IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 6, June 2015.
www.ijiset.com
ISSN 2348 – 7968

An overview of different database security approaches for distributed environment

Dr. P. K. Rai
Prof. I/C BCA,MCA & Head, Computer Centre APSU Rewa
Pramod Singh
Research scholar
M.G.C.G.V Chitrakoot Satna (M.P), Satna, India; Email: singh.jobseek@gmail.com

Abstract

Development of secured and trusted database for distributed environment is a very critical issue. The main purpose of this study to understand different security problems which has been encountered during designing of a database for distributed environment. We have try to give a brief overview about different penetration methods and different security approaches of distributed database to control the security, reliability and privacy of database in distributed environment.

Introduction

The rapid growth in computer network technology and database system technology resulted in the development of distributed database. There are many definitions of Distributed Database System have been given by different researchers but there is no standard definition. Distributed Database System is made up from a DDBMS, distributed databases and a network. Data is distributed over different databases at different geographical locations. Due to distributed nature of data the possibility of data threats is increased. Security threats of distributed database can be divided in to two categories, first categories includes the problem which can be exists in centralized system and second is specific to distributed system. The security of distributed database is dependent on different technical issues like, types of operating system used, types of network system, different system security policies and so forth. All these issues are barriers to make a global security policy for distributed database. Security requirements are stated in the form of security policy which has a set of laws and practices that governs organizations to manage protects and distributes sensitive information. Basically two terms are used to state the security policy named set of security objects and set of security subjects. Security object is a passive entity and receives or contains information whereas security subject is an active entity which is responsible for updating database states. it can be a process or a person(s) and data moves between object(s) and subject(s). Because of the diversity of the application domains for databases various security approaches and techniques have been proposed to make a secure distributed system. In this paper we have discuss about some security threats and security approaches of distributed database systems.

Threats of database security

Database security issues have been more complex due to distributed nature of database in distributed environment. Databases are a main resource of any organization there fore, policies and procedure must be put into a single place. It is important to safeguard its security and the integrity of the data it contains. Due to accessing of data between numbers of users through computer networks, increasing the risks of unauthorized access .The main objective of database security is to protect database from

ISSN 2348 – 7968

accidental or intentional lost. These threats include a risk on the integrity reliability of data .database security may be allows or refuses users to perform any action on the database. It is a responsibility of Database managers in an organization to identify threats and make policies that take effective action for handling any risks [6,7]. Such actions can be provides passwords and username to the users who access the databases and This system is called database management security system which keeps users details and actions(authority).There are different threats which can be arrived in the distributed database systems. Loss of availability means that data or systems cannot be available for any user. This problem can be arising due to the failure of the hardware, applications or networks system. This may affect the day to day activities of any organizations. Another method through which data can be lost its integrity is Excessive privilege. This can be arise when the users can have too much privilege in the database then he can be used them for malicious purposes. Each user should have required privileges according to his job profile [2,4]. privileges elevation is an Another threat of database security This can be arise when some user can acquire extra privileges through software vulnerability, where a normal user can have the privileged of database administrator and he can try to exploiting the software weaknesses in the database system. Another threat which can be occurred due to use of week internal system called a weal audit trial. Denial of service is a problem of database security which includes data corruption, network flooding and resource over load. Another type of threat of database insecurity is weak authentication system and procedures. In this Weak authentication attackers can got the rights of user and then change credentials. Other threats which can be detected to accidental losses are malfunctioning of systems and operating procedures. Besides of above threats to databases two very conmen threats are inference and Identity theft. There are many goals that can be set forth for database security issues. These are confidentiality, integrity and availability of data [1,3,5].

Types of database security

Database security is an very important and sensitive issue of distributed system which deals with protection of a database from unintended activity. These activities can be authenticated misuse, malicious attacks or inadvertent mistakes committed by authorized individuals or processes. Database security issue is very broad that includes many layers and number of security types for information security [8,9]. These can be typically classified into fallowing:

Access control: Access control is a process or a system which is used to check the authority of a user into database to control unauthorized accessing of data or information of database into distributed system.

Auditing: Auditing is a process of examining all security relevant events to discover and diagnose the security violation of database. It is a collection of well organized audit data and analysis which needs protection from modification by an intruder.

Authentication: Before accessing a system, every user is identified and authenticated .it is a confirmation of something or someone is authentic to use the resources of the system.

Encryption: encryption is a part of cryptography where an algorithm generally called as cipher is used to transform information (called plaintext) into unreadable to anyone except those user who have special knowledge and credentials.

.

ISSN 2348 – 7968

SECURITY APPROACHES IN DISTRIBUTED SYSTEMS

These are several methods has been proposed by different researchers to maintain the security and privacy of users data or information stored in database and distributed over different sites connected through computer networks. These methods can be broadly categories in fallowing types:

1. Authentication Based Security
2. Trust Based Security Approaches
3. Access Control Based Security
4. Cryptography Based Approaches
5. Other Security Approaches

Access Control Based Security

There are several models have been proposed for access control of database which is distributed between different sites. Traditional access control models can be categorized as Discretionary access control (DAC) models, Mandatory access control (MAC) models and Role-based access control (RBAC) models. The fundamental theories of security models which can be used for a long time are Discretionary security models. these model was used from 1970 through 1975,these models has work on the concept of discretionary policies. Discretionary access controls (DAC) are works on the concepts of a set of access privileges T of security subjects on security objects[10]. Most DAC store access rules in an access control matrix. Lampson (1971), Harrison et al (1976) and Fernandez et al (1981) has been proposed The basic discretionary access controls model based on access matrix[10]. Another access control models are Mandatory access control (MAC) models which is based on Bell and La Padula (1976) restrictions, has two rules. The first deals with unauthorized disclosure of database, and the second protects data from unauthorized modification[11].These rules are ensure the information does not flow from a higher sensitivity level to a lower sensitivity level[11]. Role-based access control (RBAC) models attracts users due to a generalized approach to access control with several well-recognized advantages [12,13]. The RBAC models directly supports arbitrary, organization- specific security policies where roles represent organizational responsibilities and functions.[14,15]

Trust Based Security Approaches

Trust is required at each level into the distributed system but it is very difficult to decide where to implement the trust policies. Trust focuses on the security of utility [16].A distributed environment supports database to be distributed over different sites to solve many problems where a problem is divided into many tasks or processes, each of which may be solved by different system or users. Due to open for all authorized users it leads to insecurity of data which demand confidentiality and integrity in trusted environment [17].The main focus of trusted environment to check the identity of the users of a system at each level. B. Clifford Neuman et al has been proposed password based methods to identify the trusted users for their authentication and authorization. kerbores is another approach which is used lightweight protocol based on symmetric key cryptography[16,18]. Jaeger et al [19] has been introducing the needs of trust and problems in the distributed system. An unified approach for Trust Management in distributed system has been introduced by Blaze et al [20] which

specify and interprets security policies. serhiy et al has been introducing a new Agent based approach which uses neural networks for on-line line monitoring of user actions[21]. A trust enhanced security model has been proposed by Aruna Kumari et al using kerborus security with a new approach, node registry and service level agreements has been using to ensure the trust in distributed system[22,23]. H. Li et al introduced a trust based security model for distributed environment [24].

Authentication Based Security

A path authentication technique has been proposed by M. Shehab, et al based an on demand path discovery algorithm which is supports to discover path for secured domain in distributed environment[25].A systematic security driven scheduling architecture has been introduced by T. Xiaoyong, et all which is based on direct cyclic graph[26]. A three factor based authentication approach is designed by X. Huang, et all which supports splitting the two factor authentication into three factor to provide more security for client privacy in distributed environment[27]. W. J. Seung et all has been introducing A new password based authentication approach. this approach is based on authentication with a trusted third party[28].

Cryptography Based Approaches

The Cryptography is a basic technique used for securing data or information from illegal inferences. So this technique can be used for securing database in distributed environment. This is a process of encoding plain text into cipher text with the help of secret encryption key and cryptographic cipher. The major problem of this technique is to secure keys from attacker. There are number of cryptographic security approaches has been introduced by many researchers, which is based on Pub-lic key cryptography, software agents and XML binding tech-nologies we have discuss some of them. Y. Xu, et al has been introduce a device level system control cryptographic approach for securing data in distributed environment[29].sanjeev dhavan et all has been proposed a new approach for security of database called DNA based cryptography. this is a theoretical approach which requires advance technology to reach a mature stage[30].Kritika et al has been design an algorithm using DNA Cryptography to maintain data confidentiality and integrity of data[31].

Other Security Approaches

Fernandez et al has been introduced number of security patterns for database security[32].to solve the data consistency problem in distributed database a new Intrusion – Tolerance Quorum System [ITOS] has been proposed[33]. The Role Ordering (RO) schedulers are introduced in a role based access control model which has been developed by E. Tomoya and T. Makoto [34].an automatic manually configured policy based security system has been introduced in[35]and A policy based distributed system security mechanism has been also developed in [36]which is based on domain language for verification to implement security for distributed database system. CORBA based authentication security model has been proposed by K.-A. Chang, B.-R. Lee and T.-Y. Kim [37]. Abhijeet Raipurkar has been introduced semi join plan based security for distributed database [38].

SECURITY ISSUES AND CHALLENGES

The implementation of a secured distributed database system has been emerged number of critical issues. Some of these are as follows:

1. Identify the methodology which can be used to assess the security level in any system

2. The system has an approach to Monitoring the system security.

3. Develop security matrices for the system

4. Data can be distributed over secure communication network which can be Integrate some techniques like Cryptography etc.

5. Using middle ware approaches for security of distributed system.

CONCLUSIONS

Database security is not a single problem of database but it is a total system problem .The above study has been providing a conceptual framework about the possible threats of database security and different available techniques of database security like Authentication, access control, cryptographic, trust based models and many others which can be helpful towards the generation of secure and trusted distributed database systems. The main focus of this study to explore the different technological issues involved in protecting a database into a distributed environment. Database security has been an intensive subject of research for almost three decades but still remains on of the fascinating and major research areas of the day. It is expected that rapid growth of new technology will emerged new vulnerabilities to database security and database security remain an important area of research in future.

References

[1]Kumar et al Managing Cyber threats: Issues, Approaches and Challenges Springer Publishers,2005.
[2]S. Singh, Database systems: Concepts, Design and applications New Delhi: Pearson Education India,2009.
[3]S. Sumanthi, Fundamentals of relational databasemanagement systems Berlin: Springer, 2007.
[4] P, Singh Database management system concept V.K (India) Enterprises, 2009
[5] A. Basta, and M. Zgola, Database security Cengage Learning, 2011.
[6] Coronel et al Database System Design, implementation and management Cengage Learning, 2012.
[7] Bertino et al Database security-Concepts, Approaches and challenges IEEE Transactions on dependable and secure computing, 2005.
[8] Charles P. Pfleeger, Shari Lawrence Pfleeger “Security in Computing”, www.studytemple.com/.../2830-security-computing-charles-p-pfleeger,4th Edition (2008).
[9] Dr. Sona Malhotra, Richa Punia, “A Review on Partial Security Violation in Distributed Database”, International *Journal of Emerging Research in Management &Technology ISSN: 2278-9359, Vol 2,N0.6,2013.*
[10] Harrison, M.H., Ruzzo, W.L., and Ullman, J.D. Protection in operating systems. Commun. *ACM 19*, 8 ,1976, 461–471.
[11] Sandhu, R. Lattice-based access control models. *IEEE Computer 26*, 11,1993
[12] Ferraiolo,D.F., Barkley, J.F., and Kuhn, D.R. A role-based access control model and reference implementation within a corporate intranet. *ACM Trans.Info. Syst. Security 2*,1,1999, 4–64.
[13] Proceedings of The Fifth ACM Workshop on Role-based Access Control. Berlin, Germany, Jul. 2000.
[14] Tari, Z. and Chan, S. A role-based access control for intranet security. *IEEE* Internet Computing ,1997, 24–34.
[15] Batra N., Singh M., “Multilevel policy based security in distributed database”, Advances in computing and communications, Vol. 190, 2011, pp. 572-580.
[16] Ching Lin and Vijay Varadharajan, “Trust based risk management for distributed system security- a new pproach”, in Proceedings of the First International Conference on Availability, Reliability and Security, 2006

[17] Fred B. Schneider, Steven M. Bellovin and Alan S. Inouye,"Building trustworthy systems: Lessons from the PTN and Internet", IEEE Internet Computing, November- December 1999.
[18] Wen Tei-hua, Gu Shi-wem, "An improved method of enhancing Kerberos protocol security", Journal of China Institute of Communications, Vol 25 No. 6. June 2004, pp. 76-79.
[19] Aruna Kumari, Shakti Mishra, D.S. Kushwaha ,International Journal of Computer Applications , Vol 1,No. 26 ,2010, pp.0975 – 8887
[20] Peter C. Chapin, Christian Skalka and X. Sean Wang, "Authorization in trust management: features and foundations", in ACM Computing Surveys, August 2008.
[21] Serhiy Skakun and Nataliya Kussul, "An agent approach for providing security in distributed systems", TCSET' 2006
[22] Y. Ding, F. Liu, B. Tang, Context sensitive trust computing in distrib-uted environments, Knowledge Based Systems, vol. 28, pp.105-114, 2012.
[23] B.Clifford Neuman and Theodore Ts'o, "Kerberos: an authentication service for computer networks", in IEEE Communications Magazine, 1994.
[24] H. Li, M. Singhal, Trust Management in distributed systems, Com-puter, vol. 40, no. 2 2007, pp. 45-53.
[25] M. Shehab, A. Ghafoor, E. Bertino, Secure collaboration in a media-tor free distributed environment, IEEE Transactions on Parallel and Distributed Systems, vol. 19, no.10, pp.1338-1351, 2010
[26] T. Xiaoyong, K. Li, Z. Zong, B. Veeravalli, A novel security-driven scheduling algorithms for precedence-constrained tasks in heteroge-neous distributed systems, IEEE Transactions on Computers, vol 60, no.7, 2011, pp.1017-1029.
[27] X. Huang, Y. Xiang, A. Chonka, J. Zhou, R.H Deng, A generic framework for three factor authentication: Preserving security and
[28]W. J. Seung, J. Souhan, Secure Password authentication for distrib-uted computing, International Conference on Computational Intelli-gence and Security, 2006, vol.2, pp.1345-1350.
[29] Y. Xu, L. Korba, L. Wang, Q. Hao, W. Shen, S. Lang, A security framework for collaborative distributed system control at the device level, IEEE International Conference on Industrial Informatics, 2003, pp.192-198'
[30] sanjeev dhawan , Alisha saini,"Secure Data Transmission techniques based on DNA Cryptography", IJETCAS, vol 2,No 1,2012,pp.95-100.
[31]Kritika Gupta , shailendra singh,"DNA Based Cryptographic Techniques:A Review"IJARCSSE,Vol 3,No 3,2013,pp.607-610.
[32], E. B. Fernandez, K. Falkner, Securing Distributed systems using patterns: a survey, Computers and Security ,in press, http://dx.doi,org/10.1016/j.cose.2012.04.005
[33] H. Zhou, X. Meng, L. Zhang, X. Oiao, Quorum systems for intrusion tolerance based on trusted timely computing base, Journal of Sys-tems, Engineering and Electronics, vol 21, no.1 pp.168-174,2010.
[34] E. Tomoya, T. Makoto, Con-currency control based on significance on roles; 11th International Conference on Parallel and Distributed Systems, vol. 1, pp.196-202.
[35] H. Hamdi, A. Bocehula, M. Mosbah, International Conference on Emerging security Information , systems and technologies 2007, pp.187-192
[36] H. Hamdi, M.Mosbah, A DSL framework for policy based security of distributed systems, 3rd IEEE International Conference on Secure Software Integration and Reliability Improvements, pp.150-158, 2009.
[37] K.-A. Chang, B.-R. Lee, T.-Y. Kim,Open authentication model sup-porting electronic commerce in distributed computing electronic commerce research, 2002, vol.2, no.1-2, pp. 135-149
[38] Abhijeet Raipurkar1," SECURITY IN DISTRIBUTED DATABASE USING SEMIJOIN PLAN", International Journal of Application or Innovation in Engineering & Management ,spiceal issue,2013
[39] Harpreet Saini, Kanwal Garg"Comparative Analysis of Various Biometric Techniques for Database Security", International Journal of Science and Research (IJSR),Vol 2,No4,2013