International Journal of Scientific and Technical Advancements

ISSN: 2454-1532

A Roadmap to Data Security of Automated University Examination System

Balvir Singh[1], Amarjeet Singh[2]
[1, 2]Department of Computer Science, H.P.U, Shimla-5
Email address: [1]balvir.thakur@gmail.com

***Abstract*—**Information Technology and communication (ICT) has made remarkable impact on the society. To bring efficiency, accuracy, and transparency to the system, many Indian universities are using ICT in teaching, learning, and administration processes, and management of examination system is one of them. Automated university examination system deal with student data starting from their admission/enrolment till they pass out from the university and even after when they pass out, university keep the data of student for future use. This student data is stored in database and maintained by automated examination system. The student data can be accessed and shared on internet or intranet. Then there is a need to protected this student data from destructive forces and from the unwanted actions of unauthorized users. This paper describes in brief all these data security requirements to protect crucial student information of automated university examination system and also suggest the possible technical solution to the listed data security issues.

***Keywords*—**ICT; stakeholder; data security; database; examination system.

I. Introduction

With the sharing of information on network, a threat to data security is becoming a major concern. Protection of information is necessary to establish and maintain trust between an institution and its stake holders (e.g., students, parents, teachers, administrative staff, colleges) if the institution is to maintain its reputation. The two main security threats that affect the organization are internal threats and external threats. Internal threats occur within the organizations. This is probably one of the most dangerous situations because co-workers generally know passwords to access systems and are aware of how the systems are set up. Computers that are left unattended can be easily accessed by workers. External threats include hackers and crackers who usually breach into a system just for personal benefits or thrills. Based on the sensitivity of the data, different types of security measures are applied to make the system secure. There is always the possibility of achieving total security; effective security measures and controlled procedures can considerably reduce the risks of misuse of data [Mohini Bhardwaj & Amar Jeet Singh, (2011)]. Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users[Summers, G. (2004).]. Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical.

Examination System

The student examination process in Indian universities is divided into two main phases: pre-examination and post examination. There are different independent branches and supporting cells for conducting various processes, such as registration, migration, conduct of exam, evaluation, etc., related to the exam system. Three categories of students-regular, private, and distance education appear for an exam held either annually or every semester. Regular students are on the rolls of the affiliated colleges. The colleges are authorized to maintain students' records, and only student data that are relevant for exam purpose are shared with the university. Private students data is maintained by university itself.

II. The Need for Security Measures

Academic frauds and corrupt practices are on the rise. Some of the major factors causing academic fraud and confidentiality of the information while allowing users to access permitted resources. The implications of hacking bring reputational issues and legal battles to light and may lead to closure of the university by the regulatory commission.

III. Data Security Challenges

The data security is widespread with mistaken beliefs which cause people to design ineffective security solutions. Here are some of the most common security myths:

- *Myth*: Hackers cause most security breaches. In fact, 80% of data loss is to caused by insiders.
- *Myth*: Encryption makes your data secure. In fact, encryption is only one approach to securing data. Security also requires access control, data integrity, system availability, and auditing.
- *Myth*: Firewalls make your data secure. In fact, 40% of Internet break-ins occur in spite of a firewall being in place.

To design a security solution that truly protects our data, we must understand the security requirements relevant to our site, and the scope of current threats to our data.

Understanding the Many Dimensions of System Security

In an Internet environment, the risks to valuable and sensitive data are greater than ever before. Figure 1-1 presents an overview of the complex computing environment which your data security plan must encompass.

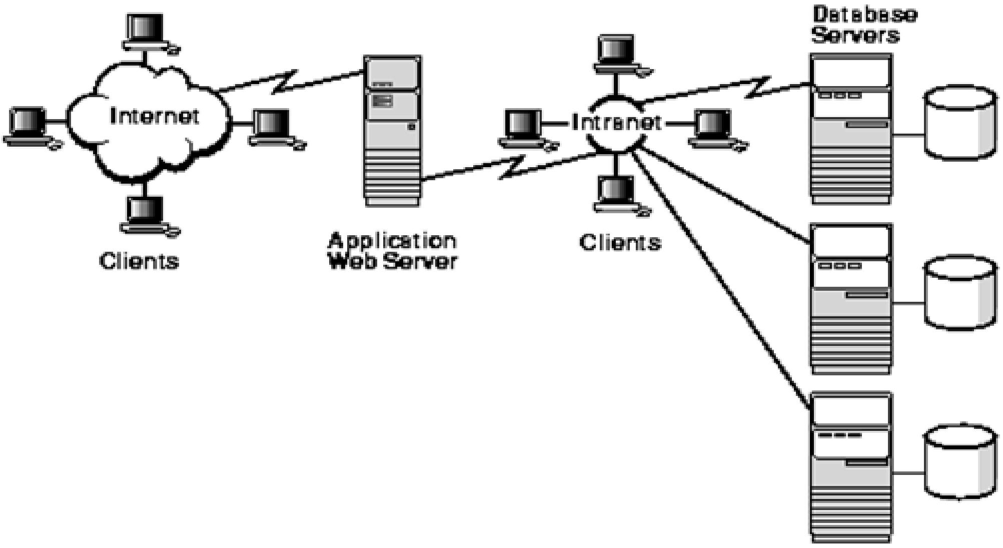

Fig. 1. Scope of data security needs.

We must protect databases and the servers on which they reside; we must administer and protect the rights of internal database users; and we must guarantee the confidentiality of customers as they access our database. With the Internet continually growing, the threat to data traveling over the network increases exponentially.

Table 1. Dimensions of data security.

Dimension	Security Issues
Physical	Your computers must be physically inaccessible to unauthorized users. This means that you must keep them in a secure physical environment.
Personnel	The people responsible for system administration and data security at your site must be reliable. You may need to perform background checks on DBAs before making hiring decisions.
Procedural	The procedures used in the operation of your system must assure reliable data. For example, one person might be responsible for database backups. Her only role is to be sure the database is up and running. Another person might be responsible for generating application reports involving payroll or sales data. His role is to examine the data and verify its integrity. It may be wise to separate out users' functional roles in data management.
Technical	Storage, access, manipulation, and transmission of data must be safeguarded by technology that enforces your particular information control policies.

To protect all the elements of University examination system, we must address security issues in many dimensions, as mentioned in Table 1.

We have to think carefully about the specific security risks to our data, and make sure the solutions we adopt fit the problems. In some instances, a technical solution may be inappropriate. For example, employees must occasionally leave their desks. A technical solution cannot solve this physical problem: the work environment must be secure.

Fundamental Data Security Requirements

The following sections describe the basic security standards which technology must ensure:

- Confidentiality
- Integrity
- Availability

Confidentiality

A secure system ensures the confidentiality of data. This means that it allows individuals to see only the data which they are supposed to see. Confidentiality has several different aspects, discussed in these sections:

- Privacy of Communications
- Secure Storage of Sensitive Data
- Authenticated Users
- Granular Access Control

Privacy of Communications

How can you ensure the privacy of data communications? Privacy is a very broad concept. For the individual, it involves the ability to control the spread of confidential information such as health, marks, employment, and credit records. For governments, privacy involves such issues as the ability to collect and analyze demographic information, while protecting the confidentiality of millions of individual citizens. It also involves the ability to keep secrets that affect the country's interests.

Secure Storage of Sensitive Data

How can you ensure that data remains private, once it has been collected? Once confidential data has been entered, its integrity and privacy must be protected on the databases and servers where it resides.

Authenticated Users

How can you designate the persons and organizations who have the right to see data? Authentication is a way of implementing decisions about whom to trust. Authentication methods seek to guarantee the identity of system users: that a person is who he says he is, and not an impostor.

Granular Access Control

How much data should a particular user see?. For example, an official working in the registration department of the university might need some access to the student table-but he should not be permitted to access marks obtained by the student. The granularity of access control is the degree to which data access can be differentiated for particular tables, views, rows, and columns of a database.

There is a distinction between authentication, authorization, and access control. Authentication is the process by which a user's identity is checked. When a user is authenticated, he is verified as an authorized user of an application. Authorization is the process by which the user's privileges are ascertained. Access control is the process by which the user's access to physical data in the application is limited, based on his privileges. These are critical issues in distributed systems. For example, an official working in the registration department of the university does not need to know all details about a student. When employee is trying to access the database, authentication would identify him as a valid user. Authorization would verify her right to connect to the database with Product Manager privileges. Access control would enforce the Product Manager privileges upon her user session.

Integrity

A secure system ensures that the data it contains is valid. Data integrity means that data is protected from deletion and corruption, both while it resides within the database, and while it is being transmitted over the network. Integrity has several aspects:

- System and object privileges control access to application tables and system commands, so that only authorized users can change data.
- Referential integrity is the ability to maintain valid relationships between values in the database, according to rules that have been defined.
- A database must be protected against viruses designed to corrupt the data.
- The network traffic must be protected from deletion, corruption, and eavesdropping.

Availability

A secure system makes data available to authorized users, without delay. Denial-of-service attacks are attempts to block authorized users' ability to access and use the system when needed. System availability has a number of aspects:

Table 2. System availability aspects.

Availability Aspect	**Description**
Resistance	A secure system must be designed to fend off situations, or deliberate attacks, For example, there must be facilities within the database to prohibit runaway queries. User profiles must be in place to define and limit the resources any given user may consume. In this way the system can be protected against users consuming too much memory or too many processes (whether maliciously or innocently), lest others be prevented from doing their work.
Scalability	System performance must remain adequate regardless of the number of users or processes demanding service.
Flexibility	Administrators must have adequate means of managing the user population. They might do this by using a directory, for example.
Ease of Use	The security implementation itself must not diminish the ability of valid users to get their work done.

Security Requirements in the Internet Environment

The Internet environment expands the empire of data security in several ways, as it allow increased data access, much more valuable data to common user and handle lager user communities. Security mechanisms deployed in systems must be standards-based, flexible, and interoperable, to ensure that they work with others' systems. They must support thin clients, and work in multitier architectures. Here we describe the risk involve and attacks that could compromise our data, when we allow our stakeholders to access the automated university examination system (through intranet / internet).

IV. Data Security Risks

The integrity and privacy of data are at risk from unauthorized users, external sources listening in on the network, and internal users giving away the store. Here we explains the risk involves and potential attacks that could compromise our data.

- *Data Tampering*: Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it.
- *Eavesdropping and Data Theft*: Data must be stored and transmitted securely. So that information such as marks obtained by students cannot be stolen.
- *Falsifying User Identities*: Identity theft is becoming one of the greatest threats to individuals in the Internet

environment. Nonrepudiation is another identity concern: how can a person's digital signature be protected.

- *Password-Related Threats*: In large systems, users must remember multiple passwords for the different applications and services that they use.
- *Unauthorized Access to Tables and Columns*: The database may contain confidential tables, or confidential columns in a table, which should not be available indiscriminately to all users authorized to access the database. It should be possible to protect data on a column level.
- *Unauthorized Access to Data Rows*: Certain data rows may contain confidential information which should not be available arbitrarily to users authorized to access the table.
- *Lack of Accountability*: If the system administrator is unable to track users' activities, then users cannot be held responsible for their actions. There must be some reliable way to monitor who is performing what operations on the data.
- *Complex User Management Requirements*: Systems must often support thousands of users, or hundreds of thousands of users: thus they must be scalable. In such large-scale environments, the burden of managing user accounts and passwords makes your system vulnerable to error and attack

Table 3. Matrix of security risks and solutions.

Problem	**Solution**	**Security Technology**	**Software product and Features**
Unauthorized users	Know your users	Authentication	Oracle9*i* Standard Edition, and Oracle9*i* Enterprise Edition: Passwords, Password management Oracle Advanced Security: Tokens, smart cards, Kerberos, and so on. PKI: X.509 Certificates
Unauthorized access to data	Limit access to data	Access control	Oracle9*i* Standard Edition Oracle9*i* Enterprise Edition: Virtual Private Database feature
	Dynamic query modification	Fine-grained access control	Oracle9*i* Enterprise Edition: Virtual Private Database feature
	Limit access to data rows and columns	Label-based access control	Oracle Label Security
	Encrypt data	Data encryption	Oracle9*i* Standard Edition, and Oracle9*i* Enterprise Edition
	Limit privileges	Privilege management	Oracle9*i* Standard Edition: Roles, Privileges Oracle9*i* Enterprise Edition: Secure Application Roles. Oracle Advanced Security: Enterprise Roles
Eavesdropping on communications	Protect the network	Network encryption	Oracle Advanced Security: Encryption .Secure Sockets Layer
Corruption of data	Protect the network	Data integrity	Oracle Advanced Security: Checksumming PKI: Checksumming (as part of SSL)
Denial of service	Control access to resources	Availability	Oracle9*i* Standard Edition and Oracle9*i* Enterprise Edition: User Profiles
Complexity to user	Limit number of passwords	Single signon	Oracle Advanced Security: Kerberos, DCE, Enterprise User Security Login Server: Web-Based SSO
Complexity to administrator	Centralize management	Enterprise user security	Oracle Advanced Security: Directory Integration. Oracle Internet Directory
Lack of accountability	Monitor users' actions	Auditing	Oracle9*i* Standard Edition: Auditing Oracle9*i* Enterprise Edition: Standard Auditing, Fine-Grained Auditing.
Overly broad access to data	Dynamic query modification	Fine-grained access control	Oracle9*i* Enterprise Edition: Virtual Private Database Oracle Label Security
Too many accounts	Centralize management	Directory services, LDAP-compliant directory services	Oracle Internet Directory
Operating system break-in	Encrypt sensitive data	Stored data encryption	Oracle9*i* Standard Edition and Oracle9*i* Enterprise Edition: Data encryption

A Matrix of Security Risks and Solutions

Table 3 relates security risks to the technologies which address them, and to the corresponding software products.

The System Security Team: Here we identified a different areas and set of people responsible for maintaining these area. This team of people is responsible to ensure security at a particular site which is the main requirement of automated examination system. Table 4 introduces the types of administrators who may be involved. Thus, by implementing the above-mentioned security mechanism, we may be able to make our Examination System a transparent, reliable, and secure system.

Table 4. The system security team.

Person	**Responsibilities**
User	Responsible for using the system for legitimate purposes, protecting sensitive data to which she has access, and managing her passwords securely.
Database Administrator	Responsible for creating and administering database users, granting system and object privileges, and assigning local roles to users.
Operating System Administrator	Responsible for maintaining the underlying security of the operating system.
Network Administrator	Responsible for ensuring the security of data in transmission.
Application Administrators	Responsible for deploying applications in such a way as to ensure security.
Trusted Application Administrator	Responsible for creating and administering users of trusted applications, and their associated privileges.
Enterprise Security Manager	Responsible for maintaining the security of the directory, and for implementing centralized enterprise user security.

V. CONCLUSION

In an Indian context, the university system is reforming itself by introducing transparency, better management, and effective usage of ICT. The exam system within a university bears the brunt of an increasing student enrolment whereas ICT promises better handling of data, ease of access, and user friendliness. However, while introducing ICT, enforcing data security is imperative, otherwise it will be subjected to numerous cyber threats, for example, unauthorized disclosure, modification, or destruction. The Automated Examination System is suitable, with appropriate security measures. The data security issues must be addressed and resolved technically to protect the student data of automated examination system and this help us to avoid the exam malpractice and fraudulent act.

REFERENCES

[1] G. Summers, Data and databases. In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited, pp. 4-5, 2004.

[2] M. Bhardwaj and A. J. Singh, “Automated integrated examination system: a security concern,” *Information Security Journal: A Global Perspective*, vol. 20, issue 3, pp. 156-162, 2011.

[3] http://docs.oracle.com/cd/B10501_01/network.920/a96582/overview.htm#1004880

[4] https://en.wikipedia.org/wiki/Data_security

[5] Cryptography and Data Security [Dorothy Elizabeth Robling Denning] ADDISON-WESLEY PUBLISHING COMPANY.

[6] M. Bishop, *An Introduction to Computer Security*, The NIST Handbook. Boston: Addison Wesley, 2005.

[7] F. Farahmand, S. B. Navathe, G. P. Sharp, and P.H. Enslow, “Managing vulnerabilities of information systems to security incidents,” *Proceedings of the 5th International Conference on Electronic Commerce*, pp. 348–354, 2003.

[8] J. Hallak and M. Poisson, “Academic fraud, accreditation and quality assurance: In learning from the past and challenges for the future,” Higher education in the world, pp. 109–122, 2007.

[9] A. T. Henriksson, Y. Yi, B. Frost, and M. Middleton, “Evaluation instrument for e- government Websites,” *Electronic Government, an International Journal*, vol. 4, issue 2, pp. 204–226, 2007.

[10] J. Murphy and D. Zwieback, Managing Emerging Security Threats, 2005.

[11] S. J. Rizv and J. R. Harita, “Maintaining data privacy in association rule mining,” *Proceeding of 28th International Conference on Very Large Databases*, pp. 682–693, 2002.

Balvir Singh and Amarjeet singh, “A roadmap to data security of automated university examination system”, *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 71-75 2015.