Republic of Iraq
Ministry of Higher Education
And Scientific Research
University of Diyala
College of Science

Secured Data in Mobile Learning System

A Thesis

Submitted to the Computer Science Department \College of Science \University of Diyala

In a Partial Fulfillment of the Requirements for The Degree of Master of Science in Computer.

By

Ibtesam jomaa Hawi

Supervised by

Prof. Dr. Ziyad Tariq Mustafa

2020 A.D. **1441 A.H.**

بسم الله الرحـمن الرحـيم

(يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا
الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ)

صدق الله العظيم

سورة المجادلة (11)

Dedication

My dear mother…

My dear husband…

My dear sisters…

My precious children lamar and Abdullah…

My dear friend Rasha…
I dedicate you with a heart full of gratitude to you the fruit of my effort and labor
Without you, the dream would not have come true.

Ibtesam

2020

Acknowledgment

In the name of Allah, the Merciful. I am grateful to my Creator who blessed me with abilities to complete this thesis.
I thank ***Prof. D. Ziyad Tariq Mustafa****, and for his guidance and ideas to complete this work, I thank him for those hours and ideas that you shared with me, and express my sincere thanks and deep gratitude.*

I would like to introduce my thanks to Department of computer science in the collage of Education of the Diyala University for their help, teaching and cooperation in the last two years

I would like to present special thanks to **Mr. Ali Hussein Fadel** *for his guidance, endless support.*

would like to express my special appreciation and deep thanks to all those who have helped to allow me to bring this letter

Finally, I would like to thank my family, who have endured the difficulties of this stage, throughout their days and nights, without her presence I would not have arrived for this day.

Ibtesam

2020

Linguistic Certification

This is to certify that this thesis entitled **“Secured Data in Mobile Learning System”** *was prepared under my linguistic supervision. It was amended to meet the style of English language.*

Signature :

Name :

Date: / / 2020

Supervisor's Certification

I certify that this thesis entitled **"Secured Data in Mobile Learning System"**, *was prepared under my supervision at Department of Computer Science\ College of Sciences\ University of Diyala by* **"Ibtesam Jomaa Hawi"**, *as a partial fulfillment of the requirements for the degree of* ***Master of Science in Computer Science***

(Supervisor)

Signature:

Name: Prof. Dr. Ziyad Tariq Mustafa

Date: / / 2020

Approved by University of a Diyala Faculty of Science Department of Computer Science.

Signature:

Name : Assist. Prof. Dr. Taha M. Hassan

Date : / / 2020

(Head of Computer Science Department)

Examination Committee Certification

We certify that we have read the thesis entitled **“Secured Data in Mobile Learning System”** *and as examination committee, examined the student* **“Ibtesam Jomaa Hawi”** *in the thesis content and that in our opinion, it is adequate as fulfill the requirement for the Degree of Master in Computer Science at the Computer Science Department, University of Diyala.*

(Chairman)
Signature:
Name:
Date: / / 2020

(Member)
Signature:
Name:
Date: / / 2020

(Member)
Signature:
Name:
Date: / / 2020

(Member)
Signature:
Name:
Date: / / 2020

(Member)
Signature:
Name:
Date: / / 2020

Approved by the Dean of College of Science, University of Diyala

(The Dean)

Signature:
Name: **Prof. Dr. Tahseen Hussein Mubarak**
Date: / /2020

Abstract

Last years, the concept of smart classroom is appeared in educational systems, this concept is focused on mobile learning environment because of increasing the flexibility of distance learning, and providing a new type of digital culture. That culture concentrates on the processing of knowledge and helps the student to be the center of the learning process and not the teacher. This thesis focuses on design and implementation of a complete wireless interaction mobile phones learning system through a server using web services, for a classroom. The proposed system gives the server (administrator) an authorization to allow mobile phone of users (student) to access the proposed system in order to take the lecture and participate in an exam after reliability of the student is checked. Reliability is an important and essential part of the proposed system depending on the location of the mobile phone student. If it is within the limits of the smart classroom, then the server (administrator) is authorized to provide ciphering keys to the student. These keys are assigned to authorized students using the key management system It provides unique and variable key assignment for each authorized student used later in encryption and decryption using Improvement RC6 (IRC6) algorithm.IRC6 key generation based on two types of chaotic maps (chebyshev , 2D logistic) in order to generate N key to N users. The results showed the success of the proposed system in detecting the location of students within the smart classroom using the min value of the Haversine formula and comparing it with the threshold value .The results prove that the average secrecy of IRC6 is better than of traditional RC6, in which: for 16 bits' key length, and 128 bits plaintext size, the average secrecy of IRC6 is (0.390 - 1.413) while for RC6 is constant value (0.244).

List of Content

Chapter one: Introduction		1
1.1	Introduction	1
1.2	Related work	3
1.3	Problem Statement	8
1.4	Aim of thesis	8
1.5	Contribution	8
1.6	Thesis outline	9
Chapter Two: Theoretical Backgrounds		10
2.1	Introduction	10
2.2	Mobile Learning (M-Learning)	10
2.3	M-Learning Security	12
2.4	Authentication	13
2.5	Password Authentication Scheme	14
2.6	Key management	15
	2.6.1 Factors that Affect Key Management	16
	2.6.2 Key Management Techniques	16
	2.6.3 key management functions	18
2.7	Rivest Cipher (RC6) Symmetric Cipher	18
2.8	Chaotic Map	24
	2.8.1 Chebyshev 1D chaotic map	24
	2.8.2 Logistic Map	25
2.9	Web Service	26
	2.9.1 WSA Functional Components	28
	2.9.2 Web Services security	28
	2.9.3 The Basic WS Technologies	29
	2.9.3.1 Web Service Description Language (WSDL) 2.9.3.2 Universal Description, Discovery, and Integration (UDDI) 2.8.3.3 Simple Object Access Protocol (SOAP)	31 31 31
2.10	Location Based Services	34

	2.10.1	Coordinates Conversion	34
	2.10.2	earth's radius	35
	2.10.3	Haversine formula	36
2.11	Average Security		37
Chapter Three: The Proposed system			39
3.1	Introduction		39
3.2	Design Objectives		39
3.3	The Primitive Proposed system		40
	3.3.1	Administrator Side	40
	3.3.2	Client Side	42
	3.3.3	Web Application Services	43
3.4	Architecture of the Proposed system		44
	3.4.1 The Main Network Structure of the Proposed system		44
	3.4.2 Design of the Proposed system		45
	3.4.2.1 Design of the Database on Server Side		45
	3.4.2.2 Design of the Administrator (Admin) Side		46
	3.4.2.3 Design of the Client (User) Side		46
	3.4.2.4 key management		47
	3.4.2.5 web application server		48
Chapter Four: Implementation and results			62
4.1	Introduction		62
4.2	Initialization		62
4.3	Implementation of The Proposed system		62
	4.3.1 Implementation of Administrator		62
	4.3.2 Implementation of Client		65
4.4	Results of the Proposed system		68
	4.4.1 Mobile Location Test		69
	4.4.2 The Results of the Proposed IKSA for IRC6 Algorithm		73
4.5	Tests		78
	4.5.1	Example of Encryption using IRC6	81

Chapter Five: Conclusions and Suggestions for Future Work		83
5.1	Introduction	83
5.2	Conclusions	83
5.3	Suggestions for Future Work	84
Reference		85

List of tables

Table (2.1):	Differences between E-learning and M-learning.	11
Table (2.2):	RC6 Operations.	19
Table (3.1):	Boundary Locations from Mobile in Classroom	50
Table (4.1):	Test Samples of Students Mobile Phone Locations	69
Table (4.2):	Haversine Distance Values using Proposed Authentication Method with Student Mobile Locations (SMLs)	70
Table (4.3):	Key generation using IKSA with Different Initial parameters for chebyshev and 2D-logistic Chaotic Maps.	74
Table (4.4):	Average security for RC6 and IRC6.	78
Table (4.5):	Highest values of average security for the RC6 and IRC6.	80
Table (4.6):	Encryption /Decryption student answer using IRC6 .	81

List of Figure

Figure (2.1)	The evolution of the learning platform	12
Figure (2.2)	Explains the RC6 algorithm cipher	20
Figure (2.3)	Bifurcation diagrams of the Logistic map	26
Figure (2.4)	The Three Thoughts Roles and Operations of Web Services	27
Figure (2.5)	Relationship between technologies (SOAP, WSDL, and UDDI).	30
Figure (2.6)	The format of the message elementary layout	32
Figure (2.7)	Web services communication stack	33
Figure (3.1)	Primitive Model of the Proposed system	40
Figure (3.2)	Diagram of Administrator Functions	41
Figure (3.3)	Diagram of Client Functions	43
Figure (3.4)	Primitive Block Diagram of the Web Application Server	44
Figure (3.5)	Main Network Structure of the Proposed system	45
Figure (3.6)	An Example of the Key Management	47
Figure (3.7)	Grid Location Points for Smart class Room	54
Figure (3.8)	Block Diagram of the IKSA and IRC6 algorithm	57
Figure (4.1)	The Interface of Administrator detect location.	63
Figure (4.2)	The Interface Administrator calculating grid location.	64
Figure (4.3)	The interface for storing grid points with database in the server	65
Figure (4.4)	The Main Interface of the Client Side.	66
Figure (4.5)	Calculates the haversine distance Interface.	67

Figure (4.6)	Interface of Student Authentication	68
Figure (4.7)	Assign secret key process in web application services side and client (student) side for user1,(a)web services input ,(b)web services output ,and (c) mobile of user1	75
Figure (4.8)	Assign secret key process in web application services side and client (student) side for user2 (a)web services input, (b)web services output ,and (c) mobile of user2	76
Figure (4.9)	Assign secret key process in web application services side and client (student) side for user3 (a)web services input, (b)web services output, and (c) mobile of user3	77
Figure (4.10)	Comparison between RC6 and IRC6	80

List of algorithms

Algorithm (2.1):	Key-Expansion RC6 algorithm	21
Algorithm (2.2):	Encryption RC6 algorithm	22
Algorithm (2.3):	Decryption RC6 algorithm	23
Algorithm (3.1):	Create Grid Points	49
Algorithm (3.2):	Authentication Test	56
Algorithm (3.3):	Improved Key scheduling algorithm (IKSA)	59

Abbreviations

$\vec{u}$	vector expressed in Rectangular Coordinates
1D	One-dimensional
2D	two-dimensional
a	ellipsoidal equatorial radius
AES	Advanced Encryption Standard
b	length of the encryption key in bytes
CTSS	Compatible Time-Sharing System
d	distance
Dec	Decryption
D-learning	Digital learning
e	base of natural logarithm
$\mathbf{e^2}$	eccentricity of ellipsoid
E-learning	Electronic learning
Enc	Encryption
H (k/c)	Entropy of a message
HTTP	Hypertext Transfer Protocol
IKSA	Improvement key Scheduling Algorithm
IRC6	Improvement RC6
Lat	Latitude
LBS	Location Based Services
log	Logarithm
Lon	Longitude
M-learning	Mobile learning
n	degree of chebyshev polynomial
NIST	The National Institute of Standards and Technology
No	Number of users
ø	geodetic latitude
Odd(x)	Odd integer nearest to x.
OTP	One-Time Password
r	number of rounds
R	radius of the earth
RC5	Rivest Cipher5
RC6	Rivest Cipher6

RPC	the rectangular coordinate to the polar coordinate
RSA	Rivest–Shamir–Adleman
SML	Students Mobile Location
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
TTP	Trusted Third Party
UDDI	Universal Description Discovery and Integration
V	Vector
W	word size
WS	Web Service
WSA	Web Services Architecture
WSDL	Web Services Description Language
$\mathbf{X_0}$	initial value of chebyshev function
$\mathbf{X_{00}}$	initial value of logistic function
XML	Extensible Markup Language
$\boldsymbol{\lambda}$	control parameter of logistic function
$\boldsymbol{\rho}$	vector length

Chapter One

Introduction

Chapter One

1.1 Introduction

Modern trends in technological development have forced learning to follow its steps. Teaching professionals have focused on the new learning methodology, such as learning. Because e-learning uses a variety of devices, many of which spread in the lives of students. Therefore, it can enhance student participation and provide opportunities to make learning an integral part of their daily activities, making the education process more durable, private, cooperative and long-lasting [1].

The contribution of technology has been to the overall learning activity level through the globe together in terms of number and outreach. The quick development in the portable diffusion person computing and devices of communication, specifically, smartphone and tablets, has allowed an extensive implementation of technology-depending learning of non-traditional [2].

The usage of mobile devices such as smart phones and tablets can host educational applications which can be used anywhere, anytime, at the user’s convenience [3].

There is extensive spreading of the Mobile learning (M-learning) due to the growth of mobile devices with progressive technology of the wireless communication which has stimulated education “on the move,” by the use of mobile devices in educational situations. This innovation of the technology has stimulated advanced education organizations to growth the mobile use technology to accomplish the prospects of their students and requirements. At current, many students who are undergraduate carry their personal digital devices to university, and they imagine to get the admittance to the academic resources by the use of their mobile devices [4].

The M-learning become the method to learn that augment classroom and e-learning because it has properties of flexibility and diversity. It is a trend that is in growing and lengthens learning outside the theatres of the lecture and can be exploited to respond to the challenges of particular educational contexts, accompaniment and improve formal schooling, increase and help learning for people of different ages and opportunities for augment learning in publics where opportunities of the educational are limited [5].

The consideration of the security of mobile learning is becoming progressively significant due to the fact that additional colleges are installing technologies of mobile to match their delivery of the classroom learning and the use of technology devices in learning by the mobile which can possibly become vulnerable if the security aspects are neglected [6].

Recently, there have been numerous violations of mobile devices since they became popular, particularly in systems of the open operating. With the increased use of portable applications and devices to store or access information that is personal and sensitive, the most worrying thing is to be open and popular platform provides such a convenient Android environment to exploit and deploy security attacks [7].

Security requirements that must be present in mobile applications are [8]:

1- Authentication – a feature that is required only if important information must be accessed in a restricted method; different types can be used for authentication like password, biometric, etc.

2- Network Security – the characteristic that is usually very limited or is missing due to the technological restrictions which are still present;
3- Application Security – for applications that are always online, the security can be controlled by a server.

This thesis concentrates on improving the authentication system by using a mobile learning system in the smart classroom by using detect location instead of password to give authorization to the student, which increases the speed of the propose system and using the create grid point algorithm to determine the location of the student for the smart class and determine whether it is authorized or not. An effective algorithm was developed to improve the security performance of the traditional RC6 encryption algorithm by adding a chaotic map to generate N key for N user with various length and use this key to encrypt lectures, exam questions, student answers, homework, etc., for more security and reliability we used the Key Management and using a Web server as a firewall.

1.2 Related Work

Many researchers have proposed many works about security and authentication in M-learning. The following are some studies and researches related to this:

- **F. D. S. Bahry et. al. in (2015) [9]**, In this work the points of view of the academics on the measure of the security on mobile learning are obtained and inspected . In common, it determines connected degree on security that comprises dependability, confidence, secrecy and security itself. The determinants are used by every measure in earlier studies and its variety in certain environments and perceptions. Determinants of the dependability and security are extensively improved to measure in terms of the environment of the infrastructure of mobile learning, even though confidence and secrecy typically measure performances and insights from the user or human to mobile learning. Additional features of the security that are deliberated at peek comprise the distribution of the key and management, confidentiality of the information and privacy, safe routing, detection of the intrusion, integrity of the data, authentication of the entity and aggregation of the secure data. It plotting on the related security measures with every mobile learning component will be expressed for additional study.

- **S. S. Oyelere, D. I. Sajoh et. al. in (2015) [10]**, In this work a number of damaging effects of cybersecurity neglect in m-learning were discussed. lecturers and students both stated their point on these problems: data lost, loss of privacy, disturbance of psychological, loss of confidentiality and trust on education, copyright breach and piracy, examination misconducts, academic performance decrease and study time loss. These problems requisite to be well show up to withstand the m-learning advantage , they suggested certain methods to decrease threat of cybersecurity on m-learning are mechanisms of connection of cybersecurity like ant phishing ,anti-malware , firewalls, and anti-virus, engagement of extremely skilled security specialists to achieve m-learning systems, data backing-up and systems of m-learning, data encryption fixing and biometric defense and boarding on public consciousness about problems of cybersecurity, Suitable plan and systems implementation useful in web-based learning and adequate cybersecurity management for m-learning platforms will convert to improved learning, effectiveness, fulfillment and suitability of m-learning.

- **S.A Shonola et. al. in (2016) [7]**, they established enhancement app of m-learning security to increase the awareness of the students, supplement current security in devices of m-learning and offer information on decreasing dangers. They offered an improvement app to deliver education for the security and consciousness between the students who involve their devices of the mobile for learning. The app aids in making the content of the learning on the portable devices over mechanism of file-lock and provides students and educators comparable, the chance to exercise tasks of simple security. The improvement app of the security does flaw checks or examinations and make suggestions for a suitable commendation. The app watching facility aids to observe additional apps that may be malware or spyware, by the use of services of the scanner and directs even announcements to the users concerning whichever problems of the security or doubtful app. The app is regard appropriate for the aim as it aid to resolve some of the problems of the security that students have met in the previous. Above all, the app does what it says as it provides extra security facilities in addition to normal device security. Thus, the app enhances the in-built security features of mobile devices.
- **Yu Li et. al. in (2016) [11]**, In this work a scheme of privacy conserving was designed for learning on distant, in that the use of smart phones by the students to get admission to online materials and courses. Technology of the ARM Trust Zone was used to stock the delicate data and they implement robust tools of the cryptographic in scheme designing, the examination and assessment prove that their scheme is certainly privacy conserving with great effectiveness. Their influences are: first to study learning on distance of privacy conserving and suggest the structure that

can defend privacy of the students in learning on distant, they examine the student’s privacy in their structure. There is no leak for any considerable information relates to the students scheme no matter it is in the server or smart phone and finally assessment displays that the system is useful with great effectiveness.

- **G. Kalpana et. al.in (2017) [13],** In this work a Shifted Adaption Homomorphism Encryption (SAHE) was proposed, that is considered as the improved choice for all the present study going on. SAHE execute the minimum public key of 32 bit and it has the capacity for integer and real numbers encryption. A main problem in research field is struggle in defensive questions of the user, that is located by considering a technique of encryption of public key that is depending on the reversed index. The schema preserves search efficiency using inverted index, by solving one-time only search. This method is appropriate for mobile learning since the suggested algorithm will not use the mobile memory or power.
- **Kai Qian, et. al. in (2017) [12]**, This work addresses the needs for pedagogical learning materials are located for education with database security and the defies of database security building capability over operative, attractive, and analytical learning methods, over moveable and integrate able mobile-constructed learning modules with hands-on confidante labs depending on the commendations of the OWASP, like validation of the input, encryption of the data, sharing of the data, checking, and others. they generate an environment of motivating learning which inspires and involves all database security ideas of the students and practices learning. The initial student’s feedback was optimistic. Students increased experiences from hands-on real world learning on Mobile Database Security (MDS) with devices of the Android

mobile that also significantly encouraged students' self-effectiveness and self-assurance in their learning with mobile security.

- **Yi Cai, et al. in (2018) [14]**, In this work they implemented a framework of the authentication that has the capability to classifier training with time sequence data. To assess the behavioral biometric performance of the system of the authentication, three experiments are designed to estimate the reliability, safety and accuracy when the data is collected in different scenarios. In decision, authentication of the online training depending on system provides equivalent performance when allocating with data of the time-series and the biometric information behavior of illustration pattern is noticeable when smartphone authentication used. This type of biometric authentication behavior system has two chief benefits: (1) update is easy and (2) without memory, is not only smartphone unlocking applications, but also can show a significant starring role in additional platforms with other sequential of time-series systems, like gait and Simband.
- **Olugbenga W. Adejo et al. in (2018) [15]**, In this work they explained the various benefits of the using m-learning platform and cloud infrastructure in higher education and examines the vulnerabilities of the platform in addition to additional challenges of the security and privacy concerning the effective execution of environment of the m-learning in cloud infrastructure. They propose a detailed data protection and security framework that is wanted for locating these problems. The predictable that the suggested structure when fully executed, will give all essential answer to problems linking to the security and protection data of m-learners in environment of the cloud computing, rise by the use of the system trust along with improve the m-learning platforms, they propose a data protection and security framework for m-learning that can be used

within cloud infrastructure with enhance protection cutting across all the three components -the devices, the network and the cloud infrastructure.

1.3 Problem Statement

Technology is explosively growing, which positively effects leaning systems and led to expression of smart classroom. The first problem with these classrooms is how to recognize their students. The second problem, is that the students must be learned through interactive learning system using mobile phone. The third problem is how to secure data and authenticate students through the mobile learning system.

1.4 Aim of Thesis

The aim of this thesis is to solve the three problems which are mentioned in section (1.3). Therefore, the aims of this research are:

1- Recognizing the students inside the smart classroom using a geographic technique that used Eclides theory to calculate distances.
2- Design and implement complete mobile interaction learning model for a smart classroom through a server using web services and android system.
3- Securing the transferred data in the mobile learning system through an improvement of RC6 encryption using chaotic map.

1.5 Contribution

The main contribution of this thesis is implementing mobile learning system for smart classroom. However, the new contribution in this thesis is using of authentication system for recognizing students which is depending on geographic technique of specifying the boundaries of classroom. Another contribution in this thesis is the using of good combination of security through an improvement of RC6 encryption using chaotic map.

1.6 Thesis Outlines

The remaining chapters are:

Chapter two which is entitled theoretical background: presents Authentication and its types, RC6 encryption algorithm with Chaotic map, mobile learning, Web service, Location based services and other concepts that are relate to the proposed system.

Chapter three which is entitled The Proposed System: presents the main proposed system, design objectives, and covers the communications and techniques that are used to authenticate communications of mobile learning.

Chapter four which is entitled The Results: This presents the results and tests of the proposed system.

Chapter five which is entitled Conclusions, and Suggestions for Future Work: presents the conclusions for the proposed systems, and suggestions for future work.

Chapter Two

Theoretical Background