

Cryptosystem for Secured E-Learning and Educational Data Mining in Higher Education

Akram Salim Khanfar¹, Firdous Ahmad Lone² and MD Moizuddin^{3*}

¹Faculty, King Saud University, Saudi Arabia. Email: Akram.khanfar2011@gmail

²Faculty, King Saud University, Saudi Arabia. Email: lonefirdous686@gmail.com

³Faculty, King Saud University, Saudi Arabia. Email: moizqa12@gmail.com

*Corresponding Author

Abstract: In the 21st century, we have plenty of data available in the society of education. Importantly, today's education system has changed, it takes place through all the available channels and one of the significant means is the digital learning e-learning. Large amounts of data are available for the students as well as teachers to access the digital data online. Today security of the data became an important concern in the society and at the education sector level. Further, we need to extract the precise data and improve the existing education system through e-learning by using Educational Data Mining. In this paper, we will focus on the security of the online education resources and the extraction of the data based on the student's level by using the mining techniques that will be helpful for the students.

Keywords: AES, Cryptography, E-learning, Educational Data Mining (EDM), Encryption, KDED (Knowledge Discovery in Educational Databases), Threats and risks.

I. INTRODUCTION

In ancient times, education was limited within a small range of society and that education system was depending only on the traditional system of teachings and the students truly learned and focused on the subject and disciplinary principles taught in the class. In traditional education, we have data as well information but it is kept on the papers. Today's education is modernized with the latest technologies and the system which we are using is digital. This transformation from traditional education to the modern education system is E-learning.

E-learning is globalization of education; people from anywhere can learn. Fundamentally, e-learning is a new way of providing knowledge to people to interact with web-based systems, which is the need of the current world. To subordinate the sharing and recycling of learning resources in different e-learning system, numerous e-learning standard formats including SCORM, IMS,

LOM and AICC etc. recently have been proposed by several international organizations [1]. For successful e-learning technology, we have to focus on the two major challenges: firstly, collect and extract the data by using the Educational Data Mining techniques and secondly, maintain the online education system secure, by minimizing information loss and providing security to the stored data by using cryptographic techniques. By integrating the standard cryptographic algorithms and data mining techniques, we can overcome the key challenges like maintaining the data online, and to secure data with authenticity, integrity [2] [3].

II. DATA MINING

Data mining is defined as discovering hidden knowledge, models and procedures from the volumes of huge databases [4]. Education is changing, more than at any time since the introduction of the e-learning and the data available on the internet are radically transforming how we learn. Data mining is the process to turn raw data into useful information, analyzing hidden patterns of data according to different perspectives for categorization into useful information, which is collected and assembled in common areas, such as data warehouses, for efficient analysis, data mining algorithms, facilitating for the development of the society.

Data mining is also known as data discovery and knowledge discovery. Major database vendors like Oracle and SQL incorporate data mining algorithms, such as clustering and regression trees, to meet the demand for data mining. Data mining tools predict future trends and behaviours that allowing companies to make proactive, knowledge-driven decisions.

In the era of digitization, data security and dispensing of data is difficult to achieve. The security of user's sentient information is vital anxiety. The day-to-day use up of word privacy about information security, data dispensing and analysis is oftentimes vogue and may be caused to stray. Every organization gather facts about their clients or users for exploration or any other

intent. Information being collected may be audio, videos, images etc. [12]. The resulting data size can consist of terabytes of data. Data mining is also known as knowledge discovery in databases is a technology used in a different discipline to search for the significant relationship among variables in a large database. It extracts knowledge to form a hidden database and find the necessary information according to the requirement.

These tasks are done by applying the various algorithm of data mining on the training dataset. The user according to the requirement uses this dataset passes through various steps of data mining and finally the filtered data. It plays an important role in an education institute.

III. EDUCATIONAL DATA MINING (EDM)

EDM is a field of data mining which work in the field of education to extract knowledge. In present educational society, schools, universities and institutions gather and holds volumes of data, such as student's admissions, registration systems, attendance records, examination results, student-produced artifacts, course management systems (Moodle, blackboard, etc.) and any other system recording the different levels of information related to the faculties [9]. EDM is the application of Data Mining technique used to extract useful patterns and discovering useful knowledge from these educational systems that will be helpful for the improving and enhancing learning quality, and improve our understanding of the learning process [4].

EDM involves different groups of users or participants. Different groups look at educational information from different angles according to their own mission, vision and objectives for using data mining [5] [6]. For example, knowledge discovered by EDM algorithms can be used to not only help teachers to manage their classes, understand their students' learning processes and reflect on their own teaching methods but also to support a learner's reflections on the situation and provide feedback to learners [6].

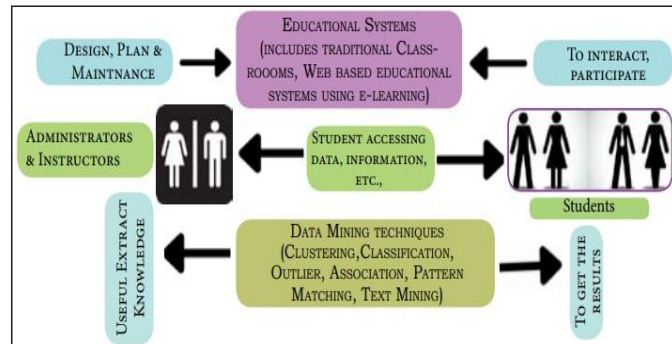
IV. CRYPTOGRAPHY AND E-LEARNING CONCEPTS

Cryptography is the way by which the information can be prevented from the unauthorized users from accessing and the data or the information flowing from administration to the end users can protect without the middle-man-attacks or other similar attacks [7].

Cryptography is defined as the system by which the normal records can be turned to the unreadable form so that the unlawful persons cannot access the plain or the normal records. Quantum systems designed in such a way that it uses quantum mechanics and depends greatly on the classical physics [7].

E-learning is described as the computer-enhanced learning environment and it has become more diverse in its form and applications.

V. DATA MINING TECHNIQUES INCORPORATED INTO E-LEARNING ENVIRONMENTS



E-number of researches have been taking place to incorporate the data mining techniques to e-learning situations. The goal of integrating the e-learning with Data Mining is to provide the instructors/mentors to progress the learning and teaching environment. Nowadays students are much dependent on the online data and can access the required information from any part of the world they are [13]. Students can share information and participate in collaborative learning have the enriched learning experience, if they depend on the information provided online through applications like LMS (Learning Management System), Moodle, etc.

Data Mining techniques are useful to extract the exact and required information by using a number of techniques such as prediction, classification, association rule mining, clustering, fuzzy logic, etc. [8].

VI. E-SECURITY CHALLENGES

E-Learning Security Challenges	Explanation
Interoperability of applications	Depend on the institutions.
Standardization and compatibility	Different e-learning systems interact with one another.
Security policy and enforcement mechanism	Managing about the Sensitive information and security policy is maintained.
E-learning infrastructure	It deals with the Hardware, Software and connectivity required for e-learning development and implementation.

VII. POSSIBLE ATTACKS AND SECURE E-LEARNING USING CRYPTOGRAPHY ALGORITHMS

The below table is taken as reference from [3].

Possible Attacks on E-Learning System	Effects on E-Learning System	Counter Measures
Availability attack	For some time, even for the authentic users also the system services and contents are unavailable. Threats: Denial of Service, Node attacks, Network infrastructure attacks.	Maintaining timely system backup is a way of countering these attacks.
Integrity attack	It refers to Data Modification and the alteration of the data. Threats: Buffer Overflow, failure to restrict URL access malicious code attacks, message injection, traffic modification, traffic deletion.	The digital signature, data hashing and shining can be used effectively.
Confidentiality attack	It exposes confidential data to unauthorized users. Threats: Group session eavesdropping, Group session traffic analysis, and Group identity disclosure.	Strong encryption methods should be used to counter a confidentiality attack.
Authentication attack	Attacker actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange, when computers are communicating at the low levels of the network. The attack is to gain access to system information by using stolen passwords, key or credentials or an attack device. Threats: Brute force attack, dictionary attack, login spoofing attacks, key management attacks, replay attacks, Man-in-middle attacks.	To counter these attacks, a strong authentication method such as Biometric-based security should be considered. A strong role-based security mechanism should be used.
Countering non-repudiation	Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.	To counter the problem of non-repudiation, digital signatures, timestamps are considered.

VIII. ELLIPTIC CURVE CRYPTOGRAPHY

ECC was first proposed by Victor Miller [10] and based on the complexity of certain mathematical problems. It is a public-key cryptographic mechanism which provides equal security with smaller key sizes compared to the traditional algorithms like RSA. ECC has a low bandwidth and keeps memory space. It results in faster calculations, lower power consumption. Because of the smaller keys in ECC, it results in power, bandwidth and computational savings.

It provides the same level of security as afforded by an RSA-based system with a larger modulus corresponding to a larger key system. For Example, 3072-bit RSA public key and a 256-bit ECC public key gives the same comparable security. Here ECC takes the smaller key sizes and the lower power consumption [11].

IX. CONCLUSIONS AND FUTURE WORK

In this paper, we have discussed the security aspects of e-learning applications, threats and protection measures. The ECC algorithm provides security to the e-learning society. The

E-learning applications should be incorporated with algorithms like ECC, which provides the secured authentication in order to run the e-learning system in a more efficient way.

In future, we intend to discuss a comparative analysis of the traditional Cryptography algorithms which provides the security of the e-learning society. The system needs to implement security services such as authentication, encryption, access control, managing users and their permissions. The communication between the administrators, content operators and the students and teachers should be done on an encrypted SSL channel without affecting the performance of the system.

REFERENCES

- [1] M.-C. Lee, K. H. Tsai, and T. I. Wang, "A practical ontology query expansion algorithm for semantic-aware learning objects retrieval," *Computers and Education*, vol. 50, no. 4, pp. 1240-1257, May 2008.
- [2] E. Madhavarao, C. JayaRaju, P. Divya, and A. S. K. Ratnam, "Data security using cryptography and steganography," *International Journal of Advanced Research*

- in *Computer Engineering and Technology*, vol. 1, no. 5, pp. 319-325, July 2012.
- [3] B. T. Adetoba, O. Awodele, and S. O. Kuyoro, "E-learning security issues and challenges: A review," *Journal of Scientific Research and Studies*, vol. 3, no. 5, pp. 96-100, May 2016.
- [4] D. Perović, "Data mining influence on e-learning," *The Sixth International Conference on e-Learning (eLearning-2015)*, Belgrade, Serbia, 24-25 September 2015.
- [5] B. Bakhshinategh, O. R. Zaiane, S. ElAtia, and D. Ipperciel, "Educational data mining applications and tasks: A survey of the last 10 years," *Education and Information Technologies*, vol. 23, no. 1, pp. 537-553, Springer US, 2018.
- [6] M. Hanna, "Data mining in the e-learning domain," *Campus-Wide Information Systems*, vol. 21, no. 1, pp. 29-34, Emerald Group Publishing Limited, 2004.
- [7] C. Romero, and S. Ventura, "Educational data mining: A review of the state-of-the-art," *IEEE Transactions on Systems, Man, and Cybernetics - Part C (Applications and Reviews)*, vol. 40, no. 6, pp. 601-618, December 2010.
- [8] Mohd. Moizuddin, J. Winston, and Mohd. Qayyum, "A comprehensive survey: Quantum cryptography," In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, IEEE, Abha, Saudi Arabia, 26-27 March 2017.
- [9] A. Lile, "Analyzing e-learning systems using educational data mining techniques," *Mediterranean Journal of Social Sciences*, vol. 2, no. 3, pp. 403-419, September 2011.
- [10] V. Miller, "Uses of elliptic curves in cryptography," *Advances in Cryptology CRYPTO '85*, pp. 417-426, 1986.
- [11] R. Krishnaveni, and V. Pandiyaraju, "A secure e-learning system and its services," *International Journal of Advanced Computational Engineering and Networking*, vol. 1, no. 4, pp. 41-43, June 2013.
- [12] P. R. Pradhan, and R. B. Kulkarni, "Secure e-learning using data mining techniques and concepts," In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, IEEE, Chennai, India, 3-5 March 2016.
- [13] V. Patil, A. Vedpathak, P. Shinde, V. Vatandar, and S. Janrao, "E-learning system using cryptography and data mining techniques," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 1, pp. 446-449, January 2018.