CÁC VẤN ĐỀ BẢO MẬT NỔI BẬT TRONG CÁC HỆ THỐNG QUẢN TRỊ DỮ LIỆU VÀ ỨNG DỤNG HIỆN ĐẠI

EMERGING SECURITY ISSUES IN MODERN DATA MANAGEMENT SYSTEMS AND APPLICATIONS

Dang Tran Khanh

Khoa Công Nghệ Thông Tin, Đại học Bách khoa, Tp. Hồ Chí Minh, Việt nam

BẢN TÓM TẮT

Những hệ thống quản trị dữ liệu có chức năng quản lý dữ liệu, trích những thông tin hữu ích từ dữ liệu và sử dụng những thông tin này nhằm hỗ trợ việc ra quyết định. Vì thế những hệ thống này bao gồm cả các hệ thống cơ sở dữ liệu, các kho dữ liệu và các hệ thống khai mỏ dữ liệu. Dữ liệu có thể thuộc dạng có cấu trúc như trong các cơ sở dữ liệu quan hệ, cũng có thể thuộc dạng bán cấu trúc hay dữ liệu XML, hoặc thậm chí là dạng không có cấu trúc như dữ liệu đa phương tiện. Hiện nay, những hệ thống quản trị dữ liệu là thành phần nòng cốt trong các hệ thống thông tin và các ứng dụng. Những hệ thống thông tin và ứng dụng này lại chính là những tài sản có giá trị nhất trong các cơ quan, doanh nghiệp. Những tiến bộ trong công nghệ Internet cùng với sự phát triển không ngừng của Web dẫn tới sự gia tăng liên tục về nhu cầu quản trị dữ liệu và thông tin. Chính điều này đã tạo nên sự cần thiết cấp bách trong việc bảo đảm an toàn cho các cơ sở dữ liệu, hệ thống thông tin và ứng dụng. Bài báo này trước hết sẽ điểm lại những vấn đề và giải pháp trong việc bảo mật của các cơ sở dữ liệu, sau đó sẽ giới thiệu những vấn đề và hướng nghiên cứu mới về bảo mật trong các hệ thống quản trị dữ liệu và ứng dụng hiện đại. Những vấn đề sẽ được thảo luận trong bài này là những vấn đề đang rất được quan tâm cả trong nghiên cứu và các ứng dụng thực tế.

ABSTRACT

Data management systems (DMSs) are systems that manage the data, extract meaningful information from the data, and put the extracted information to good use. Therefore, DMSs include database systems, data warehouses, and data mining systems. Data may be structured data like that found in relational databases, or semistructured data and XML, or even unstructured data as multimedia data. Moreover, DMSs are the core component of information systems and applications, which are among the most valuable assets in all kinds of organizations today. Advances in the Internet technologies and the continued growth of the Web result in the increasing demand for data and information management. This, in turn, introduces a critical need for maintaining the security of the databases, applications and information systems. In this paper, we review the developments in database security, then present emerging security issues in modern DMSs and applications. Our discussions include most active topics in the research community as well as real-world application areas.

1. INTRODUCTION

Data and information have become a critical resource in many organizations and therefore not only efficiently managing this resource is important, but protecting it from unauthorized access as well as malicious corruption is also indispensable. With the advent and continued

growth of the Web this objective is even more important as there is now so much data on the Web that needs new tools and techniques to manage effectively and numerous individuals have access to this data and information.

To facilitate data and information management, a vast number of innovations have been introduced and integrated into data management systems (DMSs) over the last few decades. In the same line as [10], here we define DMSs to be systems that manage the data, extract meaningful information from the data, and make use of the extracted information. Therefore, DMSs include database systems, data warehouses, and data mining systems. Data could be structured data such as that found in relational databases, or semistructured data and XML, or even it could be unstructured such as text, imagery, voice, and video. Moreover, DMSs are the core component of information systems and applications, which are among the most valuable assets in all kind of organizations today. Hence, identifying and dealing with security issues in DMSs and applications become crucial. First, to provide an overview of the problem, we modify a framework for DMSs and applications introduced in [10] and present it as shown in Figure 1 below.

Application	Visualization, Collaborative Computing, Mobile Computing, Knowledge-based Systems
Data Management Layer	**Layer 3: information extraction & sharing** Data Warehousing, Data Mining, Internet DBs, Collaborative, P2P & Grid Data Management
	Layer 2: interoperability & migration Heterogeneous DB Systems, Client/Server DBs, Multimedia DB Systems, Migrating Legacy DBs
	Layer 1: DB technologies DB Systems, Distributed DB Systems
Supporting Layer	Networking, Mass Storage, Agents, Grid Computing Infrastructure, Parallel & Distributed Processing, Distributed Object Management

Figure 1: Data management systems framework

In Figure 1, note that, the supporting and application layers do not belong to the DMSs framework. They may be part of information systems that include and are much broader than DMSs. The DMSs framework consists of three layers: Layer 1 consists of fundamental database technologies; layer 2 consists of interconnection and interoperability of databases as well as migration of legacy databases; and layer 3 is about information extraction and sharing. Essentially, layer 3 consists of technologies for some newer services supported by DMSs.

As we can see, the DMSs framework includes both traditional and modern data and information management technologies. The application technologies layer consists of systems, as collaborative computing systems and knowledge-based systems, that may utilize DMSs. Among a large number of features badly needed for application systems utilizing data management technologies, there are lots of security-related features posed. Specially, some of them that relate to modern DMSs and applications are still open and need much more research efforts. To have the first view of security issues in such systems, we present in Figure 2 a framework for database and applications security technologies.

Applications Security Technologies	Privacy, Dependable Information Management, Secure Information Management Technologies, Data Mining and Security, Digital Forensics, Secure Knowledge Management Technologies, Secure Semantic Web, Biometrics
Database Security Technologies	Relational DB Security, Distributed/Federated DB Security, Web DB Security, Object/Multimedia DB Security, Data Warehouse Security, Inference Problem, Sensor DB and Stream Data Processing Security

Figure 2: Database and applications security technologies

The above security technologies range from fundamental database systems such as relational databases to emerging applications like semantic Web and dependable information management systems. They can be employed for DMSs and systems in the application layer of the framework shown in Figure 1. We will elaborate on these security technologies in the context of DMSs and applications in later sections.

The rest of this paper is organized as followed: Section 2 reviews core security technologies for fundamental database systems. In section 3, we introduce and discuss emerging security issues in modern DMS and

applications. Section 4 discusses relevant problems and introduces notable related work. Section 5 presents concluding remarks for the paper.

2. BASIC SECURITY TECHNOLOGIES FOR DATABASE SYSTEMS

Database (DB) security encompasses a set of measures, policies and mechanisms to provide secrecy, integrity and availability of data and to combat possible threats from insiders and outsiders, both malicious and accidental [1]. Many security models for DB systems have been introduced in the literature. DB security models can be classified into two categories: discretionary and mandatory models.

Besides, despite the security models, the inference problem that exists for all types of database systems has been extensively studied. The inference problem is the process of posing queries and deducing unauthorized information from the legitimate responses received [10]. Furthermore, for multiple purposes including security ones, DBs also need to be audited. We will discuss in more detail the two DB security models, the inference problem and DB audit problem below.

2.1 Discretionary security

Discretionary security deals with granting access to the data on the basis of users' identity and of rules that specify the types of access each user is allowed for each object in the system. Basically, the types of access include read and write operations on objects existing in a DB system. A user's request to access an object is checked against the specified authorizations: if there exists an authorization stating that the user can access the object in the required mode, the access is granted, otherwise it is denied.

Before designing any secure systems, the first question that must be answered is about security policy. Essentially, security policy is a set of rules that enforce security. The most popular discretionary security policy is the access control (AC) policy. The AC policies were initially studied for DB systems in the 1970s and most commercial strength DBMSs nowadays utilize the AC policy. Of late, discretionary security also includes complex security policies, granting access to data based on roles and functions (RBAC: role based access control), and also both positive as well as negative authorization policies.

In principle, identification and authentication are the first procedure for a discretionary access control (DAC) system. Identification is the means by which a user claims who s/he is. Authentication is the means of establishing the validity of this claim. There are three means of authenticating a user's identity which can be used alone or in combination: (1) something the user *knows* (e.g., a password, PIN); (2) something the user *possesses* (e.g., an ATM card); and (3) something the user *is* (e.g., a voice pattern, a fingerprint). Based on a user's authentication, the system will be able to decide what operations s/he can do on which objects (authorization). More detailed information of identification and authorization technologies can be found in [12, 8].

In addition, discretionary security policies and mechanisms applied to relational DB systems can also be extended to apply to both object-oriented and object-relational DB systems. Again, this is also true for both centralized and distributed database systems. A lot of work has been shown in the literature detailing the above problems. More detailed discussions about security for all of these systems are beyond the scope of this paper. The sheer volume of relevant information can be found in [1, 12, 10].

Overall, protection policies in discretionary security models are flexible and therefore suitable for various types of commercial systems and applications. However, discretionary access control policies have a drawback: dissemination of information is not controlled. That means it is possible for a user who is not authorized to read and acquire data in spite of the discretionary control. This makes discretionary control vulnerable to malicious attacks like Trojan Horses embedded in programs. This problem was identified and tried to solve by a number of researchers before (see [1] for details). However, it still needs more attention, especially

as discretionary security model are applying to emerging DMSs and applications. Interestingly, this problem does not happen to mandatory security models.

2.2 Mandatory security

Mandatory security deals with granting access to the data on the basis of users' clearance level and the sensitivity level of the data. Users and data are considered as *subjects* and *objects*, individually, in the mandatory model. Each subject is assigned a security level named *clearance*, and each object is assigned a *security level*. The clearance assigned to a subject reflects the subject's trustworthiness not to disclose sensitive information to individuals who do not hold the appropriate clearance. Processes activated by a user will be assigned the security level of that user. The security level of an object reflects the sensitivity of the information stored therein. Objects are passive entities and subjects are active entities that access objects. A subject is granted access to an object with respect to the access mode if some relationship is satisfied between the security level of the subject and object. A lots of research work has been carried out to develop mandatory security policies/mechanisms, resulting a great deal of mandatory security models (see [1]). One of the most well-known mandatory model is Bell-LaPadula model. This model introduced two principles that have been adopted by all models applying a mandatory policy for information protection: no read-up and no write-down secrecy. More concretely, a subject can only read objects whose security level is dominated by the subject's clearance, and a subject can only write objects whose security level dominates the subject's clearance.

There are many work has been done to apply mandatory security to not only relational DB systems, but also other DB systems such as object-oriented and object-relational DB systems (both centralized and distributed systems), deductive, parallel DB systems, etc. Today we have many new technologies including data warehousing, multimedia systems, E-commerce systems, semantic Web, etc. (cf. section 3). However, just a few number of efforts have been reported on investigating mandatory (multilevel) security for the emerging DMSs. One of main reasons is that this problem is very hard: it is even not well-solved for the famous relational data model. As the system becomes more complicated, developing high-level assurance multilevel systems becomes an enormous challenge [10].

2.3 Inference problem

In our context, inference is the process of posing queries and deducing new information from the returned results. If the deduced information is something that the user is not authorized to know, then it becomes a problem of great concern. Although this problem appears in all DB systems, it is mainly a considerable problem in multilevel/mandatory security DBMSs (MLS/DBMSs, for short).

In fact, the inference problem was initially studied extensively in statistical DBs. For example, the system must ensure that aggregation query results, say, sum of salaries in EMP table, will not lead to divulge individual's information, say, Khanh's salary, by some inference. As with MLS/DBMSs, while a user with a clearance at "Secret" level can read data at the security level "Unclassified", he is not allowed to know some "Top Secret" information that can be deduced from results returned with respect to his queries posed. Figure 3 illustrates an example where users infer unauthorized information from the legitimate received results.

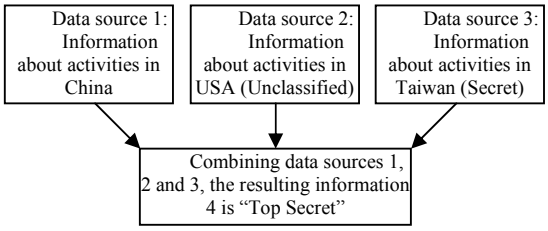

Figure 3: An inference problem example

There are two main approaches to addressing the inference problem in MLS/DBMSs: one is based on security constraints and the other based on conceptual structures. Basically, security constraints are rules that assign security levels to the data during query processing, DB updates, or DB design. On the other hand, conceptual structures are used to model and reason about an

application at the design stage in order to examine if there are potential security violations via inference. More discussions and references can be found in [10, 1].

As new technologies and applications emerge, such as data warehousing, data mining, e-health information systems, etc. the inference problem receives much more attention. We will elaborate on these new systems in following sections.

2.4 Database audit for security purposes

Auditing (and accountability) is an indispensable factor to all secure DMSs and applications. The DBs may have to be audited so that the system should be able to tell who did what, and when, and how. More importantly, by means of auditing, unauthorized access to data can be monitored. With the support of new technologies as data mining that can help analyze log data and find users' abnormal activities, audit data becomes a valuable asset for security. In addition, in this digital age, due to the increase in e-commerce of the use of digital signatures, the ability to provide proof of the origin or delivery of data (the non-repudiation problem) has gained popularity. This makes auditing and accountability (not only for DBs) more important. We will come back to these issues in section 3.2.

3. EMERGING SECURITY ISSUES IN MODERN DATA MANAGEMENT SYSTEMS AND APPLICATIONS

3.1 Secure Multimedia Systems

Multimedia data includes text, imagery, voice, and video data. Data could be in the form of streams such as image data from surveillance systems. Many of the multimedia DMSs are based on the variation of the object model. Some of recent systems such as Oracle are based on the object-relational data model. Securing multimedia DMSs is a critical need but still immature in spite of several efforts in the past.

Basically, security techniques for DB systems can be applied to multimedia database systems. Multimedia data, however, is more complex and thus there is still much more to be done on developing security policies, architectures, and query strategies. For example, assume that we are using mandatory security for the system, should we classify the entire video or just certain frames? Can we classify the pixels in an image? How can we classify a composite multimedia object where the components are at different levels?, etc. Furthermore, although numerous access methods (index strategies) have been developed for multimedia data (see, e.g., [2]), the security impact of access methods on multimedia data is not determined yet. Specially, with some special systems, say, video cameras, privacy also needs to be ensured. Who are allowed to see what (and when) is also a problem of great concern today. We need to ensure that individuals' privacy is protected. Besides, dealing with the inference problem, managing metadata and distributed multimedia DMSs are also much more complicated. These problems all are even exacerbated as new kinds of multimedia systems such as geospatial information systems emerge. For instance, geospatial data may be in the form of streams, so what are the security policies for stream data? (we will further discuss security for stream data processing later in section 3.5). Geospatial data may also emanate from a variety of sources and has to be integrated. However, data/information integration still has lots of security challenges that have not been solved yet.

3.2 Data Warehousing and Data Mining: Security and Privacy Issues

In this section we discuss security for data warehouses (DWs), and data mining (DM) applications for security purposes. Then we present impact of DWs and DM on the inference and privacy problems as well as propose related research directions.

DWs and DM are among the latest directions in DB systems [11]. DWs are one of the key data management technologies to support DM, information integration, and other decision support systems (DSS). Essentially DWs bring together the data from heterogeneous sources to provide users with a better means of querying and synthesizing information. DWs therefore provide support for the decision

support of an enterprise. In order for DWs to be useful in many applications, they must be secure. The security policies of a DW must include all security policies enforced by the back-end data sources and, possibly, additional security properties. Data in a DW is often viewed differently by different applications and different security policies may be enforced at different levels.

It is easy to observe that security cuts across all layers and operations of the DW, including secure heterogeneous database integration, statistical DBs, secure access methods, secure metadata management, etc. (see [10] for the details). Despite the sheer volume of work has been done, there are still many open or unwell-solved security issues in data warehousing systems. Just to name a few: How can we integrate different security models/policies from heterogeneous sources to a DW? What is the security impact on update propagation? How can we address the inference and privacy problems effectively as data warehousing and data mining come together or as secure multimedia data sources being integrated to form a DW?, etc.

DM is a process of extracting previously unknown, valid, and actionable information from large sets of data, say, a DW. DM has many applications for security, including both homeland security (e.g., counter-terrorism) and cyber-security. A concrete example among DM applications for cyber-security is *fraud detection* problem: DM techniques can help discover which insurance claims, cellular phone calls, or credit card purchases are likely to be fraudulent. Most credit card issuers now use data mining softwares to model credit fraud. There is rich information about DM applications available in the literature and on the Web.

In fact, DM applications for security have just become an active research topic very recently. However, its impact is very broad, including some emerging security applications such as counter-terrorism, digital forensics. As with digital forensics, for instance, as a computer crime is committed, every piece of evidence should be gathered by analyzing audit data (logs files) as well as building profiles of criminal activities and using DM techniques for further examination. In such cases, audit data takes a critical role. This again emphasizes our discussions in section 2.4. An interesting discussion about DM applications for counter-terrorism and other homeland security problems are also presented in [10].

As discussed above, thanks to DM techniques, users can now make all kinds of correlations and a plenty of applications can make use of these DM techniques. However, although DM is beneficial in many cases, it also raises lots of privacy concerns: With many DM techniques and tools currently available, together with all kinds of correlations that users can now deduce, the inference problem obviously becomes worse. To face this problem, there are some very recent work on privacy-preserving DM [13]. Specially, EU is also funding a very big project, the PRIME project [8], to deal with privacy and identity management for Europe. Even then, the question "what is the complexity of the privacy problem?" is still open inasmuch as the answer is quite different, depending not only on technology, but also on sociology and politics.

3.3 Secure Web Data and E-Commerce

With the continued and fast growth of the Web and its vitally important role in today e-commerce applications, securing Web data obviously becomes a crucial need. Protecting the traditional Web was discussed in previous literature (see, e.g., [12]). In this section we focus on the problem of securing Web data for the next generation Web and emerging applications. In particular, we will discuss security issues for XML data and semantic Web, multimedia data on the Web (digital rights management), and modern Web-related applications like Web services, digital identity management systems, and so on.

Semantic Web is among the most "hot" topics in the field today. It is an extension of the current Web in which information is given well-defined meaning, better enabling computers and people to work in cooperation [14]. A semantic Web can be thought of as a Web that is highly intelligent and sophisticated so that people need little or no human intervention to carry out tasks such as searching for complex documents,

scheduling appointments, integrating disparate DBs and information systems, etc. The *basic* components of semantic Web include (1) XML and its family members (DTD, XSL, XML schema, query language, etc.) to define, store, and exchange structured data; (2) DOM (document object model) to manipulate XML data through programs; and (3) RDF (resource description framework) and ontology to define the metadata for the Web. Although quite a lot of research activities have been done to secure these basic components, say, access control policies, XML-encryption, XML-signature, etc. (see [14, 12, 10] for more details), much research is still needed on securing XML documents and semantic Web. Some of the most important work are as follows: How can we express security constraints in RDF? What are the security implications of statements about statements? How can we protect RDF schema? How do we use ontologies (with different security levels) for secure information integration? How do we provide access control for ontologies? Do we have ontologies for specifying the security policies? How do we incorporate constructs for trust management and negotiation into XML and RDF?, etc.

Furthermore, Web data is generally in the form of multimedia data such as text, imagery, voice and video. The sheer volume of data is now available to every people. Even so, data in many situations needs to be protect from being copied and disseminated illegally. For example, songs (MP3, audio, etc.), e-learning and digital library materials need to be protect from being scattered illegitimately. This problem is named copyright protection problem. Although many techniques, say, *digital watermarking* techniques, have been developed for digital right management with respect to multimedia data, we need new techniques for non-multimedia data or new data types like XML, stream data (cf. section 3.5).

As with the next generation Web and especially the advent of XML, Web services are taking off. Currently, this area is getting the strong support and adoption by the industry (Microsoft, Sun, IBM, Oracle, and numerous others). Naturally, Web services security is of great interest and the interest in this activity is growing with time [12]. Although Web service security has been carried out, we still need more efforts to protect the Web services from new types of denial of service (DoS) attacks (against UDDI-universal description, discovery and integration, for example), or from being subverted by malicious processes, and so on.

One of the most important things that is needed for many e-commerce applications (and daily tasks) is the digital identity. As a result, digital identity management has emerged as an important area in information security. Secure identity management is essential for preventing identity theft. The person who steals the identity can masquerade as the owner and take advantage of all the benefits that the owner has. This problem, in turn, relates to many other security problems such as non-repudiation, digital forensics and privacy problems. Privacy and digital identity management is also getting much attention from many organizations (cf. section 3.2).

Apart from the above discussions, there are many other Web-related applications need to incorporate security technologies at both database and application levels: digital libraries, e-healthcare information systems, knowledge management systems, e-mail security (spam, "spoof" emails), etc. We will also need to further examine solutions to security issues for such systems.

3.4 Collaborative, Peer-to-Peer and Grid Data Management

Collaborative data management is about people working collaboratively on projects and sharing resources. Peer-to-peer data management is about nodes on the network acting as peers and working together to carry out a task. A node will communicate with its peers in case more resources are needed for the task. More recently, Grid computing has got much attention from the research community [5, 6]. The idea is to utilize clusters of computing systems including DB systems to conduct various functions in parallel. The main challenge is to efficiently allocate computing resources to various tasks of high-performance computing applications. The concept "Grid data management" closely relates to the resource allocation but is much wider [15]. In fact, there

has been several discussions recently about the similarities and differences between various terms such as federated, collaborative, Grid, and peer-to-peer data management. More concrete discussions about Grids and links to the sheer volume of resources can be found in [5].

Despite some possible differences, in terms of security, Grid data management has many similarities with those of collaborative and peer-to-peer data management. Specially, for all of these systems, the security impact on various data management functions like query processing, transaction and metadata management has to be examined. In addition to security, trust and privacy issues also raise many concerns: How do we secure our data and applications being processed and run in other computing systems (Grids)? How much does a node trust its peer? How can a node privacy be maintained? How can we effectively secure workflow and collaboration?, just to name a few. As we can see above, trust and negotiation systems will also take an important role here.

In concluding this section, we present a new security research topic related to Grid data management: secure semantic Grid. Similarly to semantic Web, the semantic Grid is an extension of the current Grid in which information and services are given well-defined meaning, better enabling computers and people to work in cooperation [9]. To make it clearer, Figure 4 illustrates the relationship between semantic Web and Grid, classical Web and Grid. Although there are some initials for securing semantic Web, security for the semantic Grid is still not investigated yet.

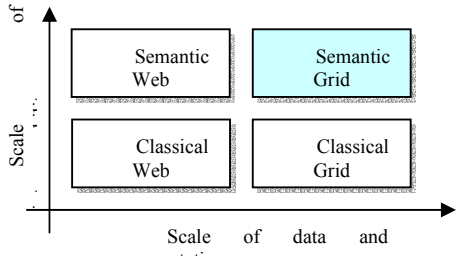

Figure 4: Semantic Grid position [9]

3.5 Stream Data Processing

Stream data processing was predicted to be one among new directions in database research [11] and it turns out to be true now. Stream data may come from many sources: sensors (e.g., video cameras and surveillance/alarm systems), telecommunication networks (e.g., mobile phones, PDAs), internet/network (e.g., monitoring Web hits, network traffic for dynamic intrusion detection), etc. Security issues in stream DMSs are quite new, including confidentiality where sensitive information about individuals is protected, secrecy where individuals can only access the data they are authorized to know, and integrity where unauthorized modifications to the data are prohibited. In the context of security, there is just little research carried out for stream data management. First of all, the privacy problem is of great concern. DM can also be used to detect, for example, intrusions in sensor networks. But DM, as mentioned before, exacerbates the inference and privacy problems. Second, merging data streams from different sources, say, at Classified and Unclassified levels, may also cause security violations. As with mobile devices, many security issues in location-based services have been raised such as how can the user's exact location be "hidden", while s/he can still get correct location-based information from the system? how can the user be dynamically authenticated with respect to his/her location?, and many more. Much more research work is needed for this area.

To conclude this section, we consider two special aspects of sensor data management. First, encryption is critical for communicating data across sensors as well as storing the data in sensor DBs. Of late, querying encrypted data, especially as the data is stored at untrusted servers, is getting some attention [3, 4]. Such techniques need to be further examined for querying encrypted sensor data. Second, in some cases, sensors act as peers and share information with each other. The question is "how much do sensors trust each other"? Trust management techniques [7] are apparently needed and must be further investigated.

4. DISCUSSIONS AND RELATED WORK

Security issues and countermeasures usually come up with the development of technologies. In our context, new security issues arise as new

directions in database systems (and data management technologies in common) emerge. All of our above discussions also follow emerging directions in data management systems and applications [11].

In a very recent work [10], Thuraisingham has given a quite comprehensive overview of database and applications security, where security issues in almost current and predictable future data management systems are covered. Remarkably, the author also discussed dependable data management, including a description of data quality related issues – an increasingly important aspect requiring comprehensive solutions related to data security. Another notable work published earlier by Umar [12] also discussed many security issues and approaches as well as many case studies for information security and auditing in the digital age. These resources are a good starting point for any people who want to work on data and information security. However, because the field is expanding rapidly and there are many developments in the field, we also have to keep up with the developments including reading about commercial products.

5. CONCLUDING REMARKS

Dealing with security issues in modern data management systems (DMSs) and applications becomes a critical need. In this paper, we briefly reviewed the developments in database security and discussed emerging security issues in DMSs and applications. Our discussions covered the most active topics in both research community and real-world application domains, including security issues for multimedia systems, security and privacy problems in data warehouses and data mining, secure Web data management and e-commerce, secure collaborative, peer-to-peer and Grid data management, and security issues in stream data processing. The list is of course not exhausted and we encourage interested readers to get further information from the references and related resources.

REFERENCES

1. S. Castano, M.G. Fugini, G. Martella and P. Samarati: Database Security, Addison-Wesley and ACM Press (1995)
2. T.K. Dang: Semantic Based Similarity Searches in Database Systems (Multidimensional Access Methods, Similarity Search Algorithms), PhD thesis, FAW-Institute, Johannes Kepler University of Linz, Austria (May 2003)
3. T.K. Dang: Oblivious Search and Updates for Outsourced Tree-Structured Data on Untrusted Servers, International Journal of Computer Science and Applications (IJCSA), ISSN 0972-9038, Vol. 2, Issue 2 (June 2005), 67-84
4. T.K. Dang: Security Protocols for Outsourcing Database Services, Information & Security: An International Journal, ProCon Ltd., Sofia, ISSN 1311-1493, Vol. 18 (2005), to appear
5. The Grid Computing Information Centre (www.gridcomputing.com)
6. The Globus Alliance (www.globus.org)
7. P. Herrmann, V. Issarny, S. Shiu (eds.): Proc. of the 3rd Int. Conf. on Trust Management (iTrust2005), LNCS 3477, INRIA-Rocquencourt, France (May 2005)
8. The PRIME project: Privacy and Identity Management for Europe (www.prime-project.eu.org)
9. Semantic Grid Community Portal (www.semanticgrid.org)
10. B. Thuraisingham: Database and Applications Security: Integrating Information Security and Data Management, Auerbach Publications, Taylor & Francis Group (May 2005)
11. J.D. Ullman: A Survey of New Directions in Database Systems, Proc. of the 8th Int. Conf. on Database Systems for Advanced Applications, Kyoto, Japan, IEEE Computer Society (March 2003)
12. A. Umar: Information Security and Auditing in the Digital Age-A Managerial and Practical Perspective, NGE Solutions, Inc. (December 2003)
13. V.S. Verykios, E. Bertino, I.N. Fovino, L.P. Provenza, Y. Saygin, Y. Theodoridis: State-of-the-art in Privacy Preserving Data Mining, SIGMOD Record 33(1): 50-57 (March 2004)

14. The World Wide Web Consortium– W3C (www.w3.org)
15. H. Stockinger, F. Donno, E. Laure, S. Muzaffar, P.Z. Kunszt, G. Andronico, A.P. Millar: Grid Data Management in Action: Experience in Running and Supporting Data Management Services in the EU DataGrid Project, the Computing Research Repository, cs.DC/0306011, (June 2003)