ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Preservation of Students Databases in Cloud

[1]R. Vijayarangan and [2]Dr. K.A. Parthasarathy

[1]*Research Scholar, Computer Science and Engineering, AISECT University, MP, India.*
[2]*Principal, Aksheyaa College of Engineering, Chennai, India*

ARTICLE INFO

Article history:
Received 16 April 2015
Accepted 12 June 2015
Available online 1 July 2015

Keywords:
Students Database,
Smartcard Systems,
AES Algorithm

ABSTRACT

This paper describes the policy regulation of a university that it enforces for maintaining the Students' Information System. The policy aimed at ensuring the students privacy and security in cloud. The goal here is to run the information system in such a way that each student owns and carries his/her own information. In such a system the person enjoys almost complete control and adequate privacy over his personal academic information. An individual can disclose her/his credentials to any one s/he chooses. In this age of open information system this kind of policy regulation is important to preserve an individual's privacy.

To Cite This Article: R. Vijayarangan and Dr. K.A. Parthasarathy**.,** Preservation of Students Databases in Cloud, ***Aust. J. Basic & Appl. Sci.,*** *9(20): 372-375, 2015*

INTRODUCTION

During the last decade the improvement of internet and web technology made it extremely easier to search for any information just in a minute or even in seconds. An individual can get almost any kind of information on any topic without spending any money, time or effort. This freedom and convenience of information is really important in order to keep up with the first pace of this current internet age. Every community of our society is enjoying the advantages of this freedom. Again information and the ability to acquire information are necessary to improve our democratic way of life by providing clarity and openness in every sector. But this kind of system is becoming a potential threat to individual's privacy. An individual is finding it increasingly difficult to keep her/his credentials secure in this open world of information. While the freedom of information is necessary, it must also respect an individual's privacy. In order to ensure that the corporations must come up with policies that can provide such security to its customers/clients. In this paper we proposed such a policy and system requirement to enforce such policy. The corporation in concern is actually a university. The policy focuses on servicing the students without violating their privacy. In fact in the proposed system each student (individual) keeps her/his own information to her/himself and s/he discloses her/his information to any one s/he wishes to. The rest of this document outlines the purpose, scope and description of this policy. At the end we included the description of a few technologies that may be required to run such system followed by the remarks.

II Purpose:

The purpose of this policy is to outline the acceptable use of a university's Student Information System. The enforcement of this policy will ensure the protection of privacy and confidentiality of each student. The policy briefly describes the scope, the acceptable usage, the unacceptable usage and exceptional usage of the systems' software and hardware

III Scope:

This policy applies to all university students, instructors and staff. The policy covers only the student information system that involves managing all the academic and financial information of each student in secured and confidential way. The objective is to confirm that information regarding an individual never disclosed other party unless required by law. The System functionalities that are covered under this policy are Student Enrollment, Registration, Accounts Management, Grading and various Administrative Services provided to the students.

IV Policy Description:

4.1 General use and ownership:

I. All the records pertaining to a student is kept on the student's smart card. While the records are

Corresponding Author: R. Vijayarangan, Research Scholar, Computer Science Engineering, AISET University, MP, India. E-mail: vijayarangan1978@rediffmail.com.

owned by the student, the smart card belongs to the university.

II. The university keeps record of the students' that are relevant only to the current semester. But the university does it anonymously without violating the privacy of any individual. At the end of each semester the student specific information will be transferred to the respective student's smart card and will be deleted from the university database. The responsibility of keeping the students smart card updated in a timely manner entirely remains with the student.

III. It is the student's responsibility to maintain the integrity of his card. The university reserves the right to verify the content of the card without violating the student's privacy.

4.2 Security:

The private key that was used to encrypt the data of the Smart Card will reside at the university database. Also every time data inside a student's card is modified a hash out of the original document will be produced and will be preserved at the university database. The hash function should be strong enough to make it impossible to reproduce the original data. Every time the student uses her/his card, a hash will be generated and it will be checked against the previous hash saved at the university database.

In case a card is lost, the student must inform the university as soon as possible. The card will be then immediately deactivated. A backup database will reside in a secured place in the university's facility, which also will contain copy of every student's data in encrypted format. Though the database is located on the university, only the student will be the owner of his data, and only s/he can access that data. With her/his id and password s/he will be able to retrieve that data and copy it back to the newly assigned card.

In order to retrieve (decrypt) information from the backup database the students' identity will be authenticated by their user id and password or alternatively by their biometric information. A biometric info record is also available in the backup database for authentication purpose

4.3 Usage policy:

4.3.1 Enrollment:

Every new student is provided with a smart card. All the information that the university keeps regarding a student is against his/her smart card hardware address. The information that university keeps in its own database is minimal and it is kept in encrypted and anonymous way.

All the academic and necessary information are put into the smart card and remains as the property of the student. Students must use the card to process any academic, financial or administrative request.

4.3.2 Course Registration:

Students must use their own card to register for courses at the beginning of each semester within the deadline fixed by the registrars' office.

Before the course registration the university system will extract the student's previous academic records in order to process the request. This information is collected programmatically from the student smart card and no information is disclosed to the administrative personals and is removed from the system as soon as the request is processed.

The system checks for any outstanding balances and in case of outstanding balance the request is not serviced, until the account is cleared.

If the balance is cleared the system searches the smart card for previous course records and analyze if all the prerequisite conditions have been met for the courses that the student is trying to register for.

Upon successful registration the students account is debited with appropriate tuition and other fees. The university keeps the registration information in its own database in an anonymous format. This is important for the university in order to carry out its administrative tasks e.g. assigning room for the classes, notify the instructors about the class lists. But again this information is minimal and kept in the system database only during the span of the semester in concern.

*4.3.3 Accounts Managemen*t**:**

The Accounts department keeps students financial record against his/her smart card hardware address. It also keeps track of the dates for the fees due date so that it may enforce legal action in case of outstanding balance.

The accounts information is also recorded in the students' smart cards. Therefore the administration can enforce the payment before processing any request made by the student.

Students may be denied any academic or administrative services in case there is any outstanding balance.

4.3.4 Grading:

All the grade information is strictly kept in the students' smart card. At the end of the semester the instructors send the grades to registrars' office. The grades are kept in the registrars system until the students remove those from the system using their smart card.

It is the students' responsibility to collect the grade information as soon as they become available.

*4.3.5 Administrative service*s**:**

Students can produce any academic certificate or document e.g. transcript, certificate of enrollment, accounts receipt using their card. The system only temporarily collects the information (if necessary) from the card to produce the documents.

Again account balance status may be enforced before providing any of such services.

4.3.6 Exceptional usage:

It is important for the university to keep record of different kind of statistical information. In many cases it is required by law for the university to keep such statistics. And in many cases it is important for the university to collect statistics in order to provide better service to the students and the community. In any cases the information is collected under the consent of the student and is kept anonymous and confidential.

If required by law the university may enforce the student to produce his/her card to the government or law enforcement agency for verification.

4.4 Unacceptable use:

Though the information in a smart card belongs to the student, s/he is not allowed to alter the information in any way. If any such misuse is found, the student will face disciplinary charges.

During servicing a student the university staff or administrative official are not allowed to keep any record of the student prior his/her consent. Any information collected (if necessary) is strictly temporary and must be deleted right after the end of the service.

V Technology:

5.1 Smart Card:

The Smart Card is the latest member of identification card of ID-1 format. It has an integrated circuit, which has components for transmitting, storing and processing data. "Smart cards are 'smart' because they control who can access the information they process. With increased fraud and security concerns in an electronic age, smart cards offer a top security alternative." A smart card has storage capacity that is many times greater than that of magnetic stripe cards. In our scenario we will be using Microprocessor-based Smart Card (2004), where the data can be transmitted using either contact on the surface of the card, or electromagnetic fields without any contact. The following image shows a typical architecture microprocessor smart card with a co-processor:

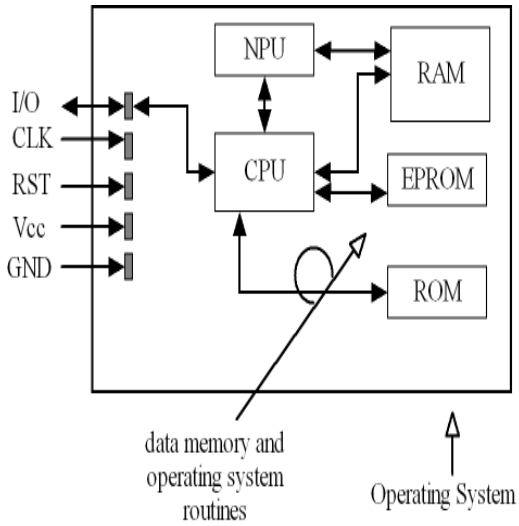

Fig. 1: The typical high level architecture of microprocessor smart card (Taken from Smart Card Handbook, John Wiley & Sons, ISBN # 0470856688).

5.2 Smart Card Security & Cryptography:

Since smart card could be used for manipulation or fraud, security is a very important aspect of it. As a result, cryptography achieved a central significance in the smart card technology. The four most important objectives of cryptography are maintaining the secrecy of the messages (confidentiality), ensuring the entirety and the authenticity of the messages and ensuring the biding force of messages. Different card has different security schemes & encryption. Our proposed system uses AES-128 encryption scheme (Chi-Feng, L., 2003). This is a symmetric block encryption algorithm with a block length of 128 bit. This encryption is easy to implement as hardware logic, also good software implementation is also possible in both low performance 8 bit processor as well high performance 32 bit processor. It can be used throughout the world free of licensing fees. The large key space obtained with a key length of 128 bit enormously increased the difficulty of attacks involving successfully testing all possible keys. The software implementation of this encryption scheme occupies approximately 4 KB of ROM in a smart card. The table below shows a typical computation times for AES in a smart card using 128 bit key:

Table 1: Typical computation times for AES in a smart card using 128 bit key (Taken from Smart Card Handbook, John Wiley & Sons, ISBN # 0470856688).

Implementation	Computation Time
Smart card, 16-bit CPU, 4.9-MHz clock, software implementation; encryption	20 ms
Smart card, 16-bit CPU, 4.9-MHz clock, software implementation; decryption	25 ms

5.3 Hash Function:

Even powerful computers require a great deal of time to compute a digital signature. Therefore a trick is used. The document is first compressed to a much shorter fixed length version than the signature of the compressed data is computed. This is called hashing. For a hash function to be effective, it must satisfy some properties. The result must be fixed length, the hash must have a high throughput, it must also be easy to compute the hash function but by contrast it should be difficult (or impossible) to reproduce the original document from a given hash, finally, the hash function must be collision resistant. In the proposed system our choice for hash function is SHA-256, which is the latest encryption system, and was designed for use with AES encryption (Aggarwal, A., 2006).

VI Conclusion:

Even though the proposed system and policies takes care most of the major privacy issues of the students, it is not completely successful. In many cases it is necessary for the institution to have some students' information available to itself. One of such scenarios is the accounts management system. According to the proposed policy the university can only enforce the student to pay his out-standings dues only when s/he requests for new grades or requests a course registration or any other academic services. If an individual never shows up (such cases are likely to happen if the student quits or changes school) than the university must have some way to contact him to take necessary legal step towards the payments of her/his dues. Therefore some privacy sacrifice has to be made to make everything running smoothly. Another scenario is when the administration tries to carry out administrative tasks like providing necessary accommodation to each class. It must need to know the size of the classes to assign rooms; it must also notify the instructors about the students list and so on. Some sacrifices have to be made for these inevitable tasks as well. In order to handle such exceptional situation the policy suggests that information collected for this procedures is always minimal, anonymous (if possible), remains confidential and temporary, e.g. all information is collected only for the semester basis and disposed after the end of the semester.

In a practical scenario it is impossible to make everything completely confidential. The parties involved in a corporation / institute must sacrifice a little of their privacies to carry on their businesses. In our policy we try to minimize such discloser within a minimum level, as much as possible.

REFERENCES

Aggarwal, A., 2006. Lecture Slides-Security and Privacy on the Internet (60-564), *http://venus.uwindsor.ca/courses/cs/aggarwal/cs60564/materials.htm*, Winter.

Chi-Feng, L., K. Yan-Shun, C. Hsia-Ling, Y. Chung-Huang, 2003. "Fast implementation of AES cryptographic algorithms in smart cards", *Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on Security Technology*, 2003, 14-16 Oct. 2003 Page(s): 573-579.

Chu-Hsing, L., L. Tri-Show, L. Hsiu-Hsia, L. Yi-Yi, 2005. "On the security of ID-based password authentication scheme using smart cards and fingerprints", *3rd International Conference on Information Technology: Research and Education, 2005, ITRE 2005*. 27-30, 30 June 2005 Page(s): 230-232.

Omar, S., H. Djuhari, 2004. "Multi-purpose student card system using smart card technology", *Proceedings of the Fifth International Conference on Information Technology Based Higher Education and Training, ITHET 2004*, 31 May-2 June 2004, Page(s): 527-532.

Schramm, K., C. Paar, 2004. "IT security project: implementation of the Advanced Encryption Standard (AES) on a smart card", *proceedings of International Conference on Information Technology: Coding and Computing 2004, ITCC 2004*, 1: 176-180.

Smart Card Handbook, John Wiley, Sons, ISBN # 0470856688 January 23, 2004.

Yanjiang, Y., H. Xiaoxi, B. Feng, R.H. Deng, 2004. "A smart-card-enabled privacy preserving E-prescription system", *IEEE Transactions on Information Technology in Biomedicine*, 8(1): 47-58.

Yen-Cheng C.Chen, Y. Lo-Ya, 2005. "An Efficient Authentication and Access Control Scheme Using Smart Cards", *proceedings of 11th International conference on parallel and Distributed Systems*, 2, 20-22 July 2005 Page(s): 78-82.