International Journal of Communication Networks and Security

Volume 1 | Issue 2 Article 10

2011

Enhanced Security Framework to Develop Secure Data Warehouse

Anshuman Kumar Saurabh
Computer Science Department, Ambedkar Institute of Technology New Delhi, India,
anshumansaurabh@gmail.com

Bharti Nagpal
Computer Science Department, Ambedkar Institute of Technology New Delhi, India,
bharti_553@yahoo.com

Enhanced Security Framework to Develop Secure Data Warehouse

Anshuman Kumar Saurabh[1], Bharti Nagpal[2]
Computer Science Department, Ambedkar Institute of Technology[1,2]
New Delhi, India
E-mail : anshumansaurabh@gmail.com[1], bharti_553@yahoo.com[2]

***Abstract*—Data Warehouse contains crucial information about organization. This information is utilized by decision maker to analyze the current status and planning the development of the organization. The data warehouse can be easily accessed by an authorized user or by an unauthorized user through unfair means. To preclude this data from unauthorized access, several measures have been taken and a lot of research is going on. In this paper, a framework is proposed to prevent the data from unauthorized access and thereby increases the security of data warehouse.**

Keywords- Data Warehouse; Data; Security; Unauthorized User, Access level

I. INTRODUCTION

Every organization accumulates its day-to-day, weekly, monthly and yearly data in a system called Data Warehouse. Data Warehouse contains data in such a way that an analysis can be done in order to take decision by decision maker for company's future plans [1] [2] [3]. Data warehouse is a system that extracts, cleans, conforms and delivers source data (operational data) into a multi-dimensional data source, which is easy to access by the end-user. This data is very critical and is used to plan the suitable strategy for future. The data in DW can be represented in multi-dimensional view for end user. This data can be managed through many tools like OLAP tools are used to facilitate multi-dimensional analysis [1], which are presently used in organizations.

Data warehouse contains the sensitive information and data of an organization which is extracted from heterogeneous sources. Such sensitive information and data are very important for an enterprise, which is used in decision making process. Therefore, Security is an important concern which should be defined in order to protect this sensitive information from unauthorized users [4].

DWs are a newest technology in any organization which has various security issues like data integration, data security, data consistency and confidentiality of data. The confidentiality and integrity of the data is very essential to provide security to organization's information. For maintaining confidentiality and integrity of data in organization, technique like encryption is used to resist from unauthorized users. A lot of research is done in the internal security of data warehouse at the time of data warehouse design. At data warehouse design level, approaches like MDA, QVT [8] [5] etc have been proposed to improve the security of data warehouse.

This paper is organized as follows: Section II covers the related work on security of data warehouse. Section III describes the design of proposed framework. Framework for enhancing security in data warehouse is in section IV. Finally the conclusion and future work is given in section V.

II. RELATED WORK

Security is an important concern in every field to furnish protection. Data Warehouse's security is also a big concern. Numerous methods have been proposed which considers the security in the data warehouse which is as follows:

A classical model proposed in which the data is handled based on the requirements of an organization. This model includes the requirement and specification of the organization and the three design levels called Conceptual level, Design level and the Physical level. These levels are followed in the same hierarchy as described. Furthermore, this model fails to store the statistical information about the data [6] [7]. This model is given below in figure 1.

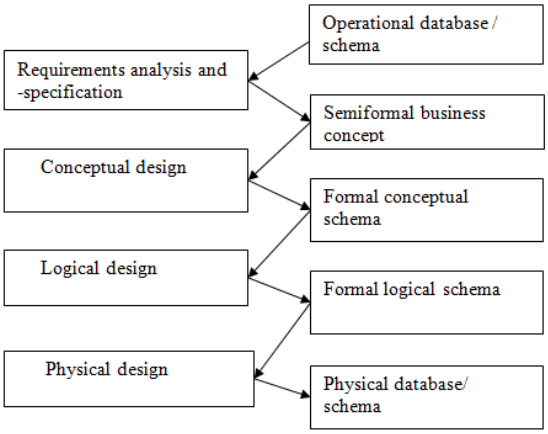

Figure 1Classical Security Model

An approach called the MDA [8] (Model Driven Architecture) approach is introduced to develop the secure data warehouse. This model allowed for defining the model at different abstraction level. That is, Code at Physical Level, Computer Independent Model (CIM) at Business level and Platform Independent model at conceptual level

and Platform Specific model (PSM) at logical level as given in below figure 2. At conceptual level, two security levels introduced namely Secret (S) and Top secret (TS) [9].

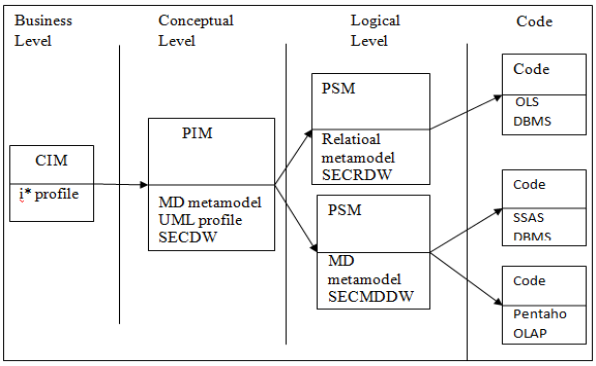

Figure 2 MDA based Approach

A framework proposed which uses the encryption filter to encrypt the data before storing it in data warehouse. Data in data warehouse is present in encrypted form (means in unreadable format) so that no one can read and understand that data. This method increases the response time and turn-around time. But succeed in providing the security to data with the help of filtration method [10]. This framework is given below in figure 3.

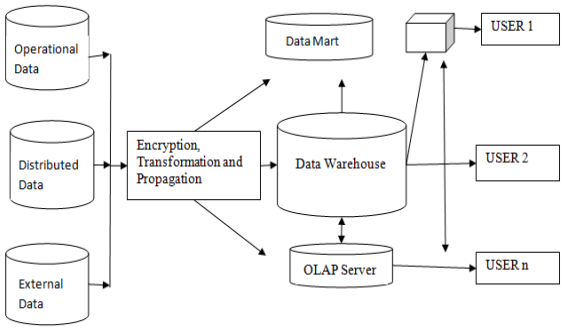

Figure 3 Data Filtration and Encryption

A hybrid approach proposed for enhancing the security of data by adding techniques like encryption filter and authentication code. Encryption filter encrypts the data before data warehouse and authentication code is the security added towards the user's end which enables the end-user to access the data with a password and identity. If user does not provide the correct identity and password then the access is denied for that particular user [11]. It can be understood by the below given figure 4.

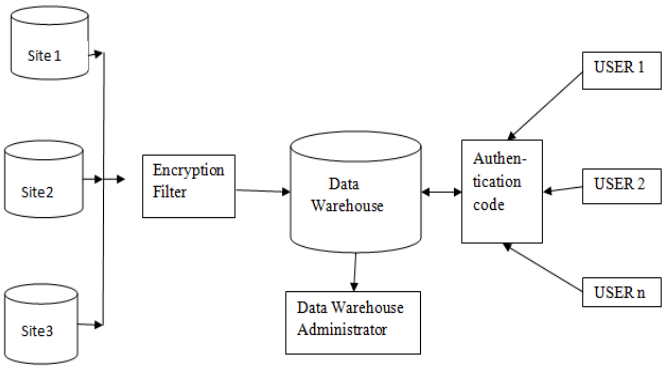

Figure 4 Hybrid Approach

III. DESIGN OF PROPOSED FRAMEWORK

The proposed framework is designed in order to increase the security of data warehouse. In this framework, three security phases are there which resist the unauthorized access to the data. The levels of security in proposed framework are as follows:

Level 1 Security Phase – In this phase, User enters the authentication code to get the access to the data. The user gets access based on the pre-defined policies by the administrator of any organization.

Level 2 Security Phase – Now the user is monitored for its activities through an administrator. Some log files of user are maintained in the historical database for matching current activities.

Level 3 Security Phase – Here a data warehouse's administrator is monitoring data warehouse for security purpose.

IV. PROPOSED FRAMEWORK

The current security in data warehouse encrypts the data which is coming from different sources. This encryption is done with the help of a filter called encryption filter [11]. After encryption, the data is saved in the system called data warehouse. An administrator monitors the data warehouse activities. Now, when the user logs in its identity and password, a filter classifies the user on the basis of access rights. All this procedure can be understood with the help of below figure 5.

As it can be seen from below figure, the proposed framework work between the end-user and data warehouse system. This framework offers three levels of security towards the unauthorized users which makes the data warehouse more secure.

The proposed framework works as follows:

Level 1 Security Phase - User enters its identity (like name) and password to log-in. Based on these credentials, the user gets access to the data warehouse. This access is based on certain policies which are defined by an administrator of any organization. This policy can be based on time, person, access level etc. Now based on the pre-defined policy, user accesses the data.

Level 2 Security Phase - After getting access, user is monitored with the help of an administrator. Moreover, some log files of all the users are maintained in the historical database. User's activities are matched with these stored log files in order to find any kind of deviation from the stored log files. If the stored log matches with the monitored activity, then it is allowed to access the data warehouse otherwise it is blocked from accessing it.

Level 3 Security Phase - Now while accessing the data, data warehouse's administrator is keeping a watch on data warehouse for any kind of illegal activity. This level is already there in current security of data warehouse. The level 1 and level 2 securities are added in the framework to increase the resistance towards the unauthorized users.

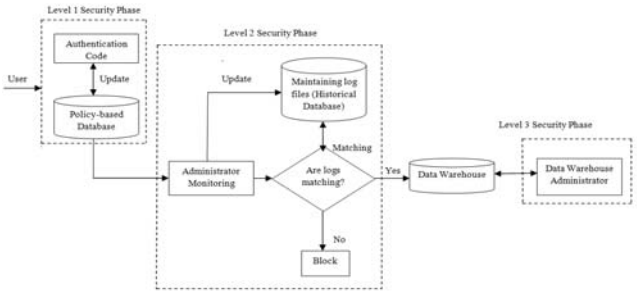

Figure 6 Proposed Security Phases

V. CONCLUSION AND FUTURE WORK

The proposed framework increases the security of data with the help of three levels. Three levels include the techniques like authentication code, administrator and policies which in turn provides a robust framework to secure data warehouse. This framework makes the access level dynamic in nature; insure the data confidentiality and privacy and resists the system from getting hacked by an intruder because of the increased security. The efficiency and accuracy of the proposed framework can be measured by implementing the model.

The below explained procedure can be understood with the help of below given figure 6 called the proposed framework with all the three levels.

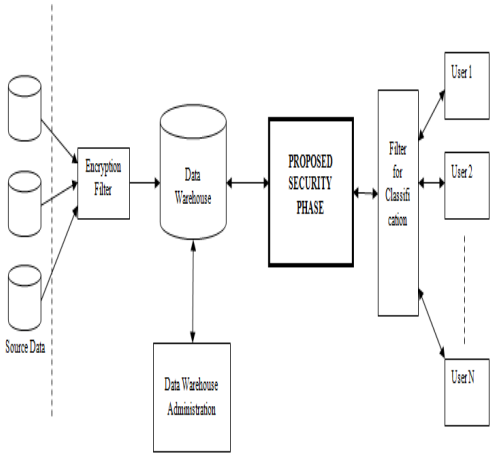

Figure 5 Proposed Security Framework in Data Warehouse

REFERENCES

[1] ***Paulraj Ponniah "Data Warehousing Fundamentals" Red Book ISBN-10 81-265-0919-8. 2007***

[2] ***W. H. Inmon, "What is a Data Warehouse?" Prism Tech Topic, Vol. 1, No. 1, 1995***

[3] ***W. H. Inmon, "Building the data warehouse", third edition Wiley & sons, 2002.***

[4] ***P. Devanbu, S. Stubblebine, Software engineering for security: a roadmap, presented at The Future of Software Engineering, 2000.***

[5] ***Emilio Soler et. al."Application of QVT for the development of Secure Data Warehouse:A case study ", Second International Conference on Availability, Reliablity and Security(ARES'07) IEEE 2007.***

[6] ***Till Haselmann, Jens Lechtenb¨orger, Gottfried Vossen, "Data Warehouse Detective: Schema Design Made Easy", in the proceedings of BTW 2007, Aachen, Germany***

[7] ***Diego Calvanese, Data Integration in Data Warehousing, International Journal of Cooperative Information Systems Vol. 10, No. 3 (2001) 237–271***

[8] ***Carlos Blanco, et. al. "Applying an MDA-based approach to consider security rules in the development of secure DWs", International Conference on Availability, Reliability and Security, (2009) IEEE.***

[9] ***Blanco, C., et al. Obtaining secure code in SQL Server Analysis Services by using MDA and QVT. in 6th International Workshop on Security in Information Systems, 2008.***

[10] ***Rosenthal and E. Sciore, "View Security as the Basic for DW Security," (DMDW'00), Sweden, 2000***

[11] ***S.Ahmad, R.Ahamad "An Improved Security Framework For Data Warehouse: A Hybrid Approach ", IEEE 2010.***