2. Literature Review

In this paper, they have proposed a new method for image authentication, which can detect a tampered block with size as small as 86 image pixels. In the proposed scheme, a prior knowledge is not necessary for detecting tampering in an image.

In this paper, a new dynamic data allocation algorithm for non-replicated distributed database systems (DDS), namely the threshold algorithm, is proposed. The threshold algorithm reallocates data with respect to changing data access patterns. The algorithm is analysed for a fragment using simulation. The threshold algorithm is especially suitable for a DDS where data access pattern changes dynamically.

In this paper, a web-based normalization tool has been developed to enhance teaching and learning of database normalization. The tool is user friendly and can be accessed through the Internet. It was evaluated by students and found to be robust. Students’ responses to the tool were mostly favorable. The students indicated that they had found the tool easy to use and the step-by-step feature helped them gain understanding of database normalization process. The tool has a positive impact on students’ perceptions. Currently, the web-based tool allows a set of 10 functional dependencies, which is adequate for teaching purposes. More features, e.g., ‘Load’, ‘Save’, and ‘Print’ are still under development. The tool can be expanded to draw entity-relationship (ER) diagram. The incorporation of relational model and ER model is suggested for future work.

Jiang Wu, D. Manivannan and Bhavani Thuraisingham. (2008)
In this paper the checkpointing has been traditionally used for handling failures in distributed database systems. If each data item is independently checkpointed, the checkpoints taken may not be useful for constructing a transaction-consistent global checkpoint of the entire database. In this paper, they have presented the necessary and sufficient condition for a set of checkpoints of a set of data items in the database to be part of a transaction-consistent global checkpoint of the distributed database.

The proposed architecture uses distributed databases driven from a central point and it is generic to be able to apply it in many environments such as information and data warehouse. The parallel programming standardizes the codification and minimizes the time of execution for determined searches. The system makes possible consolidated vision of the information possessing distributed databases that is done through the publication of the main searches in portal.

The Proposed architecture uses distributed data bases driven from a central point and it is generic to be able to apply it in many environments such as information and data warehouse. The parallel programming standardizes the codification and minimizes the time of execution for determined searches. The system makes possible consolidated vision of the information possessing distributed databases that is done through the publication of the main searches in portal. As future work, it can be studied the aspects of performance under the point of view of the net of communication between the master and the branches, as well as, implementation of a tolerant system to the imperfection.

Georgiana-Petruta F. And Florentina Anica P(2009)

The present article aims to describe a project consisting in designing a framework of applications used to create graphical interfaces with an Oracle distributed database. The development of the Project supposed the use of the latest technologies: database Oracle server, Tomcat web server, JDBC (Java library used for accessing a database), JSP and Tag Library (for the development of graphical Interfaces).


This paper aims to create a system that manages doctoral school requirements. The management of doctoral school implies administration of information like PhD personal information, Supervisors, Teachers, and other information that may be useful. We will debate on distributed database term as the proposed database project will have the same structure for four universities. Each university will be able to work on this database by accessing its own set of data and properly using the information received. This project will track the creation of a database to manage all the information needed and provide answers using these data.

J. Arokia Renjit and Dr.K.L.S. (2010)

In this paper an efficient algorithm has been developed for mining association rules in distributed databases which reduces communication costs and takes away the overhead of combining the partition database sites datasets into a centralized site. It also has the advantage of reduced size of messages passed through the network. It also reduces the time of scan of partition database by using LMatrix which increases the performance of the algorithm. Furthermore, Improved mining algorithm can be applied to the mining of association rules in a large
centralized database by partitioning the database to the nodes of a distributed system. This is particularly useful if the data set is too large for sequential mining.

**Arun Kumar Y. and Dr. Ajay A. (2010)**

In this paper various concurrency control algorithms have been proposed for use in distributed database systems. But, the number of algorithms available for the distributed concurrency control, come into one of three basic classes: locking algorithms, Timestamp algorithms and optimistic (or certification) algorithms. In this paper they are presenting a Distributed Transaction Processing Model and an approach for concurrency control in distributed database systems. The analysis of our approach is a decomposition of the concurrency control problem into two major sub-problems: read-write and write-write synchronization.

**San Francisco, Sorapak P., Vitalwonhyo L. and Parinya S. (2010)**

The objective of this paper was to evaluate the distributed database approach that can improve the performance of database system. They evaluated the system using Benchw benchmark tool. They had tested four of query types by increasing the number of storage nodes from two to eight nodes. The results represented that when we increased the number of storage nodes which data was stored, the time of processing was improve gratefully. The evaluation may be limited by the maximum number of storage nodes to eight machines. But if we have opportunity to configure more storage nodes and also to improve some other factors that would affect the system performance.

**Toshiyuki M. and Takeshi I. (2010)**

In this paper optimization of the query processing has been described, as this has a great influence over database performance. This study provides a formulation of the sub query allocation problem in a secret sharing distributed database in terms of a constraint satisfaction problem. A heuristic evaluation function is proposed for solutions in best-first searches. An experiment was conducted using an ILOG Solver to examine the effectiveness of the above function. Some issues remain for the proposed procedure when there are a large number of servers, and further research will be necessary. It will also be necessary to evaluate the performance of this method on an actual system.

**Chandrasekaran S, Dipesh Dugar M, Jitendra Kumar Jain D (2010)**

In this paper the model of AIS is designed in such a way that it should be wide in scope with very minimal cost. The proposed model can be extended to the entire state as well as the country as it is the need of the hour. Government may come forward to sponsor the GSMA device to the client instead of too many other subsidies. small scale clients may be charged less compared to the medium and large scale clients.

**Hamed k. and Hassan R. (2010)**
In this paper, the author proposed a fragile watermarking scheme for relational databases. The watermarks are embedded into a relational database on the group basis under the control of a secure embedding key. The embedded watermarks form a watermark grid which can detect and localize any modifications made to the database and also be able to recover true data from modified cells. Experimental results showed that proposed scheme is secure and true data recovery failure probability is very teeny. Security analysis showed that it is very difficult for an attacker to modify the database without affecting the embedded watermarks, and the security upper bound was given. Future work will focus on designing a watermarking scheme that can embed watermarks to non-numeric attributes. For this purpose we can choose two solutions. The first solution is to reform the structure of hash function so it can accept non numeric inputs. The second solution would be another mechanism instead of using a hash function.

Bolivar T., Qing P., Gordon W. Skelton, Scott B., Natarajan M. (2010)

Based on the results provided in this paper, I can make some relevant analysis and draw conclusions. The runtime values for the application ranged from 30 seconds to 3600 seconds (1 hour). Each test was conducted to examine whether our application runs for different ranges of time, and explore the constant detection of tags by the RFID reader. The results were fairly accurate based on the average percentage of error analysis. I observe that the largest error percentage generated was 16.17%, which corresponded to the test with polling delay of 5 seconds, and running time of 30 seconds. This value is high for a percentage error, and the conclusion we can take from here is that not only it was the smaller value for the running time that makes the reading inaccurate, but also the accuracy of the procedure to start the test, because each program must be started independently by the user. The other percentages of error were lower and less than 10%. We would also like to comment on the test with a polling delay of 2 seconds and a running time of 3600 seconds (1 hour). Although, this result shows a lower percentage of error, we can see a big difference on the number of experimental tags detected and the theoretical tags detected. This difference may be happening because of the time error. We must remember that although the Node Control and Database Control parts of the application have time delays, they may not be necessarily accurate. Thus, we must also take in consideration the time that each program takes on executing each its own instructions. Some of the suggestions for future improvements for this application include the following: (i) Make the two parts of the program to run as one, completely independent of the user; (ii) Develop a multiprocessing interface, to make the Database Control program run, and have the option to stop it, change the rate of detection, etc; (iii) Make the SNAP functions and scripts more compatible with Python so that the nodes can work independent of the Synapse Portal; (iv) Add more RFID nodes with its corresponding RFID devices integrated, so the Polling node can do a multicast RPC to all nodes to detect a tag ID; (v) Add accelerometers to the nodes of the WSN to detect movement, if there is no tag present.

In this paper authors have proposed a new model for web database security using Ultra Hybrid security system based on DSUC and Uncertainty Degree Model. Their tests and experimental results shows that our system is efficient and capable for blocking intruders from hacking into our system and discover suspicious behaviors of internal and authorized system users. They can guarantee triple security layers, and test shows that our system can block 93% of attackers on high load.

Manvjeet K., Dr. Sanjeev S., Deepak S. (2010)

This work concludes that since securing the biometric data is one of the important research aspects these days so a technique is proposed to secure any image based biometric traits using helper data. The results have been discussed by taking database of fingerprint traits, images and passwords. Images are encrypted and decrypted in this paper and results have been shown. The results are analyzed on database containing 50 images of fingerprint template, 50 images of other biometric traits and 50 different passwords. When the 50 images of biometric traits are encrypted and decrypted by using 50 images of fingerprint template and 50 different passwords than this developed technique gives 96% security. When the 50 images of biometric traits are encrypted and decrypted by using 1 image of fingerprint template and 50 different passwords than this developed technique gives 100% security. The result analysis shows that as we keep on raising the length of password the security of system increase. User can also take any size of image because this technique encrypt and decrypt properly any size of images.

K. Karpagam ; R. Balasubramanian (2011)

In this paper a new improved algorithm, NIADD is presented. The new algorithm is compared with FDM. The results indicate that the NIADD algorithm is well suited and effective for finding frequent item sets with less execution time. Also, increasing the support factor proportionately increases the performance of the algorithm. These results show the fact that the increase in Min Support is done relative to the Transaction values in the Database’s dataset. The NIADD can be used on distributed databases, as well as for mining large volumes of data based on the Memory of the main site. This leaves scope for improvement of the NIADD by using multiple-processor’s memory like the FDM.

Neera B. and Manpreet S. (2011)

In this paper, they specifically address a reduced bandwidth usage and low cost scheme for distributed database based on processes check pointing. Processes take checkpoints periodically managed by the local cluster head and log their output/input in a common table maintained by cluster head. The developed scheme reduces the cluster-to-cluster communication to a single composite message and the cluster head of each cluster is responsible for extracting the individual messages from the composite message and multicast them to the corresponding receiving processes.
In this paper, author has focused on proposing a new replication strategy to maintain the consistency of replicated data in large scale mobile environments. The replication strategy encompassed three-level replication architecture and wheel-based updates propagation protocol as a binary combination that is needed to achieve such a goal. The strategy supports frequent disconnections and mobility of hosts by enabling the users to perform their updates in a disconnected mode and then synchronizing their updates with the higher levels.

Adriana L. and Lucia R. (2011)
This paper describe the online promoting tends to become the most convenient marketing media for a company that helps it to enlarge its distribution channels for products and services. This is the point where integrating the databases in the process can make the difference between two companies.

Ramakanth D. and Vinod K. (2011)
In this paper authors shows the importance of information security and present condition about how insecure are major websites. This attack SQL injection can be eliminated and its threat can be minimized to greater extent only if government and private organization are informed about the seriousness of the security. In some countries, cyberlaw is not developed or strictly implemented, allowing hackers to take advantage of the system. Using existing technology and security measures intelligently by major sites will lead us to the internet with minimal vulnerability to database theft. SQL injection came with a bang and caused revolution in database attacking. In recent years, with the explosion in web-based commerce and information systems, databases have been drawing ever closer to the network and it is critical part of network security. This paper is incorporated with our research and firsthand experience in hacking the database by SQL injection. Database is the Storage Brain of a website. A hacked database is the source for Passwords and juicy information like credit card number, bank account number and every important thing that are forbidden. Importance should be given for preventing database exploitation by SQL injection. The aim of this paper is to create awareness among web developers or database administrators about the urgent need for database security. Our ultimate objective is to totally eradicate the whole concept of SQL injection and to avoid this technique becoming a plaything in hands of exploiters.

In this paper, In spite of the significant role of databases in information systems, not enough attention has been paid to intrusion detection in database systems. A limited number of techniques have been proposed in the last few years for the detection of intrusion in databases. Therefore, there is still an urgent need to exert more effort to improve the performance of those systems. In this context, this paper introduces an enhanced data dependency model. The
The proposed model describes the normal transactions of each user using the number of operations in each one, read data set, write data set and dependency rule. The experiment on synthetic database transactions illustrates that the proposed model reduces the false positive rate and achieves better performance than the rival methods. Hence, it overrides the shortage of traditional data dependency model. The future work will enhance the model by add additional feature to define the normal behavior of each user.

In this paper authors have proposed two approaches to detect the intrusions in database. They provide an additional layer of security in DBMS. It can be considered as generic approach for any database and overcomes the limitation of the exiting database security mechanisms. They are extending our work with the help of CBF to ensure the security in database. Their comparisons show that it performs better.

In this paper, author’s have designed a new web database security model using ultra hybrid approach. Their model consists of three layers of security using DoS attack blocking server and DSUC (Data Security Unique code) and Uncertainty degree model. In this paper also, authors have designed a simulator using VB.NET that simulates client server model for testing our model, the simulator is tested using many users and the results shows that our model is efficient and capable for blocking intruders from hacking into our system and discover suspicious behaviors of internal and authorized system users.

Rashmi M. Jogdand and Swapna S. Banasode (2011)
In this paper, Agent-Based model for database security is implemented using permission rules. The database security can be maintained better with stricter access to data through the manipulation of the permission rules. By comparison of result tables it can be concluded that by keeping the agents upto 53, the unreliability of the system can be reduced. As the number of the agents increases to 63, the unreliability of the system also increases with both strict permission rule as well as for less strict permission rule because of which the number of corrupted data becomes greater. As the number of data corrupted increases with the increase in number of agents, then there is a possibility of the database being collapsed. The Future plan of action will be: 1) Improving the reliability of database system by increasing number of agents minimum upto 70 and maximum 120 for 49 data files. 2) Exploring the Agent-Based simulation program for large database. 3) Creating a more complex hierarchical structure for data access. In this paper, the DBA granted privileges to access data by all agents. In Future plan the owners of data files will grant privileges to access data by other agents from any host. 4) Encrypting the data files using Encryption algorithm.
Pradnya B. Rane, B. B. Meshram (2012)
Here security is provided at various levels. Authentication is done by using salt with hash value which is difficult to break. Also encryption and decryption process will be done to securing the watermarking relational database. And again the encrypted watermarked relational database is stored in an image using steganography. Hence even an attacker copy the watermarked relational data it is not in human readable format.

In this paper web application has various input functions which are susceptible to SQL-Injection attack. SQL-Injection occurs by injecting suspicious code or data fragments in a web application. Personal information disclosure, loss of authenticity, data theft and site fishing falls under this attack category. It is impossible to check original data code and suspicious data code using available algorithms and approaches because of inefficient and proper training techniques of dataset or design aspects. In this paper author’s will use SVM (Support Vector Machine) for classification and prediction of SQL-Injection attack.

Burlacu I. A. (2012)
In this paper the general aspects of the distributed database have been discussed. Distributed data - data, processed by a system, can be distributed among several computers, but it is accessible from any of them. A distributed database design problem is presented that involves the development of a global model, a fragmentation, and a data allocation. The student is given a conceptual entity-relationship model for the database and a description of the transactions and a generic network environment. A stepwise solution approach to this problem is shown, based on mean value assumptions about workload and service.

Rakesh J. (2012)
In this paper the Data integration in the distributed data system is introduced to solve the problem that data model has. The data integration in the distributional systems can be supported effectively. Data conversion is still a challenge in distributed system integration. Community based system is used for distributed data integration. It comprises of three elements: community, data model and communication protocol. The integration system solves the data heterogeneous problem in production management, making users check data more transparently and conveniently. The construction of central database is a comprehensive giant engineering system, which directly serves the demands of various application subsystem developments.