogeneous Distributed Database

Components of a Distributed DBMS

The detailed components of a distributed DBMS are given (figure 1.2) right now. One segment handles the cooperation with clients, and another arrangements with the capacity. The primary significant part, which is known as the client

processor comprises of four components (Ozsu and Valduriez, 2011):

The UI handler is answerable for deciphering client ridiculously in, and arranging the outcome data as it is sent to the client.

The semantic data controller utilizes the integrity limitations and approvals that are characterized as a component of the worldwide theoretical blueprint to check if the client inquiry can be handled. This segment is likewise liable for approval and different functions.

The worldwide inquiry analyzer and decomposer decides an execution system to limit a cost work, and make an interpretation of the worldwide inquiries into nearby ones utilizing the worldwide and neighborhood reasonable diagrams just as the worldwide catalog. The worldwide question enhancer is liable for producing the best technique to execute distributed join operations.

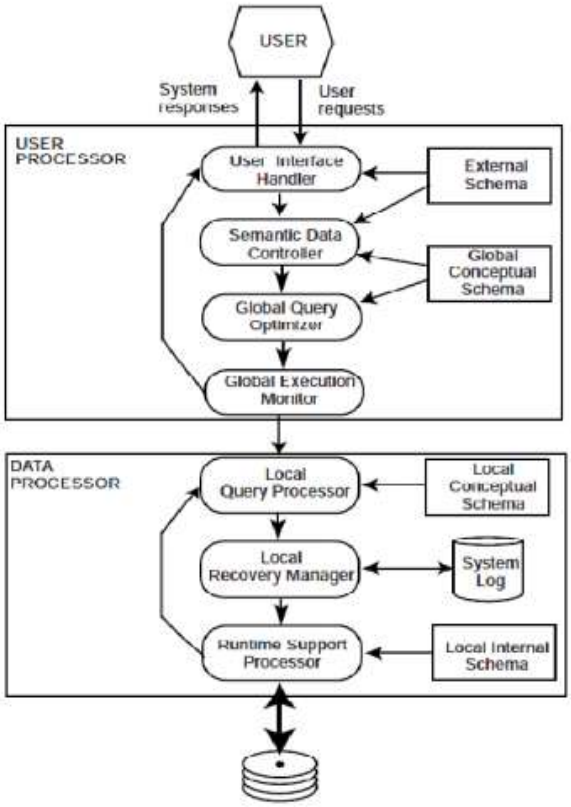

Figure 1 Components of a distributed DBMS.

NEED OF REPLICATION

Replication is the key trademark in improving the accessibility of data in distributed systems. Reproduced data is put away at various server locales with the goal that it very well may be gotten to by the clients in any event, when a portion of the duplicates are not accessible because of server or site disappointments. A Major limitation to utilizing replication is that repeated duplicates must carry on like a solitary duplicate, for example shared consistency too inner consistency must be saved, synchronization procedures for reproduced data in distributed database systems are required so as to expand the level of consistency and to lessen the chance of transactions rollback.

DATABASE REPLICATION

Replication in database systems is done fundamentally for performance reasons. The objective is to get to data locally so as to improve reaction times and dispense with the overhead of speaking with different destinations. Database replication is the way toward duplicating a database starting with one database server then onto the next server, and afterward keeping the two duplicates in synchronization, so they act as close as could reasonably be expected. Replication duplicates data or changes of data starting with one database then onto the next. Getting to the main database or the second, it doesn't make a difference since they are the equivalent, for example they are in synchronized.

Database Locality

This component of database replication keeps up the database locally so geologically far separation clients can get to data with rapid. These clients can get to data from nearby servers rather than far separation servers since data get to speed will be a lot higher contrasted with a removed area network.

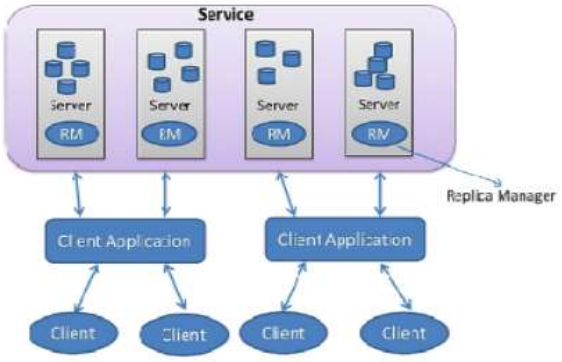

Figure 2 Basic data replication model.

Performance

Database replication regularly centers around improving both peruse and compose performances. At the point when an application is broadly utilized over an enormous network yet the database is put away at a solitary server, the database server can be a bottleneck of that system and the entire system eases back down, for example slow reaction time and low solicitation throughput limit. Numerous reproductions offer the system the data in equal and thus there is an expansion in performance.

Availability and Fault Tolerance

High accessibility of database requires low personal time of a database system. In a database system there exist two vacations the first is arranged and the other is spontaneous. Arranged vacation is caused during the support activity of all the software and equipment. Spontaneous vacation can strike whenever and it is because of unsurprising or eccentric disappointments, for example, equipment disappointments, software bugs, human blunder, and so on. Vacation is generally the essential streamlining area of database replication to expand the database accessibility. On the off chance that a database thing is put away at a solitary server and that server doesn't reactor is down or it may have slammed. In such cases database replication is the arrangement of this issue, which likewise has the ability to provide an issue tolerant database system. The imitation of a database server can provide the data things to the clients when a server disappointment happens. Database replication should be possible in any event the accompanying three unique ways.

Snapshot Replication

Data on one database server is evidently replicated to another database server, or to another database on a similar server. The snapshot replication strategy functions by occasionally sending data in mass configuration. Typically it is utilized when the buying in servers can work in read-just condition (figure 1, and furthermore when the buying in server can work for quite a while without refreshed data. Working without refreshed data for a while is alluded to as inertness. Snapshot replication works by perusing the distributed database and making documents in the working organizer on the merchant. These documents are called snapshot records and contain the data from the distributed database just as some extra information that will assist with making the underlying duplicate on the membership server.

Merger Replication

Data from at least two databases is consolidated into a solitary database. Consolidation replication is the way toward conveying data from Publisher to Subscribers, permitting the Publisher and Subscribers to make refreshes while associated or disengaged, and afterward blending the updates between destinations when they are associated (figure 1.5). Consolidation replication permits different locales to work independently and sometime in the not too distant future union the updates into a solitary, uniform outcome. Consolidation replication incorporates default and custom decisions for compromise. At the point when a contention happens, a determination is summoned by the Merge Agent and figures out which data will be acknowledged and engendered to different destinations.

Transactional Replication

Data from at least two databases is consolidated into a solitary database. Union replication is the way toward disseminating data from Publisher to Subscribers, permitting the Publisher and Subscribers to make refreshes while associated or detached, and afterward consolidating the updates between destinations when they are associated (figure 1.5). Union replication permits different destinations to work independently and sometime in the future union the updates into a solitary, uniform outcome. Union replication incorporates default and custom decisions for compromise. At the point when a contention happens, a purpose is conjured by the Merge Agent and figures out which data will be acknowledged and spread to different locales

REVIEW OF LITERATURE

Roichman and Gudes's (2016) Scheme proposes utilizing a fine-grained get to control to web databases. The creators build up another technique dependent on fine-grained get to control mechanism. The entrance to the database is administered and observed by the implicit database get to control. This is an answer for the weakness of the SQL meeting recognizability.

D. E. Denning(2016) at, depicts the significance of cryptography to make sure about the data access in online condition, they propose the utilization of mystery key encryption to be applied to database tables to encode the information contained in the table.

Almgren, M. (2015) presents an interruption detection apparatus planned for securing web servers, and legitimize why such a device is required. They portray a few intriguing highlights, for example, the capacity to run progressively and to monitor suspicious hosts. The design is adaptable and the marks used to recognize malicious conduct are not restricted to basic example coordinating of risky cgi contents. The device incorporates mechanisms to lessen the quantity of bogus alerts.

G. T. Buehrer (2016) portray a system to forestall SQL infusion vulnerabilities. Their system depends on contrasting, at run time, the parse tree of the SQL proclamation before consideration of user contribution with that subsequent after incorporation of information. Their answer is productive, adding around 3 ms overhead to database question costs. Moreover, it is handily received by application software engineers, having a similar syntactic structure as present well known record set recovery strategies. For exact analysis, they provide a contextual investigation of our answer in J2EE. They

actualize our answer in a basic static Java class, and show its adequacy and versatility.

Thomas et al. (2015) Scheme Thomas, in proposed a mechanized arranged articulation age calculation to evacuate SQL Injection Vulnerabilities. The creators execute their exploration work utilizing four open source extends to be specific: (I) Net-trust, (ii) Itrust, (iii)

Web Goat, and (iv) Roller (2016). Based on the test results, their readied proclamation code had the option to effectively supplant 94% of the SQLIVs in four open source ventures.

SQLIA Prevention Using Stored Procedures – Stored techniques are subroutines in the database which the applications can make call to . The counteraction in these put away strategies is actualized by a blend of static analysis and runtime analysis. The static analysis utilized for orders recognizable proof is accomplished through put away strategy parser and the runtime analysis by utilizing a SQL Checker for input ID

SAFELI This exploration manages the Static Analysis Framework so as to distinguish SQL Injection Vulnerabilities. This system plans to recognizing the SQL Injection assaults during the gather time. The two primary points of interest of this static analysis instrument are: first, it does a White-box Static Analysis and besides, it utilizes a Hybrid-Constraint Solver. On the off chance that we consider the White-box we found the Static Analysis, the proposed approach considers the byte-code and manages strings. While then again, the Hybrid-Constraint Solver actualizes the strategies to an effective string analysis apparatus which can manage Boolean, number and string factors.

Huang and Colleague (2012) propose WAVES, a discovery system for testing web applications for SQL infusion vulnerabilities. The instrument recognize all focuses a web application that can be utilized to infuse SQLIAs. It constructs assaults that focus on these focuses and screens the application how reaction to the assaults by use AI.

Swaddler (2013) breaks down the inward condition of a web application. It works dependent on both single and different factors and shows an amazing path against complex assaults to web applications. First the methodology portrays the ordinary values for the application's state factors in basic purposes of the application's components. At that point, during the detection stage, it screens the application's execution to distinguish unusual states.

WebSSARI utilize static analysis to check corrupt streams against preconditions for touchy functions. It works dependent on disinfected input that has gone through a predefined set of channels. The restriction of approach is satisfactory preconditions for touchy functions can't be precisely communicated so a few channels might be precluded.

Zongkai Yang, Jingwen Chen, Du Xu (2014) clarified regardless of what level of security is set up, touchy data in database are as yet powerless against assault. To maintain a strategic distance from the hazard presented by this risk, database encryption has been prescribed. Anyway scrambling all of database thing extraordinarily debases the performance of the database system. As an ideal arrangement they introduced is a database encryption scheme that provides most extreme security, while constraining the additional time cost of encryption and decoding.

Chin-Chen Chang (2015) introduced two new database encryption systems. The two systems depend on the idea of the RSA (Rivest, Shamir, Adleman) ace key. The first proposed system is a field-oriented encryption system with user ace keys that compare to the entrance privileges of numerous fields. The second proposed system is a record-oriented encryption system with a user ace key. Utilizing expert keys, we present a strategy that sets up a correspondence between the subsets of a given set and a lot of whole numbers.

Stephane Jacob (2016) clarified Protecting the confidentiality in huge databases without debasing their performance is a difficult issue, particularly when encryption and decoding must be performed at the database-level or at the application-level. They center around symmetric figures for database encryption since they are the main kind of figures with worthy performance for most applications. They call attention to that stream figures are the sufficient kind of encryption schemes.

Al-Fedaghi, S. (2015) characterizes affectability of individual information is one of the most significant factors in deciding the person's view of protection. A "degree" of affectability of individual information can be utilized in numerous applications, for example, choosing the security level that controls access to data and building up a proportion of trust when self-revealing individual information. Al-Fedaghi, presents a hypothetical analysis of individual information affectability and characterizes its extension and advances potential strategies for degree.

K Hemanth (2012) a safe and visually impaired biometric validation convention, which tends to the worries of user's security, format insurance, and trust issues. The convention depends on awry encryption of the biometric data; it catches the upsides of biometric validation just as the security of open key cryptography. The validation convention can run over open networks and provide non legitimate character check. They proposed a methodology that makes no prohibitive presumptions on the biometric data and is

henceforth appropriate to different biometrics. They break down the security of the convention under different assault situations.

Ahuja et al. (2013) have detailed about a base cost most extreme stream calculation that finds the databases to which the user profiles ought to be alloted with the end goal that the quantity of reproductions are greatest while limiting the system cost in keeping up these imitations. For all the user profiles, the calculation initially processes the cost investment funds in keeping up a user copy at all the locales and the most extreme number of unmistakable imitations that can be put away at that site.

Ceri et al. (2015) have introduced a review of some replication techniques that all keep as accuracy foundation one-duplicate serialisability. An anxious replication procedure that is called perused one-compose all (ROWA), where a read activity can be executed at any copy, compose operations must be done on all. This is an alteration of the single ace replication model. The read-one-compose all-accessible (ROWAA) approach is an alteration of the ROWA strategy, yet as opposed to keeping in touch with all reproductions, just the accessible imitations are composed, which presents the issue that copies probably won't be state-of-the-art.

Huang et al. (2012) proposed a data replication scheme that targets streamlining the correspondence cost between a mobile computer and the stationary computer. The stationary computer can be recognized as a server that stores the online database and mobile computer can be considered as workstations conveyed by mobile users. The creators have introduced and broke down both the static and the dynamic data designation schemes. In the static portion scheme a duplicate is either put away just at the server or put away at both the server and the mobile computer.

Gray et al. (2018) have revealed that the replication techniques can be portrayed by two unique measurements. In the first place, where an update is permitted to occur at a devoted server or at any server in the bunch of reproductions and second whether an update will be done synchronously at all imitations or no concurrently.

Shivakumar et al. (2013) introduced a strategy called per-user replication scheme that keeps up copies at destinations where the cost reserve funds in keeping up the imitations are most extreme. This system is an improvement over the unadulterated Home Location Register (HLR) scheme and the HLR/Visitor Location Register (VLR) scheme. In the HLR scheme, a call put by a user brings about a remote query at the HLR of the callee. A home area alludes to the site where a user is enlisted.

Bernstein and Philip (2015) have expressed that server systems for the most part rely upon an asset, generally on a database system. Recreating the server without the database improves accessibility however not performance and leaves the single purpose of disappointment issue. Performance isn't improved since a wide range of access, question and update operations are done on one single database bringing about inquiry update issues. In this way notwithstanding the replication of the server system, the asset should be recreated.

Kroegar et al. (2015) have proposed a model called Finite Multi-Order Context (FMOC). FMOC utilizes a tree based structure named trie to store arrangements of document gets to. Every hub of trie speaks to a document. The offspring of each hub speak to all the documents that have been seen after the parent. To demonstrate get to probabilities a field of emphasis number has been added to every hub. FMOC separates the tree into a few parcels and each segment contains predetermined number of hubs.

OBJECTIVES OF THE STUDY

1. It provide the insurance to the delicate data
2. It improves the performance of system.

RESEARCH METHODOLOGY

Model of Multilevel Relational Database

Inside the staggered social style, affiliations, tuples, qualities, just as components will in general be assigned security types. This sort of theory works by utilizing the specific qualification of any staggered respects seized all through the Jajodia: Sandhu type. This sort of style depends on the security differentiation uncovered on the BLP style, and no ifs, ands or buts this for the most part transforms into the specific staggered relative since comprises of the specific pair of parts. A state-independent staggered relative construction R (A1,C1,… … , An,Cn, TC) and 2) The collection point ou t focused connection is Rc (A1,C1, … A, Cn, TC).

The components of the single-level connection have a similar security order.

Integrity Constraints of MLS Database

So you can coordinate the highlights concerning MLS locales, the key genuineness limits for the social kind portrayed beforehand must be used, and a couple of extra constraints discharged. Commonplace in a social sort, a significant springs using the took a gander at important conditions. In MLS social sort this kind of key is known as the real obvious key (AK) which frequently the majority of us

think can be a user specified essential key including your subset inside data qualities Ai.

MLS integrity property (**Entity integrity): 1**

Leave AK alone the obvious key of a connection R and a staggered connection R fulfills substance integrity for all occasions Rc of R and t ε Rc

1. Ai ∈ AK ⇒ t [Ai] = invalid,

2. Ai, Aj ∈ AK ⇒ t [Ci] = t [Cj],

3. Ai ∈ AK ⇒ t [Ci] ≥ t [CAK] (where CAK is distinguished as the grouping of the obvious key)

This would imply that the unmistakable significant mustn't have an invalid worth, must be reliably assembled, and it is qualification must be took over through the differentiation of the entirety of the extra capacities.

MLS integrity property 2: Null integrity.

The connection R which will pays invalid integrity if, on the side of if, for each and every case associated with Remote control associated with Rc of R, the following two sicknesses hold:

1. For all t ∈ Rc, t [Ai] = invalid ⇒ t [Ci] = t [CAK], or we can say invalid qualities are characterized at the key level.

2. Rc is sans accommodation of progress, and it doesn't contain any couple of one of a kind tuples to such an extent that a solitary subsumes one different just as Some kind of tuple t subsumes a tuple s, when for any trademark Ai, either t [Ai, Ci] = s [Ai, Ci] or t [Ai] = invalid alongside s [Ai] = invalid.

This invalid integrity property required that the invalid an incentive inside a tuple can be ordered from the nature of the genuine mystery, which relating to subjects disposed of from bigger security goes, the real invalid values clear from diminished soundness ranges are generally changed through suitable values in a split second.

The accompanying property offers with ingenuity among the differing occurrences for a connection.

MLS integrity property (Inter-instance integrity): 3

Another staggered respects R pays between example integrity in the event that where, if and just if, for some c′ ≤ c, Rc′ = σ(Rc′ , c′), the spot that the channel work σ yields the specific c′-occurrence Rc′ originating from worldwide control the accompanying:

For each tuple t ∈ Rc to such an extent that t[CAK] ≤ c′, there is a tuple t′ ∈ Rc′ , with [AK, CAK] = t[AK, CAK] and for Ai ∈ AKt′ [Ai, Ci] = t[Ai, Ci] if t[Ci] ≤ c′ invalid, t[CAK]〉 something else

1. There are no more tuples inside Rc′ beside those individuals separated through the over idea.

2. The final product Rc′ is fabricated subsumption sans cost essentially by comprehensive destruction with respect to subsumed tuples.

The genuine filtration system run σ chart books R that can help different cases of Rc′(one for each and every c′ < c). By utilizing channel work, customers are for the most part on a just of which part of the staggered connection.

TABLE 1

DN	Dept_Name	Manpower	Dept_Location	Manager	TC
D11	Sales	53	443 South Ex.	Maxwell	S
D12	Account	23	701 Lodhi Road	Smith	TS
D13	Finance	18	302 Preemia Building	William	S
D14	General	22	C45 Ground Floor	Bell	S

DATA ANALYSIS

The Runtime Security System Architecture

All cycle providers complete the specific providers given in their brain to have the option to appraise brought about by the specific query after arrangement conveyance . Subsequently, they need to consistently been secured originating from hurt by just destructive or modest providers seeing that given before referenced.

All directions (non-worked in) required by just an outside administrator must be blended right JAR2 data document. This particular data record is typically stacked just as stored. Therefore it is definitely no association with the genuine capacity provider all through methodology execution. Moreover, demands operating together are normally separated by each other to forestall these people by trading information with one another and completed with a class loader occasion (called OG Class Loader) for every single issue. Exterior operators for the most part are remote just as spillage of information will be wiped out, as they are exclusively in a situation to talk with the little ones just as parent operators.

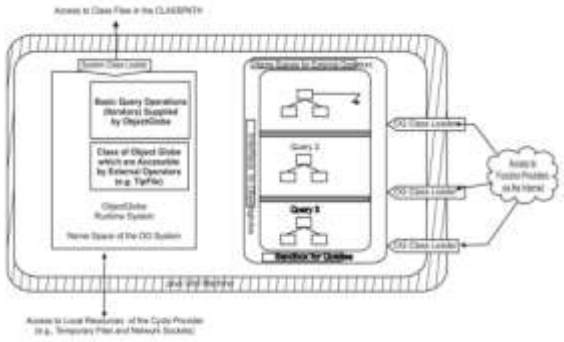

Figure 3: Resource protection by the cycle providers.

RUNTIME SECURITY SYSTEM CORRECTNESS ISSUES

Cycle providers might continually shape the device so as to access or perhaps change information without accreditation; therefore customers may restrict the cycle providers used to execute plans to have the option to two or three trustworthy cycle administrations.

Integrity of Data

You will find a couple of exceptional conditions when the morals of information can be imperiled: all through the move of information through data providers and cycle providers to the customer. During the transportation, the Data integrity will be supported through shielded correspondence courses utilizing MACs and these channels empower you to manufacture a virtual private network, one more likelihood can be which the purchaser explains designs to drive application of MAC. For similarly providers just as users to get concentrated on data integrity, this technique is significant**.**

Privacy of Data

With Object Globe, solace of data guarantees that information may simply move in the predefined way by means of information benefits so as to the users. At this moment there must not be any openings where the illicit specialist may outpouring your data, or perhaps a reproduce of computer, alongside assist it with opening up to someone else. In opposition to data quality, Object Globe may affirmation solace of information additionally with respect to the use of discretionary user-characterized operators. So as to vindicate this statement, it's significant so as to audit in more prominent detail what kind of issue will be profoundly handled all through Object Globe.

Program Generation

Guarantee 1 *The program time point gives a system which thus can't be adjusted without notice notwithstanding which will essentially wind up being done when.*

A plan will be made by approach of customer of the ObjectGlobe strategy using A SQL-like language. Forward the program and conjointly analyzer square measure work fitly, the user gets a superb XML rendering of the set up. The user will essentially bear witness to the program that inside what's to come is sometimes commented on having validation data for, e.g., wrappers (where required). Moreover, this is the ensured technique despite the oppression by the individual key of users, rousing integrity with of the set up in left over inquiry process stages to stop reprocess identified with (wire caught) endorsed ideas, every single methodology incorporates a unique ID dispensed containing a time stamp among various things. The endorsed approach could just get upheld to encourage a given timeframe, e.g., for sixty min's. Cycle providers keep the real IDs identified with handled questions until they will be noncurrent

CONCLUSION

In distributed databases for any update remaining task at hand, the nullification based strategies have provided the better update usefulness in correlation of update based convention. These sorts of the assessments can be cultivated distinctly by utilizing of the specific reenactments. It implies we are going on the end that these sorts of refutation based techniques not required the two stage submit. There is no update just as read transactions are involved in the halt. Furthermore, there is additionally no need of the rollback in object models (OMs) on the off chance that in the event that we need to prematurely end the changes. Also the results show that models gives the equivalent experience profitability other than inside strong amend remaining task at hand at whatever point essentially all says inside anxious replication can without much of a stretch completion locally on OMs, despite the fact that it is very simple to peruses in nullification based techniques because of the impressively better repudiation in the SS. Ordinarily the outcomes outline the ILBP presents somewhat better update capability as contradicted than advertised

REFERENCES

1. Roichman and Gudes's(2016) "Design and Implementation of an Intrusion Response System for Relational Databases", IEEE Transactions on Knowledge and Data Engineering, Vol. 23, No. 6, pp. 875-888, June 2011.

2. Kroegar et. al. (2015). Privacy Preserving data mining. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, Texas, 2000.

3. Bernstein and Philip (2015). Providing database as a Service" Proceedings. 18th International Conference on Data Engineering, 2002.

4. Shivakumar et. al. (2013). "A Novel Framework for Database Security Based on Mixed Cryptography" Fourth International Conference on Internet and Web Applications and Services, 2009. ICIW '09.

5. Gray et. al. (2018) "Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems", IEEE Communications Magazine, Vol. 50, Issue 3, pp. 146 - 154, 2012.

6. Huang et. al. (2012) "Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets" Third Annual Conference on Privacy, Security and Trust, St. Andrews, New Brunswick, Canada, October 2005.

7. Ceri et. al. (2015) "Intrusion Detection in RBAC-Administered Database", In proceedings of the 21st annual computer security application conference (ACSAC), pp. 170-182, 2005.

8. Ahuja et. al. (2013) "intrusion detection in real-time database system Via time signatures", real time technology and application symposium, pp. 124,2000.

9. K. Hemanth (2012) "Database intrusion detection based on user query frequent item sets mining with constraints", In proceedings of the 3rd international conference on information security, pp. 224-225, 2004.

10. Al-Fedaghi, S. (2015). A Misuse Detection System for Database systems", IFIP TC-11 WG 11.5 Conference on integrity and internal control in information system, pp. 159-178, 1999.

11. Stephane Jacob (2016). A data mining approach for database intrusion detection", In Proceedings of the ACM Symposium on applied computing, pp. 711-716, 2004

12. Chin-Chen Chang (2015). "A novel intrusion detection system model for securing web based database systems", In proceedings of the 25th annual international computer software and application conference (COMPSAC), pp. 249-254, 2001.

Corresponding Author

Meenakshi*

Research Scholar, Sunrise University, Alwar, Rajasthan