Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 6; October-December, 2016, pp. 486-491
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

A Review on Security Approaches Where Data Are Distributed In Nature

Subhra Pramanik[1], Parama Bhaumik[2] and Chhanda Ray[3]

[1]Heritage Institute of technology, West Bengal, India
[2]Jadavpur University, West Bengal, India
[3]SCERT, West Bengal, India
E-mail: [1]subhra.pramanik@heritageit.edu, [2]bhaumikparama@gmail.com, [3]raysasmal@rediffmail.com

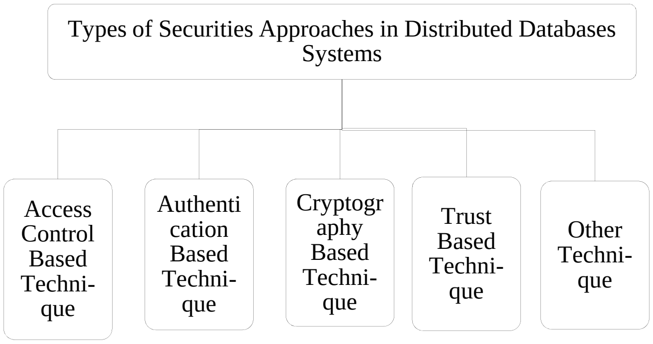
Abstract—*The structure of data is changing day by day as for socio-economic changes. The formats of data are text, number, currency, date, time, logical, Boolean, image, multimedia, voice etc. The creation, storing, and maintenance of data are facing new challenges. Thus whenever we are handling the database with these data types, the databases is evolving. The different types of databases are active database, analytical database, centralized database, cloud databases, distributed database, embedded database, end-user database, federated database, hierarchical database, hypertext database, in-memory database, mobile database, object-oriented database, object-relational database, operational database, parallel database, probabilistic database, real-time databases, relational database, spatial database, temporal database etc. As the nature of databases is evolving the security issues are also evolving. To secure the databases are facing more challenges in these days. In this paper, we review the security issues where the databases are in distributed nature.*

1. INTRODUCTION

Recently we see that the databases are evolving from centralized relational database to distributed databases, distributed multilevel database, object-oriented databases, object-relational databases, distributed object-oriented database, Mobile database, Mobile Real Time Distributed Database (MRTDDB), Multimedia databases, real-time database system (RTDBS), temporal database etc. As for socio-economic changes databases are evolving as the structure of data are changes day by day. To secure these data different technologies are proposed by different researchers till date. In this paper, we review the security issues where the databases are in distributed nature.

2. TYPES OF SECURITIES APPROACHES IN DISTRIBUTED DATABASES SYSTEMS

There are different types of security approaches which are proposed by different researchers. These different types of security approaches are applied in different types of databases to secure the data which are distributed through the internet connection.


Types of Securities Approaches in Distributed Databases Systems
Access Control Based Techni-que
Authenti cation Based Techni-que
Cryptogr aphy Based Techni-que
Trust Based Techni-que
Other Techni-que

1. Security using Access Control Based Technique
    1.1. Using Access Control List Algorithm
    1.2. Name –Based Access Control Algorithm
    1.3. Content- Based Access Control Algorithm
    1.4. Discretionary Access Control (DAC) models
    1.5. Mandatory Access Control (MAC) models
    1.6. Role-based Access Control (RBAC) models
    1.7. Task-based Authorization Controls models (TBAC)
    1.8. Context-Based Access Control model
    1.9. Fine-Grained Access Control
    1.10. Multi-Level Security Access Control policy
    1.11. Global Access Control (GAC) Federated Access Control
2. Security using Authentication Based Technique
    2.1. Challenge-Response Based RFID Authentication Protocol
    2.2. WPKI (wireless public-key system) authentication System
    2.3. Triple encryption authentication methods
    2.4. Dual user authentication mechanism
3. Security using Cryptography Based Technique
    3.1. Using Encryption Algorithm
    3.2. Using NTRU Algorithm
    3.3. Using Proxy Re-encryption Algorithm
    3.4. Elliptic Curve Cryptography (ECC) Algorithm

4. Security using Trust Based Technique
    4.1. Password Based Methods
    4.2. Kerbores
    4.3. An Unified Approach
    4.4. A New Agent Based Approach
    4.5. A Trust Enhanced Security Model
5. Security using Other Technique
    5.1. Attribute-Correlation Attack and Inference Attack
    5.2. Water-Mark Technique
    5.3. Slicing Algorithms
    5.4. Multi-party Algorithms
    5.5. Using Digital and Dynamic certificates
    5.6. An Intrusion-Tolerant Distributed Database (ITDDB) Security Model
    5.7. k-Anonymization Optimization Algorithm

3. SECURITY USING ACCESS CONTROL BASED TECHNIQUE

Access control is a technique which enables an authority to access data using access control list (ACL). Using ACL the system and users are protected the database from unauthorized access.

There are many technique uses under this.

3.1 Using ACL Algorithm

Neera Batra and Hemant Aggarwal describes the access privileges using ACL at system level as well as on object level. Security levels work efficiently in distributed environment. If user wants to access the remote data, then he can access it as per the privileges assigned to him on remote database but DBA can manage the database links [3].

3.2 Name –Based Access Control Algorithm

Here the objects are protected by specifying their names. If user wants to access the particular object he/she have to specify the actual name of the object [4].

3.3 Content- Based Access Control Algorithm

Here the system allows accessing the data based on data contents. If the user accesses a particular data he/she have to pass the credential through the username/password verification to access the particular content. If the user has passes this first level security then he/she has to pass the second level security. If the user has privileges to access the particular content then only he/she can finally access the data [4].

3.4 Discretionary Access Control (DAC) Models [4]

Using DAC it accesses of a subject to data based on the subject's identity and authorization rules. Here it allows subjects to grant authorizations on the data to other subjects.

3.5 Mandatory Access Control (MAC) Models [4]

Using MAC it can accesses the data by subjects and objects in the system. Objects are passive entity for storing information such as relations, tuples. Subjects are active entity which performs data access. An access class is consists of two components: a security level and a set of categories. The example of security level contains the levels Top Secret (TS), Secret(S), Confidential(C) and Unclassified (U), where TS>S>C>U. Access control in MAC models is based on the following Two principles, formulated by Bell and LaPadula :

No read-up: - A subject can read only those objects whose Access classes are dominated by the access class of the Subject.

No write-down:-A subject can write only those objects whose access classes dominate the access class of the subject.

3.6 Role-Based Access Control (RBAC) Models [4]

RBAC models are based on the notion of role. A role represents a specific function within an organization and can be seen as a set of actions or responsibilities associated with this function. Under this model, all authorizations needed to perform a given activity are granted to the role associated with that activity, rather than being granted directly to users. In addition, most RBAC models include role hierarchies, allowing one to represent role-subrole relationships, thus enabling authorization inheritance and separation of duty (SoD) constraints.

3.7 Task-Based Authorization Controls Models (TBAC)

Here the system allows accessing the data based on task assigned in the systems [4].

3.8 Context-Based Access Control Model

Here the access control decision functions depend on a large variety of context-dependent information, such as time and location. This mechanism is complemented by the notion of temporal authorization [4].

3.9 Fine-Grained Access Control

Here it allows accessing the tuple level based on the use of predicates. The predicates, specified as part of an access control policy, identify the tuples, in a given table, to which the access control policy applies. This mechanism is complemented by the notion of application context. Each application context has a unique identifier and consists of a number of attributes, identifying security-relevant properties [4].

3.10 Multi-Level Security Access Control Policy

Ying-Guang Sun designs an access control method for distributed database System. It designs Multi-level security system structure and defines the security tags of subjects and objects. It defines the security tag and security tag table. In the distributed application, the subject is a user or group of users, every subject has given a security level, and login by this security level. Mandatory access control is achieved by modifying the user's query statement and using security tag table in distributed database system [13]. Bhavani Thuraisingham in his paper introduce such a system is called a multilevel secure distributed database management system (MLVDDBMS). The purpose of this paper is to identify the impact of multilevel security on the functions of a DDBMS. They first defined an architecture for an MLVDDBMS(MLS/DDBMS) and discussed a security policy and multilevel data distribution issues [15][16][17].

3.11 GAC Federated Access Control

Zahir Tari and Andrew Fry Proposes Global Access Control (GAC) which is an extended access control mechanism that enables a uniform expression of heterogeneous security information. The focus of this paper is the design of a DOK (Distributed Object Kernel) security service that provides for enforcing both local security policies, and federated security policies. Their security framework provides a logic-based language, the Federated Logic Language (FELL), which can describe constraints on both single and multiple states of the federation. Currently, the DOK security Service is implemented on JacOrb, a CORBA compliant system [14].

4. SECURITY USING AUTHENTICATION BASED TECHNIQUE

Authentication is the act of establishing or confirming something (or someone) as authentic, that is, the claims made by or about the subject are true.

4.1 Challenge-Response Based RFID Authentication Protocol

Keunwoo Rhee et. al. Proposes more secure and effective authentication protocol to protect user’s privacy. This protocol is based on Challenge-Response using one-way hash function and random number. In their proposed protocol, the tag which is generated on every session is created using two random numbers received from the reader. For this reason the tag can differently responds on every session. Thus the protocol is secure against spoofing attack, tracking and replay attack [10].

4.2 WPKI (wireless public-key system) Authentication System

Bhagat .A.R et. Al. proposes this technique which can able to effectively solve the problem of identity authentication database. WPKI grant issue certificates for users and service providers. In the transaction processes user uses the certificate to ensure the confidentiality of the process of data integrity, transmission and no repudiation. Using the certificate the authentication of communication is also completed [20].

4.3 Triple Encryption Authentication Methods

Authentication is verified the class of Kerberos using triple encryption authentication methods. At first it verifies whether the authentication server is sent the test data or not. To verify it mobile clients uses the public-key to encrypt the data on the server side and decrypt it for authentication servers. Next, the decrypted data is decrypted again to obtain the relevant data. After that it randomly generated a session keys. Next the server database once again receives the data before using the private key to decrypt the data and Session key. It then uses conventional methods of encryption and decryption to decrypt that data which is issued by the authentication server. Lastly the mobile database sends a confirmation message. To verify the confirmation message is issued by the server-side database, it first use mobile clients, then confirm the private key of the server-side database which is encrypted. When the mobile clients receive confirmation message, then they use the session key encryption to communicate with the server-side database [20].

4.4 Dual User Authentication Mechanism

This authentication mechanism is used to strictly identify the user in the system. To form dual protection mechanism to implement identity authentication, the mobile database system are merged with the operating system user authentication mechanism. This dual user authentication mechanism strengthens the confidentiality of the database system. This also ensures the confidentiality of sensitive data on particular access control [20].

5. SECURITY USING CRYPTOGRAPHY TECHNIQUE

Securing a database using cryptography technique is an age old one. Here main database is going to be encoded using some key and then decoded using the same key. Here securing the key is the most challenging task.

There are many technique uses under this.

5.1 Using Encryption Algorithm

Kalpana k. Palve and R.W.Deshpande introduce an algorithm for checking data privacy using encryption algorithm. They first distributed the data using slicing algorithm for anonymization with security algorithm. After that they inspect the verification schema with trusted third party (TTP) or safe Multi Party Computation (SMC) protocols using L diversity by using binary algorithm [2].

5.2 Using NTRU Algorithm

Gurkamal Bhullar, Navneet Kaur introduces six bit encryption algorithm to enhance the security and controlling the concurrency in distributed database. This six bit encryption algorithm is based on NTRU algorithm. In this paper they also compare with RSA or DES algorithms and show that their proposed algorithms requires less time and more accurate [5].

5.3 Using Proxy Re-encryption Algorithm

G. Srilakshmi, M. Preethi uses the concept of re-encryption of data to get more security. Here the access permission of data is decided by the data stored person or owner. They proposes an identity based data storage scheme where both queries from the intra domain and inter domain are considered. This technique is collusion-resistance and it can provide secure model of cloud storage with safe data forwarding. It will get the notification of user request on android based device. It also provides security against Distributed Denial of Service attack [12].

5.4 Elliptic Curve Cryptography (ECC) Algorithm

Encryption is needed to enhance privacy in the mobile database system. At first it set a password encryption. Different levels of passwords are sets and encrypted according to the different database functional modules. Next it can use elliptic curve cryptography (ECC). It is based on the intractability of the definition of point group in the elliptic curve discrete logarithm problem. In this way it can increases the database data security [20].

6. SECURITY USING TRUST BASED TECHNIQUE

In different type of databases where data are distributed through the network, there is always high chance to insecure the data at any point of time. As the data are partially or fully distributed there must be some trusted environment where the data are distributed. There are some techniques through which we can identify this trusted environment. Many researchers has proposes many trust policies to secure the data which demand the data confidentiality and integrity in trusted environment to all authorized users.

6.1 Password Based Methods

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 [1].

6.2 Kerbores

kerbores is another approach which is used lightweight protocol based on symmetric key cryptography to identify trusted policies [1].

6.3 An Unified Approach

An unified approach for Trust Management in distributed system has been introduced by Blaze et al which specify and interprets security policies [1].

6.4 A New Agent Based Approach

Serhiy et al has been introducing a new Agent based approach which uses neural networks for on-line line monitoring of user actions. Monitoring on this actions we can identify trusted environment [1].

6.5 A Trust Enhanced Security Model

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 [1].

7. SECURITY USING OTHER TECHNIQUE

There are many others technique used now a day's to secure the databases. Many researchers have proposed many new techniques which will secure the databases which are distributed.

7.1 Attribute-Correlation Attack and Inference Attack

Sanket Divate et. al. proposes two types of attack to prevent distributed information sharing. Here they proposes "Query Segment Encryption" scheme (for privacy) for sharing the secure query routing function between the set of brokering servers. They also propose the "Privacy Preserving Information Brokering System" (PPIB) for enforcing secure and privately sharing information in distributed information sharing [6].

7.2 WaterMark Technique

Hazem M. El-Bakry and Mohamed Hamada introduce a technique which is added only one hidden record with a secret function. For each attribute, the function value depends on the data stored in all other records. This technique is more powerful against any attacks or modifications of cell values. Using this approach both textual and numerical data of distributed database is protected [7].

7.3 Slicing Algorithms

Ms. Pragati J. Mokadam, Dr. S.T.Singh introduced a notion of data privacy using slicing technique which classifies data vertically and horizontally. They used slicing algorithm for anonymization and L diversity. Using verification algorithm of data privacy it checks for security and privacy. Slicing algorithm is very useful in high dimensional data. The computation time of slicing is very less as compare to blowfish encryption algorithm. But the limitation of this algorithm is that there could be loss of data utility [8].

7.4 Multi-Party Algorithms

S.Pavithra, P.Prasanna proposed a protocol for horizontally scattered database to protect the mining of association rules. This procedure is based on the Fast Distributed Mining (FDM) algorithm. The FDM Algorithm which is proposed by Cheung et al. is an unsecured spread version of the Apriori algorithm. The two main ingredient of novel secure multi-party algorithms— one that computes the union of private subsets that each of the interacting group of actors hold, and another that tests the inclusion of an element held by one actor in a subset held by another[9].

7.5 Using Digital and Dynamic Certificates

Mr. Mahesh Singh, et al, proposes an approach of “Securing database using dynamic certificates” .Using dynamic certificates it protect the database system from insiders. It provides a mechanism to assign digital certificates to its user according to their designation/ level in the organization. These certificates will contain the types and list of queries which the user can execute on the database. This will help in implementing security principle as well as granting and revoking privileges to/from the accounts. Only after verifying the authenticity of the certificate, the authorized part of the database can be accessed by using the list of the queries attached with the certificate [11].

7.6 An Intrusion-Tolerant Distributed Database (ITDDB) Security Model

Gu-Ping Zheng and et al introduce an intrusion-tolerant distributed database (ITDDB) security model. This model can detect intrusions, isolate attacks, assess and repair the damage caused by intrusions in a timely manner. The system can maintain the integrity and availability of data. The confidential data, a (t, n) threshold secret share scheme is utilized to protect them from compromised servers in the presence of intrusions. In this way, the system can keep the integrity, availability and confidentiality of data [18].

7.7 k-Anonymization Optimization Algorithm

R.S.Venkatesh, et al proposes to disclose of sensitive data using K-anonymization optimization algorithm. It requires partitioning of microdata equivalence classes. It minimizes closeness by kernel smoothing and then determines the distances move by controlling the distribution pattern of sensitive attribute in a microdata. In this way it maintains diversity which may leads to severe computational challenges as NP-hard Problem. It faces background knowledge attack and homogeneity attack [19].

8. PERFORMANCE COMPARISON OF DIFFERENT TYPES OF SECURITIES APPROACHES IN DISTRIBUTED DATABASE SYSTEMS.

Technique Attributes	Access Control based Technique	Authentication Based Technique	Cryptography Based Technique	Trust Based Technique	Other Technique
Reliability	Lowest	High	Highest	Low	Higher
Availability	Higher	High	High	High	Higher
Visibility	Higher	Moderate	Moderate	Moderate	Higher
Flexibility	More Flexible	More Flexible	Moderate Flexible	Moderate Flexible	Highest Flexible
Running Time	Fast	Average	Less Running Time Required	Average	Fastest
CPU Utilization Time	Low	High	Moderate	High	Low
Cost	Lower Price	Low Price	Highest Price	High Price	High Price
Memory Usage	High Memory usage	Low Memory usage	Low Memory usage	High Memory usage	High Memory usage
Additional Storage Area Required	Not Required	More Required	More required	Not required	Not required
Quality	Better	Better	Good	Good	Best
Data Authenticity and Confidentiality	Low	Low	High	High	Highest
Robustness	Moderate	Moderate	Good	Most	Good
Security	Good	Good	Top most	Better	Better
Commercial Implementation	Oracle 8I - Relational Database	DB2 - Mobile Database	SQL Base - Mobile/Embedded Database	Red Brick - Enterprise(Data Warehousing)	Teradata - VLDB (Data Warehousing)
Vendor Availability	Oracle	IBM	Centura Software	Informix (Red Brick)	NCR
Customer Satisfaction	Satisfactory	Satisfactory	Satisfactory	Satisfactory	Satisfactory
Power Consumption Performance	Worst	Better	Low	Better	Low

9. CONCLUSION

As the types of databases are changing, to secure these databases we are facing many critical challenges day by day. In this paper we review the different types of security approaches which are introduced by different researcher to secure the different types of databases. These different types of techniques are basically based on cryptography, trust based, Authentication based, access control based algorithms. Except these types of well known technique there are also different kind of popular techniques are also used to secure the databases. In this paper we also compare the different security techniques with some performance parameters. Though there are many techniques introduced till date, yet as the variety of data changes security is also facing new challenges day by day. So till date distributed database security remains an open challenge to the researchers.

REFERENCES

[1] Dr. P. K. Rai, Pramod Singh, An overview of different database security approaches for distributed environment,IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 6, June 2015. www.ijiset.com ISSN 2348 – 7968

[2] Kalpana K. Palve, Prof R.W. Deshpande, Database Security Approach for Distributed Datasets: A Survey, International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 2, Issue 11, November 2014

[3] Neera Batra , Hemant Aggarwal, Autonomous Multilevel Policy Based Security Configuration in Distributed Database,IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 2, November 2012 ISSN (Online): 1694-0814 www.IJCSI.org

[4] Elisa Bertino, Ravi Sandhu, Database Security—Concepts, Approaches, and Challenges, IEEE Transactions On Dependable And Secure Computing, Vol-2, No. 1, January-March 2005.

[5] Gurkamal Bhullar, Navneet Kaur, Enhancing Security and Concurrency in Distributed Database with 6 Bit Encryption Algorithm, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2718-2722

[6] Sanket Divate, Pratap Ghayal, Saurabh Mamidwar, Mayur Narawade, Meghna Lokhande, Securing And Maintaining Privacy Information Brokering In Distributed Data Sharing, International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-3, Issue-6, June-2015

[7] Hazem M. El-Bakry and Mohamed Hamada, A Developed WaterMark Technique for Distributed Database Security, Conference Paper January 2010 DOI: 10.1007/978-3-642-16626-6_19 · Source: DBLP

[8] Ms. Pragati J. Mokadam, Dr. S.T.Singh, Data attribute security and privacy in Collaborative distributed database Publishing, International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 3, Issue 12 (July 2014) PP: 60-65

[9] S.Pavithra, P.Prasanna, A Novel Secure Multiparty Algorithms in Horizontally Distributed Database for Fast Distributed Database, International Journal Of Engineering And Computer Science ISSN:2319-7242 ,Volume 4 Issue 3 March 2015, Page No. 10924-10929.

[10] Keunwoo Rhee, Jin Kwak, Seungjoo Kim, and Dongho Won, Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment

[11] Mr. Mahesh Singh, Ms. Alka, A Dynamic Approach For Database Security, Mahesh Singh *et al*, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May-2014, pg. 1247-1253.

[12] G. Srilakshmi, M. Preethi, Security Schemes in Distributed Data Storage Using Proxy Re-encryption,Volume 4, Issue 11, November 2014 ISSN: 2277 128X , International Journal of Advanced Research in Computer Science and Software Engineering

[13] Ying-Guang Sun, Access Control Method Based on Multi-level Security Tag for Distributed Database System, Computer Center , Liaoning University of Technology, Jinzhou 121001, P.R.China

[14] Zahir Tari, Senior Member, IEEE, and Andrew Fry, Member, IEEE, Controlling Aggregation in Distributed Object Systems: A Graph-Based Approach,1236 IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 12, NO. 12, DECEMBER 2001

[15] Bhavani Thuraisingham, Multilevel Security Issues in Distributed Database Management Systems II ,The MITRE Corporation, Burlington Road, Bedford, MA 01730, U.S.A.Computers & Security, 10 (1991) 727-747

[16] Bhavani Thuraisingham, The MITRE Corporation, Security for Distributed Databases,Information Security Technical Report, Vol 6, No. 2 (2000) 95-102

[17] Bhavani Thuraisingham, Member, IEEE Computer Society, and William Ford, Senior Member, IEEE, Security Constraint Processing in a Multilevel Secure Distributed Database Management System,IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 1, NO. 2, APRIL 1995

[18] Gu-Ping Zheng and Lu-Feng Xu, Distributed Database System Security Model of Power Enterprise Based on Intrusion Tolerance Technology,2006 International Conference on Power System Technology

[19] R.S.Venkatesh, P.K.Reejeesh, Prof.S.Balamurugan, S.Charanyaa, Further More Investigations on Methods Developed For Database Security, International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization)Vol. 4, Issue 1, January 2015

[20] Bhagat.A.R, Prof. Bhagat.V.B, Mobile Database Review and Security Aspects, Bhagat.A.R *et al*, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014, pg. 1174-1182