Technical Implementation of Visual Steganography in Structured Document based on CSS

Zhijie Liu

Information Engineering Department, Jinan 250104, China

gangster115@126.com

Abstract. This paper addressed the visual redundancy of typeface in a structured document. Achieving information embeds through modifying the appearance of words by CSS. The idea combines encryption and hiding, has widely application. Meanwhile，it has high density and safety in information hiding，and is easy to implement by software. The embedding method proposed in this paper has important guidance for the information hiding of the format text.

Introduction

With the upcoming era of Big Data the traditional way of data processing faces stem challenges. Big Date processing has many new characteristics such as high volume, variety, velocity and low density of value, which outperforms the traditional ways of searching. The only way to survive is to follow the development of the Big Data technologies and turn challenges into opportunities. [1] By better using of Big Data, the important strategic resources, mathematic models and tools can be effectively constructed to change the massive data into real useful information.

As the application of database becomes more and more popular, the security of the data attracts more eyes on it. Data security is not a single problem but a systematic scheme. This paper introduces the technology of information and database security, depicts Audit, Log miner and Trigger of database, analyzes the advantages and disadvantages of these three technologies used to monitor the operation to database. [2] What's more, this paper brings forward a practical scheme according to the instance. Together with the technology of database security, redundant backup recovery and network security, it makes an all around security system.

With the repaid development of computer technology, computer has come into many areas of modern society and everyday life. Now, in our country, a lot of information infrastructure is being under construction and many new services such as electronic competence, remote education, electronic cash, etc are supplied by Internet. [3] Due to the urgent demand on high-security DBMS and the government's policy of developing information security product, it is significant to make research on secure DBMS, both in theory and application.

Security analysis

Security analysis and attack-defense modeling are effective method to identify the vulnerabilities of information systems for proactive defense. The attack graph model reflects only attack actions and system state changes, without considering the perspective of the defenders. To assess the network information system and comprehensively show attack and defense strategies and theirs cost, a defense graph model is proposed. [4] Compared with the attack graph, the model makes some improvements. Defense graph will be mapped to the attack and defense game model, in order to provide a basis for active defense policy decision. What's more, a generation algorithm of defense graph is proposed. A representative example is provided to illustrate our models and generation algorithm. As shown in Fig. 1 and 2.
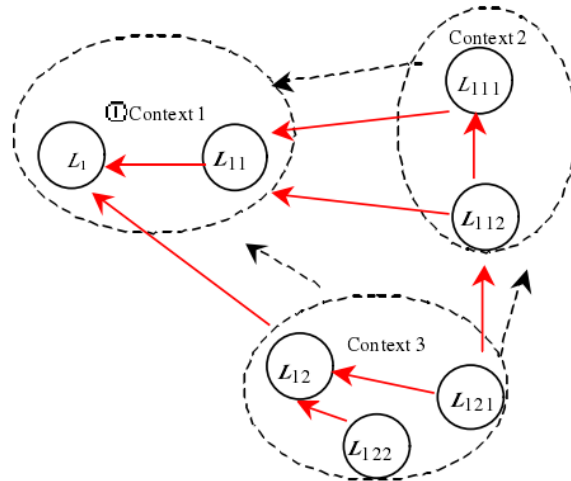
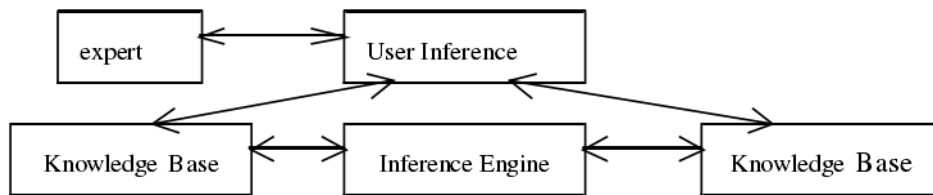Fig. 1 Context information flow/security level-context relation

Fig. 2 Database system configuration

Secure database

With the repaid development of computer technology, computer has come into many areas of modern society and everyday life. Now, in our country, a lot of information infrastructure are being under construction and many new services such as electronic competence [5], remote education, electronic cash, etc are supplied by Internet .Due to the urgent demand on high-security DBMS and the government's policy of developing information security product, it is significant to make research on secure DBMS, both in theory and application.

Based on the analysis of current access control model, the realization of mandatory access control in role-based protection system is discussed. At first, the definition of role and the application in security are discussed. Then the concept of MAC is introduced and a scheme of Role-based protection is developed, which realizes MAC by viewing each of the role contexts as a independent security-level and imposing non-cyclic information flow requirement. An application case is shown in Table 1.

Table 1 Application case

EMP_ID	Grade	location	salary
1	2	CA	8000
2	3	NY	6000
3	5	TX	5000
4	8	TX	2000
5	2	CA	7000,C
6	8	CA	2000
7	5	TX	5000,C
8	5	CA	4000
9	7	NY	3000
10	7	NY	3000

The computer suffers the attack of the external world easily. Therefore the safety of database has the higher realistic meaning and theories meanings. The security of database information becomes the key part of the modern information. Encrypted database are an effective method to realize database security. A quick index is raised in paper. But there is deficiency about security and task allocation.

Privacy homomorphism is raised to discuss this p problem in paper. A module based on privacy homomorphism is presented, and mathematic method on p privacy homomorphism is discussed. It is proved that this method is impossible in the range of the real, and a new operation must be defined.
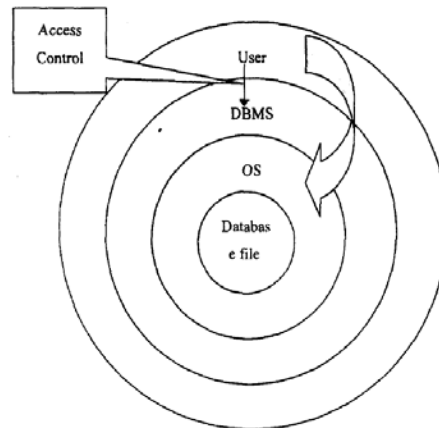

Fig. 3 Logical Database Operation

Logical Database Operation is follows as Fig. 3. In order to improve personal data security in database, and to avoid information exposing of personal privacy, personal data was used as the encrypted principle, applying homomorphism and random perturbation to strengthen personal data security. This paper analyze the usage of personal data in electronic commerce firstly, And then discuss realization security of personal data. In light of this, a new algorithm was used to acquire improved security. The proposed algorithm uses homomorphism as principle to preserve privacy. This method can make the important data to be appeared with secret content imp the web service, and prevent personal data from being misused. The simulation results proved that the modified method can protect personal privacy effectively, and can carry on data mining to provide the characteristic service for the customer, and modify Ed method has shorter response time.

Security framework

DDB is combination of computer network and database system. Communications and network technology make DDB security more complex. It is a key problem how to ensure DDB security. This paper addresses the problems of DDB security from the viewpoint of information security management, establishes an iterative DDB security framework using PDCA method, which composed of 5 basic construction unit including security demands and security risk analysis, security model establishment, security implementation, backup and fault recovery and security detection and assessment, researches the five basic construction units.
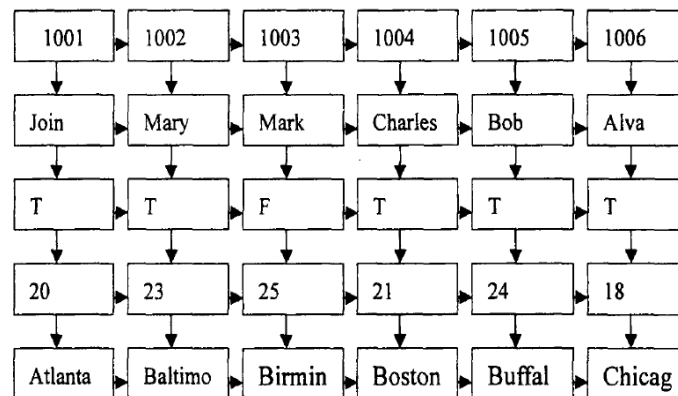

Fig. 4 Data security constructure

Data security constructure is shown in Fig. 4. This paper firstly makes DDB security determines and researches from 4 aspects: security demands, security risks, security abilities and security services. Then security model PBSM-DDB (Policy-Based Security Model of Distributed Database) is brought forward to accurately describe DDB security demands with 9 formalized regulations. In

security implementation unit 4 key features including data fragmentation and distribution, DBMS, data encryption and secure authentication are identified and researched. In the 4 unit distributed backup method and consistency of fault recovery are researched. In security detection and assessment unit a security detection method EASD-DDB (Executable Assertions-based Security Detection of DDB) is brought forward to detect DDB security at runtime. At last this paper gives a case demonstration of this framework and an expectation of farther research of this framework. Data based on encrypted is shown in Fig. 5.
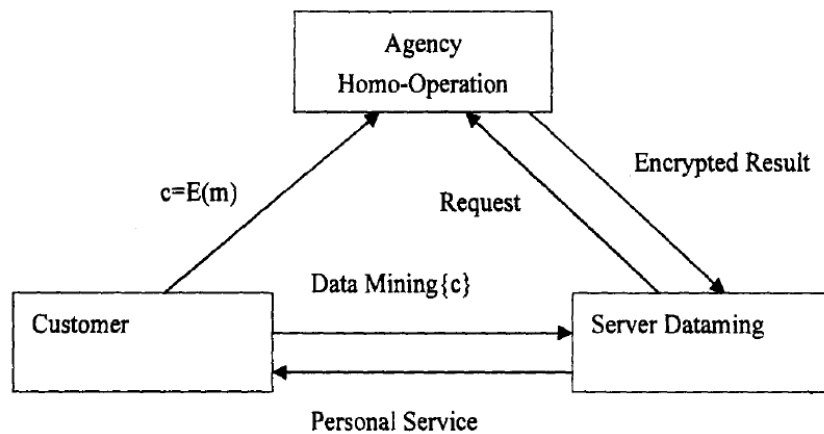

Fig. 5 Data based on encrypted

Summarily, the dissertation does a great deal of work in the aspect of studying encrypted database theory applications, while having acquired many achievements of which inject blood for secure database. Besides, these models will be further enriched and consummated. Our research, from now on, will be focused on compressively studying their theoretical foundations and exploring their applying area.

Conclusions

The most significant feature of the information age is the digitization trend evident, it can be said that the information age is the era of big data, data subtle appear in our lives, constitutes a variety of data collection. The data in some cases, it is an intangible asset, and the resulting security thinking has gradually attracted the attention of modern people. Based on our database security data security defense system formed gradually improve and play an important role in data security. In this paper, the next big data context, the establishment of a database security system for analysis, to explore the construction of our database security system, thereby contributing to the security and confidentiality of data and information.

References

[1] Jiang Wei, Fang Binxing, Tian Zhihong, et al. Evaluating network security and optimal active defense based on attack-defense game model. Chinese Journal of Computers, 2010, 32(04): 817-827. (in Chinese)

[2] Hadi O, Mona M, Chadi A, et al. Game theoretic models for detecting network intrusions. Computer Communications, 2011, 31(10):1934-1944.

[3] Theodorakopoulos G, Baras J S. Game theoretic modeling of malicious users in collaborative networks. IEEE Journal on Selected Areas in Communications, 2010, 26 (7):1317-1327.

[4] Kotenko I. Multi-agent modelling and simulation of cyber attacks and cyber-defense for homeland security. Information & Automation, 2012, 11(8):614-619.

[5] Sanhu R.S, Coyne EJ.Feinstein H L, et al. Role-based access models. IEEE Computer, 2013, 29(2): 38-47.