International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 169 - 172

Protecting Scattered Database by Enforcing Data Preservation Using Data Protection Facilitator

Akhilesh Kumar Misra[1]*
Department of Computer science and Engg
Suyash Institute of technology
Gorakhpur (U.P.)
akhilesh.mishra87@gmail.com

Surya Pratap Singh
Department of Computer Science
DDU Gorakhpur University
Gorakhpur (U.P.) – 273009
spsingh8161@htomail.com

Harsha Gupta
Department of Electronic and Communication Eng.
Jaypee Institute of Information Technology, Sector 128, Noida
guptaharsha54@gmail.com

Dr. Upendra Nath Tripathi
Department of Computer Science
DDU Gorakhpur University
Gorakhpur (U.P.) – 273009
untripathi@gmail.com

Abstract: In this paper we are incorporating data preservation in scattered database structure i.e. method of preserving data in scattered database structure and having secure access over it. In this paper data preservation is examined and solution is provided on the aforesaid condition.

This paper is a summarized concept of documentation, authorization, access control and encryption that are main points to be taken in consideration in data preservation in scattered database structure. We propose a new method for secure access based on service provider comprising security application. This model set out for safe search on server and user relation. In this paper we used heuristic approach for preservation for scattered database system regarding security, as the importance of secure access is increasing in scattered domains on different issues, in this way we enhanced the database security in Scattered database environment.

Keywords: *Scattered systems, security management, access security, Data Preservation, Data Protection Facilitator.*

*****

I. INTRODUCTION

In present scenario the organizations has a great problem to tackle i.e. protection of data against the outside attacks. Therefore all the organizations are worrying on taking the steps to save it or establish safety measures in order to prove the ability to prevent attacks on the availability, Integrity and reliability [7].Developing a secure system is a big problem in this era of networked system. Application being single system can be access through entire system including different computer and storage device[6].

Before discussing any problem, none of the organizations have paid attention to take precautions towards the attack on its security. So measures are given for sound system of security.

A. SCATTERED SYSTEM

The essential part in distributed system is its overlapping with data which is of core importance to the organization, it's taken care by maintenance and development team of organization known as technology development. A channel of independent system in different organization under different heads and service provider from distant system[8].

B. USER SERVER SYSTEM

Scattered system basically allows the use of data and application from distant places in the absence of identification of network and their relationship. Presently scattered system divided into two parts:

User: Sends request for the service to service provider for the services needed.

Service facilitator: Accepts the request of the client and provides him with the required output.

As per classification a components of networked syatem may be the most useful one for transferring data among server and user[5].

C. PROBLEM IN DATA PRESERVATION

The evolution of data preservation in scattered system and evolution of computer network are being conceded, this evolution is causing problem of security sensitivity[4].In manual end non automatic system the user requires to enter id and password. This system together with being ineffective reveals the security system, password may be with the user and he may use same password for all accounts.

D. SCATTERD SYSTEM COMPRISING OF PROTECTIVE COMPONENTS IN COMPUTER

In scattered system there are four main components [13]-

1. Document security
2. Authorization
3. Access control
4. Encryption

Document Security: It is a small "Encrypted symbol" in the form of credit card, it is provided with the password connected with server and the aforesaid connected to the network.

Authorization: It allows the user to access resources that are given by the system controller. It is accessed by service provider and the client computer in turn identifying user as service provider system. Hence its create security without sending information through network.

Encryption: It is the process of encoding the data with the help of various complex algorithms such as DES, RSA etc.

Access Control: It monitors over access list and its feature. The validity of material available for user access is specified in this approach.

E. CHARASTERISTIC OF DATA SAFETY IN USER/SERVICE FACILITATOR

From the view point of system controller following threat may occur for User/Service facilitator [9,12]:

1. No proper monitoring mechanism of user node.
2. Installation of user nodes in the public places is at great risk.
3. Protection system is ignored when nodes have taken advantage of hardware and powerful tools.
4. Mostly one user can access the system being in place of other.

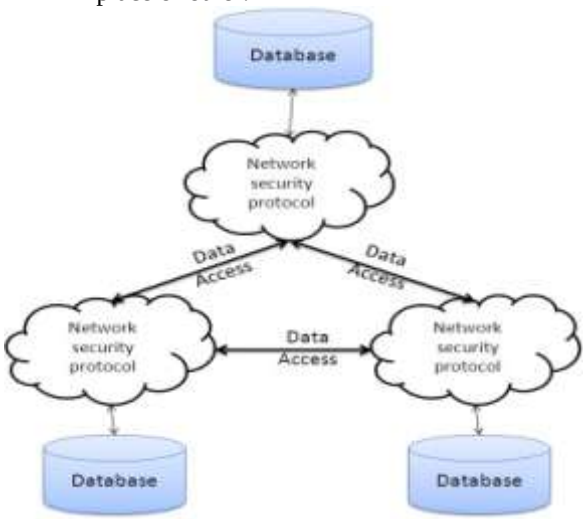

Figure 1: Security in Scattered system

II. SYSTEM INGRESS PROTECTION MODEL

Access security is defined here on local network with number of users and station in efficient way. The under described model is useful for systems where more query and transaction are there be it update, cancel and add[10].

It includes table with query and banking transactions managed by employee at branch hierarchy of transaction in user takes place, the director, the deputy, local director and staff are together with the hierarchy of money in banks being currency, security, current account. In a bank, employee can access information of current account and its transactions, this is when all the other transactions have closed. In this paper we present the model as perfect solution of the problem described.

The given model includes two main characteristics of secure access, eligibility and authorization. User being able to do it is very important and is again used in hierarchical mode.

Therefore, Authorization in simple sense is localization of authorization with respect to the activities which is arranged with objectives of organizations.

A. SOFTWARE DESIGN OF USER/SERVICE FACILITATOR

This model describes User/Service facilitator while Access security of serving software is independent application on the network station[2]. A unified interface will be provided for access security to the application or user where in need. The operating environment for Windows or NT system is programmed with certain changes.

PIPE is a communicative channel between user interface on user system and server software, here in PIPE the information is transferred from one computer to another. It has an important feature of FIFO (First In First Out) i.e. the first data which is given through PIPE is renewed first and so on.

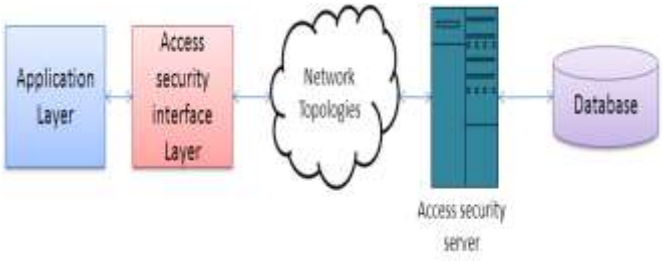

Figure 2: Software Architecture of User/Service facilitator

III. CHARACTERISTIC OF ACCESS PROTECTION IN SYSTEM

With the increase in number of transactions user face certain problem and this is what access security system provides, these transactions keep on occurring and on their occurrence the security tag is defined in two main symptoms:

1. **Level of Protection.**
2. **Types of Protection.**

Authority system gives security access to the station for the user at highest level.(Figure 3)

A. BASIC PROTOCOLS OF PROTECTION

The Basic Protocols/ rules are provided as a whole or made as an option explained bellow [3,11].

1. Even in case of absence of the appropriate access level prescribed by the system, users can link to the workstations.
2. Circumstances are to be created which does not reduce the power of transaction.

User must have adequate power and does not reduce the power of a transaction

B. MONITORING THE SERVICES BY THE SYSTEM

A good search security can be provided through number of user applications by given security. Together with this a backup copy is provided, Number of services and user demand are as follows:

1. USER
   - User's Description
   - Removal of user.
   - Renewal of user's old description of user.
   - User's proof.
   - Perform user's password check.
   - Having receipt of qualification of user.
   - Alter existing password of user.
   - Receipt of new lot of user.

2. TRANSACTION
   - Transaction's description.
   - Deletion of present transaction.
   - Up-gradation of transaction.
   - Having a detail of qualified transaction.
   - Getting a control over transaction.
3. ADDITIONAL SERVICES
   - Password's reliability.
   - Actual password.
   - Deposition of transaction

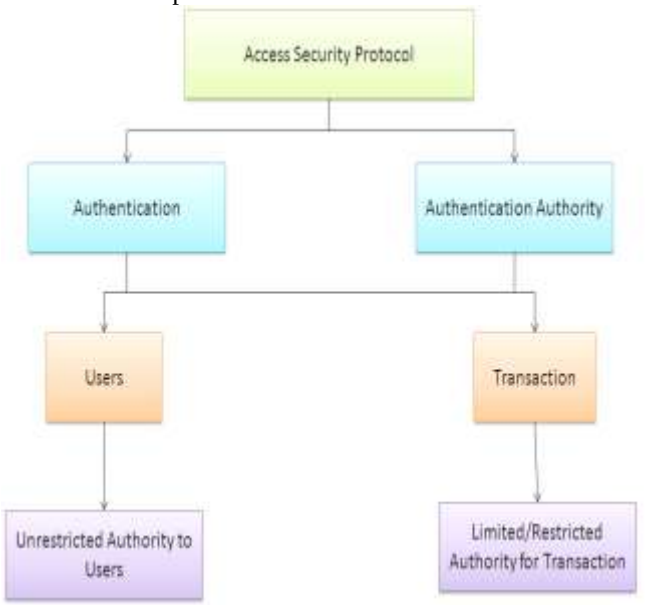

Figure 3: Characteristic of ingress protection

IV. PROPOSED METHODOLOGY

A process by which all complex programs are developed in a layered form is called the layer design. Operation in a layer is done by interface, Upper layer can be made stronger and downstream is evaluated at all time and the layered system has strong framework. A relationship is there in to program in single layer.

The pillars of layered system depend on:

1. User and facilitator are provided with a service jointly by the parallel layer. This signifies the division of work and formatting of messages and transactions.
2. The lower layer and the other layers receive messages through system interface and the user interface is made invisible from the lower layer and keeps all detail hidden.
3. At one side lower layer responsible for controlling hardware resources in system on the other side topmost layer examines as well as transfer files.

In the proposed model we use the layered design to explain protective structure with the user/facilitator's approach. In the model facilitator system stores all data such as documents, images, videos.

A. APPLICATION LAYER

The implementation of Application layer with customer demands, file path, qualified user, check password, change password and user profile, it sends all detail of user as the profile, validity user.

B. COMMUNICATION HANDLER

This monitor request of user, identifies request and prepare suitable result in case of transaction and refer the Application layer so as to how the result will perform, after getting all details of composed messages given to server.

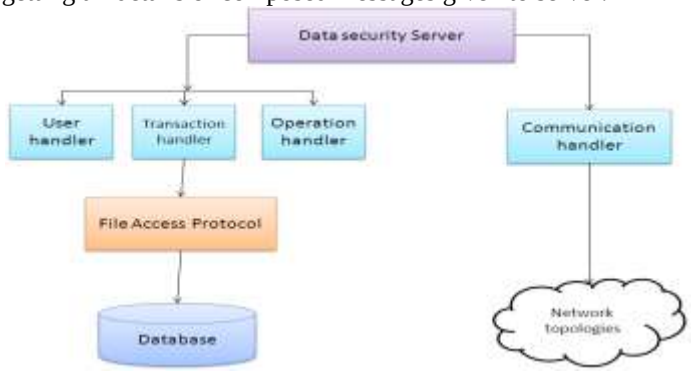

Figure 4: Data protection facilitator, Software design

C. DESIGN OF INGRESS PROTECTION SOFTWARE

Ingress protection includes some layer connecting to many software's.

1. **COMMUNICATION LAYER:** Communicating face to face receipt and reply of message to customer.
2. **COMMUNICATION HANDLER:** Categorization of messages of customer on basis of division of messages.
3. **APPLICATION LAYER**: It has three categories-
   a. Request of service.
   b. Request of node.
   c. Request of transaction.

D. SERVER SIDE APPLICATION LAYER

Input in this layer is demanded by user and output is in the form of message of the information needed by the user.

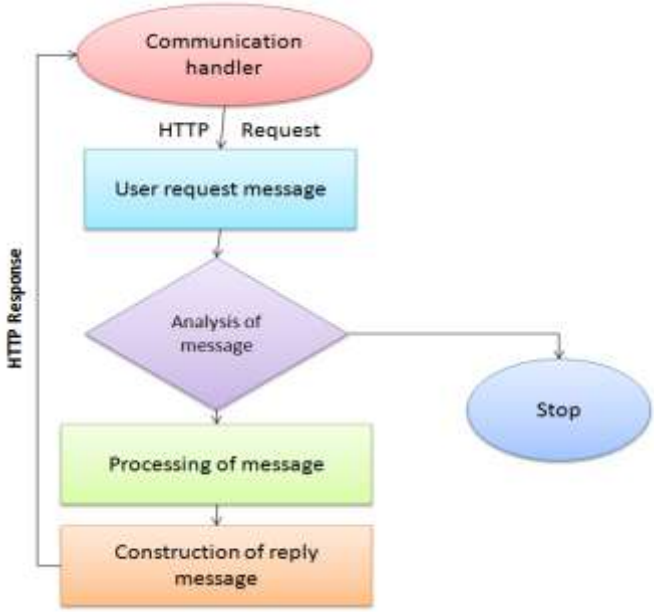

Figure 5: Communication handler

V. CONCLUSION

The cooperative sectors are dealing with some problem in system that can be reduced by providing with new and innovative methods of ingression on protective model. The model in this paper is highly protected model in user/ facilitator system. There are many models on ingress protection but none describes all the features, here in this paper four features are described:

1. Protective credential.
2. Authorization.
3. Ingress control.
4. Encryption.

Therefore, security requirement in scattered system is different from concentration requirement on a system. This model also poses layered model represented through PIPE software. The controller of vast network implements the model with large number of user and node for better concept on service classification, password exchange and authorization of user and nodes.

REFERENCES

[1] Anderson RJ. Security engineering. A guide to building dependable distributed systems. 2nd ed. Wiley 2008.
[2] Bass L, Clements P, Kazman R. Software architecture in practice. 2nd ed. Addison Wesley professional, 2003.
[3] Belapurkar A, Chakrabarti A, Ponnapali H, Varadarajan N, Padmanabhuni S, Sandarajan s. Distributed systems security: issues, processes and solutions, wiley 2009.
[4] Benatar M. Access control systems: Security, identity management and trust models. Springer 2006.
[5] Suza Jt, Matwin S. A Pattern language for providing client/server confidentional communication. In: proceeding of SugarLoafPlop 2001. Rio de Janeiro, Brazil 2001.
[6] Robinson P. Extensible security patterns. In: International workshop on database and expert systems applications. Los Alamitos,CA, USA, : IEEE computer society; 2007, p.729 – 33.
[7] Rassebo JE. Braek R. Towards a framework of authentication and authorization patterns for ensuring availability in service composition. In proceeding of the first international on availability , reliability and security (ARES). IEEE; 2006, p 15-206.
[8] A. Mei, L.V Mancini, S. Jajodi. Secure dynamic fragment and replica allocation in large-scale distributed file systems. IEEE transaction. Parallel distributed systems. 14 (9) : 855 – 896, 2003.
[9] Bernstein P, Melnik S. Model management : 2.0 Richer mappings. In : Proceeding of ACM SIGMOD international conference on management of data. Page 1-12, 2007.
[10] Buneman P, Cong G, Fan w, Kementsietsidis A. Using partial evaluation in distributed query evaluation. In proceeding 32nd, very large databases, page 211-222, (2006).
[11] S. Gutierez – Nolosco. Exploring adaptability of secure group communication using formal prototype techniques in : Workshop on reflective and adaptive middleware, Toronto, 2004.
[12] White D. Distributed systems security, DBMS, 10, pp. 44-48.
[13] Yskout K, Heyman T, Scandariato R, Joosen W. A system of security patterns : 10 years later. CW reports, Vol CW Ku Leuven : Department of computer science 2006.
[14] Raul B. Layered fault tolerance for distributed embedded systems, PhD Thesis, Department of computer science and engineering, Chalmers university of Technology,2008.

Author's Profile

Akhilesh Kumar Misra is M.TECH scholar from Suyash Institute of Technology affiliated to UPTU; He has done BTECH from Sachdev Institute of Technology. The area of research interest is Distributed Database Security. Mr. Akhilesh Kumar Misra has published 3 papers in different national and international conferences/Journals.

"Surya Pratap Singh is MCA and UGC-NET qualified. He is pursuing Ph.D In the department of Computer Science Deen Dayal Upadhyay Gorakhpur University, Gorakhpur (U.P. India) under the supervision of Dr. U.N. Tripathi. His area of research interest is Database Security, Algorithm design and Networking. Surya Pratap Singh has published more than 20 papers in different national and international conferences/ Journals.

Harsha Gupta is Perusing B.TECH from Jaypee Institute of Information Technology, Sector 128, NOIDA in Electronics and Communication Branch. She worked on projects like Evolution of Wireless Network from 1G to 5G, Density Based Traffic Control System Using IR Sensors. The area of Research interest is Networking and Database security.

Dr.Upendra Nath Tripathi is Assistant Professor in Department of Computer Science DDU Gorakhpur University, Gorakhpur (U.P. India). He has 14 years of teaching and research experience. He has published more than 40 papers in various National and International Journals/conferences. His area of research interest is database systems and networking.