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 الرحمن الرحيم

(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

Chapter Two
Theoretical Background

2.1 Introduction

This chapter presents the theoretical background of this work. Mobile learning (M-Learning) and Mobile learning Security is presented in subsection (2.2) and (2.3). While, subsection (2.4) presents an authentication concept. Password authentication is given in subsection (2.5). Subsection (2.6) shows key management. RC6 algorithm is covered in subsection (2.7). Chaotic map is clarified in subsections (2.8). Subsection (2.9) introduces the idea of Web service. Subsection (2.10) shows location finding. Finally, subsection (2.11) presented the average security.

2.2 Mobile Learning (M-Learning)

M-learning provides an opportunity to learn anywhere, anytime and to keep convenience of learners. With the comprehensive presence of mobile devices among students, educational institutions around the world have begun using mobile technology to facilitate learning in new and innovative ways. Mobile phone technology can improve the students' learning experience and performance [16].

The wide distribution of technologies of mobile and becoming inexpensive and obtainable between large age groups range, and their influence on scope learning embraces flexibility, availability, proximity, location, outreach, comfort and context. M- learning has the potential to transform the learning from the students through numerous conceptual, physical and societal spaces.

M- learning definitions include common characteristics such as portability, originality, context, social interaction and customization [17].M-learning would be a natural evolution of E-learning, permitting both students and users to have a process of learning over technology of mobile [18]. Every distribution of educational awareness across the internet is defined by E-Learning, which make it a subdivision of technology-constructed on training [19].

M-Learning is often described as occupying a sub-space within the E-Learning space, which is in turn a sub-part of digital learning. The major variances among E-learning and M-learning are describe in table (2.1) .

Table (2.1): Differences between E-learning and M-learning [15].

	E-learning	**M-Learning**
Aim	For in-depth knowledge about a subject	Quick accessibility and knowledge transfer when Needed
Approach	Formal learning	More flexible and informal than E-learning. Allow more freedom
Medium	Desktops or Laptops	Mobile devices- Phone, tablet, PDA
Accessibility by user	Limited to where there is internet and Static	Anywhere, No geographical boundaries
Design	Detail information and more media Interactivity	Sometimes the information may not be detailed but bite-sized modules
Retention	Varied	High due to level of accessibility on the go
Cost	High cost of acquisition of desktop or Laptop	Mid-range cost, affordable by many

Because of the shortcomings of E-learning in the areas of cost and time disadvantages as well as advances in internet technologies, the world is witnessing a shift in the use of E-learning for M- learning. Figure (2.1) below displays the development of the learning platform [15].

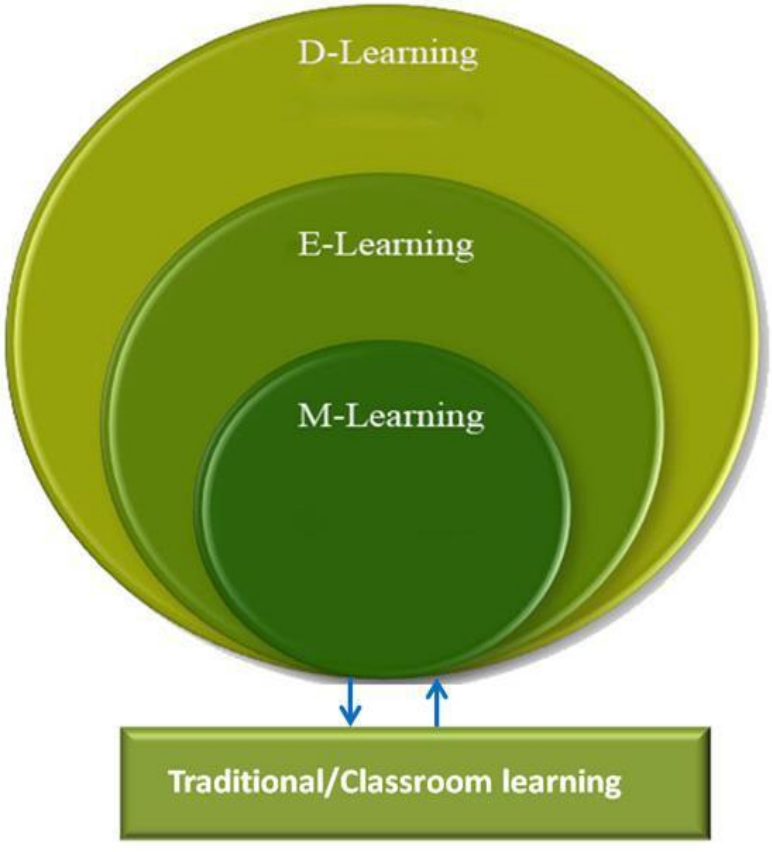


Figure (2.1): The evolution of the learning platform [15].

2.3. M-Learning Security

The element of security plays a major role in any type of application. Higher institution members are concerned about the authentication and security of M-

learning. There is some certain characteristic that a communication of secure mobile should contain: key distribution and management, Information confidentiality and privacy, secure routing, intrusion detection, data integrity, entity authentication and secure data aggregation. All of the above features must be provided if we want to have a fully secured transmission of learning materials by the means of the mobile devices mentioned as well as wireless computing. The two significant requirements of the security: confidentiality and data integrity which can be obtain by executing mechanisms of simple link-layer security in which the packets are encrypted and employ message authentication codes, the authentication is also an important security property as it ensures the receiver that the message did came from the originated or right sender [9].

2.4 Authentication

Authentication and the various measures of authentication are used to verify that a specific user or process is who they say they are. There are four standard ways that users are authenticated [20]:

1- **Something you know** – the most common method that many users are acquainted. The method in which this standard is presented by username or password that is recognized only to the user.

2- **Something you have** – This form of authentication is represented by the user having possession of a physical entity or device. This can be represented as a physical token such as the user's smartphone or other media device generating a temporary and sometimes single use authentication code.

3- **Something you are** – This type of authentication is symbolized as a biometric signature like fingerprint, scan of retina, or recognition of the face. This is usually considering one of the toughest type of authentication when implemented properly.

4- **Someplace you are** – This form of authentication corresponds to where a user or process is located, and in response gives or denies access to resources accordingly. An IP addresses can be used to implement this form through the use of a variety of IP or geographic site points for multifactor authentication to be showed properly.

Regrettably, each factor has its own disadvantages. For example, passwords are susceptible to attack of off-line guessing, phishing, etc. there are a chance of losing or the stealing of the smart card, and the data kept can be removed. Data of the biometric cannot be easily altered or canceled. An operational method to release these issues is to merge all these three factors, that is recognized as authentication of the three-factor [21].

2.5 Password Authentication Scheme

Today's systems use the traditional authentication system to authenticate users by secretly entering a word of their choice for example password. When the password entered, the system will look for the arrived username and password in the hash of the password. If the system's kept password equals the arrived password for the stated username, the authenticated of the user is done in the system . There are many disadvantages of this system. Passwords of this sort are severely weak against brute force attacks and dictionary attacks. It is also vulnerable to key logging, shoulder surfing, guessing attack, multi factor authentication and offline attacks [22]. The compounds of the password are a secure phrase or characters string which can be used to obtain access to a protected resource. The first time the passwords were used in the Institution of Massachusetts of Technology in 1961 for retrieving a huge time-sharing depending on the computer called Compatible Time-sharing system (CTSS) Password can be classified in two:

1- Static Password: Is a type of password that does not change. A merged alphanumeric and distinctive characters are used for the authentication. This method is weak to the attacks of the key logging, dictionary and brute force.

2- Dynamic password (one-time password) OTP: Is a type of authentication technique that the password changes. Dynamic password varies based of on the change factors and function, factor could be time lapse, or occurrence of an activity, function define how this factors take in the factors as parameters to change the accepted password at a particular time. Authentication by the dynamic password uses a system of third party for producing accepted password. The static passwords are easier to recall compared to the dynamic passwords [23]. There for many schemes of authentication for one-time password have been suggested to protect the authentication data and user password. Schemes of authentication for one-time password are regularly assessed depending on three features, simplicity, security and efficiency. Simplicity denotes how simple it is to realize the one-time password authentication scheme [24].

2.6 Key management

A network has to achieve security requirements in terms of authentication, confidentiality, integrity, availability and non-repudiation. These security requirements rely on the availability of secure key management scheme. Fundamental goal of key management is to manage the keys used in the network and to prevent the improper use of legally issued keys, such as unauthorized modification, disclosure, or replaying of keys as well as the use of obsolete keys etc. The intruder can interrupt the network by using the authorized keys malevolently if there is no secure use of keys. If there is no secure key

management the network become vulnerable to attack, therefore key management is the basic part of any secure communication in a network. Most cryptography relies on some underlying secure, robust and efficient key management. Secure communication normally involves a key distribution, updating and revocation procedure between communication parties [25].

2.6.1 Factors that Affect Key Management

Factors affecting key management are itemized below [26]:

1- Size of the key like digits' number, symbols or characters, size of the message and encryption time.
2- Sequence of key organization, arrangement of the random order is nominated to stop attacks.
3- Key maintenance for compromised nodes in multiple servers and update certificate authority.
4- Alternate keys number for changing topology alteration, size of the node and strength.
5- Trusted Third Party (TTP) Number in the maintenance of the key.

2.6.2 Key Management Techniques

In symmetric encryption, the sender and the receiver use the same key. In cryptography of the public key, there is a used of two keys, one is named private key and other one is public key. The public key is available to the public and it is used for encryption. The other used for decryption and is prepared obtainable only for receiver and this key is certainly not available or communicated to anyone by the receiver. Thus, the private key remains invulnerable. Proper management of the private keys increases compliance management and reduce

the risk of data loss. Every communication needs formation of new couple of public and private key. Number of keys required are less as compared to symmetric key cryptography [27]. Key management is categorized using methods of the centralized and distributed. In management for the centralized key, the key is managed by the cluster head that is organized by a group of servers for the centralized key, while the other method, nodes produce keys with respect to servers of the key and nodes of the destination. Trusted Third Party (TTP) uses on-line and off-line techniques to manage keys between sender, receiver and intermediate nodes. Key management essentially contains of key generation and key maintenance phases, key maintenance consists of key update, key revoke and key store. Different key management phases are:

1. Key Generation - Number of unique public key(s) to be produced for servers which are centralized and nodes for each server in a network.

2. Key Distribution - Key distribution is done through a secure channel, key distribution center, trusted third party or mobile agent. Key distribution is set in private and confidential manner for secure applications.

3. Key Update - Keys are updated when nodes join or leave the network or when malicious nodes attack the network.

4. Key Revocation – Compromised nodes block or alter the route path and change the message content. Servers revoke the assigned keys, disable the compromise node entry in the key distribution table and broadcast the update key table to adjacent nodes and neighboring servers.

5. Key Store/Key Pool - Set of keys are stored in the centralized data base. Whenever keys are assigned, the key is being chosen from the pool when the

keys are allocated. Disabled keys for compromised nodes are saved in the key store and the status bit is set to compromise. After a period, the bit of status is fixed to useable key [26].

2.6.3 key management functions

There are following are additional functions used in key management:

1. **Key Discovery** -The key of the nodes is shared with contiguous nodes and their identity is confirmed. In this function, the keys of contiguous nodes match and the corresponding pair of nodes share a secure path; else an alternate path is searched using path establishment technique.
2. **Key Path Establishment** – In the case there is wrong match of the key among contiguous nodes, key path establishment is invoked to find an alternate path that lead toward destination node [26].

2.7 Rivest Cipher (RC6) Symmetric Cipher

RC6 is a Symmetric block cipher submitted to NIST for consideration as the new Advanced Encryption Standard (AES).RC6 the diffusion results are much faster as compared to RC5, which permits RC6 to be implemented with fewer rounds at much higher security and with higher throughput and thus the RC6 is compatible so that all the need is met of the Advanced Encryption Standard [28]. RC6 designed by Ron Rivest, Matt Robshaw, Ray Sidney and Yiqun Lisa Yin. The algorithm was also submitted to the NESSIE and CRYPTREC projects. RSA security patented this algorithm which consider exclusive, RC6 is considered the derivation of the RC5 and there are two central new characteristics that differ from RC5: the integer multiplication inclusion and the four w-bit working registers use as an alternative of two w-bit registers [29].

RC6 block cipher is widely uses as the delay is low and complexity of the computational is less that meet the constrain of the real-time [30]. The main two characteristics are confidentiality and the integrity of the data which can be accomplished by the symmetric ciphers use. The RC6 has some certain features that make it parameterized which are size of the block, the size of the key, and the rounds number, the higher limit on the size of the key is 2040 bits, RC6 can be more precisely stated as RC6w/r/b where the size of the word is w bits, encryption involves of a nonnegative rounds number r, and b signifies the key encryption length in bytes [31].For all variants, RC6-w/r/b operates on four w-bit words using the following six basic operations explain in Table (2.2) .

Table (2.2): RC6 Operations [28].

Operation	Description
a + b	Integer addition modulo 2^w
a – b	Integer subtraction modulo 2^w
a ⊕ b	Bitwise exclusive-or (XOR) of w-bit words
a × b	Integer multiplication modulo 2^w
a <<< b	Rotate the w-bit word a to the left by the amount given by the least significant ($\log_2$ w) bits of *b*
a >>> b	Rotate the *w*-bit word a to the right by the amount given by the least significant ($\log_2$ w) bits of b(where lg w denotes the base-two logarithm of w)
Enc:(A,B,C,D) = (B,C,D,A) **Dec**:(A,B,C,D) = (D,A,B,C)	Parallel assignment of values on the right to registers on the left.

Operations of the data-dependent is being exploits by RC6 like that multiplication of 32-bit integer is effectively applied on greatest processors. Multiplication of the integer is very operational diffusion and RC6 used it to calculate the amounts of the rotation so that these amounts are reliant on completely other bits of alternative register. As a consequence, RC6 has much quicker diffusion than RC5 [28], the RC6 cipher explains in Figure (2.2) .

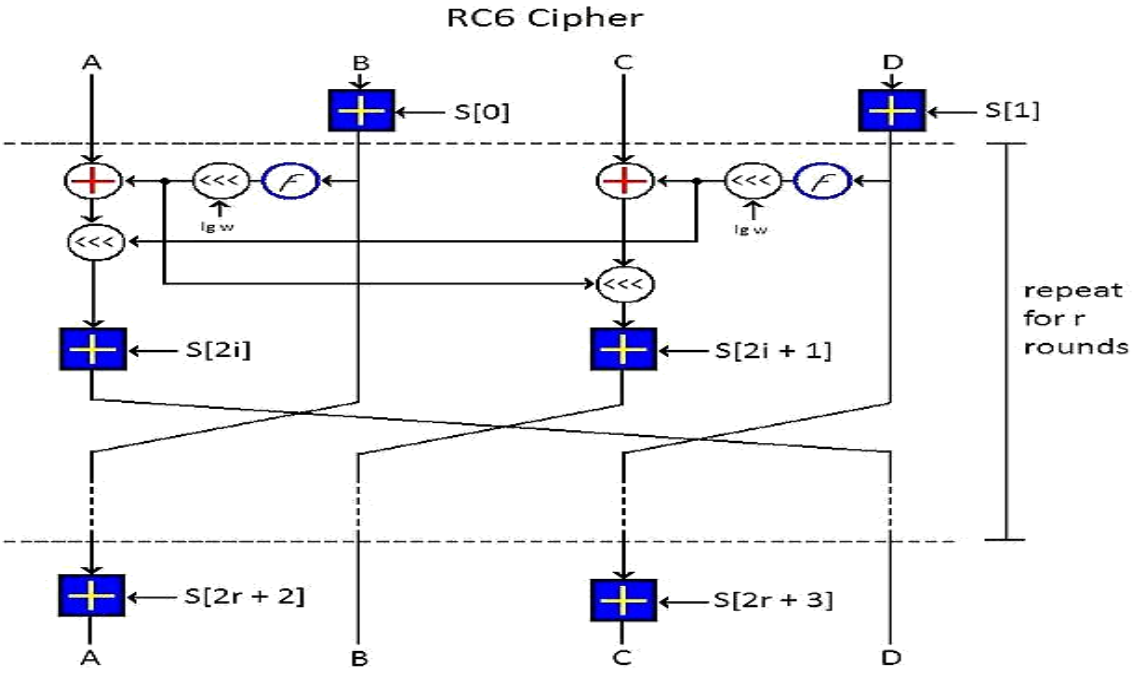


Figure (2.2): Explains the RC6 algorithm cipher [31].

RC6 algorithm has three parts Key expansion, Encryption and Decryption .

A- Key-Expansion Algorithm

Key-Expansion Parameter: Use two magic constants:

$$\mathbf{p_w = Odd\ ((e-2)2^w} \qquad \mathbf{\dots (2.1)}$$

$$\mathbf{Q_w = Odd\ ((\text{ø}-1)2^w} \qquad \mathbf{\dots (2.2)}$$

Where:

e = 2.718281828459 (base of natural logarithm).

ø = 1.618033988749 (golden ratio = (1 + √5)/2).

W=word-bit (word size)

L= key length

S= Key expansion table

Odd(x) = the odd integer nearest to x.

The steps for - Key-Expansion RC6 Algorithm are shown in algorithm (2.1).

Algorithm (2.1): Key-Expansion RC6 algorithm [31].

Input: L denotes the byte key that is preloaded into c word array L [0,1, …, c-1], r denotes the number of rounds.
Output: w-bit round keys S [0,1, ..., 2r+3]
Begin
Step1: S [0] = P_w
Step2: Repeat step 3 for i= 1 to 2r +3 do
Step3: S[i] = S [i- 1] + Q_w
Step4: A = B = i = j = 0
Step5: Iteration = 3 × max (c, 2r +4)
Step6: Repeat Step7 to Step10 for j=1to Iteration do
Step7: A = S[i] = (S[i] + A+ B) <<< 3
Step8: B = L[j] = (L[j] + A + B) <<< (A + B)
Step9: i = (i + 1) mod (2r +4)
Step10: j = (j + 1) mod c
End

B. Encryption

Four w-bit registers A, B, C, D contain the initial input plain-text as well as the output cipher text at the end of encryption. The first plaintext byte is located in the minimum important byte of A, the last plaintext byte is located into the greatest important byte of D, the stapes for RC6 algorithm encryption are presented in algorithm (2.2).

Algorithm (2.2) :Encryption RC6 algorithm [31].

Input: plaintext stored in four w-bit input registers (A, B, C, D), r: number of rounds, w-bit round keys S [0 … 2r+ 3]

Output: cipher text stored in A, B, C, D

Begin

Step1: B = B +S [0]

Step2: D = D +S [1]

Step3: repeat step4 to step8 for i = 1 to r do

Step4: $t = (B \times (2B + 1)) <<< \log w$

Step5: $u = (D \times (2D + 1)) <<< \log w$

Step6: $A = ((A \oplus t) <<< u) + S[2i]$

Step7: $C = ((C \oplus u) <<< t) + S[2i + 1]$

Step8: (A, B, C, D) = (B, C, D, A)

Step9: A = A + S [2r + 2]

Step10:C = C + S [2r + 3]

End

C-Decryption

In the case of cipher-text decryption is being loaded into registers A, B, C, D. integer subtraction modulo 2w and right rotation on registers is used by the algorithm to get the plain text, it does opposite registers operations, the steps for RC6 algorithm decryption are presented in algorithm (2.3) [31].

Algorithm (2.3): Decryption RC6 algorithm [31].

Input: Cipher text stored in four w-bit input registers A, B, C, D
r: number of rounds, w-bit round keys S [0, …, 2r + 3]

Output: Plaintext stored in A, B, C, D

Begin

Step1: C = C - S [2r + 3]

Step2: A = A - S [2r +2]

Step3: Repeat step 4 to step8 for i = r down to 1 do

Step4: (A, B, C, D) = (D, A, B, C)

Step5: u = (D × (2D + 1)) <<<log w

Step6: t = (B × (2B + 1)) <<<log w

Step7: c = ((C -S [2i + 1]) >>> t) ⊕u

Step8: A = ((A - S[2i]) >>> u) ⊕t

Step9: D = D -S [1]

Step10: B = B -S [0]

End

2.8 Chaotic Map

The chaotic sequences have various useful features of application based on security. These features are: - (1) the chaotic is dynamic system in discrete time to generate complicated sequence which behaves randomly in easy and simple way. (2) the chaotic signal is not random but it is deterministic, this feature let us to renewal it. (3) The chaotic signal has high sensitivity of initial condition this lead any change in initial condition create other sequence. This feature makes the chaotic sequence very difficult to predict by attackers to renewal it and increase the security level. (4) the chaotic sequence path has random behavior in the specific space, this causes the restoration of this sequence is impossible in its specific space. Chaotic maps are separated into two classes, 1D (one-dimensional) and multidimensional maps [32].

2.8.1 1D Chebyshev chaotic map

Chebyshev is one of the most commonly used security mechanisms in authentication methods because it contains a semi-group property. The Chebyshev polynomial is presented in three definition of as following equation:-

Def.1 The Chebyshev polynomial in degree n is determined as:

$$T_n(x) = \cos(n * \arccos(x)) \quad \ldots (2.3)$$

where **n** is integer number, $x \in [1,-1]$

Def.2 Semi-group features for Chebyshev can achieved as:

$$Trs(x) = Tr(Ts(x)) = Ts(Tr(x)) \quad \ldots (2.4)$$

Def.3 The Chebyshev polynomial in n degree, present:

$$(x, Tx\ (x))$$

it is infeasible in computation to determine the polynomial order n [33]

2.8.2 Logistic Map

The logistic map is a polynomial mapping and is an example of non-linear recursive algorithm which generates chaotic relations. There are two kinds of logistic: 1D logistic Map and 2D logistic map. 2D logistic used to generate chaotic numbers which are utilized in diffusion process. This process leads to that the image that encrypted to own more uniform histogram and in addition used process of decryption as Symmetric-key. 2D logistic map is useful to produce chaotic(M×N) matrix by the original image that is then is been used as a secret-key which lead to a large key space so it would be considered secure and confident. The 2D logistic Map equation is defined as following:

$$\mathbf{x_{n+1} = \lambda(3y_n + 1)x_n(1 - x_n)} \ ,$$

$$\mathbf{y_{n+1} = \lambda\,(3x_{n+1} + 1)y_n(1 - y_n)} \qquad \ldots \textbf{(2.5)}$$

where $\boldsymbol{\lambda}$ belong to (**0,4**] and the ($\mathbf{x_0}$, $\mathbf{y_0}$) belong to (0,1) diagrams of bifurcation of the Logistic map is shown in Figure (2.3) [34].

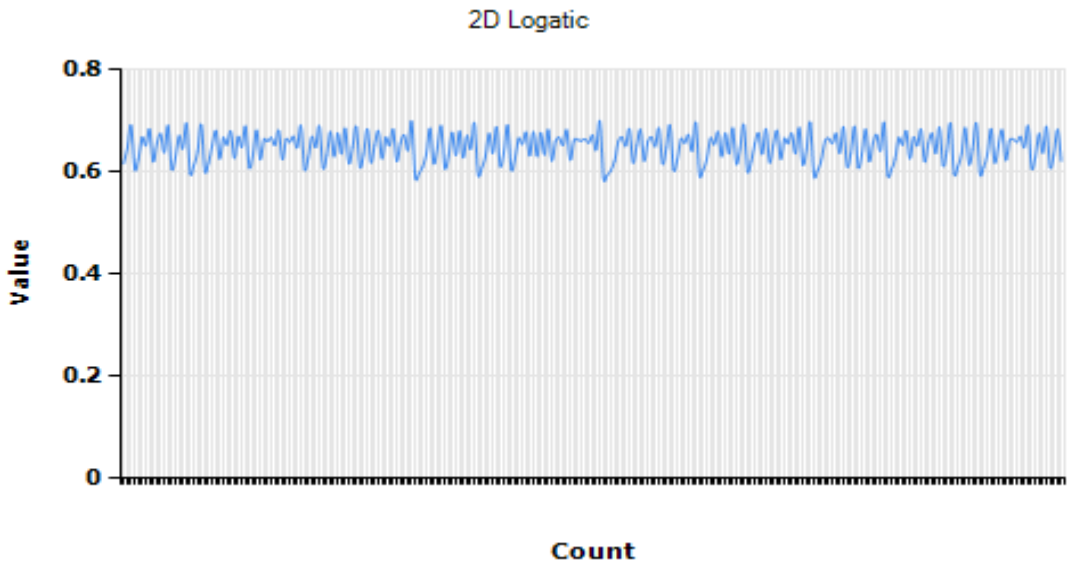


Figure (2.3): bifurcation diagrams of the Logistic map [34].

2.9 Web Service

A group of operations which are network available over standardized XML messaging that is explained by the Web Service (WS). The description of web service by standard, notion of formal XML, named its description of service. It includes all the parts essential to interrelate with the service, comprising formats of the message that detail the operations, protocols of the transport and position. The program to-program communications are composed by WS. The charge of implementing e-business is reduced by permission of the WS, and also arrange solutions quicker and to exposed new chances. The key to reaching this new horizon is a common program-to-program communications model, built on existing and emerging standards such as (Hypertext transfer protocol) HTTP, Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) and Universal Description Discovery and Integration (UDDI).

One of the most important features of WS is the integration to create a web environment because it depends on standardized extensible Markup Language (XML). This language provides WS a platform-neutral mechanism to represent data for compatibility and flexibility. This means, that if a client is working on many old, modern, and developed systems on different operating platforms and in different programming languages to be integrated. One of the advantages of Web Services is offering a model of combined programming for the services of private Intranet and public Internet growth and usage as a consequence, as a result, the choice of network technology will be transparent to the developer of the service. Architecture of the web services is depending on the exchanges among three parts: provider of the service, registry of the service and service requestor. The exchanges include the issue, determine and merge operations. Collected, these parts and operations perform on the artifacts of the web services. Figure (2.4) illustrates these operations, the mechanisms offering them and their interactions [35].

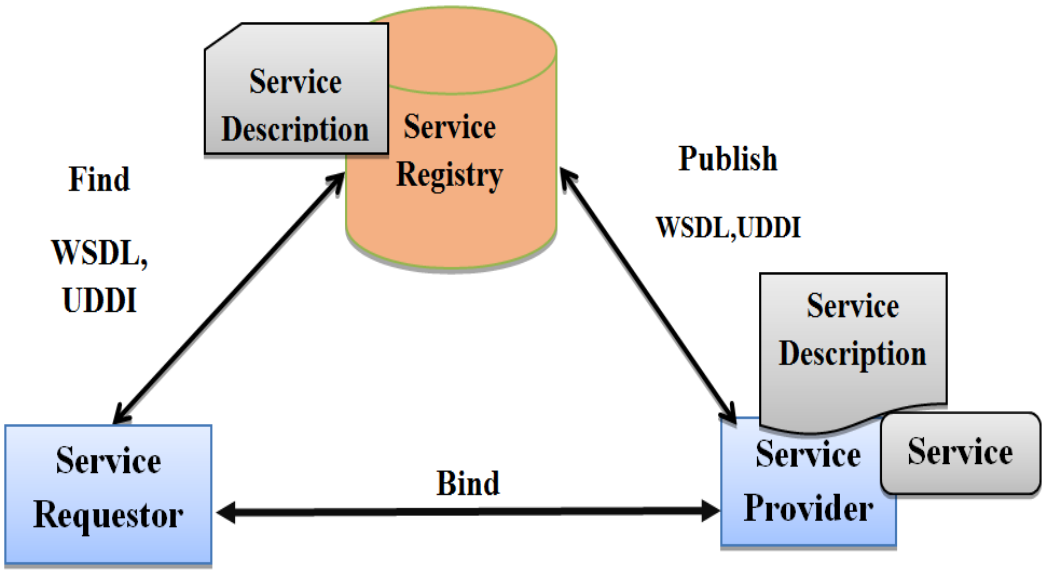


Figure (2.4): The Three Thoughts Roles and Operations of Web Services [35].

2.9.1 WSA Functional Components

The three operations of conceptual WS to complete the roles, WSA (Web Services architecture) must provide three basic functional components of its architecture [36]:

1. **Transport:** To communicate with a specific service the uses that included protocols and formats is represented within the transport component. Data types are defined within the data format of messages. A control of message transfer within application semantics is determined in transfer protocol. The transport protocol declares the actual message transfer.
2. **Description:** The description of the service across the programming languages used is represented by the description components. Where the binding information, message format, and exchanges parameters with the service is provided within this component.
3. **Discovery:** The mechanisms of registering a service or advertising for a service or descriptions of the service are represented within this component.

2.9.2 Web Services security

There are four elementary security needs that the layer of the web services security should deliver [35]:

1-Confidentialityis the property that information is not made available or disclosed to unauthorized individuals, entities, or processes, and guarantees that the contents of the message are not disclosed to unauthorized individuals.

2-Authorization The characteristic that make sure of the authority, that comprises the permitting of access depending on access rights and promises that the sender will have the authorization for sending a message.

3-Data integrity is the property that data has not been undetectably altered or destroyed in an unauthorized manner or by unauthorized users. Thus make sure that there is no modification on the message unintentionally or purposely in transit.

4-Proof of origin is evidence identifying the originator of a message or data. It gives emphasizes that the transition of the message was done correctly by the recognized sender and is not a replay of a previously transmitted message. This requirement implies data integrity.

2.9.3 The Basic WS Technologies

There are number of technologies have been presented beneath the web service title and additional ones will be presented in coming years. Actually, the paradigm of the web service has grown-up very fast that numerous technologies of competing are trying to offer the same ability, figure (2.5) offers a diagram that proves the relationship among these technologies.

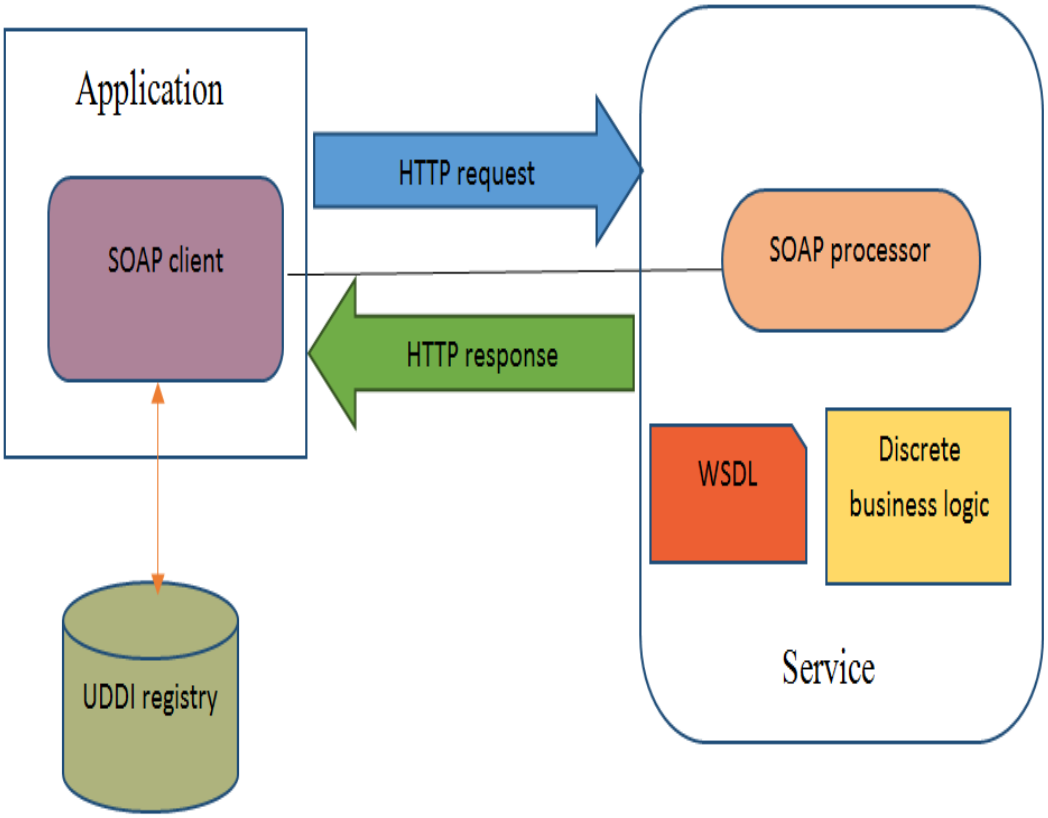


Figure (2.5): relationship between technologies [36].

The relationship between these pieces (SOAP, UDDI, and WSDL) can be defined as follows: an application acting in the role of a web services client needs to locate another application or a piece of business logic located somewhere on the network. The client queries a UDDI registry for the service either by name, category, identifier, or specification supported. Once located, the client obtains information about the location of a WSDL document from the UDDI registry. The WSDL document contains information about how to contact the web service and the format of request messages in XML schema. The client creates a SOAP message in accordance with the XML schema found in the WSDL and sends a request to the host (where the service is) .

2.9.3.1 Web Service Description Language (WSDL)

Technology of XML is WSDL which defines a web service interface in an identical method. WSDL regulates how the parameters of the input and output is represented by a web service of an invocation visibly, the structure of the function, the invocation nature and the protocol service tie. WSDL permits unlike clients to robotically know how to interrelate with a web service.

2.9.3.2 Universal Description, Discovery, and Integration (UDDI)

UDDI provides a worldwide registry of web services for advertisement, discovery, and integration purposes. Analysts of the business and scientists use UDDI to find obtainable web services by examining for titles, identifiers, classes, or the conditions executed by the web service. UDDI offers a construction for demonstrating businesses, relationships of business, web services, metadata with specification, and web service admission plugs [36].

2.9.3.3 Simple Object Access Protocol (SOAP)

The SOAP specification and development is preserved by commendation of W3C 27 April 2007.SOAP is a protocol used by Web services to construct and understand the messages they exchange. SOAP is at the heart of Web services architecture in that it allows the interacting parties in the architecture to communicate with each other using a standard, well-understood message format .The specification give the definition of a format of XML-based standard message, labeling how the metadata of the message and payload should be packed into document of XML.

The format of the message elementary layout describes in Figure (2.6) SOAP Envelope signals the beginning of message of the SOAP. every message

involves of SOAP sections of header and body. The body section involved in the payload. The additional details of the processing instruction, like the protocol of the transaction or policies of the security, go into the header section of the message.

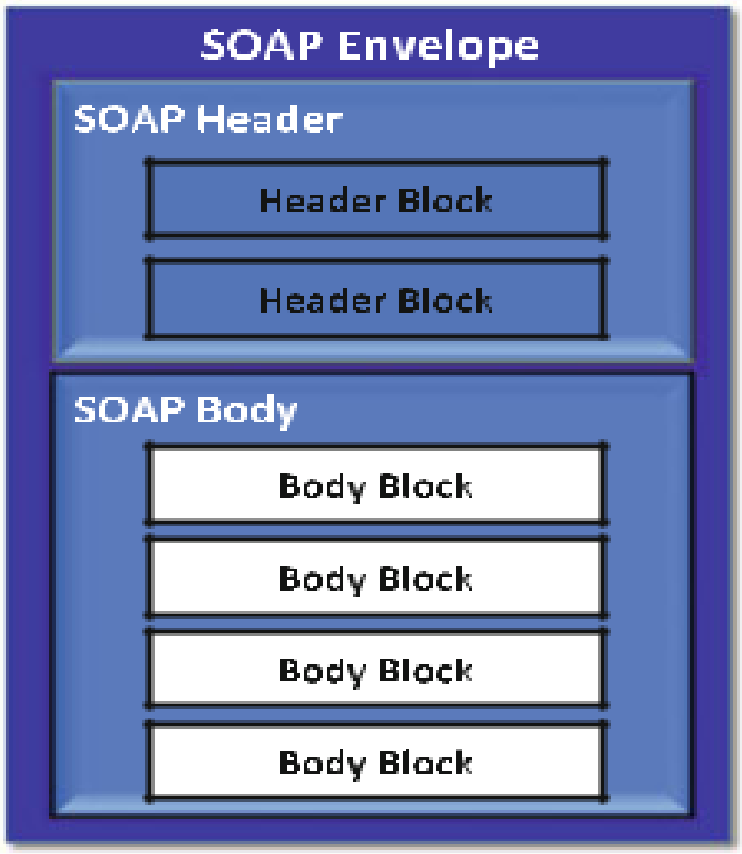


Figure (2.6): The format of the message elementary layout [37].

As shown in the communication of the Web service stack in Figure (2.7) a message of the SOAP is communicated through the Internet by any transmission protocol of the application-level like HTTP or SMTP. The term 'SOAP binding' is mean to point to the mechanism of the transference by that a SOAP is communicated. For example, when a SOAP is bound to HTTP, the SOAP

message is embedded in the body section of the HTTP request (and response) [37].

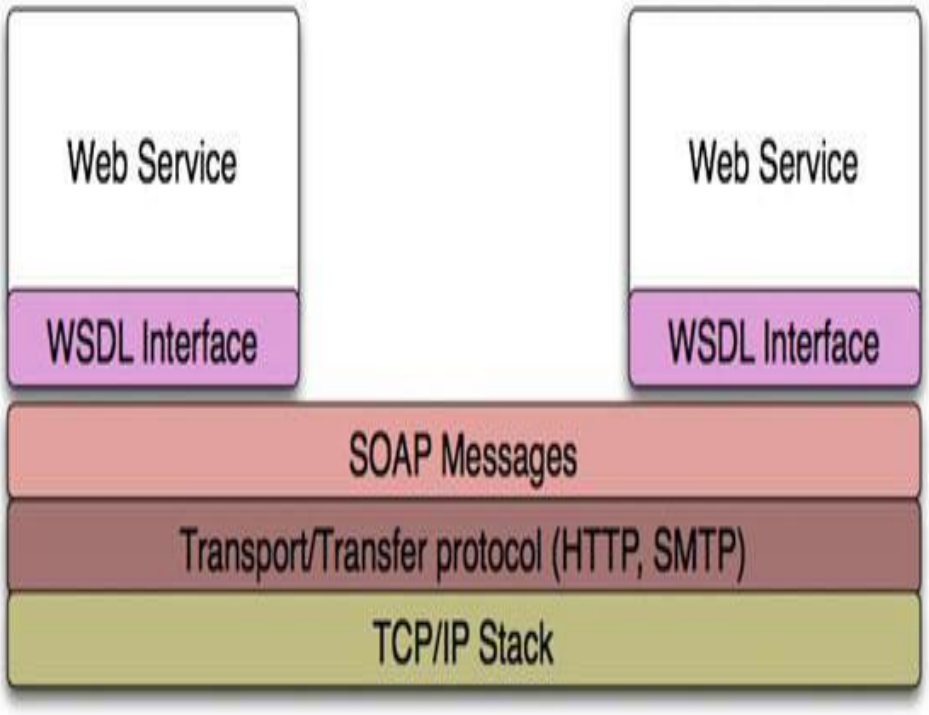


Figure (2.7): Web services communication stack [37].

SOAP web service provides a standard and more effective way of web communication and a good option for enterprise web applications to communicate with other systems or organizations in a more flexible manner. SOAP is an easy to use extensible communication technology that can be used over the web. The technology follows standards, from architecture to security of communication. The SOAP security is not only in the level of the transport, but likewise at the level of application, for example the messages is been transformed only to the requesting application. SOAP is a technology of flexible online communication, and been flexible it improves effectiveness and can guarantee a more effective and serviceable architecture [38].

2.10 Location Based Services

Some of the modern technologies is Location Based Services (LBS) is to obtain a location in the geographical existence of mobile devices. There are many ways to calculate the location of an object. These ways have common concepts:

2.10.1 Coordinates Conversion:

I-the (Cartesian) match to the coordinate of the polar:

In systems of digital communication, the change from the coordinate of the rectangular to the coordinate of the polar is one of the operations of the key. Let (**x, y**) signify a coordinate of the rectangular, the change is to calculate the angle **φ** among the x-axis and vector and the length of vector **ρ** by the Eq. (2.6).

$$\varphi = \tan^{-1}(y/x),\ \rho = \sqrt{x^2 + y^2} \qquad \dots \quad (2.6)$$

The RPC (the rectangular (Cartesian) coordinate to the polar coordinate) process can be regarded as discovery a rotation to line up the specified vector alongside the x axis [39].

II-the polar coordinate to the (Cartesian) coordinate:

The azimuth and distance (**φ, ρ**) states coordinates of the polar, coordinates of the orthogonal (**x, y**) signifies Cartesian coordinates, polar Coordinates-Cartesian coordinate conversion method is defined by the Eq. (2.7):

$$x = \rho \sin\varphi\ ,\ y = \rho \cos\varphi \qquad \dots \quad (2.7)$$

where

ρ describes the distance in polar coordinate system, **φ** describes the azimuth in system of polar coordinate [40].

III-Vectors (Algebraic Approach) the Cartesian coordinate to the Rectangular Coordinates:

The vector will be expressed in Rectangular Coordinates as follows [41]:

In 3D Vector $\vec{u}$ $$\vec{\mathbf{u}} = \mathbf{u_1}\hat{\mathbf{i}} + \mathbf{u_2}\hat{\mathbf{j}} + \mathbf{u_3}\hat{\mathbf{z}} \quad \ldots \quad (2.8)$$

Magnitude of $\vec{u}$ $$\|\vec{\mathbf{u}}\| = \sqrt{\mathbf{u_1^2} + \mathbf{u_2^2} + \mathbf{u_3^2}} \quad \ldots \quad (2.9)$$

Unit Vector in the Direction of $\vec{u}$ $$\hat{\mathbf{u}} = \frac{\vec{\mathbf{u}}}{\|\vec{\mathbf{u}}\|} = \frac{\vec{\mathbf{u}}}{\sqrt{\mathbf{u_1^2}+\mathbf{u_2^2}+\mathbf{u_3^2}}} \quad \ldots \quad (2.10)$$

2.10.2 earth's radius:

The coordinate of the calculation of an earth-centered (**X, Y, Z**) system for a trajectory referenced by altitude, latitude, and longitude is Earth of forthright in biaxial (WGS-84) ellipsoid. The difficult rises using the coordinate of the earth-centered system for the opposite operation to recalculate the altitude, latitude and longitude of the path, this calculation can only be implemented nearly. A mathematical depiction of the earth form is of excessive attention to numerous communities engineering. The biaxial ellipsoid is a respectable estimate to the traditional geodetic difficult That model leaves only marginally from the triaxial ellipsoid estimate, yet it uses greatly fewer complex calculation, coordinates

(x,y,z) of point P can be determined from its geodetic coordinates (ø,λ,h) by the Eq.(2.11):

$$\mathbf{R_n = \frac{a}{\sqrt{1-e^2 \sin^2 ø}}} \quad \ldots \quad \mathbf{(2.11)}$$

Where

a is the ellipsoidal equatorial radius (a = 6378.137 km for model WGS-84)

e is the eccentricity of ellipsoid (e^2 = 0.00669437999for model WGS-84)

ø is the geodetic latitude (positive North) [42].

2.10.3 Haversine formula

The Haversine formula is used to calculate the distance between two points on the surface of the earth using latitude and longitude as an input variable. The Haversine formula is an important equation in navigation, giving a large circular spacing between two points on the surface of the earth with longitude and latitude. The formula use takes up to disregard the effect of the ellipsoidal, quite precise for most controls, also disregards the low hills height and valleys on the earth surface [43].

This technique is used for geographic information systems applications. On the maps use which are previously have 2D will have points showed in integers. In the computation's phases, haversine are main will change the latitude and longitude value integer number to radians, then these numbers are considered in the algorithm haversine. The haversine formula is defined by the Eq. (2.12):

$$\mathbf{d = 2r\ arcsin}\sqrt{\mathbf{sin^2}\left(\frac{\theta_2-\theta_1}{\theta_1}\right) + \mathbf{cos}(\theta_1)\mathbf{cos}(\theta_2)\mathbf{sin^2}\left(\frac{\lambda_2-\lambda_1}{\lambda_1}\right)} \qquad \text{... (2.12)}$$

Where:

θ: Latitude

λ : Longitude

r: radius of the earth (r = 6.731 km), **d** : Distance

To achieve computations of the distance using formula of the haversine, we need each point location. The latitude, longitude, and the radius area of the event are need for distance calculation. This information will be arrived into database, so it can make easy to recover data when finish to calculate using haversine formula [44].

2.11 Average Security

Measurement is entropy it represents the amount of information exist in a random variable, the exchanged information, and the amount of information shared between two random variables, entropy is a measure of the degree of indeterminacy of a random variable. This measure is also known as Shannon entropy, which provides the average case entropy measure for an independent distribution of random variables [45]. Secrecy of ciphers is calculated in terms of the key equivocation (conditional entropy of key given cipher). Entropy of a message, called H (k/c), is the minimum number of bits needed to encode all possible occurrences (meanings) of the message, assuming all messages are equally likely. Entropy of a given message is defined by the Eq. (2.13) [46].

$$H\left(\frac{K}{C}\right) = \sum_{j=1}^{L} \sum_{i=1}^{n} q_i \; P_{ij} \log P_{ij} \qquad \ldots \textbf{(2.13)}$$

Where

qi = Pr (C = ci) = Probability of cipher text

Pij = Pr (K=ki / C = ci)= Probability of (key/ cipher text)

C= cipher text **, K=** key**, L** is the key length, **n** is the cipher text length

Chapter Three

Proposed System

Chapter Three

The Proposed system

3.1 Introduction

The recent breakthrough in education has transformed e-learning from its traditional concept to learning beyond time and space. However, mobile devices used in learning can become weak if the security aspects are neglected. Thus, authentication is one of the important lines of defense. In this thesis, a new authentication technique has been developed. This technique represents an intelligent classroom to allow only authorized students to enter the class resources using a new geographic method. Also, the resources of this classroom are transferred securely by modifying the traditional RC6 encryption algorithm through using chaotic map.

Section (3.2) introduces the design objectives of the proposed system. Section (3.3) is described the design details of the proposed system

3.2 Design Objectives

The design objectives of the proposed system are:

1. Building a mobile learning system that is used in a classroom. This system has a robust authentication technique based on a new geographic technique.
2. The proposed system transfers secure data using an improvement of RC6 algorithm with chaotic map.
3. Authentication technique uses web server for creating user mobile location and the keys for (n) users.

3.3 The Primitive Proposed system

The primitive system of the proposed system consists of four sides. Server (database) side, administrator side, client side, and the web application server side. These sides are collaborated with each other as shown in Figure (3.1).

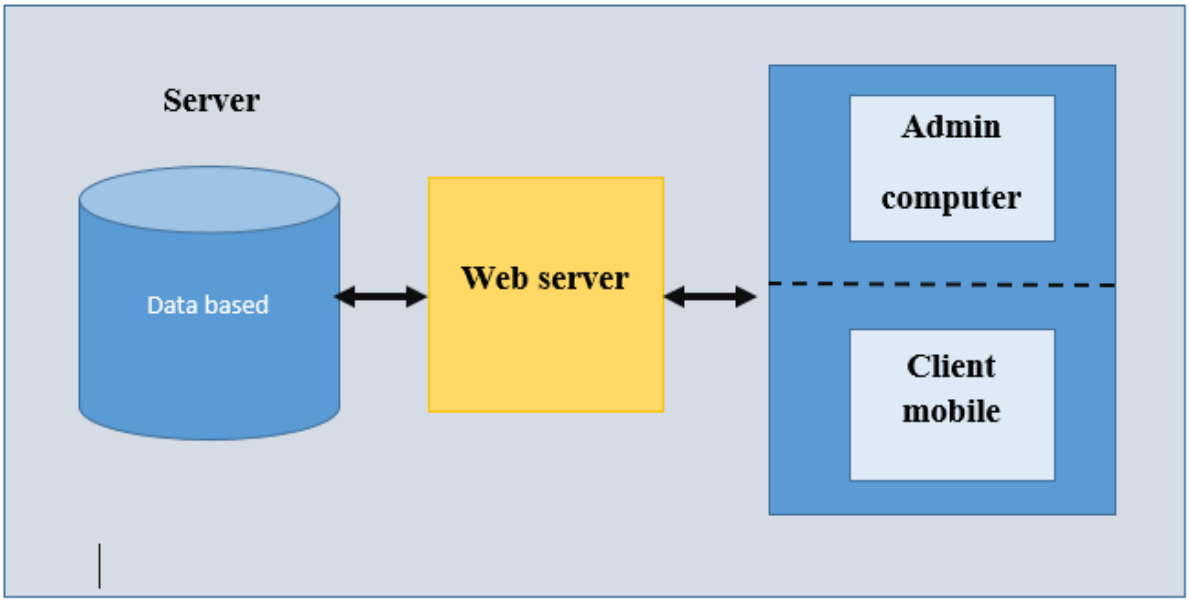


Figure (3.1): Primitive model of the Proposed system.

3.3.1 Administrator Side

Figure (3.2) shows the administrator side. This side includes the following functions:

1- **Login (Authentication and Authorization):** The administrator (lecturer) is authorized to access the system using (username and password).

2- **Student creation**: The administrator (lecturer) can add new users (student), delete the other students.

3- **Course creation**: The administrator (lecturer) can add a new course and can delete what he wants.

4- **Exam**: The administrator (lecturer) can create questions, choose the pattern of questions, add questions about exams, and change or delete questions.

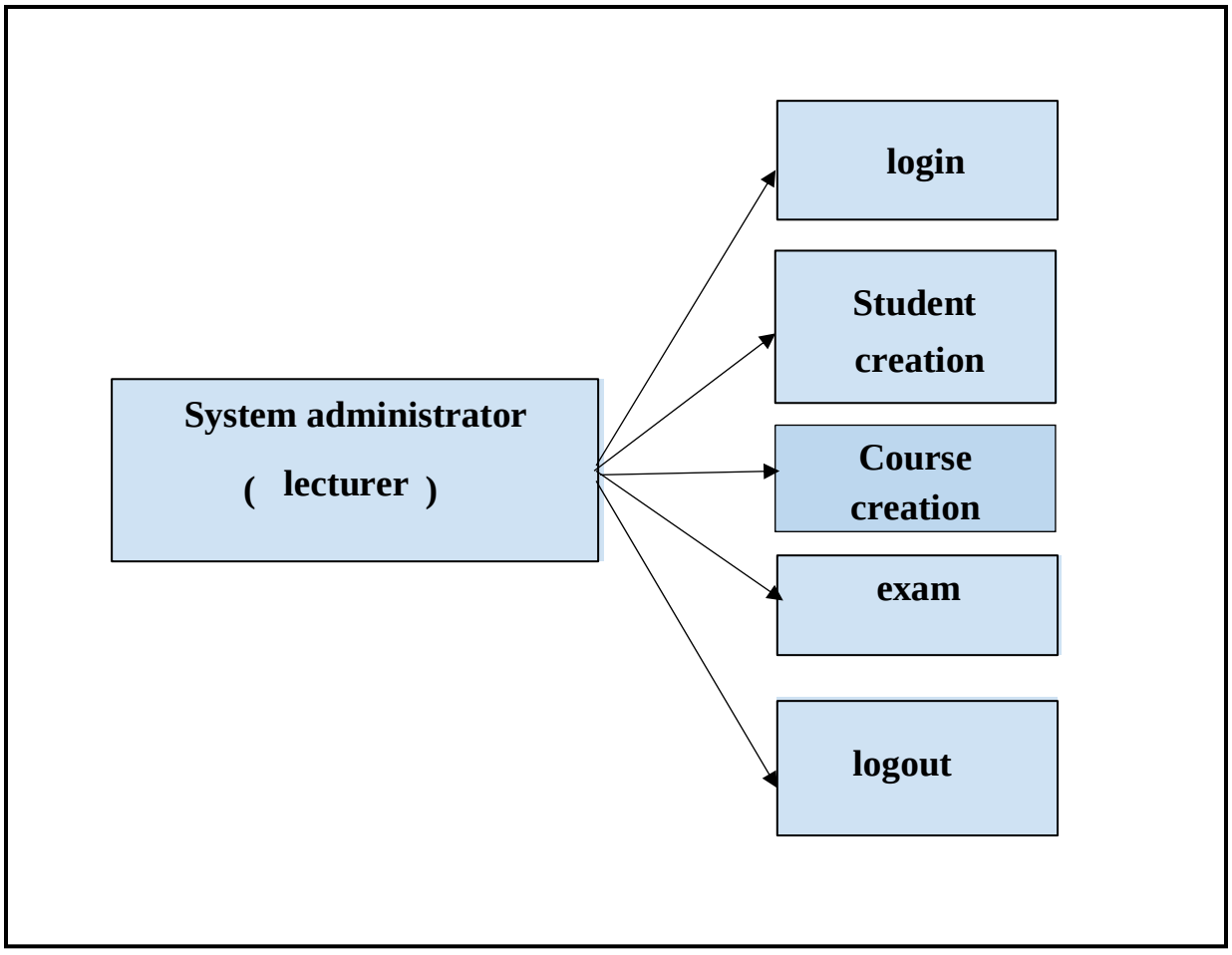


Figure (3.2): Diagram of Administrator Functions.

3.3.2 Client Side

Figure (3.3) shows that the client side, which it includes the following functions:

1- **Login (User Authentication and Authorization)**:

The client (student) can access to server through web server. The web server uses a proposed technique to check if the client (student) is valid or not based on location services and web service uses a proposed improved key scheduling algorithm to generate secret key for all valid users and use this key in IRC6 algorithm encrypte/decrypte process.

2- **Registration at class**: Students can register in the class as long as their authentication is confirmed. In this step a secret key will be assigned to each student using the key management.

3- **Course Subject**: The student is now authorized to access the course material, get the course, and the lecturer aids, and will receive a notice of any modification from the lecturer, on the other hand, he /she can send his/her inquiry about course material, exams, homework etc. in an encrypted form using the improvement RC6 (IRC6) algorithm, and communicate with the lecturer.

4- **Participate in the Exam**: Students can obtain the exam if they can prove that they are authorized .

5- **Get the Exam Results**: The student can get the exam results at the end of the exam.

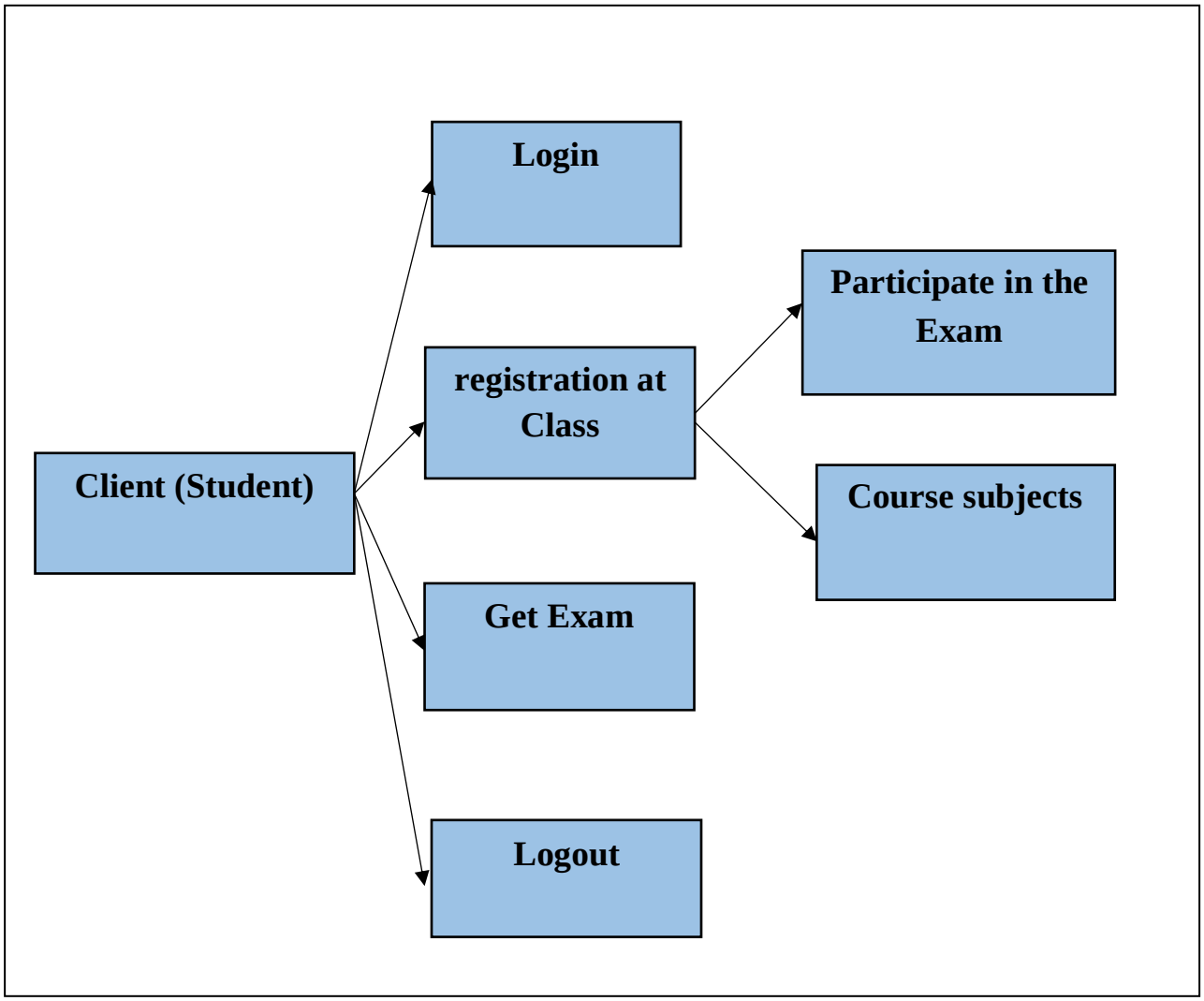


Figure (3.3): Diagram of Client Functions.

3.3.3 Web Application Services

The primitive block diagram of the web application server shows in Figure (3.4).

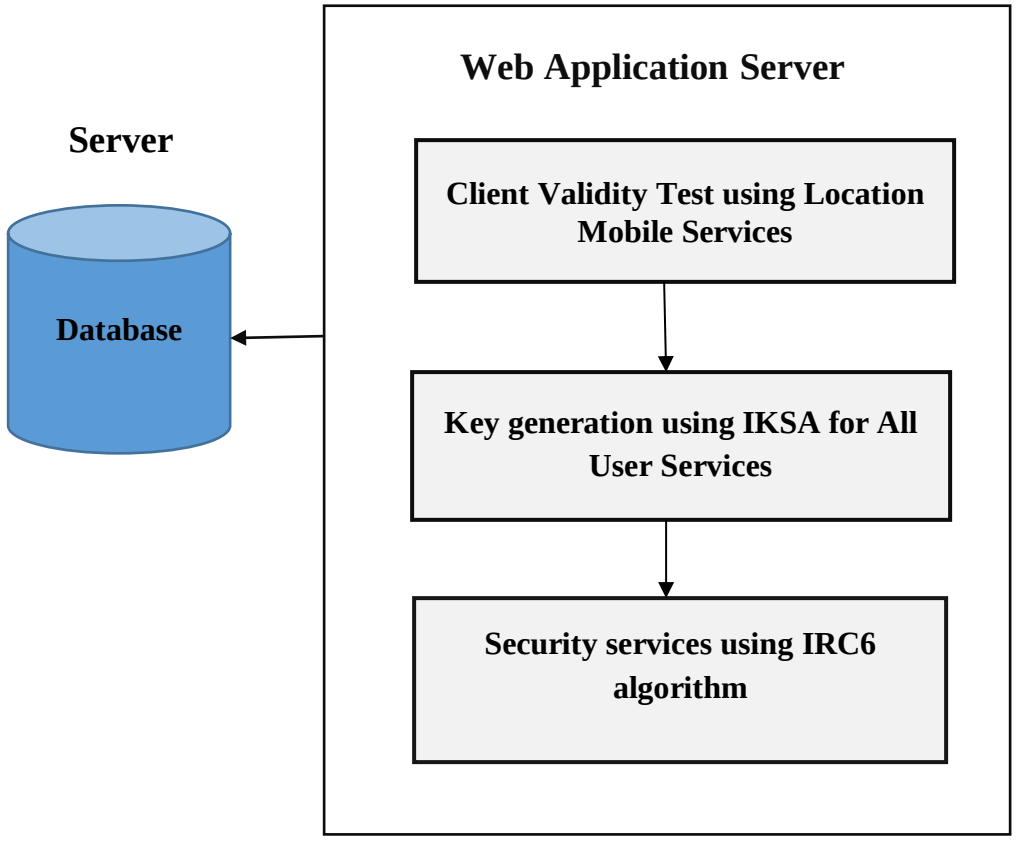


Figure (3.4): Primitive Block Diagram of the Web Application Server.

3.4 Architecture of the Proposed system

This section introduces the main network structure and the design of the proposed system.

3.4.1 The Main Network Structure of the Proposed system

As shown in figure (3.5), the main network structure of the proposed system consists of a server (database), an administrator (lecturer), a client (student) and a web application server that serves as an intermediate stage between the (administrator and client) side and the server side.

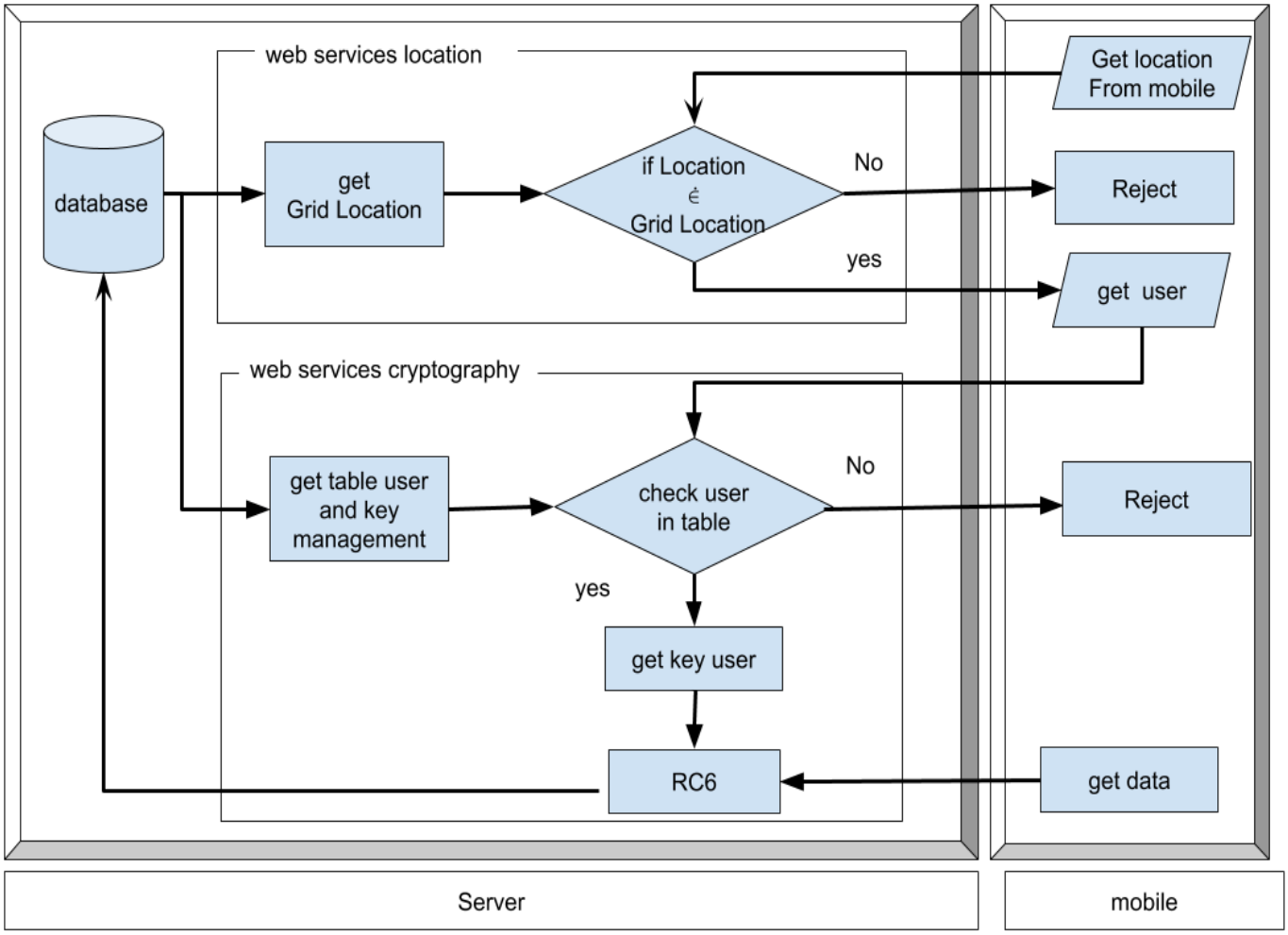


Figure (3.5): Main Network Structure of the Proposed system.

3.4.2 Design of the Proposed system

The proposed system demands a cooperation of several modules, which are shown in figures (3.5) such as (server database, administrator computer, client mobiles, and web application server).

3.4.2.1 Design of the Database on Server Side

The database is designed in SQL server that serves as the underlying information repositories. These repositories are composed of (grid location point and earth

radius) which are represent grid location points for smart classroom used for validity testing, user name and password used for authentication, Student information(Student name, Student age , Student stage, Student section), secret key for all users used for encrypte/decrypte process, and contents of learning materials authored or uploaded by instructors.

3.4.2.2 Design of the Administrator (Admin) Side

The administrator (a lecturer) is a user with permissions authorizing him to add and update the information in the data base of the server side. The first step in admin side is to check the validity of student mobile location in order to allow the student from enrolling the learning system by get the key points which are represent boundary of smart class room from database through connecting with a web page of the web application server. Web application server allows admin to distribute (user name and password) to each valid student, assign secret key from database to each valid users(student), Add or update an educational material, solve problems, answer questions by interaction with users(student), add/delete users(student), and create new exam sheet.

3.4.2.3 Design of the Client (User) Side

The client here does not know how to locate the smart classroom in order to engage in smart class activities and does not know the secret key used to encrypt / decrypt Information exchanged with the lecturer. The student at this point has only a user and password. Therefore, the mobile client (student) side communicates with the network to access the web application server and the propose system enter the mobile client location for testing if the location belongs to a smart classroom in which case it is considered a valid student to get the course and perform the exam

and the secret key assigned to the student to safely transmit of educational material, notices and exam performance.

3.4.2.4 Key management

This section presents the permanence of the system based key management the propose system use of Improved key scheduling algorithm (IKSA) and shows its power in the ability to key management in a new way because the Improved key scheduling algorithm (IKSA) generate N keys with variable length for N of users. This requires the Admin to know the key assigned to each user by providing a server database to save number for each user and its assigned key and the length of each key as shown in the Figure (3.6) shows Generate key using chaotic map.

	#	Logist_2D	_	Mod_round	Chebyshev_mod_255	Key
Select	User[1]	0.378286738313747	378286738313747	11	1,1,1,1,1,242,98,242,169,169,1,	òbò©©
Select	User[2]	0.604907566120297	604907566120297	9	22,94,82,193,229,1,166,163,106,	^RÁå¦£j
Select	User[3]	0.942699401149351	942699401149351	7	46,226,1,46,151,151,91,	.â.——[
Select	User[4]	0.446447899221967	446447899221967	15	1,118,118,67,1,154,67,1,154,67,67,154,154,67,154,	vvCšCšCCšš Cš
Select	User[5]	0.71332552526167	71332552526167	7	169,13,13,169,1,13,13,	© ©
Select	User[6]	0.332850639597567	332850639597567	15	144,198,198,186,9,228,192,192,228,78,9,171,198,192,219,	ÆÆº äÀÀäN «ÆÀÛ
Select	User[7]	0.855583954498669	855583954498669	13	109,151,184,109,79,16,214,79,244,244,244,184,214,	m—¸mOÕOôôô¸Ö
Select	User[8]	0.473247929695031	473247929695031	7	166,16,166,41,176,11,116,	¦¦)° t
Select	User[9]	0.455327772222905	455327772222905	9	125,80,20,55,55,70,245,245,5,	}P77Fõõ
Select	User[10]	0.350002543970569	350002543970569	9	4,1,4,4,4,1,1,1,4,	
Select	User[11]	0.890626310835273	890626310835273	9	147,147,144,177,219,147,219,3,219,	""±Û"ÛÛ
Select	User[12]	0.671585684408691	671585684408691	11	171,21,81,171,21,21,171,186,81,81,186,	«Q««ºQQº
Select	User[13]	0.993667953335461	993667953335461	5	16,76,196,16,196,	LÄÄ
Select	User[14]	0.624747008149597	624747008149597	13	49,166,97,28,49,229,163,229,28,97,166,97,16,	1¦a1å£åa¦a
Select	User[15]	0.9623546347663	9623546347663	15	217,1,1,217,169,169,208,169,208,1,217,208,217,169,208,	ÙÙ©©Ð©ÐÙÐÙ©Ð
Select	User[16]	0.693741013224041	693741013224041	9	1,131,71,131,151,151,11,11,166,	ƒGƒ—— ¦
Select	User[17]	0.140922353250703	140922353250703	15	7,166,229,148,73,88,106,112,1,16,133,94,166,73,133,	¦å"lXjp...^¦l...
Select	User[18]	0.330979142387833	330979142387833	9	28,106,82,19,28,19,163,94,49,	jR£^1
Select	User[19]	0.534561047348655	534561047348655	15	210,60,135,120,180,15,135,15,15,15,75,105,30,135,165,	Ò<‡x´‡Ki‡¥
Select	User[20]	0.558598375315503	558598375315503	15	174,87,234,87,213,174,171,87,93,87,117,87,87,234,186,	®WêWÕ®«W]WuWWêº
Select	User[21]	0.689483917202035	689483917202035	11	145,115,70,40,100,190,160,40,115,220,130,	'sF(d¾ (sÜ,
Select	User[22]	0.144521865763383	144521865763383	7	117,174,174,93,213,174,171,	¿®®]Ô®«
Select	User[23]	0.85675005400685	85675005400685	13	65,215,220,5,20,115,5,205,5,205,25,245,220,	A×ÛsÍÍõÛ
Select	User[24]	0.785745325041693	785745325041693	13	189,108,78,21,81,78,171,252,198,108,171,81,186,	½lNQN«üÆl«Qº

Figure (3.6) : An Example of the Key Management.

The use of key management to give flexibility to the adman to know the key assigned to each user and the length of this key in addition to the contents of the key to be able to send the correct key allocated to the user to use in the process of encryption and decryption Code Thus providing high security and here lies the strength of the system.

3.4.2.5 Web Application Server

The web application server presents three main services:

A- Finding and Authenticating Mobile Location:

Web application server uses a proposed technique to determine the location of the mobile student and then it decides whether he/she is authorized or not.

This service is implemented by using two stages: (Create grid points and Authentication test.

i-First Stage (Create Grid Points):

First stage depends on principles of geometry theory. This technique is applied on a set of points representing the boundaries of the smart classroom in order to get a network of points called (grid points) to cover a whole area of classroom. Algorithm (3.1) describes Create grid points algorithm.

Algorithm (3.1): Create Grid Points

Input: Mobile location(latitude , longitude).

Output: grid Location points, Earth Radius for Each Grid Point

Begin
Step 1 determine four locations from mobile in classroom where
1-1 Get Location Top Left Call A, Get Location Top Right Call B
Get Location Bottom Left Call C, Get Location Bottom Right Call D
1-2 Add (A, B, C, D) in Grid points in data base
Step 2 Calculate midpoint from Four location between each two Location point using Eq. (2.6) (2.7)
2-1(A, B) mid-Point call AB , (A,C) mid-Point call AC
(B, D) mid-Point call BD, (C,D) mid-Point call CD
2-3 Add (AB, AC, BD, CD) in Grid Location points
Step 3 Calculate nearest point to each corner in Grid Location points where three Location point using Eq. (2.6) (2.7) (2.9) (2.10)
3-1 (A,AB,AC) get Z1
(AB,B,BD) get Z2
(AC,C,CD) get Z3
(CD,D,BD) get Z4
3-2 Add (Z1, Z2, Z3, Z4) in Grid Location points
Step4 using Eq. (3.20)
For each grid Location points do
Get Earth Radius at latitude call Earth Radius
Add (Earth Radius) in list Earth Radius
End for
Step5 Stored grid points and their Earth Radius in databased
End

Algorithm (3.1) can be explained by these steps:

1- Determination of grid location points: which are consist from 16 points in coordinate spherically (latitude and longitude).

2- Determination the boundary locations from mobile in classroom. Table (3.1) represents example of the boundary location from mobile in classroom and stored in grid location points at database.

Table (3.1): Boundary Locations from Mobile in Classroom

Points	Latitude	Longitude
A	33.7442276	44.6149608
B	33.74572335	44.6148985
C	33.7453186	44.6150334
D	33.7456524	44.6150866

3- Calculation four mid-point locations (AB, AC, BD, and CD), then store them in the grid location points at database. The middle point is half the distance between two points so the latitude and longitude of these two points must be used as input variables. For example, in order to calculate AB location between A and B points:

I. Finding the distance at longitude between A and B points as shown in Eq. (3.1).

$$distance_{long} = longitude_B - longitude_A \quad \textbf{... (3.1)}$$

II. Converting A and B from the spherical coordinates to the Cartesian form using Eq.(2.7)

$$x = \rho \sin\varphi \, , y = \rho \cos\varphi \quad \textbf{… (2.7)}$$

and as described in Eq. (3.4) and (3.5) They were obtained from the following:

$$y = \sin(\lambda 2-\lambda 1) * \cos(\varphi 2) \quad \textbf{... (3.2)}$$

$$x = \cos(\varphi 1)*\sin(\varphi 2) - \sin(\varphi 1)*\cos(\varphi 2)*\cos(\lambda 2-\lambda 1) \quad \textbf{... (3.3)}$$

where

φ1, λ1 is the start point, φ2, λ2 the end point

$$X = \text{Cos}(\text{latitude}_B) \times \text{Cos}(\text{distance}_{long}) \quad \textbf{... (3.4)}$$

$$Y = \text{Cos}(\text{latitude}_B) \times \text{Sin}(\text{distance}_{long}) \quad \textbf{... (3.5)}$$

III. Finding location AB (latitude , longitude) using equation (3.8) and(3.9) They were obtained from the following:

The formula is for the initial bearing (sometimes referred to as forward azimuth) which if followed in a straight line along a great-circle arc will take you from the start point to the end point

$$\text{latitude} = \text{atan}^{-1}(\sin\Delta\lambda \cos\varphi2 \times \cos\varphi1 \times \sin\varphi2 - \sin\varphi1 \times \cos\varphi2 \times \cos\Delta\lambda) \quad \textbf{… (3.6)}$$

Where

φ1,λ1 is the start point, φ2,λ2 the end point (Δλ is the difference in longitude)

$$\text{longitude} = \text{atan}^{-1}(y, x) \quad \textbf{... (3.7)}$$

$$\text{Latitude}_{AB} = \frac{\tan^{-1}(\text{Sin}(\text{latitude}_A) + \text{Sin}(\text{latitude}_B)}{\sqrt{(\text{Cos}(\text{latitudeA}) + x) * (\text{Cos}(\text{latitudeA}) + x) + y2)}} \quad \textbf{…(3.8)}$$

$$\text{longitude}_{AB} = \text{longtiude}_A + \tan^{-1}(y, \text{Cos}(\text{latitude}_A) + x) \quad \textbf{…(3.9)}$$

Since atan^{-1} returns values in the range $-\pi \ldots +\pi$ (that is, -180° ... +180°), to normalise the result to a compass bearing (in the range 0° ... 360°, with values transformed into the range(180° ... 360°), convert to degrees and then use (θ+360) % 360, where % is (floating point) modulo. For final bearing, simply take the initial bearing from the end point to the start point and reverse it (using θ = (θ+180) % 360).

IV. Add AB (latitude , longitude) to grid Location points at database.

5- Calculation of four nearest points to each corner in grid location points (A, B, C, D) and store them in the grid location points at database. The corner consists from three location points so the latitude and longitude of these points must be used as input variables. Since the classroom has a square or rectangular shape, therefore it has four corners Z_1 (A,AB, AC) , Z_2(AB,B,BD) , Z_3(AC,C,CD) , Z_4 (CD , D , BD). For example, in order to calculate nearest point Z1 (A , AB, AC).

where:

a point on the earth's surface can be represented by an n-vector, on a spherical model earth, this will be a vector originating from the centre of the earth. On an ellipsoidal model earth, it will intersect the equatorial plane at an angle equal to the geodetic latitude.

I. Converting the location (A,AB,AC) points from spherical coordinates $P = (r, \theta, \emptyset)$ to Cartesian coordinates (x,y,z) using Eq. (2.7).

$$x = \rho \sin\varphi \, , y = \rho \cos\varphi \qquad \dots \textbf{(2.7)}$$

II. Calculation of vector product using Eq.(2.9) to find vector T[x,y,z].

$$\|\vec{u}\| = \sqrt{u_1^2 + u_2^2 + u_3^2} \qquad \dots \textbf{(2.9)}$$

III. Normalization the vector T[x,y,z] to find vector $\hat{u}$[x,y,z] using Eq (2.10),(3.10),(3.11),(3.12) and (3.13)

$$\hat{u} = \frac{\vec{u}}{\|\vec{u}\|} = \frac{\vec{u}}{\sqrt{u_1^2+u_2^2+u_3^2}} \qquad \dots \textbf{(2.10)}$$

Length=$\sqrt{T[X]^2 + T[Y]^2 + T[Z]^2}$ **… (3.10)**

$\hat{u}$ [x]= T[x]/length **… (3.11)**

$\hat{u}$ [y]= T[y]/length **… (3.12)**

$\hat{u}$ [z]= T[z]/length **… (3.13)**

IV. Multiplying the vector $\hat{u}$ [x,y,z] by equator radius = 6378.137 km, the result of this step put in vector M[x,y,z] using Eq.(3.14),(3.15)and(3.16)

M[x]= $\hat{u}$ [x] × equator radius **... (3.14)**

M[y]= $\hat{u}$ [y] × equator radius **... (3.15)**

M[z] = $\hat{u}$ [z] × equator radius **... (3.16)**

V. Converting M[x,y,z] from Cartesian coordinates to spherical coordinates using eq.(2.6)

$\varphi = \tan^{-1}(y/x)$, $\rho=\sqrt{\mathbf{x^2 + y^2}}$ **… (2.6)**

the formulae for converting between latitude/longitude points and n-vectors apply equally to spherical and ellipsoidal model earths:

a) From latitude/longitude to n-vector, the n-vector for a point φ, λ on the earth's surface, where latitude = φ and longitude = λ, is defined as

$$v[x,y,z] = \begin{bmatrix} \cos\varphi \times \cos\lambda \\ \cos\varphi \times \sin\lambda \\ \sin\varphi \end{bmatrix} \quad \textbf{... (3.17)}$$

b) From n-vector to latitude/longitude, for a given n-vector, the latitude φ and longitude λ of the point it represents on the surface is defined as:

$\varphi = \text{atan}^{-1}(v_z, \sqrt{v_x^2 + v_y^2})$, $\lambda = \text{atan}^{-1}(v_y, v_x)$ **... (3.18)**

The equation (3.19) was obtained :

Latitude $_{z1}$ = sin $^{-1}$ (z / equator radius)

Longitude $_{z1}$ = tan^{-1} [(y, x)] **... (3.19)**

VI. Adding location Z_1(latitude, longitude) to grid location point databased.

5-Repeate step 4 for calculate addition four nearest points for each corner in grid location (Z_1,Z_2,Z_3,Z_4) and stored in grid location points at databased. These nearest points are C_1 (Z_1,Z_2,Z_3) , C_2 (Z_1,Z_2,Z_4) , C_3 (Z_1,Z_3,Z_4) and C_4 (Z_2,Z_3,Z_4).

The results of determining grid location points for smart class room step includes (boundary point location, midpoint location, and nearest point location) which are shown in figure (3.7).

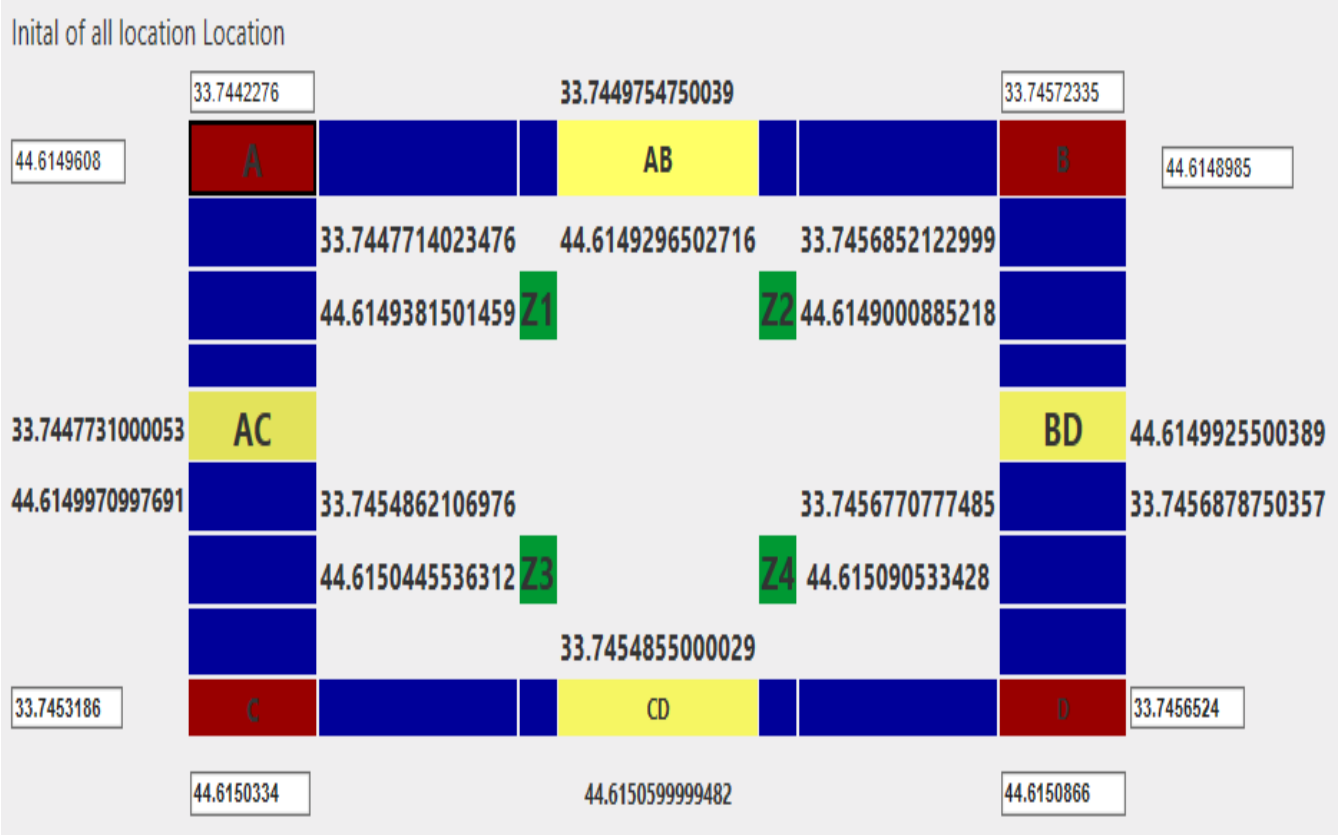


Figure (3.7) : Grid Location Points for Smart class Room.

6 - Calculation of Earth Radius for Each Grid Point:

For each location point in grid location points, the proposed technique calculates the radius of the earth in the latitude of these points and store them in the database in the form of (point, radius of the earth). In this step, the proposed technique creates function to return the earth radius in a degree system for each point in database.

For example, in order to calculate the earth radius for location A (33.7442276, 44.6149608):

1- Converting Latitude $_A$ form degree to radian (33.7442276 * PI / 180.)
2- Applying equation (3.20):

$$\mathbf{R = equator\ radius * \frac{\sqrt{\frac{Polar\ radius^4}{equator\ radius^4 \times \sin(Latitude_A)^2 + \cos(Latitude_A)^2}}}{\sqrt{(1-(1-\frac{polar\ radius^2}{equator\ radius^2}) \times \sin(Latitude_A)^2}}} \quad \ldots(3.20)$$

Where

polar radius = 6356.7523142 km , equator radius = 6378.137 km.

The earth is an ellipsoidal in shape, ellipses have a minor axis and a major axis. For Earth the minor axis passes through the poles and has an approximate polar radius = 6356.7523142 km, The major axis is equivalent to the radius at the equator with an approximate radius equator radius = 6378.137 km and earth radius = 6367 km , In the real world the angle of latitude is the angle between the radius of curvature in the minor axis and the equatorial plane (R).

3- Adding the result: (point name, (latitude, longitude), earth radius) to database.

the results of the first stage are create grid points consist of three elements (point name, location of grid points (latitude, longitude), earth radius for each grid location points).

ii-Second Stage (Authentication Test):

In the second stage, instead of places, the location distance of the student mobile is analyzed. Distances can be calculated by using the Haversines E**q. (2.12)** and the threshold value to get more accurate results. Grid point locations from database are used to get the latitude and longitude of each grid point and their earth radius. Then, the minimum haversines distances are checked, if the min value less than or equal to (0.01) then this location of mobile student is authenticated otherwise is not authenticated. This process is described in algorithm (3.2).

Algorithm (3.2): Authentication Test

Input: Mobile location (latitude , longitude)
Output: Authenticate, not Authenticate
Begin **Step1:** get all Location grid points and their Earth Radius in database **Step2** : get Location from student Mobile **Step3** : get Haversine distance for each grid Location points and their earth radius using eq. (2.12) **Step4** : get min distance for step3 and check If min ≤ 0.01 then Authenticate Else not Authenticate **End**

B- Key Generation Service

After the first service has been determined, the students are authorized to use the learning system. The data transferred between (students- lecturer) and web application server must be safe. Here the key generation service take place, and the web application server uses a proposed algorithm (IKSA) (Improved Key Scheduling Algorithm) as an improvement version of KSA for RC6 to generate variable length key for N users by using two types of chaotic map (Chebyshev,2D-logistic). Chebyshev determines the length of the key, while 2D-logistic determines the key elements as shown in block diagram of figure (3.8).

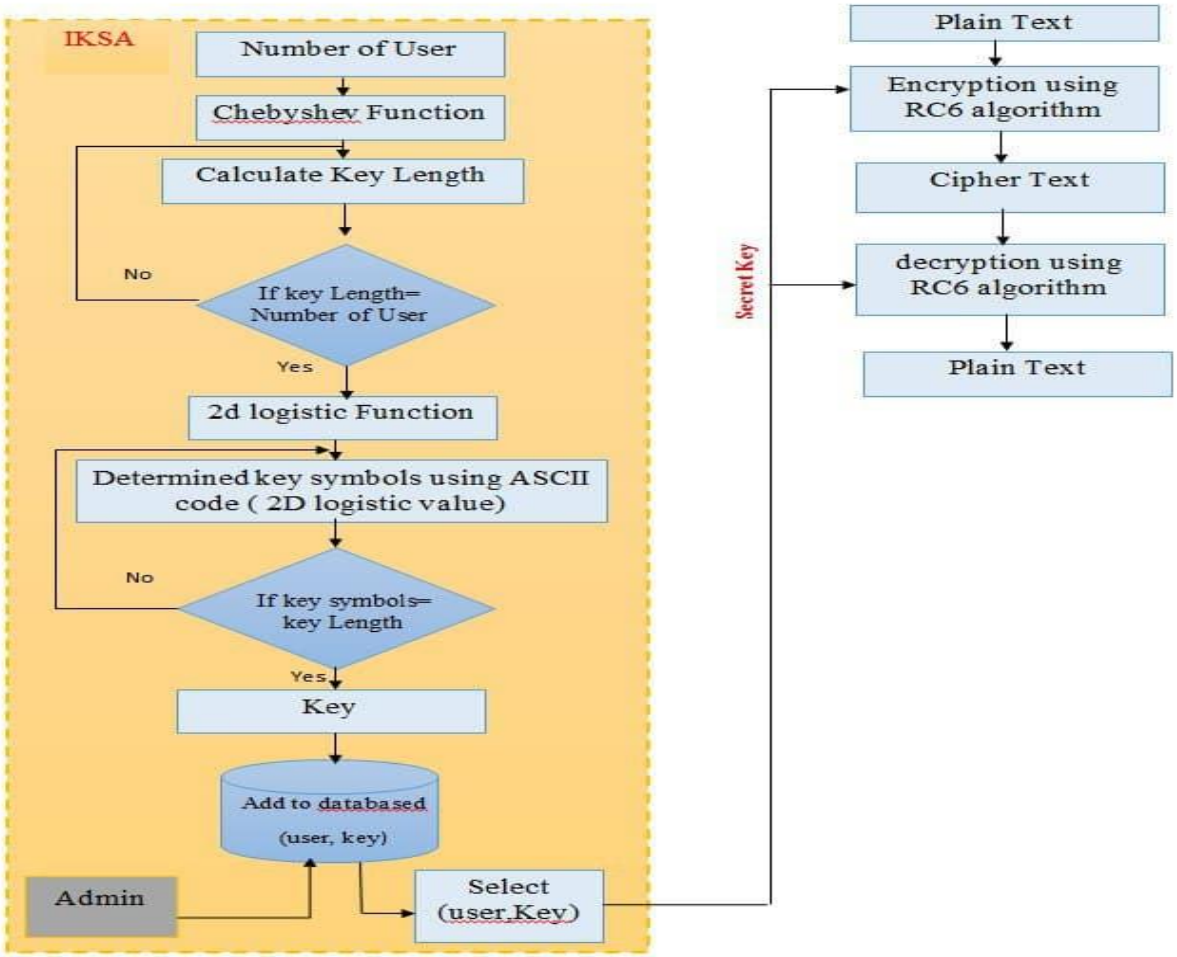


Figure (3.8): Block Diagram of the IKSA and IRC6 algorithm.

Proposed algorithm can work with different word size (denoted by w), the rounds number (denoted by r), block length (denoted by b). Hence the short-notation IRC6-w/r/b is used to refer to size of word, the rounds number and block length and a key of b bytes is assigned to each user , where 0 <= b <= 255 . IRC6-w/r/b uses same structure for RC6 encrypte/decrypte process.

proposed IKSA uses chebyshev and 2D logistic maps to design the chaotic key schedule for RC6 to produce unpredictable, uncorrelated and highly randomness rounds keys using a deterministic function that can generate the same sequence at both encryption and decryption methods identically. The outputs of IKSA is N keys for N of users stored in database of an administer side. The administer selected user to assign to him a unique key and use the key in RC6 encrypte/decrypte process.

- **Improvement key scheduling algorithm (IKSA)**

Chaotic map is employed in the proposed system at key scheduled stage, more over to enhance security of the system in a perfect manner. The used chaotic systems are chebyshev maps and 2D logistics. Chebyshev and 2D logistic maps are used to create a N number of keys to N of users with variable lengths as shown in algorithm (3.3).

Algorithm (3.3) Improved Key scheduling algorithm (IKSA)

Input (No) Number of users, ((X_0) initial value ,(n) degree of chebyshev polynomial)parameter of chebyshev function.
((X_{00}) initial value, (λ) control parameter) parameter of logistic function.

Output database (user, key)

Begin

Initialize IKSA by enter the (No) number of users to provide each of them a unique key
For (User=1 to No)
While (! Key length < =3)
Calculate $Chevbyshev_{value}$ by equation (2.3)
Swap (X_0 , $Chevbyshev_{value}$)
Data = Split ($Chevbyshev_{value}$, '.') and take only digits after the dot '.'
Key length= Convert 'Data' to integer number of 64- bits
End while
For (i=1 to key length)
Calculate logistic $_{value}$ by equation (2.5)
Swap (X_{00}, Logistic $_{value}$)
Convert Logistic $_{value}$ to integer number 64-bits
Key [i]= Convert Logistic $_{value}$ to its ASCII equivalent value
End For
Add to databased (user, key)
End For
End Algorithm

The main function of proposed IKSA is generate N key for N users with variable length. In order to achieve this, IKSA can be divided into two parts:

1- Determine **key length** using chebyshev map, where the minimum limit for key length that is not equal and less than (3 symbols) to avoid create short keys that are not secure to be used for IRC6 algorithm. Chebyshev function used

parameter as inputs to its function, for example these parameter are: $\mathbf{X_0}$ (initial value) = 0.2 and **n** = 5 and number of round [0-255], if the chebyshev value = 0.334612078527893, spilt this value and take digits after dots '.' (334612078527893) and converted to integer number 64-bits using Mod operation then key length = Mod(334612078527893) = 9 .

2- Determine the key symbols using 2D logistic map, here the key represent as vector and length of this vector is equal **key length** value and each key symbol can be represented using logistic value after converted to Ascii code that its equivalent value. for example, 2D logistic function used parameter as inputs to its function, these parameters are: $\mathbf{X_{00}}$ (initial value) = **0.4** and $\boldsymbol{\lambda}$**=0.7** and number of round [0-255]. since the key length = 9, must be generate 9 logistic value using 2D logistic function and stored in array vector as **V** =(1,1,1,1,242,98,242,169,1) then convert each value in **V** to its equalized Ascii code to produce key = □□□□ _ h _ &□

C- Ciphering using IRC6 Service

web application server using Encryption /Decryption Process in IKSA. The input of encryption algorithm are four registers include plains text denoted by: A, B, C, and D each of which is of length w words. In additional to the keys generated from the IKSA, length of the encryption key in bytes denotes by b, rounds number denotes by r.

The administer selected user from data base to get (user, key), then encryption algorithm shown in algorithm (2.2) is used to convert the plain-text to the cipher-text populated in the four registers.

in the decryption algorithm shown in algorithm (2.3), The four registers A, B, C, and D Includes the cipher-text are fed into IRC6 along with the round number (r) and same key is used in encryption process which is get from database will be used in decryption process. The output of IRC6 decryption is the plaintext.

Chapter Four

Implementation and Results

Chapter Four

Implementation and Results

4.1 Introduction

This chapter describes the implementation of the proposed system, also it presents the practical results, initialization is given in section (4.2). The implementation of the proposed system is illustrated in section (4.3). While, section (4.4) clarifies the results of the proposed mobile learning system. Tests are presented in section (4.5).

4.2 Initialization

The proposed system is implemented by using Microsoft visual studio environment 2017 by the C# programming language, Android Studio 3.4.1, SQL Server 2012, with a laptop computer (core i7) and Windows 10 as an operating system. Mobile devices with Android as an operational platform.

4.3 Implementation of The Proposed system

Implementation of the proposed system is clarified in subsections (4.3.1 and 4.3.2).

4.3.1 Implementation of Administrator

The main page of administrator starts with " detect location" as shown in figure (4.1) for logging in. The administrator enters the four borders of the smart class room (top left, top right, button left, and button right) in generation grid point.

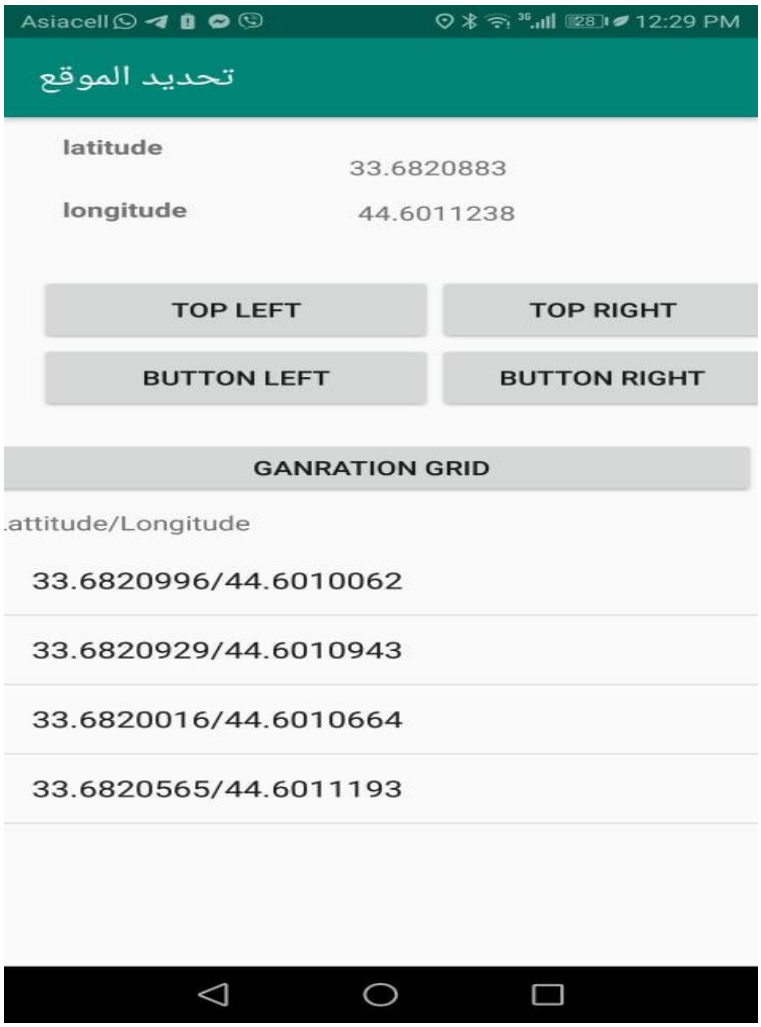


Figure (4.1): The Interface of Administrator detect location.

The interface of administrator for calculating grid location is shown in figure (4.2).

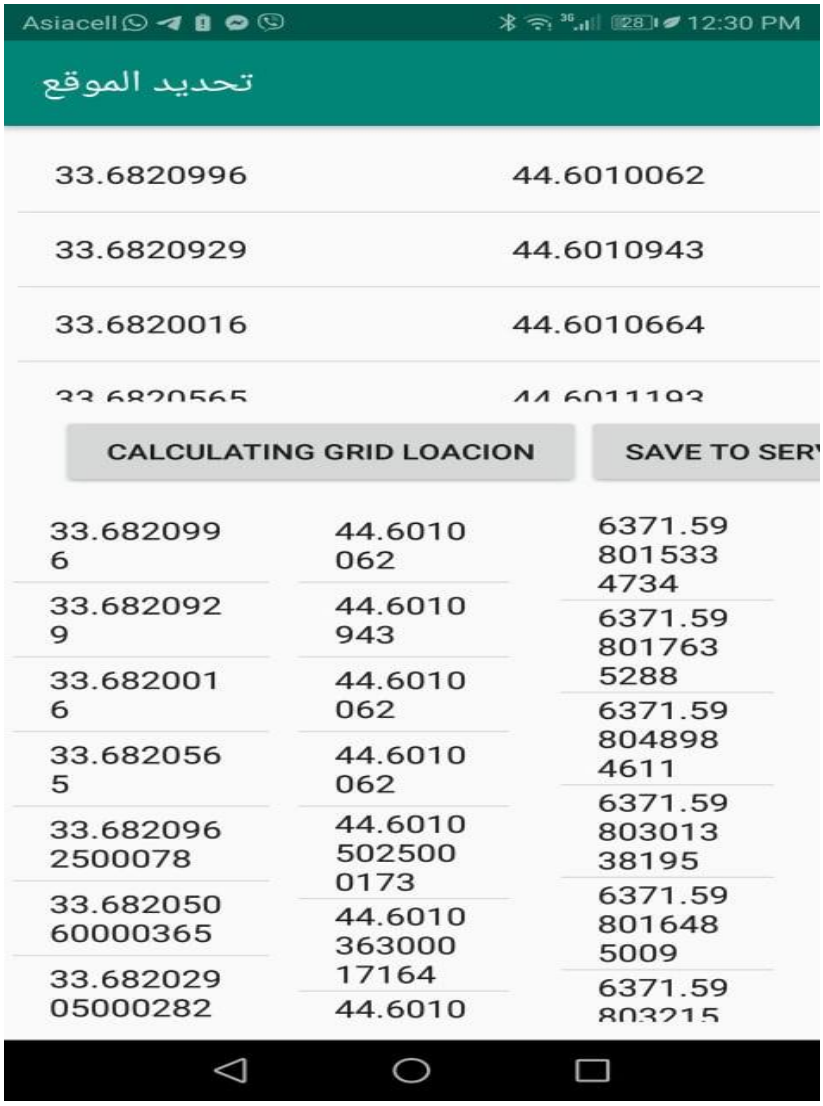


Figure (4.2): The Interface of Administrator Calculating Grid Location.

After calculating grid locations for smart classroom, the points are saved in database of server as show in figure (4.3).

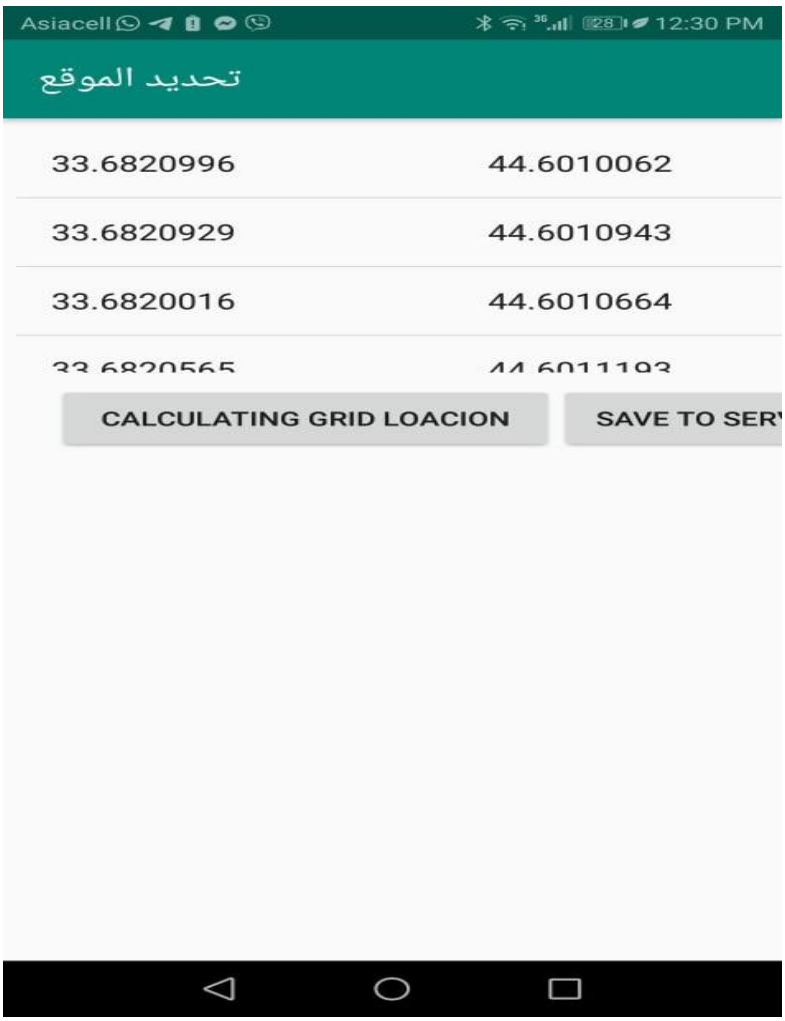


Figure (4.3): The interface of Stored Grid Points in Database of the Server.

4.3.2 Implementation of Client

The implementation of the client side is shown in figure (4.4), starting with the main interface of the application that requires (Latitude and longitude) to log in.

Figure (4.4): The Main Interface of the Client Side.

The client login process begins by sending a request involve student mobile location to the server (administrator) in order to login in, while the server determines whether the student is authorized or not. After the student mobile location is authenticated, the proposed system calculates the haversine distance which are shown in figure (4.5).

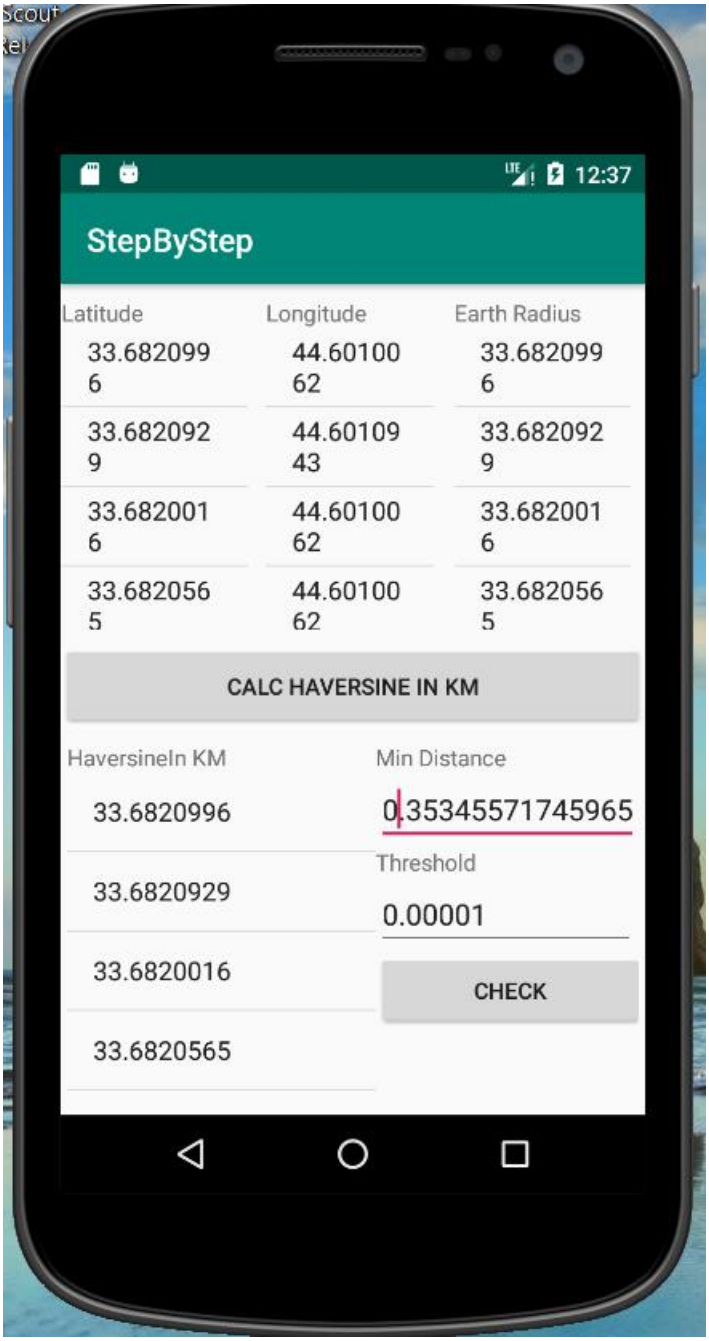


Figure (4.5): Interface of Calculation the Haversine Distances

After calculation the haversine distance, the result is compared with the threshold value, if the haversine distance is smaller than threshold value then the student is authenticated and if it is larger, the student is unauthenticated. This is shown in figure (4.6).

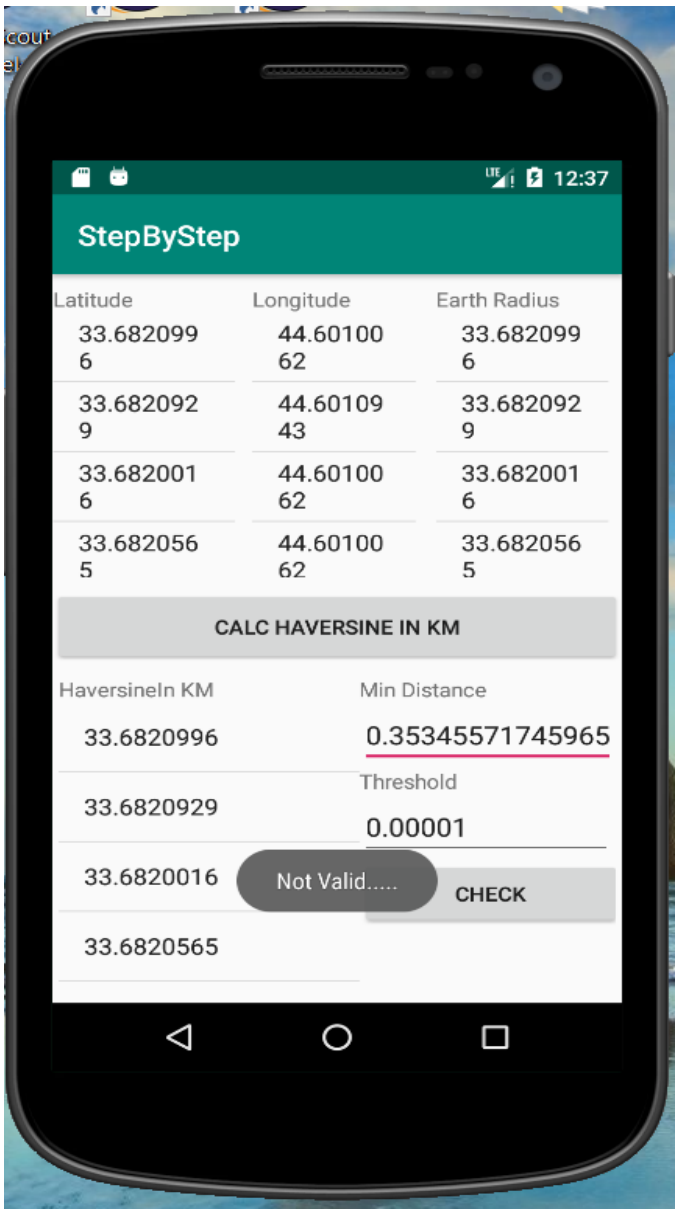


Figure (4.6): Interface of Student Authentication .

4.4 Results of the Proposed system

The results of the proposed system are concentrated on the proposed authentication and encryption techniques. These results are described in subsections (4.4.1 and 4.4.2).

4.4.1 Mobile Location Test

The test samples of student's mobile phone locations that are used in the proposed authentication technique, are shown in the table (4.1).

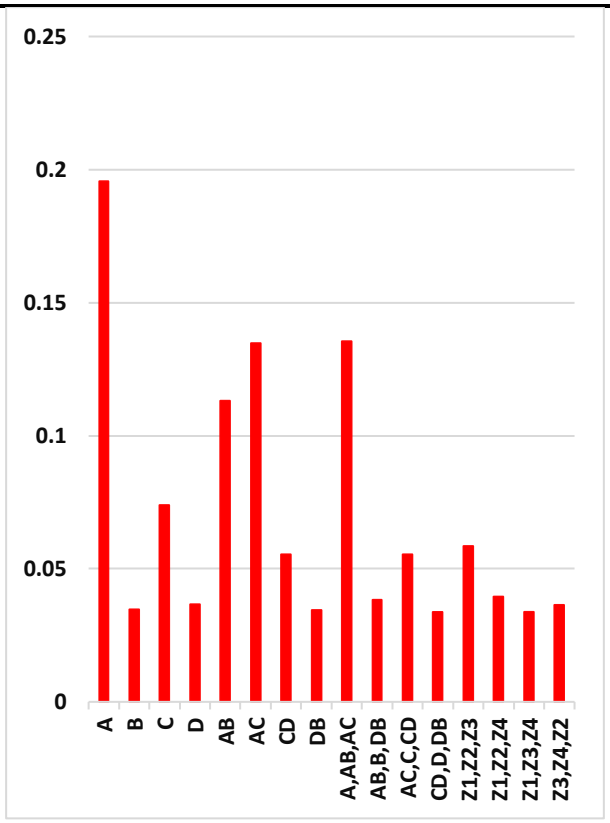
Table (4.1): Test Samples of Students Mobile Phone Locations.

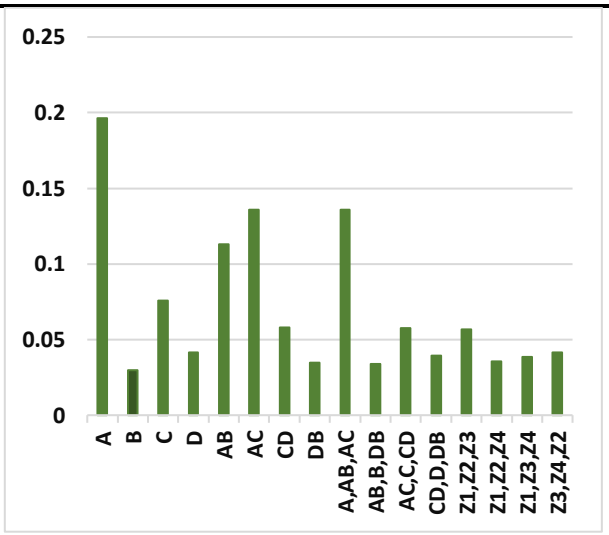
Boundary Points for Smart Classroom	Student Mobile Location (SML)
A= (33.7442276,44.6149608) B= (33.74572335,44.6148985) C= (33.7453186,44.6150334) D= (33.7456524,44.6150866)	SML_1=(33.7459811, 44.6151115)
	SML_2=(33.7459908 ,44.6148963)
	SML_3=(33.7459906 ,44.6148962)
	SML_4=(33.7459907, 44.6148964)
	SML_5=(33.7455859,44.6146099)
	SML_6=(33.7456891,44.6148047)
	SML_7= (33.7457325,44.614823)

Location detection algorithm plays an important role in proposed authentication technique at both sides' client (mobile phone) and administrator (server). Therefore, table (4.2) clarifies the results of calculating haversine distance values using location detection algorithm with different sample mobile phones location.

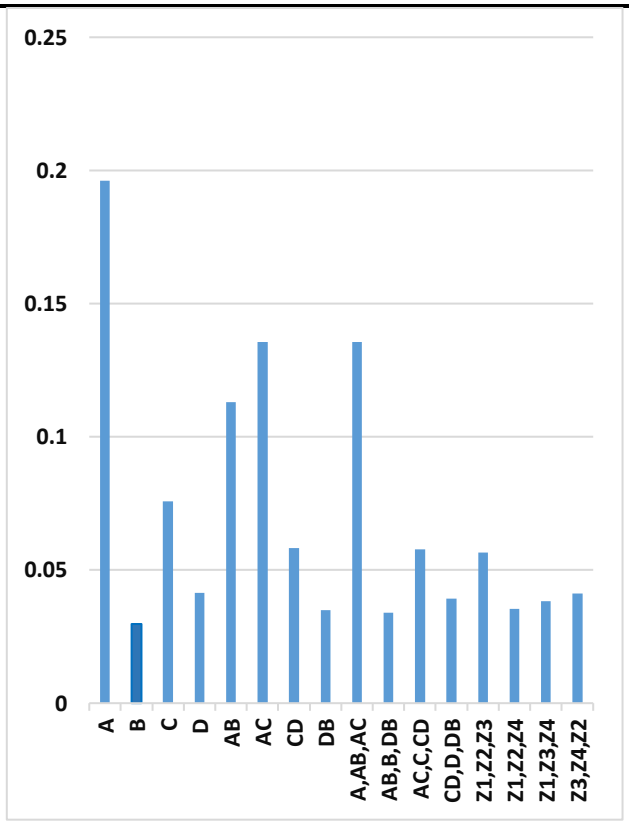
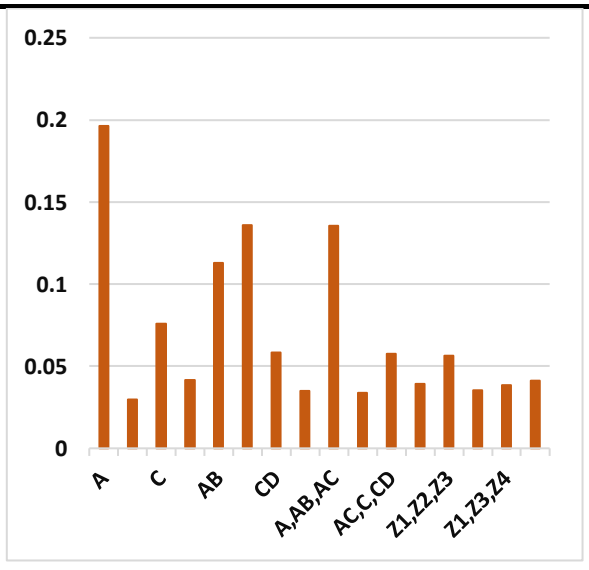
Table (4.2): Haversine Distance Values using Proposed Authentication Method with Student Mobile Locations (SMLs).

SML	Location		Validity test
	point	Haversine	
SML_1	1	0.195495235957958	Not valid
	2	0.0347777611219854	
	3	0.0740264106813489	
	4	0.03662552119342	
	5	0.113087666756994	
	6	0.134751486968794	
	7	0.0553185450249468	
	8	0.034413169971128	
	9	0.135476048580421	
	10	0.0382732466764902	
	11	0.0553812204424769	
	12	0.0338643313281451	
	13	0.0585585453405051	
	14	0.0395554195634142	
	15	0.0337965225543528	
	16	0.0364125948071356	
SML_2	1	0.196167329860777	Not valid
	2	0.0297424682807273	
	3	0.0758193678435688	
	4	0.0415426618218899	
	5	0.112951309135386	
	6	0.135734718412825	
	7	0.0581949905915337	
	8	0.0348426335942007	
	9	0.135658308556048	
	10	0.0339846805184378	
	11	0.0577631454194811	

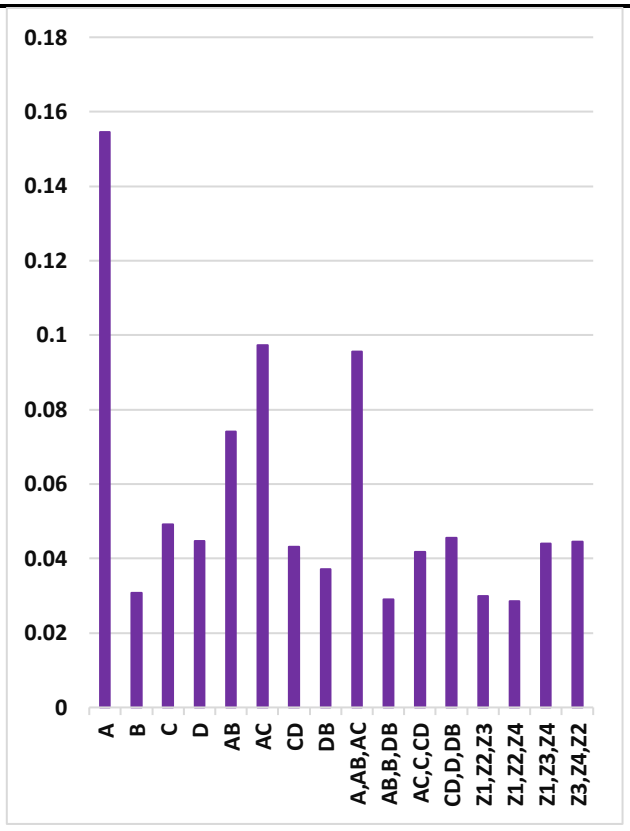
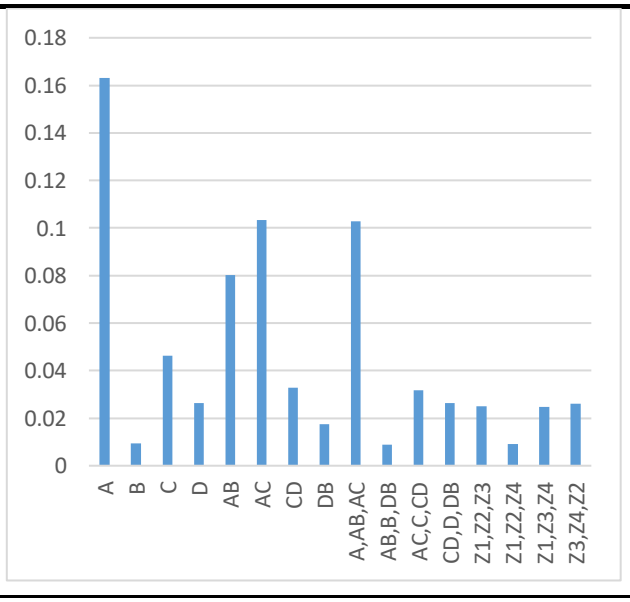




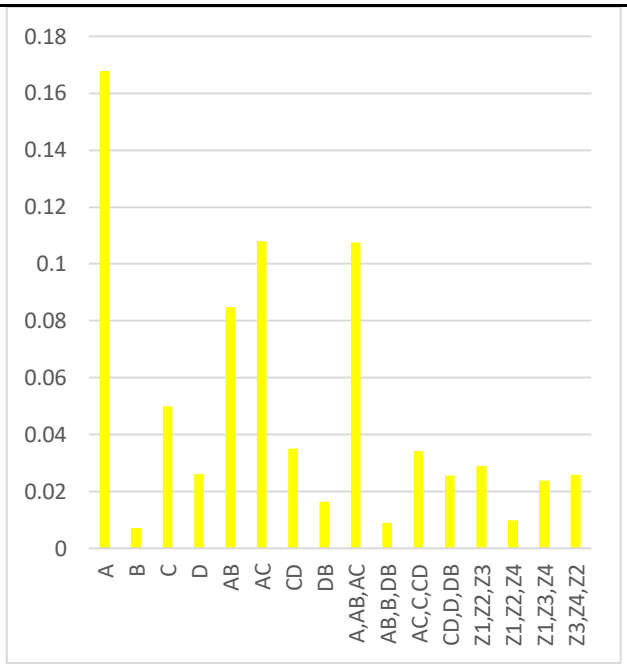
Continue Table (4.2)

	12	0.0392391591476396		
	13	0.0565597530241772		
	14	0.0354978417478786		
	15	0.0383538912908137		
	16	0.0412811525555562		
SML_3	1	0.196145380536134		**Not valid**
	2	0.0297202925357182		
	3	0.0757989871597563		
	4	0.0415264352219047		
	5	0.112929329319978		
	6	0.135713165317053		
	7	0.0581759221893665		
	8	0.0348234954558652		
	9	0.135636340747102		
	10	0.0339625373420649		
	11	0.0577437361322294		
	12	0.0392236214468211		
	13	0.0565377023555486		
	14	0.0354757083552028		
	15	0.0383377237978427		
	16	0.0412649114073129		
SML_4	1	0.196155933563946		**Not valid**
	2	0.0297312862113843		
	3	0.0758068581289265		
	4	0.0415286716220559		
	5	0.112939940674439		
	6	0.135722989453125		
	7	0.0581818480049235		
	8	0.0348295205778028		
	9	0.135646929098329		
	10	0.0339734665211876		
	11	0.0577501484682986		

Continue Table (4.2)

	12	0.0392250396488473		
	13	0.0565484504281861		
	14	0.0354866182357335		
	15	0.0383398890899395		
	16	0.0412671653640106		
SML_5	1	0.154495492883826		Not valid
	2	0.0307537901222449		
	3	0.049164192206172		
	4	0.0446956596250639		
	5	0.0740419302111835		
	6	0.0972203823819272		
	7	0.0430915561220768		
	8	0.0371558114995097		
	9	0.0955266771311265		
	10	0.029017110397195		
	11	0.0416925927027503		
	12	0.0455852896209056		
	13	0.029921946535414		
	14	0.0285251334195443		
	15	0.0440728792250577		
	16	0.0445937029166189		
SML_6	1	0.163165816960123		valid
	2	0.00947294162862459		
	3	0.0463117381741539		
	4	0.0263843544792238		
	5	0.0801953305577988		
	6	0.103405732730537		
	7	0.0327097528944773		
	8	0.0173706914977957		
	9	0.102795909456771		
	10	0.00883099526297143		
	11	0.0316379426314989		
	12	0.0264642993740326		
	13	0.0249218813572636		
	14	0.00908348133752909		

Continue Table (4.2)

	15	0.0248566554918129		
	16	0.0262109793026962		
SML_7	1	0.167836787759717		**valid**
	2	0.0070551089281767		
	3	0.0499706290429793		
	4	0.0259512232322551		
	5	0.0847606140808372		
	6	0.107897824881451		
	7	0.0351388272590424		
	8	0.016444628469533		
	9	0.107407935106675		
	10	0.00885804254130753		
	11	0.0342029188428414		
	12	0.0254945198472654		
	13	0.0289266248251888		
	14	0.00986975508815527		
	15	0.0238949362038389		
	16	0.0257425186189239		

Results of Table (4.2) showed the ability of detecting different student locations based on Haversine distance values.

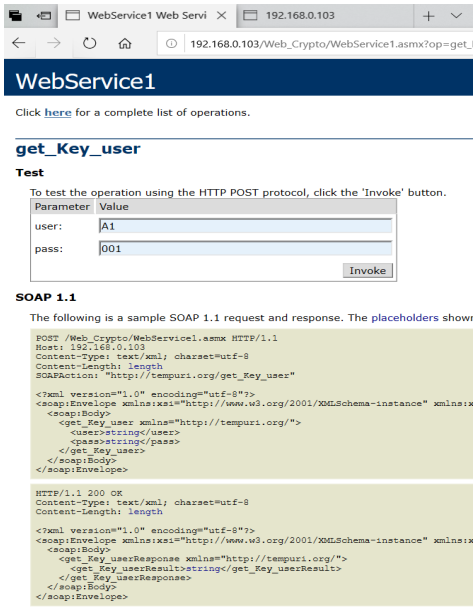
4.4.2 The Results of the Proposed IKSA for IRC6 Algorithm

Table (4.3) shows two cases to generate keys for 10 users by using the proposed IKSA. Case 1: using (X_0 = 0.2) as initial value for chebyshev map and (X_{00} =0.4) as initial value for 2d logistic map. Case 2: using (X_0 = 0.1) as initial value for chebyshev map and (X_{00} = 0.3) as initial value for 2d logistic map.

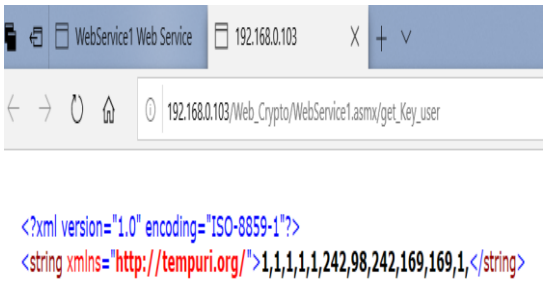
Table (4.3) : Key generation using IKSA with Different Initial parameters for chebyshev and 2d-logistic Chaotic Maps.

#users	*Case 1*	*Case 2*
1	1,1,1,1,1,242,98,242,169,169,1,	1,1,1,1,1,166,106,166,16,16,1,
2	22,94,82,193,229,1,166,163,106,	162,234,42,168,234,171,186,138,186,42,42,171,42,
3	46,226,1,46,151,151,91,	144,144,48,171,63,48,177,186,219,177,81,144,147,27,219,
4	1,118,118,67,1,154,67,1,154,67,67,154,154,67,154,	69,18,69,69,222,222,69,171,222,222,69,222,222,171,69,
5	169,13,13,169,1,13,13,	180,165,165,180,75,60,120,210,165,
6	109,151,184,109,79,16,214,79,244,244,244,184,214,	85,85,85,85,85,85,85,85,85,
7	166,16,166,41,176,11,116,	56,56,56,146,71,106,16,106,116,56,131,146,116,41,11,
8	125,80,20,55,55,70,245,245,5,	106,106,151,244,244,139,214,
9	4,1,4,4,4,1,1,1,4,	186,42,42,42,186,171,186,42,138,138,234,
10	147,147,144,177,219,147,219,3,219,	164,121,44,121,209,121,166,164,209,16,194,164,16,121,14,

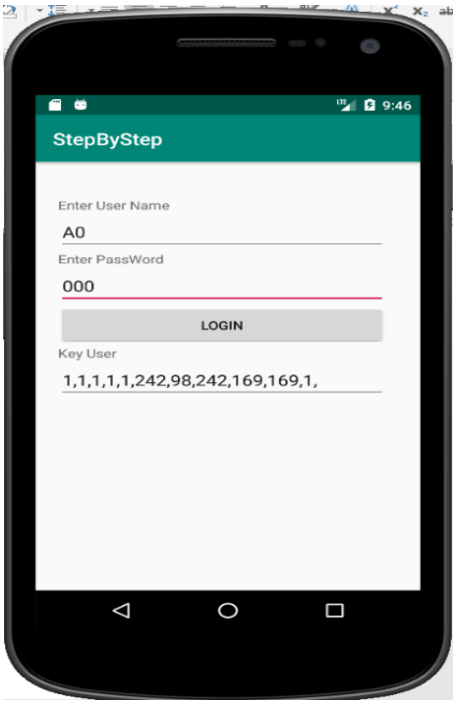
Explanation assign secret key of the IKSA process in web application services side and client (student) side for three students in Figure (4.7,4.8 and 4.9)



a

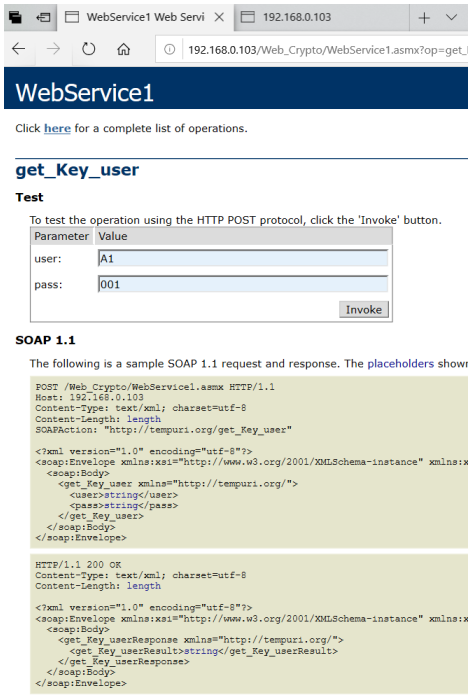


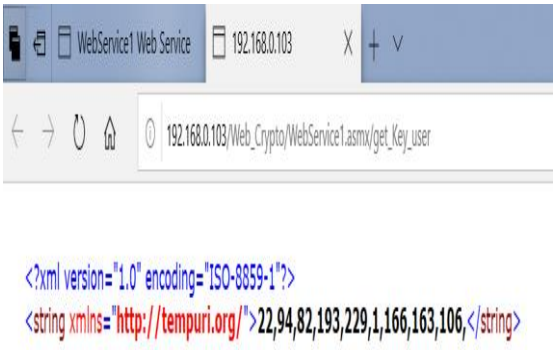
b



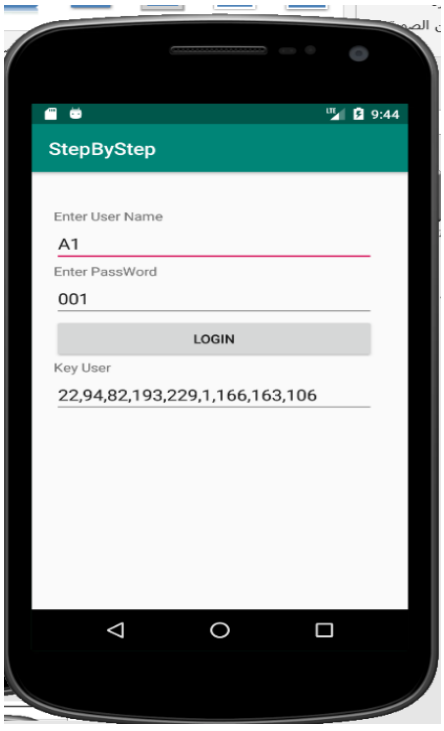
c

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



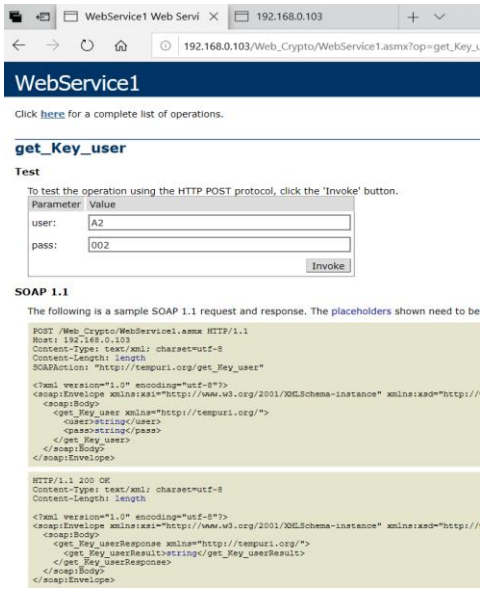


a **b**

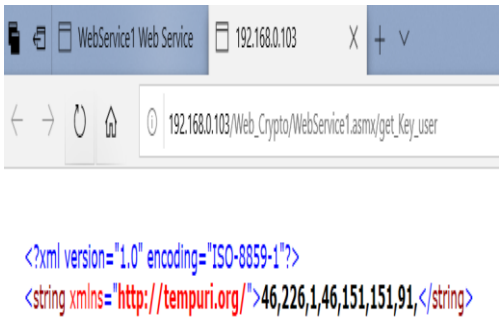


c

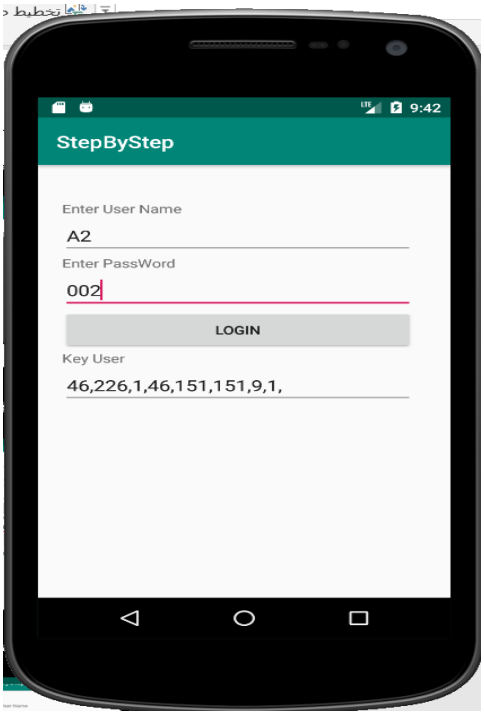
Figure (4.8) Assign secret key process in web application services side and client (student) side for user2 (a)web services input, (b)web services output ,and (c) mobile of user2



a



b



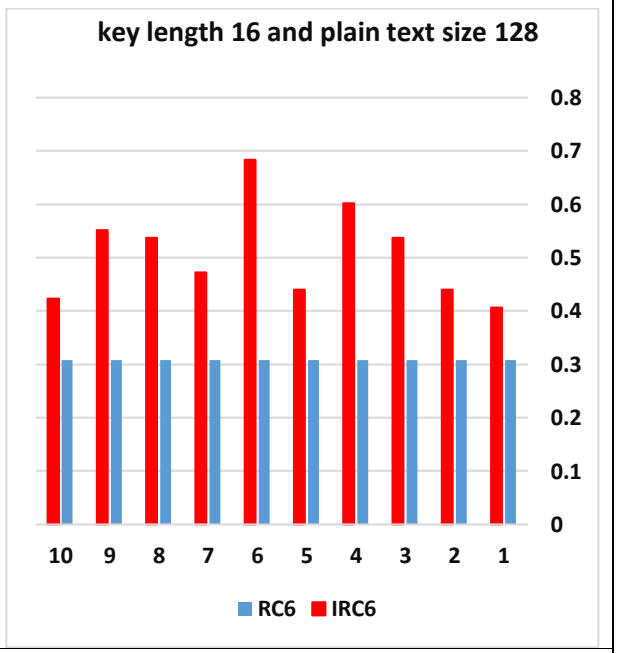
c

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

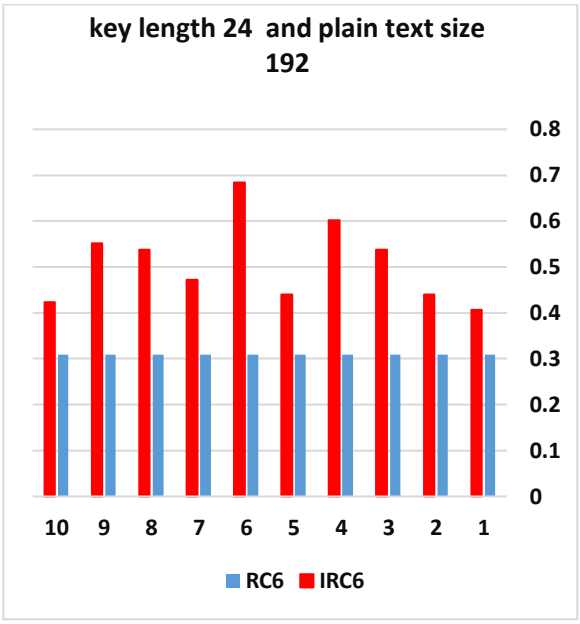
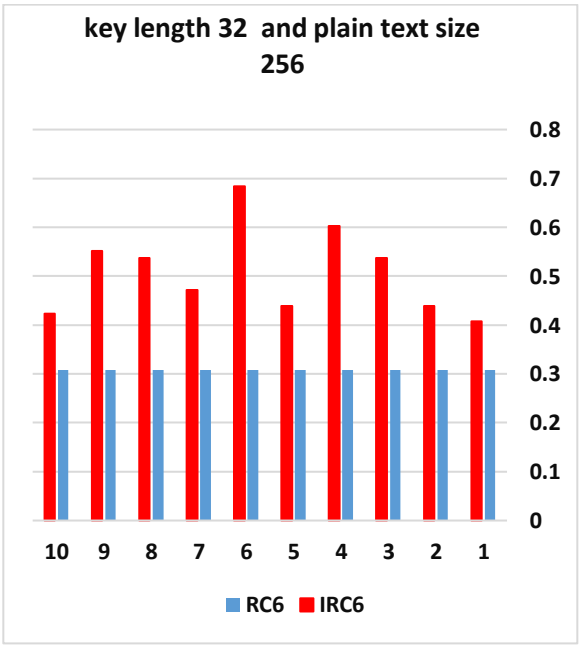
4.5 Tests

Depending on section (2.11), secrecy of IRC6 is tested in terms of the key equivocation (conditional entropy of key given cipher). Table (4.4) shows the average security of original RC6 algorithm with KSA, and IRC6 algorithm with IKSA using a fixed size plaintext (128,192, and 256) bits and fixed key length (16,24, and 32) bits.

Table (4.4): Average security for RC6 and IRC6.

Keys Length\ Bits	Plaintext Size\ Bits	User	Average Secrecy for RC6	Average Secrecy for IRC6	Average security for RC6 and IRC6
16	128	1	0.244180662225532	0.922843090385818	
		2	0.244180662225532	0.439525192005959	
		3	0.244180662225532	0.471306701932767	
		4	0.244180662225532	0.569754878526243	
		5	0.244180662225532	0.617039187564824	
		6	0.244180662225532	1.41359924196203	
		7	0.244180662225532	0.568591010971349	
		8	0.244180662225532	0.390689059560852	
		9	0.244180662225532	0.667427143416456	
		10	0.244180662225532	0.390689059560852	
24	192	1	0.244180662225532	0.4546400352661	
		2	0.244180662225532	0.358131637930781	
		3	0.244180662225532	0.487585412747803	
		4	0.244180662225532	0.4546400352661	
		5	0.244180662225532	0.781378119121704	

Continue Table (4.4)

		6	0.244180662225532	0.439525192005959	
		7	0.244180662225532	0.455803902820994	
		8	0.244180662225532	0.569754878526243	
		9	0.244180662225532	0.537197456896172	
		10	0.244180662225532	0.615875320009931	
32	256	1	0.308519593782412	0.406967770375887	
		2	0.308519593782412	0.439525192005959	
		3	0.308519593782412	0.537197456896172	
		4	0.308519593782412	0.602312300156314	
		5	0.308519593782412	0.439525192005959	
		6	0.308519593782412	0.683705854231491	
		7	0.308519593782412	0.47208261363603	
		8	0.308519593782412	0.537197456896172	
		9	0.308519593782412	0.551924344304682	
		10	0.308519593782412	0.423246481190923	

The highest values of the average security for the three tests key length and plain text size for the RC6 and IRC6 are shown in the table (4.5).

Table (4.5): Highest Values of Average Security for the RC6 and IRC6.

Key length\ Plain text size	RC6	IRC6
16\128	0.244180662225532	1.41359924196203
24\192	0.244180662225532	0.781378119121704
32\256	0.308519593782412	0.683705854231491

Figure (4.10) shows a comparison between RC6 and IRC6 based on highest values of average security.

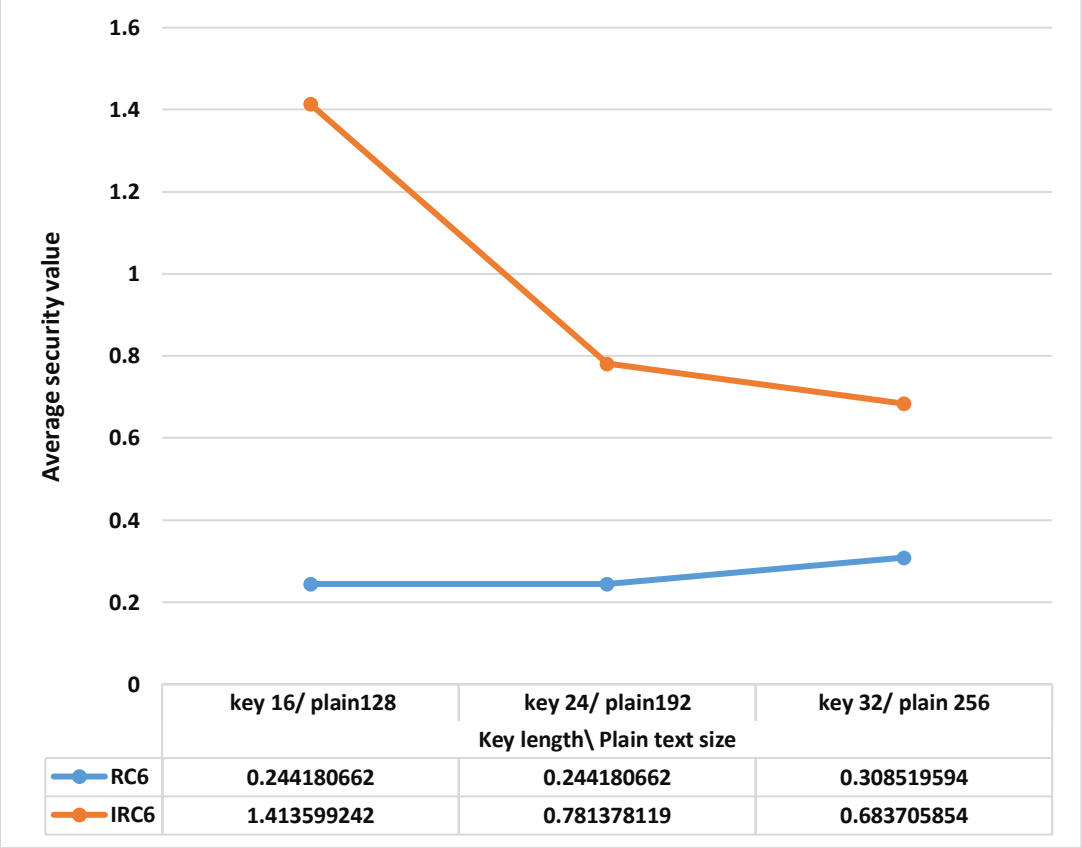


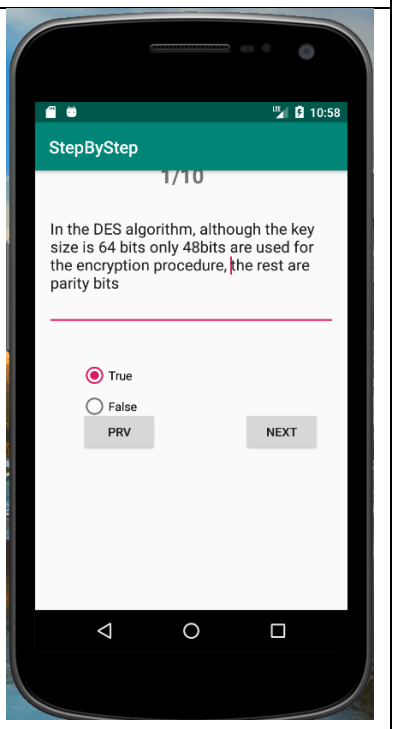
Figure (4.10): Comparison between RC6 and IRC6

Table (4.5) and figure (4.10) show the average security for IRC6 better than RC6.

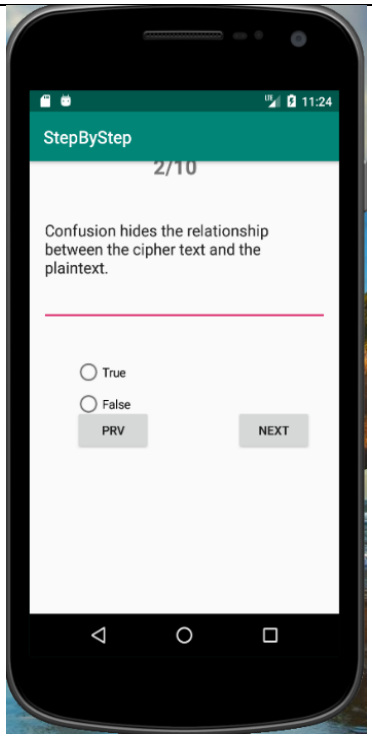
4.5.1 Example of Encryption using IRC6

In the proposed system the student can take an educational course and interact with the lecturer and participate in the exam, but the exam is shown only as an example of the encryption process using IRC6, table (4.6) illustrated encryption /decryption answer of the client (student) using secret key which is generate in IKSA.

Table (4.6): Encryption /Decryption student answer using IRC6 .

Question		User	Key	Encrypt questions	Mobile
1	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits	1	,1,1,1,1,1, 242,98,24 2,169,169, 1	198,201,8,244,183,93,171,218,52,110,103,2,110,20,98,49, 9,13,8,166,54,9,101,15,212,134,1,28,138,68,190,169,156,2 15,102,207,152,204,169,104,215,229,27,55,49,96,222,133, 198,193,238,232,149,120,85,214,54,95,214,30,245,40,141, 143,86,220,227,119,45,27,185,108,191,211,77,36,202,163, 93,233,124,231,186,143,192,237,9,23,63,111,102,232,77,2 34,173,162,141,206,196,75,251,193,164,206,5,168,34,42,3 8,195,186,189,102,174,238,168,141,190,99,153,12,105,13 8,218,59,242,103,47,121,176,32,75,133,106,143,105,147,7 3,7,231,2,237,164,40,	
		2	22,94,82,1 93,229,1,1 66,163,10 6	230,68,246,99,189,231,247,72,148,201,27,68,244,48,59,60 ,77,127,228,238,54,196,147,241,95,249,142,241,186,127,9 7,17,83,87,166,141,165,21,122,202,223,176,119,39,82,36, 37,4,83,84,48,115,89,193,71,228,45,188,101,213,176,254, 229,192,12,218,133,145,235,180,135,135,19,5,234,246,10 7,182,207,241,124,89,15,250,57,35,32,25,121,102,174,95, 64,33,200,5,147,66,185,90,3,87,234,37,84,158,218,132,13 6,20,219,223,104,211,196,52,236,134,119,93,81,155,192,1 50,241,164,107,147,13,158,164,119,66,31,80,53,245,114,2 1,196,158,52,214	

Continue Table (4.6)

2	Confusion hides the relationship between the cipher text and the plaintext.	1	,1,1,1,1,1,242,98,242,169,169,1	240,141,160,95,178,218,239,155,47,215,63,190,225,146,198,213,140,49,94,241,35,240,125,44,189,251,100,86,151,153,169,188,44,139,20,157,109,143,23,36,207,195,10,192,137,61,252,234,250,160,229,47,92,116,29,229,20,112,7,53,174,28,111,88,249,172,135,165,240,108,57,94,5,100,49,135,81,187,100,19,	
		2	22,94,82,193,229,1,166,163,106	2,227,202,207,183,183,114,213,204,212,179,19,17,215,109,19,125,91,129,37,126,60,151,56,81,22,5,243,249,166,75,8,255,5,115,55,164,137,241,81,95,105,210,203,179,200,203,252,187,160,146,140,36,135,45,12,227,238,245,209,41,199,227,11,90,201,155,157,233,243,229,12,194,14,37,201,113,230,14,194	

Chapter Five

Conclusions and Suggestions for Future Work

Chapter Five

Conclusions and Suggestions for Future Work

5.1 Introduction

This chapter concludes some conclusions about the implementation and results of the proposed secured mobile learning system. These conclusions are given in section (5.2). Section (5.3) outlines the suggestions for future work.

5.2 Conclusions

Some conclusions can be drawn from the results and tests of this work as follows:

1- Results in section (4.4) clarifies that the proposed mobile learning system is successfully implemented through collaboration between mobile phones and the server through web service technology. However, authentication is an important issue to protect this system.

2- Results of sections (4.4.1, 4.4.2) and tests in section (4.5) prove that adoptive authentication system is efficient through utilizing mobile location detection algorithm to achieve high security.

3- There is significant work in implementation of this work that is invisible to the user through using web service technology, especially in dealing with mobile devices.

4- Table (4.3) shows that the proposed system to generate keys is very sensitive to any change in the initial values, this is because of using chaotic function.

5- Figures (4.7,4.8 and 4.9) shows assign secret key of the IKSA process in web application services side and client (student) side.

6- Table (4.4) shows the highest average security value for IRC6 is 1.41359924196203 with key length =16 and plain text size=128. While, the highest average security value for RC6 is 0.308519593782412 with key length =32 and plain text size=256. In addition, table (4.5) and figure (4.10) prove the proposed IRC6 algorithm is more secure than original RC6.

7- Authentication using location which is used in this model is an important step toward smart classroom.

5.3 Suggestions for Future Work

in this work, several topics have been identified that will provide significant support in the field of secure mobile learning system such as:

1- Developing a stream cipher by depending on the RC7 for increasing authentication with the addition of other types of chaotic map such as: (symplectic, tangent, tent, tinkerbell , interval exchange map).

2- Using other media such as (picture, voice) overlapping with using texts and video in order to increase unpredictability.

3- Use multi smart classes to provide the opportunity to take the lecture and the exam for as many students as possible.

4- Use the iPhone OS (ios) to apply the proposed system.

References

References

[1] S. R. Jan, F. Ullah, H. Ali and F. Khan, ***"Enhanced and Effective Learning through Mobile Learning an Insight into Students Perception of Mobile Learning at University Level"***, International Journal of Scientific Research in Science, Engineering and Technology (ijsrset.com), Vol. 2, pp. 674 - 681, 2016.

[2] S. K. Sharma, M. Sarrab and H. Al-Shihi, ***"Development and validation of Mobile Learning Acceptance Measure"***, Interactive Learning Environments, Vol. 25(7), pp. 847–858 ,2016.

[3] M. A. Riedesel and P. Charles, ***"Learning Any Time, Anywhere: Big Educational Data from Smart Devices",*** Frontiers of Cyber learning, Lecture Notes in Educational Technology, 2018.

[4] I. Han, W. S. Shin, "***The use of a mobile learning management system and academic achievement of online students",*** Computers & Education, United States of America, Vol. 102, pp. 79–89,2016.

[5] S.A. Shonola and M.S. Joy, ***"S ecurity of m-learning system: A collective responsibility",*** International Journal of Interactive Mobile Technologies (IJIM), Vol. 9, pp.64-70, 2015.

[6] S. A. Shonola, M. S. Joy, "***Security of m-learning System: A Collective Responsibility",*** International Conference on Interactive Mobile Communication Technologies and Learning (IMCL), IEEE, 2014

[7] S. A. Shonola and M. Joy, "***ENHANCING MOBILE LEARNING SECURITY",*** International Journal on Integrating Technology in Education (IJITE) Vol.5, pp.1-15, September 2016.

[8] P. Pocatil, C. Cirurea, and M. Doinea, "***Security Evaluation in Collaborative M-Learning Systems***", Journal of Applied Quantitative Methods (JAQM), VOL. 5, NO. 4, December 2010.

[9] F. D. S. Bahrya, N. Anwara, N. Amrana and R. P. M. Riasb, "***Conceptualizing security measures on mobile learning for Malaysian higher education institutions",*** Procedia - Social and Behavioral Sciences, Vol. 176, pp. 1083 – 1088, 2015.

[10] S. S. Oyelere, D. I. Sajoh, Y. M. Malgwi, L. S. Oyelere, ***"Cybersecurity issues on web-based systems in Nigeria: M-learning case study",*** International Conference on Cyberspace (CYBER-Abuja), pp. 259 – 264, IEEE 2015.

[11] Y. Li, B. Zhang and Y. Ji, "***Privacy Preserving Distance Learning with Smart Phones",*** 12th International Conference on Mobile Ad-Hoc and Sensor Networks, pp.370-373, IEEE 2016.

[12] K. Qian, D. Lo, H. Shahriar, L. Li, F. Wu, P. Bhattacharya, ***"Learning database security with hands-on mobile labs",*** IEEE Frontiers in Education Conference (FIE), IEEE, 2017.

[13] G. Kalpana, P. V. Kumar, S. Aljawarneh, and R. V. Krishnaiah, ***"Shifted Adaption Homomorphism Encryption for Mobile and Cloud Learning",*** Computers & Electrical Engineering, Vol. 65, pp.178–195 ,2018.

[14] Y. Cai, H. Jiang, D. Chen and Ming-Chun Huang, "***Online Learning Classifier based Behavioral Biometric Authentication",*** 15th International Conference on Wearable and Implantable Body Sensor Networks (BSN), pp.62-65, Las Vegas, Nevada, USA ,2018 IEEE.

[15] O.W. Adejo, I. Ewuzie, A. Usoro and T. Connolly, "***E-Learning to m-Learning: Framework for Data Protection and Security in Cloud***

Infrastructure", I.J. Information Technology and Computer Science, Vol.4, pp.1-9, MECS 2018.

[16] B.A. Kumar, P.Mohite, ***"Usability of mobile learning applications: a systematic literature review",*** Journal of Computers in Education, Vol. 5(1), pp.1-17, 2017.

[17] E. Baran, ***"Professional Development for Online and Mobile Learning: Promoting Teachers' Pedagogical Inquiry",*** Springer International Handbooks of Education, pp.1-16, 2018.

[18] J.Nagata, F. M. Abad, J.G.Giner and F. J. Grrcia- Penalvo, ***"Augmented reality and pedestrian navigation through its implementation in m-learning and e-learning :Evaluation of an educational program in Chile,"*** Computer and Education, pp: 1-17, 2017.

[19] Y. Mehdipour and H. Zerehkafi, ***"Mobile Learning for Education: Benefits and Challenges",*** International Journal of Computational Engineering Research, Vol. 03, pp.93-101, 2013.

[20] W. Kennedy, A. Olmsted, ***"Three Factor Authentication",*** The 12th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 212-213, IEEE 2017.

[21] Q. Jiang, F. Wei, S. Fu, J. Ma, G. Li and A. Alelaiwi, ***"Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy",*** Nonlinear Dynamics, Vol. 83(4), pp. 2085–2101, 2015.

[22] J. P. Joy, T. S. Jyothis, ***"Secure Authentication",*** International Conference on Green Engineering and Technologies (IC-GET), IEEE,2016.

[23] S.I. Yusuf, M.M. Boukar, A. Mukhtar, and A.D. Yusuf, ***"User Define Time Based Change Pattern Dynamic Password Authentication Scheme",*** 14th International Conference on Electronics Computer and Computation (ICECCO), 2018.

[24] D. Zhaoa and W. Luoa, ***"One-time password authentication scheme based on the negative database",*** Engineering Applications of Artificial Intelligence, pp. 1-9, 2016.

[25] K. K. Chauhan and S. Tapaswi, ***"A secure key management system in group structured mobile ad hoc networks",*** International Conference on Wireless Communications, Networking and Information Security, IEEE 2010.

[26] M. B. Krishna and M. N. Doja ***"Symmetric key management and distribution techniques in wireless ad hoc networks",*** International Conference on Computational Intelligence and Communication Networks, IEEE,2011.

[27] N. Singh, S. Singh, N. Kumar and R. Kumar, ***"Key Management Techniques for Securing MANET,"*** ACM, 2016.

[28] m. y. Rhee, ***"wireless mobile intent security"***, second Edition book of Wiley , ISBN 978-1-118-49653-4, 2013.

[29] N. Liu, J. Cai, X. Zeng, G. Lin and J. Chen ***"Cryptographic Performance for Rijndael and RC6 Block Ciphers",*** IEEE, PP. 36-39, 2017.

[30] A. I. Sallam, O. S. Faragallah and E. M. EL-Rabaie , ***"HEVC Selective Encryption Using RC6 Block Cipher Technique",*** IEEE Transactions on Multimedia, Vol. 20(7), pp. 1636–1644, 2018.

[31] K. Aggarwal, ***"Comparison of RC6, Modified RC6 & Enhancement of RC6",*** International Conference on Advances in Computer Engineering and Applications (ICACEA), pp. 444 – 449, IEEE,2015.

[32] A.S.Ibrahim and R.S.Hammed , "***Halftone visual cryptography scheme for color imag using dynamic codebook and chaotic maps "***, Journal of engineering and applied sciences ,pp.8600-8608, 2019.

[33] Ch. Quan, J. Jung, H. Lee, D. Kang and D. Won, ***"Cryptanalysis of a chaotic chebyshev polynomials based remote user authentication scheme",***

International Conference on Information Networking (ICOIN), pp. 438 – 441, IEEE,2018.

[34] R. M. Saffari and S. Mirzakuchaki, ***"A Novel Image Encryption Algorithm Based on Discrete Wavelet Transform Using Two Dimensional Logistic Map",*** 24th Iranian Conference on Electrical Engineering (ICEE), pp. 1785 – 1790, IEEE, 2016.

[35] H. Kreger, "***Web Services Conceptual Architecture***", International Business Machines Corporation (IBM), May 2001.

[36] D. Chappell and T.Jewell, "***Java Web Services***", First Edition book of O'Reilly, ISBN: 0-596-00269-6, March, 2002.

[37] H. Paik, A. L. Lemos, M. C. Barukh, B. Benatallah ,A. Natarajan, ***"Web Service Implementation and Composition Techniques",*** Springer International Publishing, 2017.

[38] A. W.Mohamed and A. M. Zeki, ***"Web services SOAP optimization techniques",*** 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), IEEE, 2017.

[39] A. W. Mohamed and A.M. Zeki, ***"Low-cost designs of rectangular to polar coordinate converters for digital communication",*** IEEE Asia Pacific Conference on Circuits and Systems, IEEE, 2012.

[40] L. Baiping and L. Dan ***"Research and Realization of Coordinate Conversion in Radar Video Display",*** Ninth International Conference on Computational Intelligence and Security, 2013.

[41] D. Varberg, E. Purcell and S. Rigdon, ***"calculus",*** ninth edition**,** Prentice-Hall, 2007.

[42] J. J. Sudano**,** ***"An exact conversion from an Earth-centered coordinate system to latitude, longitude and altitude",*** Proceedings of the IEEE 1997 National Aerospace and Electronics Conference, NAECON 1997.

[43] A. D. Hartanto, M. R. Susanto, Ilham, H. Dardjito , R. Retnaningsih and H. Nurdiyanto, *" **Mobile Technologies of Formulation Haversine Application and Location Based Service"*** ICASI, pp: 91-100, 2018.

[44] C. N. Alam, K. Manaf, A. R. Atmadja, D. K. Aurum, ***"Implementation of haversine formula for counting event visitor in the radius based on Android application",*** 4th International Conference on Cyber and IT Service Management ,2016.

[45] B.C.M. (Bas) Visser, ***"Additional Source of Entropy as a Service in the Android User-Space"***, Master Thesis, Nijmegen, July 2015.

[46] Naji M. Sahib, Ali H. Fadel and Noora S. Ahmed ***"Improved Rivest Cipher 4 (RC4)Algorithm Based on Multi-Chaotic Maps",*** Research Journal of Applied Sciences, Engineering and Technology, Vol.15(1), pp. 1-6, Maxwell Scientific Publication Corp,2018.

الخلاصة

ظهر في السنوات الاخيرة مفهوم smart classroom في النظم التعليمية ويركز هذا المفهوم على بيئة التعلم المتنقلة من اجل زيادة مرونة التعلم عن بُعد وتوفير نوع جديد من الثقافة الرقمية, تركز هذه الثقافة على معالجة المعرفة وتساعد الطالب على أن يكون هو مركز عملية التعلم وليس المعلم. تركز هذه الأطروحة على تصميم وتنفيذ نظام تعليمي كامل للهواتف المحمولة للتفاعل اللاسلكي من خلال خادم يستخدم خدمات الويب لفصل دراسي. يمنح النموذج المقترح الخادم (Administrator) تفويضًا للسماح للهاتف المحمول للمستخدمين (student) بالوصول إلى النظام المقترح لأخذ محاضرة او أداء الامتحان بعد التحقق من موثوقية الطالب .تعد الموثوقية جزءًا مهمًا وأساسيًا من النظام المقترح اعتمادًا على موقع الهاتف المحمول للطالب إذا كان الطالب داخل حدود (smart classroom) فان الخادم (Administrator) سيولد مفتاح للطالب يتم تخصيص هذه المفاتيح للطلاب المخولين باستخدام key management system والذي يوفر مفتاح فريد ومختلف الطول لكل طالب مخول ,يستخدم هذا المفتاح لاحقًا في التشفير وفك التشفير باستخدام خوارزمية التشفير المحسنة (IRC6) .تم توليد مفتاح خوارزمية IRC6 استنادًا إلى نوعين من الخرائط الفوضوية (chebyshev, 2D logistic) من أجل إنشاء N من المفاتيح لN من المستخدمين. النتائج اظهرت نجاح النظام المقترح في تحديد موقع الطلاب داخل الفصل الدراسي الذكي باستخدام القيمة الأصغر لل Haversine formula ومقارنتها مع قيمة ال threshold وتثبت النتائج أن متوسط سرية Improved RC6 algorithm(IRC6)أفضل من Traditional RC6 algorithm(RC6) ، بالمقارنة مع الحالات المختلفة لطول المفتاح وحجم النص الواضح وظهرت اعلى قيمة لمقياس الأمنية المستخدم في طول مفتاح 16 بت، وحجم النص الواضح 128 بت حيث بلغ متوسط سرية IRC6 (1.413 - 0.390) في حين بقى متوسط السرية بقيمة ثابتة في RC6(0.244) .

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة ديالى

كلية العلوم

امنية المعلومات في نظام التعلم الجوال

رسالة

مقدمة الى قسم علوم الحاسوب /كلية العلوم /جامعة ديالى وهي جزء من متطلبات نيل درجة الماجستير في علوم الحاسوب

من قبل

ابتسام جمعة حاوي

بأشراف

الأستاذ الدكتور زياد طارق مصطفى

هجرية 1441 **ميلادية 2020**