Digital Signing of Data in the Web-based Information Systems

D. Pilev

Abstract. Digital signing of data in the Web-based IS is one of the most secure methods for guaranteeing the authenticity of data. Storage of user keys is particularly important for this methodology. The present development proposes a new algorithm for storage and usage of user keys for the database by the digital certificate of the client. The proposed methodology was designed for protection of data in a particular information system. One of the characteristics of this system is the great number of authorized users with rights for access and modification of various parts of data. With such systems it is extremely important to guarantee the authenticity of data stored in the system. Digital signing of data provides such guarantee of their authenticity.

Key Words: Information security; digital certificate; data authentication; digital signature.

Introduction

Currently, there are numerous methods for provision of the security of data, stored in the information systems. Generally, these are related to the application, database and operation system security. Database (DB) security [1,2] is particularly important. [1] provides a description of the classical DB attacks, along with the methods for their prevention. One of the most frequently used methods for guaranteeing the security of data in the DB is the encryption [3]. It consists in using techniques for encryption, which transform the ordinary text into an encrypted one. This way, the data can only be read by those who possess the required decryption key. [4] and [5] present different methods for encryption of data in the DB, an essential problem with all of them is the storage of the decryption keys [6].

The present development proposes and implements methodology for digital signing of sensitive data, stored in the system for information provision of the academic activities in the Higher Education Institutes [7,8]. This IS is characterized by the many authorized users (teachers in specific disciplines) who have access for modification of different parts of the data. It is particularly important in such systems to authenticate the genuineness of the stored data. Furthermore, the access of each authorized user to the data is to be valid for a specific time period. This necessitates to use temporal DB.

One of the most frequently used approaches to ensure the security of data stored in the database is the encryption. It offers high security of data in the DB. Development of encryption strategy however, requires selection of an encryption level, data for encryption, algorithm for encryption, access to the cryptographic keys etc. All these factors affect system performance. Signing of data in the temporal DB [9] using the proposed methodology is implemented at the application level. This permits signing of only part of the stored data, which in turn increases the system operation speed. On the other hand, it does not require additional methods for storage of the private keys of the authorized users. These keys are never stored in their pure form neither in the DB, nor in the application nor in the file system of the web-server. This considerably increases the security of data.

Description of the Information System

The present development provides an implementation of an efficient mechanism for storage and usage of keys of authorized users, used for digital signing of the sensitive data in the system for information provision of Higher Education Institutes.

One of the requirements of the modern web-based IS is that many authorized users are to have access for modification of different data. With the IS considered herein, each teacher must be provided with the opportunity to enter the results from the examinations in the particular discipline. Quick publication of the results from the examinations is very important. In this case, it is also important to guarantee that all data have been entered into the system by the particular teacher. To this end, using digital signing is proposed. It will be implemented at application level, and can be done selectively – of one or several fields. The private and public key of the teacher, necessary for the digital signing and verification of data modified, are stored in the DB. The public key, used for verification of the signature, is stored in pure form, whereas the private key to it, which is used for digital signing of data, is stored in the DB in and encrypted form. Encryption is implemented by means of symmetric algorithm [10]. The symmetric encryption and decryption key (SEDK) of the private key of the user is generated by specific algorithm. Data, extracted from the user digital certificate is used to this end. With the methodology proposed, it is not necessary to store any SEDK in the DB, in the application or in the disk.

MongoDB [11] DBMS is used to store sensitive data (marks and credits) in the IS. The whole information is stored in two collections – Teacher and Student.

The Teacher collection contains personal information for each teacher. Each document in the collection comprises 5 fields, each one of which contains: identification number, name of the teacher (a two-field object – name and surname), user name, access password and certificate. The certificate field stores the public and the private keys of the
authorized user, and the serial numbers of their digital certificates (figure 1).

For greater security, the digital certificates of the authorized users are set to be valid for a particular time period. Thus, it is necessary to keep the history of the certificates used by the user. To this end, the value of the Certificate field is set as an array, storing the digital certificates used by the user, marked with effective time [8], setting their period of validity. In order to achieve this, each object storing data about the certificate, has an additional Period field (a two-field object – begin and end), containing the beginning and end of the efficient period of time, respectively. The efficient time is the time, during which the facts from the modelled subject area are both, valid and saved in the DB. The current time as at the moment of recording of the item in the DB is set as the beginning of the efficient time period. The end of the time period is a future moment, setting the end of validity of facts. This way, using the effective time, the certificates of the authorized users (their encrypting and decrypting keys) can be changed over certain periods of time. This opportunity considerably increases the security of data stored in the IS. Using temporal DB allows automation of system administration. After expiry of the efficient period of time, the values of the fields will be logically deleted. Furthermore, the history of encrypting and decrypting keys used by different teachers can also be traced.

Using the identification number of the teacher, recorded in the field _id, which is the primary key in the Teacher collection and the value of idt field in the Student collection, provides the connection between them (figure 2).

Each document from the Teacher collection contains the private keys of the teacher, valid for certain period of time (privateKey field). The private key is encrypted with SEDK using symmetric encryption. Using data from the fields idt and dateIn from the document stored in the Student collection one can find both, the private key used by the authorized teacher for digital signing of data entered into the DB, and the public key required for verification of the teacher signature. Both keys are stored in the Teacher collection.

Algorithm for Digital Signing of Data

A user can be granted authorized access to the resources of the web-based system for information provision, if he/she possesses a valid client digital certificate. Using their client certificate, users can prove their identities to the server and the application, servicing the IS.

In order to guarantee the authenticity of data, and to establish the user who saved this data, it is necessary to use additional means for validation and authentication. Figure 3 shows algorithm for digital signing of data, implemented in the system for the information provision of the academic activities.

What is specific about the algorithm proposed is the way of storing the public and private keys used for signing and validation of data in the DB. The algorithm for digital signing of data sensitive to modification is as follows:

1. Upon successful logging in the system (user name, password and valid digital certificate are required) the teacher enters the data of the particular student in the specific discipline (credits, mark). This data must be signed and stored in the DB of the IS.
2. Data from the client certificate is extracted and SEDK is generated.
3. The encrypted private key of the teacher included to the system is extracted from the DB.
4. The private key of the teacher is decrypted using the SEDK generated in item 2.
5. Concatenation of entered data for storage into the database. The following sequence is applied – identification number of the student, discipline, credits and mark of the student.
6. The hash value of data concatenated in item 5 is extracted.
7. The hash value extracted in item 6 is encrypted using the private key of the respective teacher.
8. Data supplied by the teacher, hash value of data signed by the private key, date and information about the teacher who made the record in the DB (relation Results, fig.) are saved.
9. SEDK and decrypted private key of the teacher are deleted from the web-server’s memory.

10. End of algorithm.

Using the proposed algorithm, no additional procedures for storage and manipulation of private keys of teachers, used for digital signing [12] of data in the database, are applied. Keys, which were used for decryption of the private keys are neither stored in the DB, nor in the application of the IS, nor in the file system of the web-server. This way, even in case of unauthorized access to the DB, the application or the web-server, the private keys of the authorized teachers cannot be extracted. The digital certificate, using which the teacher logged in the system is required to gain access to the private key of the teacher, which is used for signing of data. Only this way, from the information recorded in the certificate of the teacher, can be generated the SEDK, which is required for decryption of his/her private key.

**Verification of Digitally Signed Data in the System**

Verification digitally signed and stored data is performed using the well-known algorithm for verification of digitally signed data [13]:

1. Query to the DB for extraction of the results related to the credits collected and the mark of certain student in the particular discipline.

2. Extraction of data (identification number of the stu-
dent, discipline, credits and mark of the student in European variant), signed hash value, date of entry of the results and information about the user who signed the data from the DB (relation Student, figure 2).

3. Extraction of the public key of the teacher who signed the data (collection Student, figure 2).

4. Decryption of the hash value of the signed data using the public key extracted in item 3.

5. Concatenation of data, extracted from the DB. The following sequence is applied – identification number of the student, discipline, credits and mark of the student.

6. Hash value of data concatenated in item 5 is calculated.

7. Comparison of hash values, obtained in item 4 and item 6. In case of coincidence the procedure moves to item 8 otherwise, an error message is generated.

8. Return of the results from the query to the user.


**Conclusion**

Methodology for digital signing of sensitive data, stored in the system for the information provision of academic activities in the Higher Education Institutes was proposed and implemented. The system provides information about the collected credits, marks from examinations held and additional statistical information concerning the academic results of the students sorted by groups, disciplines, cohorts, etc. What is characteristic about this system is the great number of authorized teachers in the particular disciplines, who have rights of access and modification of different parts of the data. With such system, it is particularly important to guarantee the authenticity of data stored in the system – i.e. marks of the students. The access of each authorized user to the data is valid for specific time period. This necessitates using temporal DBs. Digital signing of
marks of the students guarantees their veracity and the authenticity of the teacher, who enters them. One of the most important parts in the process of digital signing of data is storage of keys used for the electronic signature. What is characteristic about the methodology for digital signing used in the IS is that the private key of the authorized user is stored in encrypted form in the DB. Symmetric encryption was applied. The symmetric key for encryption and decryption (SEDK) of the private key of the user is automatically generated. Data from the digital certificate of the user is used to this end. This way, SEDK is stored neither in the DB, nor in the application, nor in the file system of the web-server. This significantly increases the security of data. Using temporal DB allows tracing the history of encrypting and decrypting keys used by the individual teachers.

References


Manuscript received on 14.06.2016

Dimitar Pilev is Associate Professor in Department of Informatics, University of Chemical Technology and Metallurgy, Sofia. He received his M.Sc. degree in Information Technologies (2007) and PhD degree (2011). His professional interests and research activity are in the areas of optimizing and modeling of temporal database queries, real-time web programming, information system security and NoSQL temporal database models.

Contacts:
Department of Informatics
University of Chemical Technology and Metallurgy
e-mail: pilev@uctm.com