Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 149 – 157

Procedia
Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

Security Issues In Data Warehouse: A Systematic Review

Anjana Gosain[a], Amar Arora[b]

[a] Professor, USICT, Guru Gobind Singh Indraprastha University, Delhi, India
[b] Scientific Assistant, National Informatics Centre, DeitY, Govt. of India , India

Abstract

As Data Warehouse store huge amount of data with the span of more than decades, the security of this huge information base is crucial for the sustainability and reliability of data warehouse. Since its advent the data warehouse has gone through various technological changes, which has prompted changes in the security strategies as well. This article, is taking a deep look at the various changes in the security mechanisms of the Data Warehouse, along with the changes in the strategies for the data warehouse development. It helps in understanding the various security aspects related to Data Warehouse, in coherence with the different methodologies employed for its development and functioning.

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication
and Convergence (ICCC 2015)

Keywords: Data Warehouse Security;Systematic Review; Security

1. Background

Data Warehouses (DWs) [Inmon, 1991] coined by Inmon in 1991, were further enhanced with its advanced generations [Inmon, 2005][Inmon, 2006]. According to Inmon, data warehouse is defined as a collection of subject-oriented, time variant, integrated, non-volatile data that supports the management decision making process [Inmon,

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)
doi:10.1016/j.procs.2015.04.164

1991]. Traditionally, it is meant to store the historical data and needs special task of extracting, transforming and load procedures [Becker et al., 2008]. These procedures help DW to provide useful information to decision makers, which aid them to improve their business process. However, in order to provide richer insights into the dynamics of today's business, the data warehouse cannot work in isolation. It requires combining the organization data with data from outside, which complements the company's internal data with value-adding information (e.g., production details of the competitor's organizations) [Blanco et al., 2013]. This combining of data became possible with the advent of internet, which enhanced data warehouses reach at the global level. This global reach of data warehouse attracted attention of research community towards its security requirements. As a result, the confidentiality emerged as one of the major issue that should have taken into consideration in every information systems (ISs) development [Dhillon, 2000]. However, data threats took a leap further with the advent of major technological changes. Among the various advances, the access of databases through web along with development of e-commerce is one of the kinds [Clifton et al., 1997]. Advancements like these further strengthen the requirement of incorporation of security in all stages of Information System's development.

This article, reviews the major security advancements in the field of DW. It has been divided in the subsections as Background which explains historical view of the DW and its security aspects. The Review Questions section formulates all the review questions for this article. In order to answer these questions the adopted mechanism is explained by section namely Review Methods. The Technology section explains each category of DW in detail with respect to the security solutions in the articles belonging to the respective category. In Results and Discussion section different security aspects have been discussed among different categories along with respective security solutions. The Summary and Conclusion section summarizes the whole review process and provides constructive conclusion based on the inputs from the discussion section.

2. Review Questions

This article reviews various proposals considering solutions for security concerns of the DWs and tries to answer the following research questions:-

1. Assessing how technological changes in development of DW affect the security mechanism adopted.
2. Analyzing the possible future research area in the field of securing DW.
3. Assessing each security mechanism on the basis of various quality parameters such as Encrypted Data, Audit Control, Extendibility, etc.

3. Review Methods

This review adopts a systematic approach [Keele, 2007].Initially about 85 research articles were identified. Then these articles were classified in to their respective categories in accordance to methodology adopted respectively. While reviewing those articles, few more articles were identified which act as the supporting articles. All these articles were then combined to find the individual contribution to the respective category and analysis was done to find out the current development. Some articles mentioned in this review do not really explain security aspects of the DW, but these articles are included as they can give better insight of the working of the DW. During the review process, some articles were filtered, as they were not in coherence with the review objectives.

4. Technology

As mentioned in the previous section, we look at the various approaches for development of DW along with respective security solutions:-

4.1. Queries Over Encrypted Database

The Encryption strategy for the database is a very old technique in which one of the initial solutions is being given in the form of in-stream encryption [Caserta & Kimball, 1998]. But since then the database encryption was not considered worth wile, but with the advent of DAS (Database as a Service) over the cloud and usage of outsourced data the privacy of data inside databases became an important issue. As a result you can find several recent studies dealing with query processing over encrypted data [Amagasa et al. 2009] [Canim et al., 2012] [Amagasa et al., 2013] [Liu & Wang, 2012] [Balakrishnan et al., 2012] [Liu, 2014] [Liu et al., 2014]. However, little attention has been devoted to deal with encryption strategy for dimensional data in a DW allowing processing of analytical queries. As a result recent solution has been provided [Ciferri et al., 2014] which investigates the method for encrypting and querying a DW hosted in a cloud.

4.2. Adapted Mandatory Access Control Based OLAP

In [Kirkgoze et al., 1997] a security approach based on adapted mandatory access control for OLAP-cubes is presented. The primary advantage of using this approach is its flexibility of assigning roles to different virtual sub-cubes [Kirkgoze et al., 1997]. In order to achieve this, a seven phase structure is proposed containing: 1) identification of data, 2) classification of data, 3) quantifying the value of data, 4) identification of data security vulnerabilities, 5) data protection measures and their costs determination, 6) selection of cost-effective security measures, and 7) evaluation of effectiveness of security measures.

4.3. Metadata based Security Model

Metadata, which describes the contents of the data warehouse [Berson & Smith, 1997], can also be used to describe security mechanisms in a data warehouse environment. In this case access rules with corresponding information about security objects and subjects are stored as metadata. Security subjects are responsible for changes in the data warehouse and cause information to flow within different objects and subjects. When user accesses data, the secure query management layer checks whether this access is allowed. To ensure this, it verifies the corresponding access authorizations by analyzing security metadata. So in this approach, security aspects have been considered in the design phase of the data warehouse in order to better match the security requirements. It was done to avoid fundamental, cost-intensive adaptations [Katik et al., 1998].

4.4. OLAP Security Design

OLAP is meant to provide quality information to the end user [Berson & Smith, 1997], by allowing user to navigate through the dimensions of the DW. This unique feature makes it popular among the users accessing a data warehouse. So over the period of time, steady growth in the number of OLAP users is highly noticeable, which necessitates the requirement of proper access control mechanisms to ensure the confidentiality of the sensitive data [Santos et al., 2011]. However, a data warehouse which is primarily built as an open system, its very nature creates a security conflict [Kimball, 1997]. Especially during exploratory OLAP analysis, which is of open nature; the security controls may hinder the analytical discovery process. To deal with this issue, [Kimball, 1997] propose that auditing should also be performed on the multidimensional level of an OLAP engine (i.e. at the same level where authorization semantics are defined). Deriving the access control policies from the operational data sources is very difficult, though some research efforts have been made in this area [Rosenthal et al., 1999]. Some commercial systems [Cogos, 1998][Microsoft, 1999][MicroStrategy, 2000][Oracle, 1998][Thomsen, et al., 1999] provide mechanisms to cope with these requirements; however the approaches are highly proprietary. Thus, it opens up issues related to OLAP security design and makes way towards requirement for ME/R [Sapia et al., 1999] or UML like approach for the future.

4.5. UML Based Secure DW

The Unified Modeling Language (UML) [Rumbaugh, 1999] is extended to UMLSec [Jurjens, 2002], for the sole purpose of encapsulating knowledge on prudent security engineering and making it available to developers who may be not specialized in security. This idea itself of extending UML has triggered the process of extending the UML for the specific requirements of different category of systems. Within the same line, the confidentiality problems regarding DW's are discussed and an extension of UML for the secure DW is provided [Eduardo, 2004]. It allows designers to specify main security aspects in the conceptual MD modeling, thus resulting in design of a secure DW system. Various other approaches of the UML extension for the DW Security [Fernandez-Medina et al., 2005][Emilio et al., 2006][Eduardo et al., 2006][Eduardo et al., 2007][Emilio et al., 2009][Ali et al., 2012] have been proposed.

4.6. MDA Based Secure DW

Model Driven Architecture (MDA) [Miller & Mukerji, 2003] [Bast et al., 2003] is a framework based on UML and other industry standards for visualizing, storing and exchanging security designs and models. There are various proposals to integrate security using MDA approach [Auguston et al., 2003] [Basin et al., 2006] [Karapagam & Sivanandam, 2004] [Schreiner & Lang, 2004] but all of them are related with information systems, access control, security services and secure distributed applications. None of approaches related with the design of secure DWs. As a part of solution, a framework based on Model Driven Architecture (MDA) for the development of secure DW that covers all the phases of design (conceptual, logical and physical) and embeds security measures in all of them is proposed in [Eduardo et al., 2007]. Another proposal extending the relational package from CWM has been applied to the construction of a star schema for DWs [Emilio et al., 2008]. But the primary advantage of MDA approach has been put to use by automatic generation of secure MD code for the DWs by allowing definition of models at different abstraction levels, along with the automatic transformations between them [Carlos et al., 2008]. This approach allows automatic development of DWs, thus saving time and money, obtaining better quality and security by translating the requirements identified at early stages of development into the final implementation. Despite all these improvements, there were still open areas in the field in the MDA based security approaches, some of which were tried to fill up by number of proposals [Arnulfo et al., 2009] [Blanco et al., 2009] [Emilio et al., 2009] [Xaio, 2009]. MDD (Model Driven Development) approach [Alfonso et al., 2010] to secure DWs extended it further to develop high-level (platform independent) models which can be transformed into more specific (according to specific platforms) models and can in turn be transformed into code dependent models.

4.7. XML Based Secure DW

Increased popularity of XML DW lead the research community to look at the security aspect of the XML based DW. Some security solutions for the XML Databases are discussed, which include proposal for development of semantic cache framework [Feng et al., 2008]. A detailed literature review on XML Security has been done in [Elehart et al., 2008] which looks at the security point of view of XML in application use. Alongside advancement in XML security, the analysis on development of XML based DW has also been performed [Ravat et al., 2010]. In overall conclusion, it is observed that rather than considering security once the system has been completely built, the security and privacy measures should be integrated in all layers of the DW design. Which means that much more robust, secure and platform independent products can be produced [Giorgini & Mouratidis, 2006] [Iyer et al., 2007]. Taking inspiration from the above fact, the use of Model Driven Architecture do define security in the MD modeling of XML DWs was proposed [Belén et al., 2010]. It was later demonstrated, validated using Secure MD (Platform Independent Model) PIM and Secure XML PSM which includes both MD and the security aspects [Belén et al., 2012]. This conceptual model has been made practical by defining transformations to obtain secure XML schema using QVT transformation rules [Blanco et al., 2013]. Other security viewpoints for XML DWs were also presented, which includes privacy preserving OLAP [Alfredo & Elisa, 2011] and Access control for secure XML query processing [Dongchan & Seog, 2011]. Though lot of research viewpoints have been mentioned here, but still the field of securing XML DWs is open for further research and scrutiny.

5. Results and Discussion

Out of 55 articles discussed in section 3, 19 focus on the DW security aspects. These articles are being compared on the basis of security parameters as follows:-

- **Encrypted data:** The data inside the data warehouse is encrypted or not.
- **Audit control:** Inclusion of security audit parameters in the Data warehouse.
- **Extendibility:** DW Model Extendibility to the new security requirements.
- **Platform Independence Model security:** Security consideration at the PIM level of data warehouse development.
- **Transformation:** The level of automation in transformation between models after inclusion of security parameters.
- **Creation of PSM:** Platform Specific Model is being provided by author or not.
- **QVT support:** Solution supporting security has a mention of Query / View / Transformation procedures or not.
- **Integration of multi-platform data:** Does the DW development technology supporting security allow integration of data from heterogeneous sources.

Some general criteria are also considered which provide information about the research article regardless of their solutions category, like Journal, Number of citations, Impact factor, Publication year and Solution category.

Table 1.Brief Analysis of Security Solution for Data Warehouse

Articles	ED	AC	Ex	CI	PI	Tr	PS	QVT	I	ID	P	Cit	IF	SC
[Caserta & Kimball, 1998]	Y	N	N	N	N	N	N	Y	Y	N	Wiley	959	NA	In-stream Encryption
[Kirkgoze et al., 1997]	N	N	N	N	N	N	N	Y	N	N	IEEE Conf.	60	NA	Role Based Access Profile
[Katic et al., 1998]	N	N	Y	N	N	N	N	Y	N	N	IEEE Conf.	86	NA	Meta Data
[Eduardo et al., 2004]	N	N	Y	N	Y	N	N	N	N	N	LNCS Springer	26	NA	UML Extension
[Emilio et al., 2006]	N	Y	Y	N	Y	N	N	N	N	N	LNCS Springer	4	NA	UML2.0 + CWM
[Eduardo et al., 2006]	N	Y	Y	N	Y	N	N	N	N	N	JRPIT	30	0.22	UML2.0/ OCL Extension
[Eduardo et al., 2007]	N	N	Y	N	Y	N	Y	N	Y	N	Elsevier	66	1.235	UML Ext.
[Jose & Juan, 2008]	N	N	Y	Y	Y	SA	Y	Y	N	N	Elsevier	159	2.036	MDA + QVT
[Emilio et al., 2008]	N	N	Y	N	Y	SA	Y	Y	Y	N	Elsevier	20	1.177	CWM
[Carlos et al., 2008]	N	N	Y	Y	Y	FA	Y	Y	Y	N	LNCS Springer	7	NA	MDA + QVT + SSAS
[Emilio et al., 2009]	N	Y	Y	Y	Y	N	Y	N	Y	N	Elsevier	14	1.177	UML 2.0 + MDA
[Arnulfo et al., 2009]	N	Y	Y	Y	Y	FA	Y	Y	N	N	LNCS Springer	6	NA	MDA + ADM
[Emilio et al., 2009]	N	Y	Y	Y	Y	SA	N	Y	N	N	Elsevier	23	1.328	MDA + SPEM

[Xiao, 2009]	N	N	Y	Y	Y	N	Y	N	Y	N	Elsevier	16	1.328	Agent oriented MDA + RBAC
[Ravat et al., 2010]	N	N	Y	N	N	N	N	N	N	Y	Elsevier	19	1.235	XMLDW
[Belén et al., 2010]	N	Y	Y	N	Y	SA	Y	N	Y	Y	ACM	6	NA	MDA + XMLDW
[Ali et al., 2012]	N	Deals with Access Control and Data Interference							Y	N	LNCS Springer	Nil	NA	UML Ext + RBAC + MAC
[Belén et al., 2012]	N	Y	Y	Y	Y	SA	Y	N	Y	Y	Elsevier	6	2.036	XMLDW + MDD
[Blanco et al., 2013]	N	Y	Y	Y	Y	FA	Y	Y	Y	Y	Elsevier	1	1.328	XMLDW + QVT

ED: Encrypted Data I: Implementation Performed, CI: Security at Computation Independent Model Level, AC: Security Audit Control, Ex: Extendibility on New Security Requirement, PI: Security at Platform Independent Model, Tr: Transformation from model to model, PS: Platform Specific Security Model creation, QVT: Query-View-Transform support, ID: Integration of Multi-Platform Data, P: Publication, Cit: Number of Citations, IF: Impact Factor, PY: Publication Year, SC: Solution Category, SA: Semi-Automatic, FA: Fully-Automatic, MDA: Model driven Architecture, UML: Unified Modeling Language, QVT: Query/View/Transform, CWM: Common Warehouse Meta Model, SSAS: SQL Server Analysis Service, ADM: Architecture Driven Modernization, SPEM: Software Process Engineering Meta Model, RBAC: Role Based Access Control, XML: XML Based Data Warehouse, MAC: Mandatory Access Control, MDD: Model Driven Development, Y: Yes, N: No

Below we observe the graphical analysis of the security considerations by the articles in the consolidated manner.

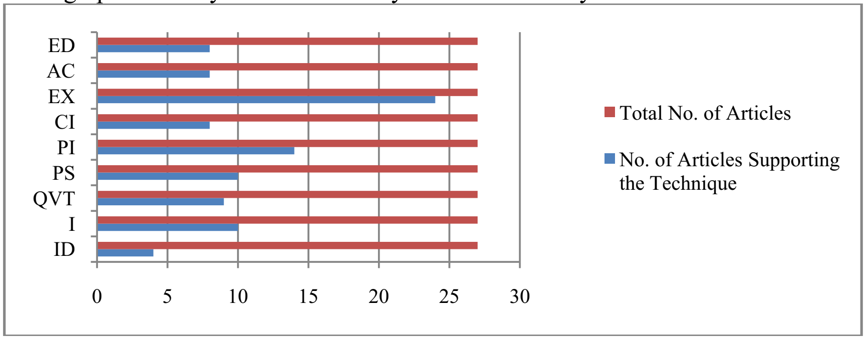

Fig. 1.Number of articles supporting different security techniques

It can be inferred from figure 1, that although most of the articles supports extendibility, but less than half has given support to audit control and security at computational independent (CI) model. It is also noticed that most of the articles supports extendibility and platform independence security.

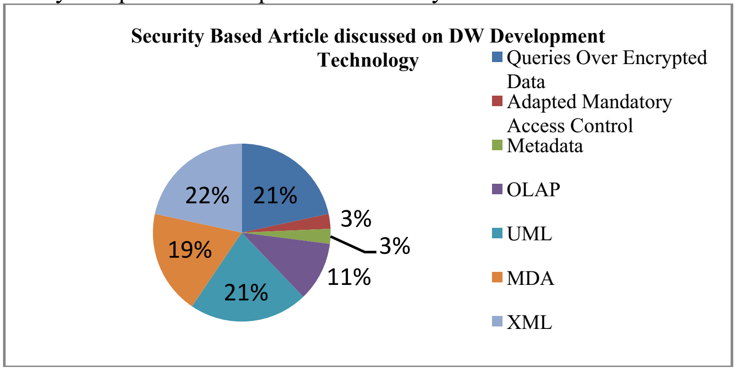

Fig. 2. Percentage of articles discussing security on basis of DW development technology

In Figure 2, it is easily noticeable that almost 32% articles belong to OLAP and UML whereas other category forms 68% only. Out of this 68%, 21% each goes to UML and Encrypted Data Queries based techniques and 19% articles belong to MDA. The old techniques like Adapted Mandatory Access control is not discussed with the advent of new DW development techniques.

6. Summary and Conclusion

In order to summarize the whole security aspects of the Data Warehouse, Let's first answer the research questions:
2(1): Out of the 6 major technological changes in the DW, every category has seen a major change in the security approach. This is because of the fact that each category has its own security requirements and applicability. However the data encryption which has not been considered in DW can be used further to strengthen the security along with the individual access control strategy adopted.
2(2): Ontology based DW are the upcoming research area in field of DW, so there is requirement of assessing the security aspects of Ontology based DW. In this area there is greater scope of research to extend an XML based access control to support ontology based structure. There is further scope of including the encrypted data feature in order to make is suitable for the usage over cloud environment.
2(3): Out of 19 security approaches, it has been observed 8 deal with audit control, 16 support extendibility, 8 support computational independent, and 14 support platform independent model, 10 has provided platform specific model creation. Out of all articles, only one has been able to achieve all the security goals considered.
It can be concluded with the statement that lot of effort has been made in DW security. But still the security of Data Warehouses is an open area, as proposal to use ontology to develop Data Warehouse has also been coined recently [Pardillo & Jose-Norberto, 2011]. The technological changes such as advent of XML and Ontology based Data Warehouse has posed new challenges which can be addressed in the further research.

References

1. Inmon, W. H. (1991). Building the Data Warehouse. Wiley and Sons.
2. Inmon, W. H. (2005). Building the Data Warehouse. Wiley.
3. Inmon, W. H. (2006). DW 2.0-Architecture for the next generation of data warehousing. DMReview. DM Direct Newsletter.
4. Caserta, J., & Kimball, R. (1998). The Data Warehouse ETL Toolkit Practical Techniques for Extracting, Cleaning, Conforming, and Delivering Data. Wiley Publications.
5. Becker, B., Kimball, R., Mundy, J., Ross, M., & Thorthwaite, W. (2008). The Data Warehousing Lifecycle Toolkit. John Wiley & Sons.
6. Kirkgoze, R., Katic, N., Stolba, M., &Tjoa, A. (1997). A security concept for OLAP. Database and Expert Systems Applications (DEXA), proceedings Eighth International Workshop. IEEE.
7. Katic, N., Quirchmay, G., Schiefer, J., Stolba, M.,& Tjoa,A. (1998). A prototype model for data warehouse security based on metadata, Database and Expert Systems Applications (DEXA), Proceedings Ninth International Workshop. IEEE.
8. Berson, A., & Smith, J. S. (1997). Data Warehousing, Data Mining & OLAP. McGraw-Hill Series on Data Warehousing and Data Management.
9. Santos, R., Bernardino, J., & Vieira, M. (2011). A survey on data security in data warehousing: Issues, challenges and opportunities. EUROCON - International Conference on Computer as a Tool (EUROCON), pp. 1-4. IEEE.
10. Kimball, R. (1997). Hackers, Crackers, and Spook, Ensuring that your data warehouse is secure. In Journal DBMS, vol. 10, no. 1, pp. 14-16.
11. Rosenthal, A., Sciore, E., Doshi, V. (1999). Security Administration for Federations, Warehouses, and other Derived Data. In Database Security, IFIP 11.3.
12. Cognos Incorporated. (1998). Schrittweise Anleitungen for Transformer. Cognos Power-Play Version 6.0.
13. Microsoft Corporation. (1999). Microsoft SQL Server OLAP Services Cell-level. Security White-paper.
14. MicroStrategy Incorporated. (2000). MicroStrategy. 7 Administrator Guide.
15. Oracle Corporation. (1998). Oracle Express Database Administration Guide. Release 6.2, Part No. A59962-01.
16. Chase, D., Spofford, G., & Thomsen, E. (1999). Microsoft OLAP Solutions, John Wiley & Sons, Inc., New York.
17. Blaschka, M., Dinter, B., Höfling, G., & Sapia, C. (1999). Extending the E/R Model for the Multidimensional Paradigm. Advances in Database Technologies, LNCS vol. 1552. Springer.
18. Booch, G., Jacobson, I., Rumbaugh, J. (1999). The Unified Modeling Language Reference Manual. Addison-Wesley.

19. Jurjens, J. (2002). UMLsec: extending UML for secure systems development. UML 2002-the unified modeling language, model engineering, concepts and tools, LNCS, vol. 2460, pp. 412-425. Springer Berlin Heidelberg.
20. Eduardo, F., Juan, T., Mario, P.,Rodolfo, V. (2004). Extending UML for designing secure data warehouses. Conceptual Modeling–ER 2004, LNCS, vol. 3288, pp. 217-230. Springer Berlin Heidelberg.
21. Fernandez-Medina, E., Piattini, M., Trujillo, J., & Villarroel, R. (2005). A UML profile for designing secure data warehouses, Latin America Transactions, vol.3, no.1, pp. 40-48. IEEE.
22. Emilio, S., Eduardo, F., Juan, T., Mario, P., & Rodolfo, V. (2006). Using UML Packages for Designing Secure Data Warehouses. Computational Science and Its Applications - ICCSA, LNCS, vol. 3982, pp. 1024-1034. Springer.
23. Eduardo, F., Juan, T., & Rodolfo, V. (2006). A UML 2.0/OCL extension for designing secure data warehouses. Journal of Research and Practice in Information Technology 38.1, pp. 31-44.
24. Eduardo, F., Juan, T., Rodolfo, V.,& Mario, P. (2007). Developing secure data warehouses with a UML extension. Information Systems, vol. 32, no. 6, pp. 826–856. Elsevier.
25. Emilio, S., Eduardo, F., Juan, T., & Mario, P. (2009). A UML 2.0 profile to define security requirements for Data Warehouses. Computer Standards & Interfaces, vol. 31, no. 5, pp. 969-983. Elsevier.
26. Ali, S., Hanêne, B., Nouria, H., Omar, B., & Salah, T. (2012). Verification of Security Coherence in Data Warehouse Designs, Trust, Privacy and Security in Digital Business. LNCS, vol. 7449, pp. 207-213. Springer.
27. Miller, J., & Mukerji, J. (2003). MDA Guide Version 1.0.1. OMG.
28. Bast, W., Kleppe, A., & Warmer, J. (2003). MDA Explained: The Model Driven Architecture: Practice and Promise. Addison-Wesley Professional.
29. Eduardo, F., Emilio, S., Juan, T., & Mario, P. (2007). A Framework for the Development of Secure Data Warehouses based on MDA and QVT.In: Second International Conference on Availability, Reliability and Security (ARES). IEEE.
30. Auguston, M., Burt, C.C., Bryant, B.R., Raje, R.R., & Olson, A.M. (2003). Model Driven Security: Unification of Authorization Models for Fine-Grain Access Control. In: Proc. Seventh International Conference on Enterprise Distributed Object Computing (EDOC'03), pp. 159-171. IEEE.
31. Basin, D., Doser, J., & Lodderstedt, T. (2006). Model Driven Security: From UML models to access control Infrastructures. ACM Transactions on Software Engineering and Methodology (TOSEM), vol. 15, no. 1.
32. Karpagam, G. R., & Sivanandam, S. N. (2004). A Novel approach for Implementing Security services. Academic Open Internet Journal, vol. 13.
33. Schreiner, R., & Lang, U. (2004). OpenPMF: A Model-Driven Security Framework for Distributed Systems. Proceedings ISSE'04 - Securing Electronic Business Processes. Teubner Verlag, pp. 138-147. Springer.
34. Jose, M., & Juan, T. (2008). An MDA approach for the development of data warehouses. Decision Support Systems, vol. 45, no. 1, pp. 41-58. Elsevier.
35. Emilio, S., Eduardo, F., Juan, T.,& Mario, P. (2008). Building a secure star schema in data warehouses by an extension of the relational package from CWM. Computer Standards & Interfaces, vol. 30, no. 6, pp. 341-350. Elsevier.
36. Carlos, B., Eduardo, F., Ignacio, G., Juan, T.,& Mario, P. (2008). Automatic Generation of Secure Multidimensional Code for Data Warehouses: An MDA Approach. In: On the Move to Meaningful Internet Systems: OTM 2008, LNCS, vol. 5332, pp. 1052-1068. Springer.
37. Arnulfo, H., Carlos, B., Eduardo, Juan, T., & Ricardo, P. (2009). Towards a modernization process for Secure Data Warehouses. Data, LNCS, vol. 569, pp. 24-35, Springer Berlin Heidelberg.
38. Blanco, C., Eduardo, F., Juan, T., & Mario, P. (2009). Data Warehouse Security. Encyclopedia of Database Systems, pp. 675-679. Springer US.
39. Emilio, S., Eduardo, F., Juan, T., & Mario, P. (2009). An engineering process for developing Secure Data Warehouses. Information and Software Technology, vol. 51, no. 6, pp. 1033-1051. Elsevier.
40. Xiao, L. (2009). An adaptive security model using agent-oriented MDA. Information and Software Technology, vol. 51, no. 5, pp. 933-955. Elsevier.
41. Alfonso, R., Ignacio, G., Eduardo, F., & Mario, P. (2010). Semi-formal transformation of secure business processes into analysis class and use case models: An MDA approach. Information and Software Technology, vol. 52, no. 9, pp. 945-971. Elsevier.
42. Feng, J., Li, G., &Ta, N. (2008). A Semantic Cache Framework for Secure XML Queries. Journal of Computer Science and Technology, vol. 23, no. 6, pp. 988-997. Springer.
43. Elelhart, A., Fenz, S., Goluch, G., Sttinkellner, M., & Weipppi, E. (2008). XML Security — A Comparative Literature Review. Journal of System and Software, vol. 81, no. 10, pp. 1715-1724. Elsevier.
44. Ravat, F., Teste, O., Tournier, R., & Zurfluh, G. (2010). Finding an application-appropriate model for XML data warehouses. Information Systems, vol. 35, no. 6, pp. 662-687. Elsevier.
45. Blanco, C., Fernández-Medina, E., Trujillo, J., Marcos, E., Mazón, J., & Vela, B. (2013). Development of Secure XML Data Warehouses with QVT. Information and Software Technology, vol. 55, no. 9, pp. 1651-1677. Elsevier.
46. Dhillon G. (2000). Information security management: Global challenges in the new millennium. IGI Global.

47. Clifton, C., Jajodia, S., Lin, T., Samarati, L., Schlipper, L.,& Thuraisingham, B. (1997). Security issues in data warehousing and data mining: panel discussion. In: proc. of the IFIP TC11 WG 11.3 Eleventh International Conference on Database Security XI: Status and Prospects. Chapman & Hall Ltd.
48. Giorgini, P., & Mouratidis, H. (2006). Integrating Security and Software Engineering: Advances and Future Vision. IGI Global.
49. Iyer, S., Kantarcioglu, M., & Thuraisingham, B. (2007). Extended RBAC-based design and implementation for a secure data warehouse. Int'l Journal of Business Intelligence and Data Mining (IJBIDM). vol. 2, no.4, pp. 367-382.
50. Belén, V., Carlos, B., Ciudad, R., & Eduardo, F. (2010).Model driven development of secure XML data warehouses: a case study. In: proceeding EDBT '10. ACM.
51. Belén, V., Carlos, B., Eduardo, F.,& Esperanza, M. (2012). A practical application of our MDD approach for modeling secure XML data warehouses. Decision Support Systems, vol. 52, no.4, pp. 899-925. Elsevier.
52. Alfredo, C., & Elisa B. (2011). Privacy Preserving OLAP over Distributed XML Data: A Theoretically-Sound Secure-Multiparty-Computation Approach. Journal of Computer and System Sciences, vol. 77, no. 6, pp. 965–987. Elsevier.
53. Dongchan, A., & Seog, P. (2011). Efficient access control labeling scheme for secure XML query processing. Computer Standards & Interfaces, vol. 33, no. 5, pp. 439–447.Elsevier.
54. Pardillo, J., & Jose-Norberto, M. (2011). Using ontologies for the design of data warehouses. Journal of Database Management, vol. 3, no. 2. IGI Global.
55. Keele S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
56. Amagasa, T., Kadhem, H., & Kitagawa, H. (2009). A novel framework for database security based on mixed cryptography. In Internet and Web Applications and Services. ICIW'09. Fourth International Conference, pp. 163-170. IEEE.
57. Canim, M., Hore, B., Kantarcioglu, M., & Mehrotra, S. (2012). Secure multidimensional range queries over outsourced data. The VLDB Journal—The International Journal on Very Large Data Bases, vol. 21, no. 3, pp. 333-358.
58. Amagasa, T., Kadhem, H., & Kitagawa, H. (2013). Optimization Techniques for Range Queries in the Multivalued-partial Order Preserving Encryption Scheme. In Knowledge Discovery, Knowledge Engineering and Knowledge Management, pp. 338-353. Springer Berlin Heidelberg.
59. Liu, D., & Wang, S. (2012). Programmable order-preserving secure index for encrypted database query. In Cloud Computing (CLOUD), IEEE 5th International Conference, pp. 502-509. IEEE.
60. Balakrishnan, H. Popa, R. A., Redfield, C., & Zeldovich, N., (2012). CryptDB: Processing queries on an encrypted database. Communications of the ACM, vol. 55, no. 9, pp. 103-111.
61. Liu, D. (2014). Securing Outsourced Databases in the Cloud. In Security, Privacy and Trust in Cloud Systems, pp. 259-282. Springer Berlin Heidelberg.
62. Liu, Z., Li, J., Li, J., Jia, C., Yang, J., & Yuan, K. (2014). SQL-Based Fuzzy Query Mechanism Over Encrypted Database. International Journal of Data Warehousing and Mining (IJDWM), vol.10, no.4, pp. 71-87.
63. Ciferri, R. R., de Aguiar Ciferri, C. D., Lopes, C. C., Matwin, S., & Times, V. C. (2014). Processing OLAP queries over an encrypted data warehouse stored in the cloud. In Data Warehousing and Knowledge Discovery, pp. 195-207. Springer International Publishing.