Chinese Traditional Medicine Journal

ISSN : 2693 6356
2023 | Vol 6 | Issue 5

Using a Circular Queue Data Structure for mLMS Application Security Analysis

Dr.M.Shanmugapriya,
Assistant Professor , Shree Venkateshwara Arts and Science (Co-education) College, Gobichettipalayam.

ABSTRACT
The rapid development of mobile technology and its applications have transformed society into one that is increasingly interdependent in recent years. It helps individuals in several ways to improve the quality of their everyday lives. The introduction and widespread use of mobile technology has facilitated rapid communication, increased knowledge, and brought together previously isolated groups of people. In our suggested architecture, the Learning Management System (LMS) serves as the backend server for a Mobile Learning application (M-Learning) that prioritizes data protection. Today's students may choose from a plethora of M-Learning options, yet many of them are unsafe. Protecting information from malicious actors is an ongoing problem. It is crucial to have solid security in order to counteract the various hacker attempts. The data is protected from malicious users by using Circular Queue (CQ). Data is encrypted using logical and shift operations to produce an unbreakable ASCII binary representation. The Multiple Circular Queue Algorithm (MCQA) is 50% simpler, but this one is 50% simpler yet. The suggested approach is more versatile and may be used in any situation since it encrypts data in addition to using a Fibonacci structure and a variable format.
Key terms: Security, Fibonacci numbers, binary numbers, MCQs, mobile learning platforms, and ASCII text.

I. INTRODUCTION

New learning modes have emerged thanks to the exponential growth of information technology. M-Learning allows for group study and productive dialogue between students and teachers. The M-Learning App makes it possible for students to study almost anywhere, at any time. Students are more engaged and inspired to take on a wider range of coursework. More benefits to the students are attributed to M-Learning than to E-Learning in the areas of education, design, learning format, and a well-thought-out User Interface (UI). While M-Learning opens up exciting new avenues of study, it also raises serious security issues among educational institutions and their students. Due to the prevalence of mobile device usage among students using the M-Learning Application, concerns have been raised about the safety and confidentiality of student information. The primary focus of M-learning has been on the creation and distribution of courses, with little thought given to the safety and confidentiality of student information. It became clear from a review of the available information that researchers were unconcerned about the safety of M-Learning. The paper's contribution is a framework for protecting the M-Learning platform against malicious actors. Cryptography, stenography, watermarking, and data integrity methods are used to protect the data. Cryptographic algorithms are first categorized as either symmetric or asymmetric. When using a symmetric approach, both the sender and the recipient share the same secret key. The encryption and decryption keys in an asymmetrical algorithm are different. All sensitive data is encapsulated under a "cover variable" while using stenography. When data is accessed, watermarking verifies the legitimacy of the source. The data integrity tool serves to verify the accuracy of the data. Hash, Message Authentication Code (MAC), and Digital Signature are all included. These cryptographic protocols allow for secure data transit and user-to-user interaction. Users' communications are protected in this way. In The approach we propose for protecting M-Learning data is based on a notion of a circular queue. It has several potential uses, including in M-Learning, networking, and messaging services, to name a

few. As the world of information technology evolves rapidly, it opens up new learning modes. M-Learning allows for group study and productive dialogue between students and teachers. The M-Learning App makes it possible for students to study virtually anywhere, anytime. It piques their curiosity and encourages them to explore a wide range of subjects. More benefits to the students are attributed to M-Learning than to E-Learning in the areas of education, design, learning format, and a well-thought-out User Interface (UI). The educational institutions and students have serious worries about the risks and assaults over updating the data, despite the fact that M-Learning gives new learning techniques. Due to the prevalence of mobile device usage among students using the M-Learning Application, there is a potential risk to students' personal information and right to privacy. The primary focus of M-learning has been on the creation and distribution of courses, with little thought given to the safety and confidentiality of student information. By looking at the several studies, we can see that experts aren't too worried about safety concerns in M-Learning. The paper's contribution is a framework for protecting the M-Learning platform against malicious actors. Cryptography, stenography, watermarking, and data integrity methods are used to protect the data. The cryptographic algorithm is first categorized as either asymmetric or symmetric. The symmetric approach uses a shared secret key between the sender and the recipient. Two separate encryption and decryption keys make up the asymmetrical algorithm. For privacy reasons, stenography always places the sensitive data within the cover variable. When information is accessed, watermarking verifies the legitimacy of the source. Data integrity serves as a method for ensuring the correctness of data. Hash, Message Authentication Code (MAC), and Digital Signature are all included. These cryptographic protocols allow for secure user-to-user data transfers and communications. It ensures the privacy of each user's communication. Our suggested model employs an approach based on a circular queue data structure to protect M-Learning information. It has a wide range of potential uses, including M-Learning, networking, and messaging.The other sections of this study are structured as follows: a literature review in Section II, a detailed explanation of our suggested model in Section III, a discussion of the experimental findings and results in Section IV, and a summary and conclusion in Section V.

II. LITERATURE REVIEW

Matetic et al [1], the paper presents the discovery of knowledge about the process of learning using batch data analysis performed by Artificial Neural Networks (ANNs). ANNs are not a common method in the field of educational data mining. Although highly accurate, the resulting black-box model is not interpretable, which is a major drawback. For the opening of the ANN black-box model, as well as for other models of this type, several agnostic methods have appeared recently, some of which we illustrate in the LMS system analysis. Septia et al [2], where the development of ICT technology has delivered a significant impact on the development of the game industry. Currently, the gamification method is widely applied in the world of education. The Gamification learning method means applying a game into the learning process, to foster motivation to learn and change student behavior. It makes teachers more creative in designing the learning process. Some of the developers have learned more about psychology science or other sciences that study human motivation and behavior. The aim is to motivate students in the learning process and maximizing feelings of enjoyment and involvement with the learning process, besides this media can be used to capture the things that interest students and inspire them to keep learning. This study aims to propose a gamification model that is flexible in LMS, have good performance and can be improved student performance in their study. Information security to make the ciphered message more difficult to decipher. For instance, the authors of paper [5] developed an algorithm that uses the shifting and replacing operations of bi-column-bi-row for the circular queue to increase security. A random number was used in this algorithm to control the shifting between the row and column, eventually, this leads to an increase in

the complexity of plaintext decryption. In the same vein, an elliptic curve algorithm was designed based on matrix scrambling using a circular queue [6]. This research also utilizes the shifting process to accomplish the encryption and the decryption of the text. Besides, a multiple circular arrays algorithm was developed to encrypt data using three circular arrays. This algorithm enabled the shifting (elements in the outer or inner array), swapping (elements among the circular arrays) and XOR function (for encrypting the text) based on generating random numbers

[7]. In contrast, a double encryption double decryption technique is proposed, which means the transmitter encrypts the text two times that leads the receiver to decrypt the cipher text twice using public key [8]. Also, an elliptic curve algorithm is developed to produce a cipher text [9]. Actually, in this work, the text firstly formed into ASCII code, and then the prime number and random number are chosen and formed into binary format. Where the "0" representation of the prime number is responsible for shifting the row/column in upward and left respectively. Besides, a multiple access circular queues algorithm is proposed with variable length in [10]. In this work different numbers of rotations are applied to the circular queues, swapping the elements in the same queue and XORing the elements with generating key numbers. The authors recommended that these processes would make a secure plaintext over the transmission line. On the other hand, the Fibonacci sequence is mostly used for image encryption. A text to image encryption algorithm is designed using the Fibonacci sequence [11]. This algorithm firstly converts the plaintext using the Fibonacci sequence, and then the Unicode is converted to a hexadecimal number and an RGB matrix. Finally, a shuffling operation is made to obtain the image to be sent.

PROPOSED METHOD

The M-Learning proposed model concern securing the data of the client and server.

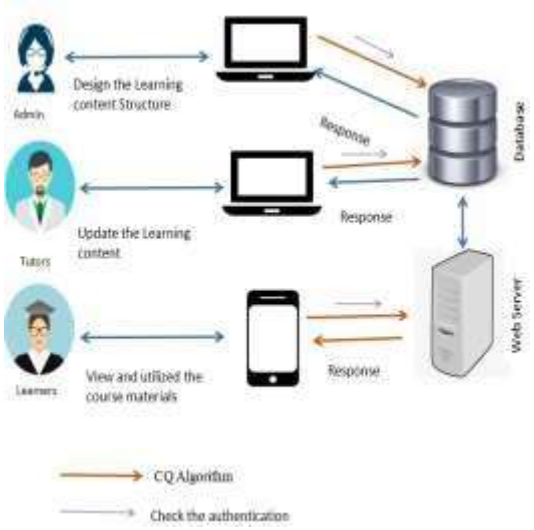

Fig 1: Architecture Diagram of Proposed Model

The architecture diagram of the proposed model is depicted in Fig 1. The Circular Queue algorithm is used to secure the client and server data from the attackers. The learning content is stored in the LMS. The admin can access the database based on the authentication role, if the authentication is failed then they can't access the data from the database. The model constitutes three roles such as Admin, tutors, and learners. Admin is responsible for structuring the courses and maintaining the databases. The admin contains an authorized username and password for accessing the server. The role of tutors has to update the course materials, monitored the performance of the learners, conduct a test, and improving their learner's skills. Each tutor is provided with a unique username and password. At last, the learners can access the M-Learning Server if they get the authentication for login. We concern about securing user privacy by encrypting all the profile details and user data with the CQ algorithm.

3.1 User Privacy

In mLMS, it collects some personal data such as learner's preference, personal details, assessment details, goals which help the system to collaboration the users and enhance collaborative learning. For example, the learners are learning some content from the mLMS, geographical location, browsing behavior are easily monitor by the Application which can be hacked by the

attacker if there is less security. It is easy to gather information from the devices, it is essential to preserve the privacy of the users. To secure sensitive data such as IP address, International Mobile Equipment Identity (IMEI), call record, web browsing log files, security credential, etc..

3.2 Circular Queue Algorithm

The Circular Queue provides encryption and decryption of the data and it is difficult to decryptthe original data. The factors of the Algorithm is represented below such as,

- The size of the circular queue is variable
- Beginning of the keywords is variable
- The Fibonacci Format

Encryption process

The input data is distributed to the circular queue algorithm where the letters are converted into equivalent 8 bits ASCII code and XOR function with each other. Then it represented in the decimal format.

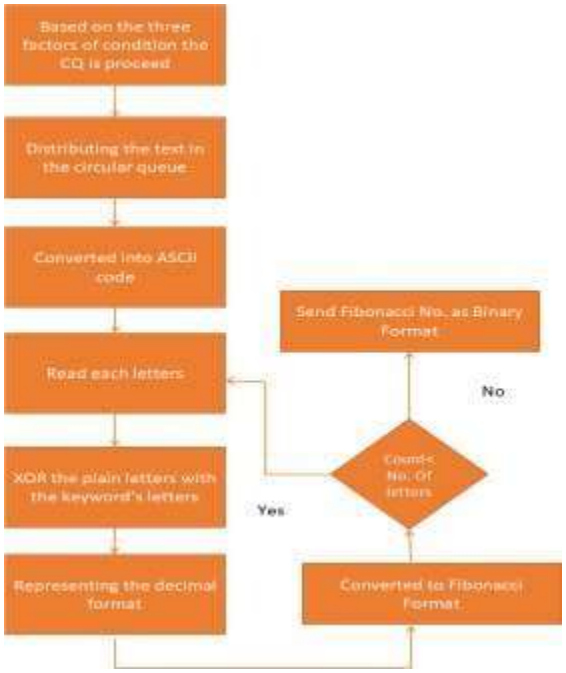

Fig 3: Encryption Process

At last, it demonstrated in Fibonacci format and sent as the cipher text and stored in a databasewhich is represented in Fig 2. The Encryption algorithm flow is depicted in Fig 3.

3.3 Decryption Process

The reverse process of encryption is decryption to recover the original message. After receivingthe Fibonacci format then the output value is XOR function with the key letters. At last, the original

data is recovered which is depicted in Fig 4.

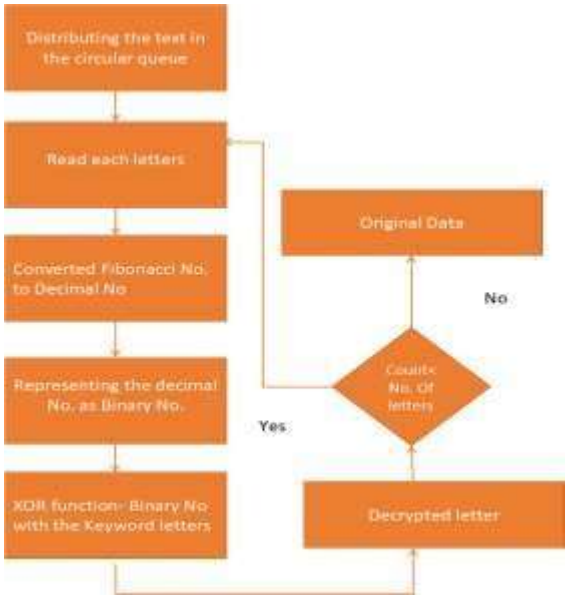

Fig 4: Decryption Process

3.4 Implementation of Proposed Model

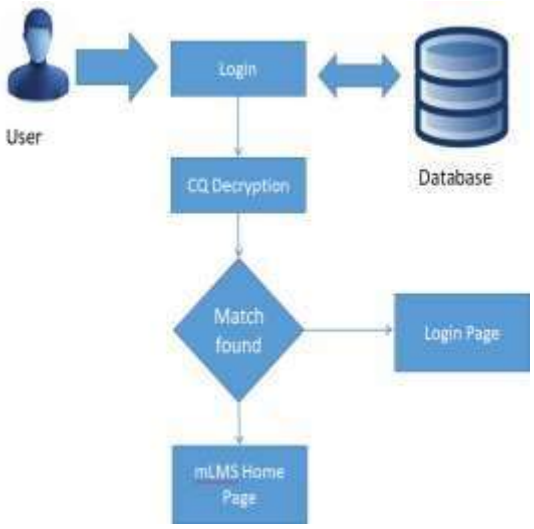

Fig 5 Authentication Process

The mLMS application provides security to the user privacy thereby providing security to the learning content stored in the LMS. The PHP and MYSQL code is used to develop the mLMS Application. The tutors have to log in to the mLMS using their username and password. The system checks tutor id in the database by decrypt using the CQ algorithm. If matched find then it allows accessing the data which is depicted in Fig 5.

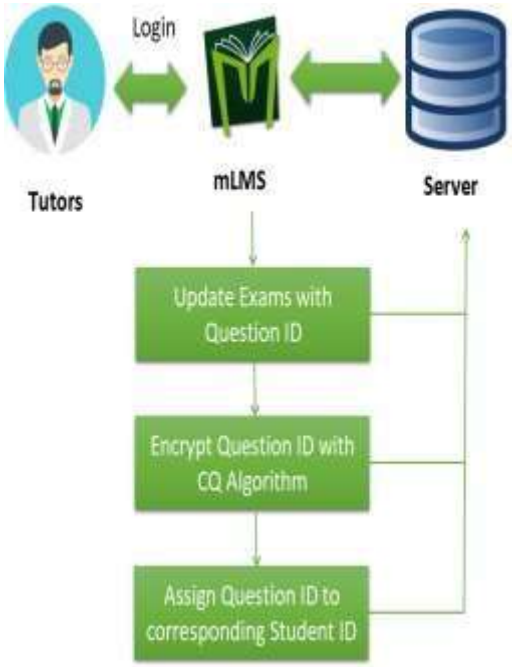

Fig 6 Upload Encrypted Exams to server

The tutors have to align the questions and appropriate options for it. He/she has to mention the subject name, duration, exam level such as easy, moderate and difficult, and percentage level or grade which is depicted in Fig 6. Then the tutor has to encrypt the exam content with the Corresponding exam Id and uploaded it to the server. Based on the client-server interface the questions will be integrated into the corresponding student labels. Each data will be stored in the encrypted format in LMS. After that, the teacher has to assign an exam Id for the different learners based on their skills. Once the student login to the Application they will access exam Id without constraint. The Learner can answer all the question and submit to the server where the mLMS generate the result. The result will display to the learners where the evaluated test results are automatically encrypted and stored in the server which is depicted in Fig 7.

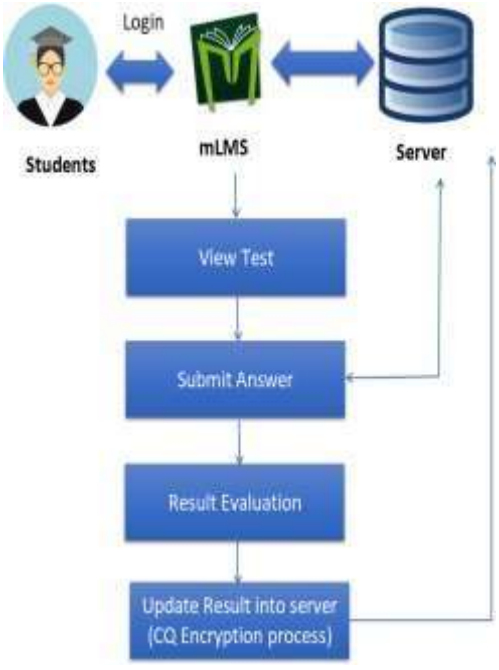

Fig 7 Submit Answer to server

III. RESULTS AND DISCUSSION

In this section, we review the security level of the mLMS Application using the CQ Algorithm.

Fig 8 Home Page of mLMS (Tutor)

The authenticated tutor can log in to their account for updating the upcoming exams for the learners which are depicted in Fig 8.

Fig 9 Adding Questions by Tutors

Server

Encrypted Question Id to server

Fig 10 Uploaded the Question ID to Server

The tutors can add numerous questions as per the question pattern. Once he/she completes the question pattern then they can update the question to the server which is depicted in Fig 9. The questions and answers are updated in the database where the question Id is encrypted using the CQ algorithm and send to the Server which is depicted in Fig 10.

(a) (b)

Fig 11 (a)mLMS menu (b)mLMS Home Page

The students can install the mLMS application in their android Mobile which is depicted in Fig 11(a). The authorized learner can log in into their account which is depicted in Fig 11 (b).

(a) (b)

Fig 12 (a) Learner Page (b) Test menu

The learner can use the test menu to take the exam based on the courses which are depicted in Fig 12 (a). The learner can answer the questions by selecting the options and then they can move on to the next questions. The exam allocated time is scrolled automatically at the starting of the exam which is depicted in Fig 12 (b).

(a) (b)

Fig 13 (a) Submitting Answer (b) Result Evaluation

After answering all the questions the learner can submit their answers using the submit button which is depicted in Fig 13 (a). Once the answer sheet is submitted the evaluation takes place automatically which is depicted in Fig 13 (b).

Fig 14 The Learner's Score

Based on the learner's answers, the mLMS generate the result for the answers and displayed instantly which is depicted in Fig 14. The evaluated result will be stored in the application memory.

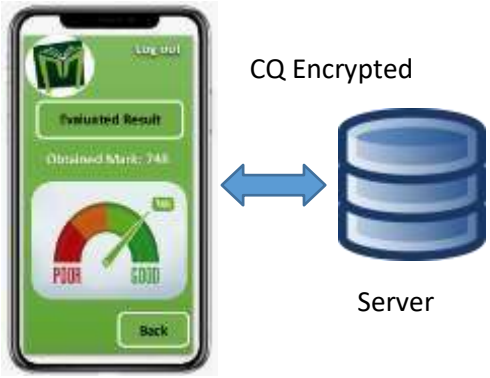

Fig 15 Evaluated Results send to the server

The Evaluated results are encrypted and stored in the Server which is depicted in Fig 15. The learner can only view their results and their upcoming exams.

Our Algorithm	Complexity	MACQ Algorithm	Complexity
XOR with keyword	$O(n^2)$	XOR with inner most queue	$O(n^2)$
		XOR with second inner most queue	$O(n^2)$

Table 1 Complexity Evaluation

From Table 1 we represent the complexity of two algorithms where n is a number of bits for the process. Compare to the MACQ algorithm, our algorithm is less complex and highly secure for transmission data.

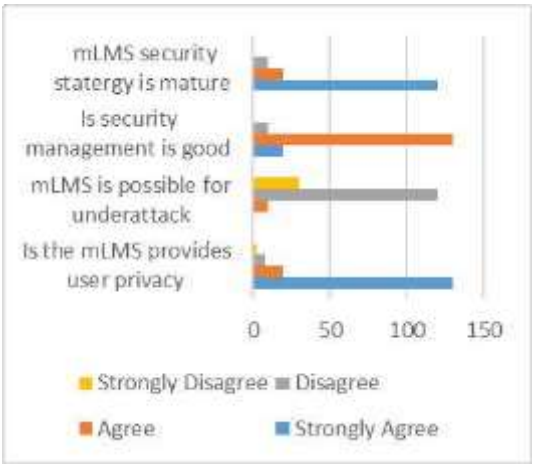

Fig 16 Survey on mLMS security

We surveyed the mLMS security level where 160 volunteers were responded to the security-based questions. The answers are categorized into strongly agree, agree, disagree and strongly disagree. mLMS got positive feedback from the learner's regard's the security level which is depicted in Fig 16. Due to the CQ algorithm, the system is highly secure and efficient for the users.

IV. CONCLUSION

We analyze the safety of user information and mLMS course materials in our suggested paradigm. We upgraded mLMS's security by relying on a brand-new data structure. The new information is encrypted using a combination of circular queues and Fibonacci numbers. High security for mLMS data is ensured by the use of a variety of variable parameters that make decryption challenging. When compared to the current method (MACQ), ours is far quicker. When compared to the current method, its complexity is modest. Therefore, the solutions we have described are a potential answer to efficiently protect the mLMS and user data.

REFERENCE

1) In the 2019 edition of the 42nd International Conference on Information and Communication Technology, Electronics, and Microelectronics (MIPRO), Metetic published "Mining Learning Management System Data Using Interpretable Neural Networks."

2) Septia Redisa Sriratnasari and others published "Applying Innovative Learning Management System (LMS) with Gamification Framework" at an international symposium on the use of information and communication technology in education. 2019

3) Thirdly, "Cryptography and Network Security" by Atul Kahate, published in 2013 by Tata McGraw-Hill Education.

4) 4) Ali J. Abboud, "Multifactor Authentication for Software Protection", Diyala Journal of Engineering Sciences, Volume 08, Number 04, Special Issue, 2015.

5) Ali J. Abboud, "Protecting Documents with Visual Cryptography," International Journal of Engineering Research and General Science, 2015.

6) Computer Security Division (Information Technology Laboratory), "Recommendation for Key Management-Part 1: General (Revision 3)", 2016. 6) E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid.

7) 2012 IEEE International Conference on Network Security and Systems (JNS2), "An Elliptic Curve Cryptography based on Matrix Scrambling Method" by Amounas, Fatima.

8) 8) S. S. D. Pushpa R. Suri, "A Cipher based on Multiple Circular Arrays", International Journal of Computer Science Issues (IJCSI), Volume 10, Issue 5, Pages 165-175 (2013).

9) In 2015, Springer Science & Business Media published "Guide to Elliptic Curve Cryptography" by Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone.

10) 2016 Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, S. Phull and S. Som, "Symmetric Cryptography using Multiple Access Circular Queues (MACQ)".

11) Data Encryption Using Fibonacci Sequence and Unicode Characters, by P. Agarwal, N. Agarwal, and R. Saxena, MIT International Journal of Computer Science and Information Technology, Volume 5, Issue 2, Pages 79-82, August 2015.