International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-8)

Research Article | **August 2017**

Enforcing Distributed Database Security using Multi-Scope based Authentication and Enhanced Distributed Firewall

[1]Surya Pratap Singh[*], [2]Arvind Kumar Maurya, [3]Manish Mishra, [4]Upendra Nath Tripathi
[1, 2, 4] Department of Computer Science, DDU Gorakhpur University, Gorakhpur, Uttar Pradesh, India
[3] Department of Electronics, DDU Gorakhpur University, Gorakhpur, Uttar Pradesh, India

Abstract—

The data is the most valuable asset of any organization, it resides data in the database system that is used to store data of every running application. So the security of database is very important. One of the most widely used types of a database is Distributed Database which has the capabilities of both a relational database and distributed network architecture. Hence the security of database is of the prime concern and at the same time, it is very tough to ensure, because different types of attackers and hackers are trying everything to compromise the distributed database security. Various researches are done to preserve the distributed database security but some security problems are still unresolved. In this paper, we propose the use of Multi-scope based authentication and Enhanced Distributed firewall by which the integrity and security of distributed database can be achieved.

Keywords—Distributed Database, Database Security, Security Threats, Multi-scope based Authentication, Enhanced Distributed Firewall.

I. INTRODUCTION

In the distributed database, data is distributed in various locations called sites and the client/server architecture is followed. The site having some particular data works as a server for those data and as a client for other data. The distributed database possesses the problem related with the traditional database and, some of which are totally relevant to only distributed database. For example

- Access control is easier to implement for local user in traditional database system. Whereas centralized or decentralized access strategies in distributed environment is not easier such as. Thus, we will concern about authentication of users on different level of distributed platform.
- Preservation of integrity is much more difficult in a heterogeneous distributed database than a homogeneous one.

In this paper, we introduce issues on such problems.
And afterword, proposed a mechanism to resolve it effectively.

II. CHARACTERISTICS OF DISTRIBUTED DATABASE

Main characteristics of Distributed Database System (DDBS) are given below:-

A. Data Management across Multiple-Sites

Distributed Database System manages the data across several geographical distributed data-centres.

Real world applications can have multiple running instances that deployed across multiple data-centres for data storage, is referred to as a multi-site application.

Such applications applied by distributed computing that uses Distributed Database System for their data management. Therefore, Distributed Database System is more applicable where an organization resides geographically multiple sites. Here, data is not only stored at multiple sites but it is managed there, means, tables are created, data entered by different users from multiple sites and these multi-site applications running individually their own processes.

This contributes to increasing reliability and availability of data and improves ease and flexibility of application development.

There is an issue in a centralized system when a failure at a single site makes the whole system unavailable to all users. Whereas in a Distributed Database System, some of the data may be unreachable, but users may still be able to access other parts of the database. If the data in the failed site had been replicated at another site prior to the failure, then the user will not be affected at all.

B. Users' direct concerned Requirements at Local Sites:-

Data on each data-centre located on different site is managed by Local Database System (LDS).

These Local Database Systems are governed or controlled by the local application that referred to as Local DBMS. This improves the performance of database system while data localization is used across multiple sites.

As a result, by keeping the data closer to where it is needed most for the users directly associated with that local site, called local users.

Hence, local queries and transactions accessing data at a single site have better performance because of the smaller local databases. In addition, each site has a smaller number of transitions executing than if all transactions are submitted to a single centralized database.

Data localization also reduces access delay of the resources involved in wide area network.

When a large database is distributed over multiple sites, smaller databases exist at each site. Moreover, query parallelism can be achieved by executing multiple queries at different sites, or by breaking up a query into a number of sub-queries that execute in parallel.

C. Transparent to the users' Global Requirements:-

Apart from catering the local requirements, the Distributed Database System also fulfils the global requirements. These requirements are generated by the central management. The Distributed Database System fulfils the global requirements in a transparent way, i.e. the data for these requirements are fetched from all the local sites, merged together and is presented to the global users. All this activity of fetching and merging is hidden from the global user who gets the feeling as if the data is being fetched from a single place. This refers design transparency means, freedom from knowing now the distributed database is designed and where a transaction executes.

III. SECURITY THREADS TO DISTRIBUTED DATABASE

We take various kind of decision when distributed database is modeled for a given applications; first, we consider the security issues and efficiency of the model. That is, how it would be more secure and efficient for that application. For this, the decision concerned with security is taken on the basis of security measure available in DDBS i.e.-

A. Authentication

Controlling access to DDBS become profoundly more difficult with the spread of WAN-Wide Area Network and the Internet.

One security measure is to require some form of physical authentication, such as an object (a key or smart card) or a personal characteristic (fingerprint, retinal pattern, hand geometry, or signature).

B. Authorization

Another common security measure is to assign a unique password to each lawful user.

Many systems combine these types of measures- such as ATM, which rely on a combination of PIN and a magnetic-strip identification card.

C. Encryption

A different way to prohibit access to DDBS is via data encryption, which has gained particular importance in electronic commerce (or current trend in IT world). A number of industry standard encryption algorithms are useful for the encryption and decryption of data on the server, some most popular algorithms are RSA, DES, PGP.

To ensure confidentiality, only the intended addressee has the key needed to decrypt messages. e.g.: - Electronic cash is a type of message as well, and sometimes encryption is used to ensure the purchaser's anonymity. So, it leads to cashless economy safely nation-wide.

D. Multilevel Access Control

To incorporate multilevel security notions into the DDBS, users are limited from having complete data access. Means, login to the database is done in the same fashion as in a case of a traditional database but the login is valid for a relevant data only.

Policies restricting user access to certain data-part may result from confidentiality requirement or they may result from reliability to the principal of least privilege.

Access policies for the multilevel system are typically either open or closed.

- In an open system, all the data is considered unclassified unless access to a particular data element is expressly prohibited.
- A closed system is just the opposite in this case access to all data is prohibited unless the user has specific access privileged.

Security in DDBS [2] has focused on multilevel security. Specifically, approaches based on distributed data and centralized control architectures were proposed. Prototypes based on these approaches were also developed during the late 1980s and early 1990s.

These security measures placed between an organization's internal network and the Internet are known as firewalls.

IV. REVIEW OF LITERATURE

Here, we are discussing some security issues used in DDBS that introduced by various researchers, previously. Their works based on different factors on which they introduce some emerging security tools. Some of their related works are discussed below:-

In relating this paper to other work, we observe that the work by Danny M. Nessett, William Paul Sherer[3] is more relevant to us. Both are invented a Pervasive Multilayer Firewall, distributing firewall functionality throughout many layers of the network in a variety of network devices.

William Dixon et al. [4] introduced a Extensions of the Internet key exchange protocol (IKE) to provide the desired user authentication plus application/purpose are also provided.

David A. Roberts [5] suggested a manager function may broker the requests and offers to match services and requirements.

Stephen J. Boies et al. [6] invented the firewall that is utilized to protect the subscriber's computer systems when the subscriber's computer systems receive communications transmitted utilizing the external network.

Thomas Y.C. Woo and Siman S. Lam [7] proposed a logical approach to representing and evaluating authorization.

V. PROBLEMS IN EXISTING DISTRIBUTED DATABASE

The main problems of distributed database are-

A. Lack of Multilevel Authentication

One of the major problems associated with distributed database is a lack of multilevel access control. In distributed database, the whole data is distributed among different distributed servers. When we want to access the content the user has to supply the username and password. Once the user is validated he/she can access any server belongs to the distributed database. This situation may lead to several problems.

Suppose any intruder somehow bypasses the authentication process of one distributed database, then he/she is allowed access to the entire content of the entire distributed database. This situation is explained in Fig-1.

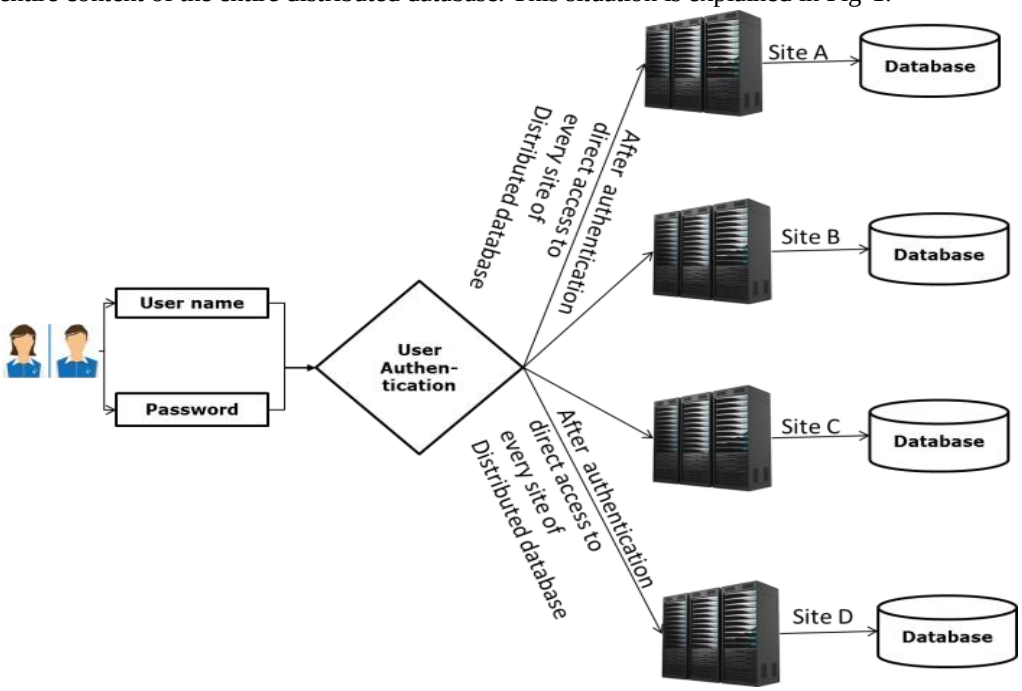

Fig-1: Lack of Multilevel Authentication

B. Propagation of Security threat

Another instance problem related with distributed database security may arise due to the propagation of malicious threat from one site to another. All the sites of distributed database are connected with each other having objective to allow data sharing every time when needed this also makes the database vulnerable to security breaches. For instance, if one site of distributed database becomes affected by some malicious software like Trojan then the same can propagate the boundaries of one site and can affect other sites.

VI. PROPOSED METHODOLOGY

To overcome the problems related to distributed database security we propose the use of Multi-scope base Authentication and Enhanced Distributed firewall.

A. Multi-scope based Authentication –

In this approach the authentication of the user is done on several levels. Firstly when the user wants to use the content of database he/she have to supply the username and password and once authenticated the user can access the content of the database, but the scope of authentication is valid for a single site only. If the user wants to access the contents of another site he/she have to supply different security credentials for authentication. If again the user is authenticated then only he/she can access the content otherwise the access is not provided. The architecture of this approach is presented in the following Fig2.

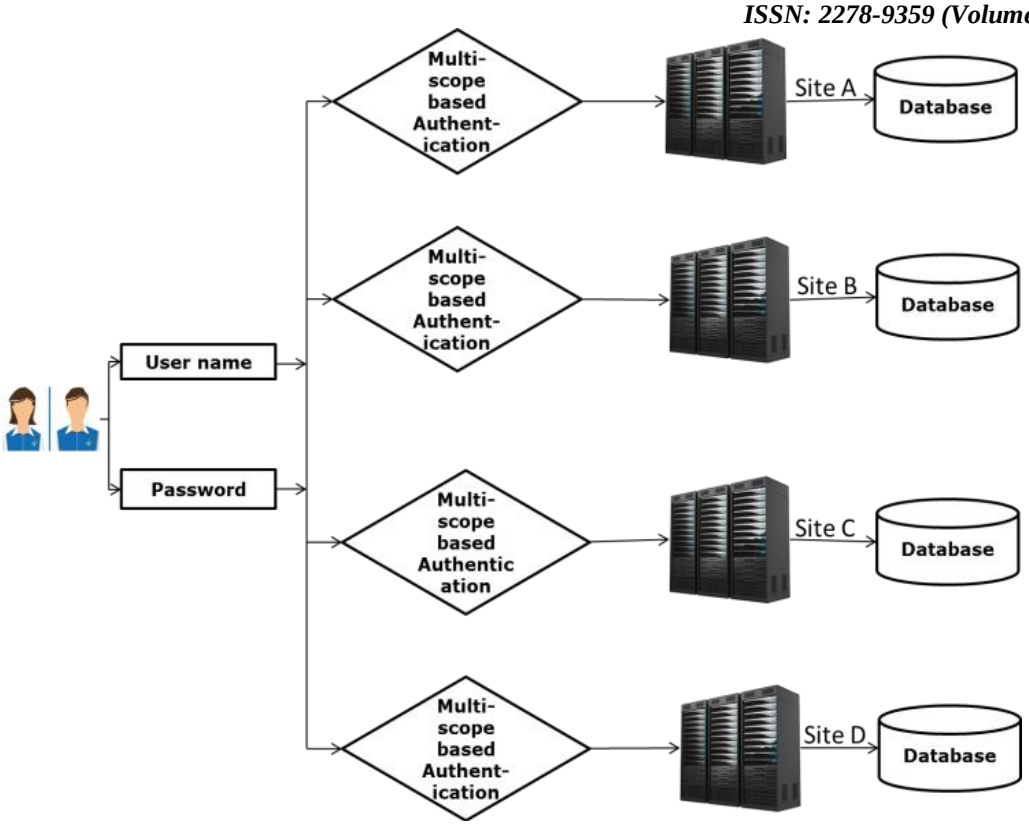

Fig2: Architecture of Multi-scope based Authentication

B. Enhanced Distributed Firewall –

The different sites of a distributed database are connected with each other so the malicious attack done at one of the sites may propagate to others. To overcome from this problem of propagation of security threat we propose the use of Enhanced Distributed Firewall.

In this approach, the enhanced distributed firewall is placed between each server and reactively traces each and every data packet sent and received, the architecture of this approach is represented in the following Fig3.

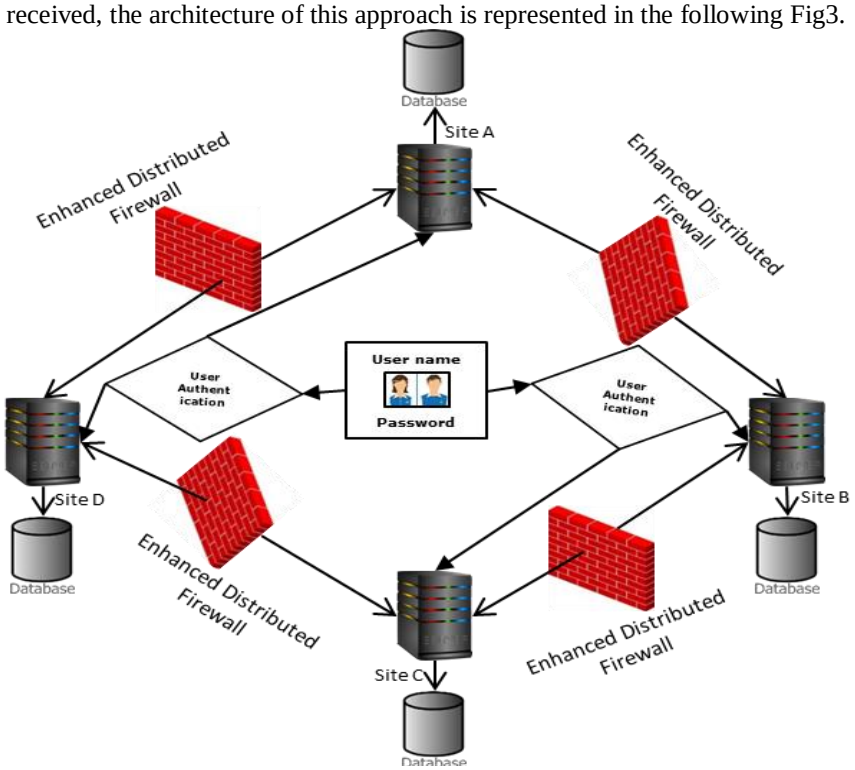

Fig3: Architecture of Enhanced Distributed Firewall

From the above figure, it is clear that the different sites of distributed database servers are interfaced by Extended distributed firewall. It protects the distributed database site from the propagation of security threats. Suppose if one database site is infected by any security threat and wants to spread by utilizing network resources then the extended distributed firewall can detect it and may prevent from propagation.

VII. CONCLUSIONS

This paper observes the fundamental features of the distributed database architecture. Building a triumphant distributed database system requires to acknowledge the importance of security issues. Such issues may arise and possibly settlement of the access control and the integrity of the system. We suggested some solutions for some security aspects such as Multi-Scope based authentication and Enhanced Distributed Firewall that affect the security issues of a distributed database system. And, we review all the security and design features & issues of databases in a general form. Moreover, review all these aspect in distributed databases in particular. And, also investigate the security problems and then evaluate it

REFERENCES

[1] Bell, David and Jane Grisom, Distributed Database Systems. Workinham, England: Addison Isley, 1992.
[2] Thuraisingham, Bhavani and William Ford—Security Constraint Processing In A Multilevel Secure Distributed Database Management System," IEEE transactions on Knowledge and Data Engineering, v7 n2, pp. 274-293, April 1995.
[3] Danny M. Nessett, William PaulSherer—Multilayer Firewall system
[4] William Dixon, Gurdeep Pall, AshwinPalekar, Bernard Aboba, Brian Swander—Methodfor providing user authentication/authorization and distributed firewall utilizing same.
[5] David A. Roberts—Distributed firewall implementation and control
[6] Stephen J. Boies, Samuel H. Dinkin, Paul A. Moskowitz, Philip S. Yu—Firewall subscription service system and method
[7] Thomas Y.C. Woo and Siman S. Lam—Authorization in Distributed System.
[8] James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach Featuring the Internet, Pearson Education, Inc, New York, 2003.
[9] Paul Lothian and Peter Wenham, Database Security in Web Environment, 2001.
[10] Pfleeger, Charles P., (1989) Security in Computing. New Jersey: Prentice Hall. 1989.
[11] Simon Wiseman, DERA, Database Security: Retrospective and Way Forward, 2001.
[12] Stefano Ceri, Giuseppe Pelagatti: Distributed Databases: Principles and Systems. McGraw-Hill Book Company 1984, ISBN 0-07-010829-3.
[13] Thuraisingham B., Security for Distributed Database Systems, Computers & Security, 2000.
[14] A.Berqia, G.Nacsimento, "A distributed approach for intrusion detection systems", Information and Communication Technologies: From Theory to Applications, 2004. Proceedings 2004 International Conference pp:493-494, 19-23 April 2004.
[15] M.Petkac and B.Lee, "Security agility in response to intrusion detection", Proceedings of the applied computer security associates conference 2000, Louisiana, USA, Dec. 11-15, 2000.
[16] K.Hwang and M.Gangadharan, "Micro-firewalls for Dynamic Network Security with Distributed Intrusion Detection", IEEE international Symposium on Network Computing and Applications",8-10 Oct 2001, pp: 68-79.
[17] Rafeeq Ur Rehman, "Intrusion Detection Systems with Snort, Pearson Education inc. 2003

AUTHORS PROFILE

Dr. Surya Pratap Singh is MCA, UGC-NET qualified and Ph.D. from the department of Computer Science DDU Gorakhpur University, Gorakhpur (U.P. India).. The area of research interest is Database Security, Networking. Dr. Surya Pratap Singh has published more than 30 papers in different national and international conferences/ Journals.

Arvind Kumar Maurya is MCA and UGC-NET qualified and pursuing Ph.D. In the department of Computer Science DDU Gorakhpur University, Gorakhpur (U.P. India) under the supervision of Dr. U.N. Tripathi. The area of research interest is Distributed Database Security, Networking. Arvind Kumar Maurya has published 5 papers in different national and international conferences/Journals

Dr. Manish Mishra is Assistant Professor in Department of Electronics DDU Gorakhpur University, Gorakhpur (U.P. India). He has 15 years of teaching and research experience. He has published 55 papers in various National and International Journals/ conferences. His area of research interest is Computer Technology, fast processor design.

Dr. Upendra Nath Tripathi is Assistant Professor in Department of Computer Science DDU Gorakhpur University, Gorakhpur (U.P. India). He has 15 years of teaching and research experience. He has published 50 papers in various National and International Journals/conferences. His area of research interest is database systems, networking.

