





## Article

# Secure Data Exchange in M-Learning Platform using Adaptive Tunicate Slime-Mold-Based Hybrid Optimal Elliptic Curve Cryptography

Ghadah Aldabbagh <sup>1</sup>, Daniyal M. Alghazzawi <sup>1,\*</sup>, Syed Hamid Hasan <sup>1</sup>, Mohammed Alhaddad <sup>1</sup>, Areej Malibari <sup>1</sup> and Li Cheng <sup>2</sup>

<sup>1</sup> Faculty of Computing and Information Technology, King Abdulaziz University, P.O. Box. 80221, Jeddah 21589, Saudi Arabia; galdabbagh@kau.edu.sa (G.A.); shhasan@kau.edu.sa (S.H.H.); malhaddad@kau.edu.sa (M.A.); aamalibari1@kau.edu.sa (A.M.)

<sup>2</sup> Xinjiang Technical Institute of Physics & Chemistry Chinese Academy of Sciences, Urumqi 830000, China; chengli@ms.xjb.ac.cn

\* Correspondence: dghazzawi@jau.edu.sa

**Abstract:** The utilization of mobile learning continues to rise and has attracted many organizations, university environments and institutions of higher education all over the world. The cloud storage system consists of several defense issues since data security and privacy have become known as the foremost apprehension for the users. Uploading and storing specific data in the cloud is familiar and widespread, but securing the data is a complicated task. This paper proposes a cloud-based mobile learning system using a hybrid optimal elliptic curve cryptography (HOECC) algorithm comprising public and private keys for data encryption. The proposed approach utilizes an adaptive tunicate slime-mold (ATS) algorithm to generate optimal key value. Thus, the data uploaded in the cloud system are secured with high authentication, data integrity and confidentiality. The study investigation employed a survey consisting of 50 students and the questionnaire was sent to all fifty students. In addition to this, for obtaining secure data transmission in the cloud, various performance measures, namely the encryption time, decryption time and uploading/downloading time were evaluated. The results reveal that the time of both encryption and decryption is less in ATF approach when compared with other techniques.

**Keywords:** mobile learning; cloud storage; hybrid optical elliptic curve cryptography; adaptive tunicate slime mold; encryption; decryption; security



**Citation:** Aldabbagh, G.; Alghazzawi, D.M.; Hasan, S.H.; Alhaddad, M.; Malibari, A.; Cheng, L. Secure Data Exchange in M-Learning Platform using Adaptive Tunicate Slime-Mold-Based Hybrid Optimal Elliptic Curve Cryptography. *Appl. Sci.* **2021**, *11*, 5316. <https://doi.org/10.3390/app11125316>

Academic Editors:  
Luis Hernández-Callejo and  
Jifeng Liu

Received: 4 April 2021

Accepted: 1 June 2021

Published: 8 June 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

In the past few years, breakthrough technological innovation and progression have brought forth another new approach to learn in university surroundings, named mobile learning or m-learning [1]. Mobile learning is an emerging recent trend in which the user can access the study materials everywhere and, on any occasion, using mobile devices. In addition, by managing and providing the study materials and educational contents, mobile learning also provides sufficient visualization and adaptation on the small display of mobile phones. The modern characteristic traits in smart phones, namely the browsing feature, color display screen and video streaming, make mobile learning both practical and promising [2]. In addition to this, mobile learning possesses the following advantages: mobility, sharing of information, independent self-education and facilitating communication among the students and teachers. The utilization of mobile learning continues to rise and has attracted many organizations, university environments and institutions worldwide. In general, mobile learning includes learning with diverse mobile devices, namely web tablets, pocket PCs, cell phones, wireless cameras, palms and various other handheld devices [3].

Mobile learning has attracted the people of Asian, European countries and the United Nations. On the other hand, the integration of both e-learning and mobile computing is

referred to as mobile computing [4]. Recent mobile terminals consist of strong computational capability containing CPUs with high frequency. Mobile learning also implements suitable service applications based on multimedia, containing various modes of operation and friendly human interfaces. In addition, it also accesses numerous resource networks using diverse network connection approaches [5]. Currently, the computing network [6] plays a vital role due to its rapid development. Therefore, the proficient advancements of wireless sensor networks transformed pocket PC, iPods and mobile phones into various learning devices. Additionally, Wi-Fi and Bluetooth, the general packet radio services, are considered as the fundamental system in transferring the network data to each mobile terminal [6]. Users can gather the study materials and communicate with teachers or other professionals if the signal location through GPRS is available in the neighborhood [7].

Therefore, the GPRS system enables learners to access the Internet everywhere and on any occasion. Due to the rapid progression of mobile learning, distance education has turned to challenge both traditional classroom teaching and formal schoolings [8]. Even though distance education provides the bridge between experimental and formal learning, it is necessary to reconsider the physical classroom anatomy [9]. Thus, feature-based mobile learning is utilized in various educational activities and acts as a mediating tool to gather the educational materials and to learn the relevant topics using mobile devices via wireless technologies [10]. The cloud storage system consists of several defense issues since data security and privacy have become known as the foremost apprehension for the users [11].

This paper proposes a safe and protected cloud-based mobile learning system that comprises various security characteristics, namely privacy and confidentiality of information, intrusion detection, entity authentication, secure routing and data aggregation, key management and distribution, and data integrity. Here, the mobile learning system is influenced directly by progressive technological advancements and the issues based on security and privacy are entirely different from the e-learning system. This paper proposes a cloud-based mobile learning system using a hybrid optimal elliptic curve cryptography (HOECC) algorithm comprising public and private keys for data encryption. The proposed approach selects optimally the random value, and the adaptive tunicate slime-mold (ATS) algorithm is employed for generating the optimal key value. The major contribution of the paper can be summarized as follows:

- Proposing hybrid optimal elliptic curve cryptography for data encryption, thereby generating the public and private keys;
- Proposing an adaptive tunicate slime-mold algorithm to select optimally the random value and to generate optimal keys;
- Comparing the proposed ATS approach with various other existing techniques to determine the system effectiveness.

The remainder of the paper is structured as follows: Section 2 reviews and provides a comparative analysis of existing literature on the mobile learning system. The problem definition and the motivation of the paper are discussed in Section 3. Section 4 provides the empirical design for the cloud-based secure mobile learning model. In Section 5, the performance evaluation and the comparative analysis are portrayed. Section 6 concludes the research paper.

## 2. Related Literature Review

Ennouamani et al. [12] proposed a context-aware mobile learning system adapting the learning content. A dynamic mobile adaptive learning content and format (D-MALCOF) was employed in appropriate learning for every student. Moreover, this approach was provided with encouraging feedbacks and positive perceptions. It becomes a necessary task to collect the feedback, but this approach failed in the feedback collection activity.

A context-aware mobile learning system (CAMLS) and usability assessment were proposed by Pensabe-Rodriguez et al. [13]. The usability assessment was evaluated and the experimental results revealed that the acceptance, applicability and satisfaction were enhanced while comparing with several other context-aware mobile learning schemes.

The augmented reality and collaborative works were poor, however, which are the two common disadvantages of this approach.

Romero et al. [14] demonstrated the structural equation design for good teaching practice based on mobile learning in higher education. The main intention of this approach employed was to investigate the factors that influence the progression of good teaching. The teaching activity and the interaction among the student and teacher association were very high. However, the sample size was limited, which further affects the effectiveness of the system.

An integrative evaluation of learning process, based on the effects of mobile learning for nursery students, was established by Li et al. [15]. The learning process was evaluated by employing the Framework for Rational Analysis of Mobile Education (FRAME) approach that investigates the relationship among diverse variables. This approach was provided with enhanced learning motivation but poor theoretical establishment.

Bi et al. [16] introduced pedagogical practices of mobile learning in K–12 and higher education settings. The most significant objective of this research was to provide theoretical foundations for mobile learning. The satisfaction level high was very high when comparing this approach with various other existing approaches. Low effectiveness and acceptance rate were the major drawbacks of this approach.

A conceptual model for examining the impact of knowledge management factors on mobile learning and acceptance was developed by Al-Emran et al. [17]. Here, the mobile learning acceptance was determined by using partial least squares–structural equation modeling (PLS–SEM) for developing a conceptual model. The education environment was good, but the acceptance rate and the rate of satisfaction were very poor.

Mutambara et al. [18] developed the determinants of mobile learning acceptance for STEM education in rural areas. The major objective of this approach was to examine the acceptance rate of high school learning, which includes high psychological readiness and skilled readiness. However, the motivation for learning was very low.

Advanced technology, i.e., mobile and wearable technology, in measuring and understanding the role of mobile technology in education was demonstrated by Bernacki et al. [19]. The major contribution of this approach was to provide a balanced consideration of learning for obtaining very high learning processes. However, this approach failed to collect the data accurately and was the disadvantage of this approach.

El-Sofany et al. [20] investigated the effectiveness of using mobile learning techniques to improve learning outcomes in higher education. This approach aimed at evaluating the student's perceptions and recognizing quality. The positive perception of the students, skill of every student and flexibility rate were very high. However, an unsatisfied education environment was the major drawback of this approach.

Mobile game-based learning in higher education using collaboration and a dynamic fuzzy-based model was proposed by Troussas et al. [21]. This approach analyzed the pedagogical affordance to provide high learning outcome rate, but failed to analyze and classify various sentiments.

Similarly, Korac et al. [22] implemented information security in mobile learning systems. The significant objective of this approach was to enhance the security awareness and behavior in the m-learning system. The personal information was highly secured by employing this approach, but the acceptance and satisfaction rate were poor.

Khairi et al. [23] presented a secure mobile learning system by employing voice authentication. This approach utilized a human-behavior-based particle swarm optimization algorithm to obtain a secure m-learning approach. The authentication performance of this approach was very high, but low efficiency was considered as its major drawback.

A secure mobile learning system based on a cloud system is presented by Al shehri et al. [24]. A secure mobile learning framework was developed to ensure mutual authentication and end-to-end security. The integrity and privacy of this approach was high, but implementation failed in the simulation environment.

The summary of prior work is tabulated in Table 1.

**Table 1.** Review and comparative analysis of existing literature for mobile learning systems.

Literature	Studies/Framework	Objective	Merits	Demerits
Ennouamani et al. [12]	Dynamic Mobile Adaptive Learning Content and Format (D-MALCOF)	Providing appropriate learning for every student	Positive, perception and encouraging feedback	Failed to collect the feedbacks
Pensabe et al. [13]	Context Aware Mobile Learning System (CAMLS)	Evaluating usability assessment	Enhanced acceptance, applicability and satisfaction	Poor augmented reality and collaborative works
Romero et al. [14]	Structural equation design for mobile learning	Investigating the factors that influencing the progression of good teaching	Enhanced teaching activity	Limited sample size
Li et al. [15]	Framework for Rational Analysis of Mobile Education (FRAME)	Studying the relationship among the variables	High learning motivation	Poor theoretical establishment
Bai et al. [16]	Mobile learning in higher education and K-12	Providing theoretical foundations to mobile learning	Highly satisfied	Low effectiveness
Al-Emran et al. [17]	Partial Least Squares–Structural Equation Modeling (PLS-SEM)	Developing a conceptual model	High education environments	Poor satisfaction and acceptance
Mutambara et al. [18]	STEM-based mobile learning	Examining the acceptance of high school learning	High psychological and skilled readiness	Low learning motivation
Bernacki et al. [19]	Mobile and wearable technology	Providing balanced consideration in learning	Enhanced learning processes	Failed in collecting the data accurately
El sofany et al. [20]	Web-based platform	Evaluating the students perceptions and recognizing the quality	Positive perception, enhanced students skill, high flexibility rate	Unsatisfied education environment
Troussas et al. [21]	Dynamic fuzzy logic approach	Analyzing pedagogical affordance	High learning outcome	Failed to analyze sentiments
Khairi et al. [22]	Human-behavior-based particle swarm optimization algorithm	Obtaining secure m-learning approach	Enhanced authentication performances	Low efficiency
Korać et al. [23]	Privacy and security technique	To improve security awareness and behavior in m-learning system	Highly secured personal information	Poor acceptance and satisfaction
Al Shehri et al. [24]	Secure mobile learning framework	Ensuring end-to-end security and mutual authentication	High privacy and integrity	Failed to implement in a simulation environment

### 3. Problem Identification and Motivation

Currently, diverse m-learning approaches have been concentrated on the progression of various courses. The mobile learning system is becoming more prevalent due to the presence of the Internet everywhere. Therefore, it is an excellent chance and large opportunity for various organizations, such as educational institutions, various universities and cloud service operators, to provide several assessment services and mobile learning. In various cases, the privacy and security during data sharing are considered as the most significant issue, and it needs to be solved. On the other hand, the mobile learning system

is influenced directly by progressive technological advancements and the issues based on security and privacy is entirely different from the e-learning system. Let us consider an illustration. While concentrating on privacy, the concerned parties have worries and doubts regarding the usage of personal sensitive information (mobile number, IP address, individual phone ID) that are gathered indirectly without the permission of the data owner. The cloud storage system consists of several defense issues since data security and privacy have become known as the foremost apprehension for the users. Uploading and storing specific data in the cloud is familiar and widespread, but securing the data is a complicated task. The following points provide few issues faced by the contributor.

- Under cloud computing ambiance, one relies on the cloud provider to store the data in the cloud from unknown locations. Thus, the provider defends the user data from diverse conditions.
- Protection of data derived to supply the counterfeit, and identifying the nonrepudiation of information or data.
- User's apprehension regarding the hacking threats, both internally and externally.

From these points, it is apparent that the requirement of preserving a privacy mechanism is more significant than safeguarding sensitive and personal data. Name, date of birth, email address, history, locations and biometric features of comprise the particular data. These drawbacks of the diverse existing work inspired us to work on securing the data in the cloud storage system [23]. The cloud storage system consists of several defense issues since data security and privacy have become known as the foremost apprehension for the users. Uploading and storing specific data in the cloud is familiar and widespread, but securing the data is a complicated task. Such shortcomings were overcome by our proposed mobile learning system.

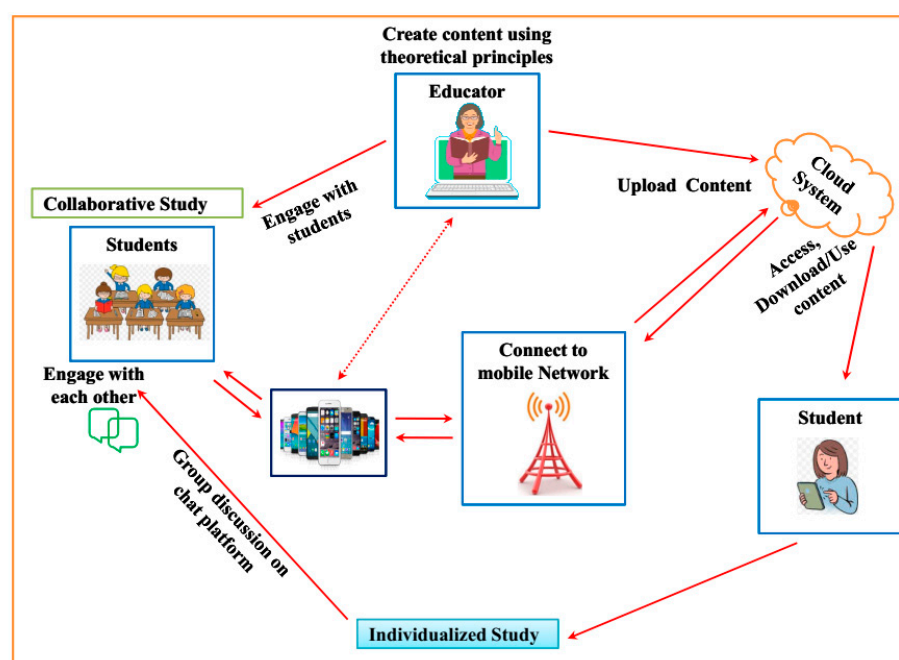
#### 4. Proposed Mobile Learning System

The architecture (Figure 1) provides an overview of the proposed empirical cloud-based mobile learning model. The structural design for the cloud-based mobile learning model comprises an educator who uploads the educational content data into the cloud system. The uploaded data are then downloaded by the students using mobile phones. Here, the teacher can engage with the students and the students can engage among themselves for collaborative study. The step-by-step procedure involved in the proposed methodology is discussed in the subsequent section.

##### 4.1. Data Collection

The data collection process includes collecting necessary domain knowledge about the m-learning approach from handbooks. Here, the survey was conducted among King Abdulaziz University (KAU) sophomore students from the Faculty of Computing and Information Technology (FCIT). The inputs were used for selecting programming language and other factors in developing the tool. The study investigation employed a survey comprising 50 students, and the questionnaire sent to all fifty students. In general, the initial phase involved the collection of indicators from the KA University for building the classification of platforms for selecting the technology and to determine the usability and effectiveness of the system. Here, both the pre-testing and the post-testing conducted were employed in testing the tool efficiency. The questionnaire was employed for data collection as there was no device to calculate good teaching practices in mobile learning. The scale generated referred to an analysis of mobile learning practice at King Abdulaziz University (KAU) by evaluating good teaching practice in mobile learning. The following section describes the questionnaire items:





**Figure 1.** Empirical architecture of the cloud-based mobile learning model.

1. Whether or not the students have mobile devices to learn.
2. Do the security and risk activities affect the teachers while utilizing mobile devices?
3. Is the mobile learning technology important for students?
4. Do the planned activities with the mobile devices permit the students to generate digital content?
5. Whether or not the activities executed by using mobile devices allow you to track the students learning process.
6. Whether or not the task or activities evolved using mobile device encourage the student to reflect on his/her own learning.
7. Do the activities developed encourage collaborative work?
8. Do the planned activities with mobile devices motivate communication among students?
9. Will the proposed activity allow for group discussion?
10. Whether or not the planned activities with mobile devices permit the students to share data?
11. Do security threats create dangerous impact affects from mobile learning?

The data for the study were collected from 50 students of FCIT at King Abdulaziz University. Several techniques were implemented to evaluate the stability and the efficiency, such as post-test, pre-test and usability features corresponding in a number of Saudi Arabia universities. The questionnaire was sent to 50 students; only 35 students responded. The data for this research were collected using the survey and from observational methods. The researcher intimately examined group chat activities in the face-to-face class sessions. Most of the questions used were based on the 5-point Likert scale, in which 1 represents strongly agree and 5 represents the strongly disagree. The first Likert scale consists of 15 questions regarding whether or not cloud computing has any consequences on infrastructure restrictions and the student's knowledge of m-learning. The second scale consists of 12 questions, which compare student attitude to m-learning before and after the trial.

#### 4.2. Secure M-Learning Design

The consequences based on the privacy problem in mobile learning systems are specifically emphasized since they are infused as a challenge of considerable significance. Privacy and security are considered as the two most subjective aspects that provide diverse

meanings to various users [25]. This implies that using similar mobile-based technological advancements provide diverse definitions to various scholars and undergraduates. Thus, the mobile technological advancements provide imprecise boundaries among infringing and protection of the privacy factors (i.e., tracking the movement of the students and monitoring the student's characteristic behavior). The constituent of privacy and security plays a significant role in various mobile learning-based applications. Here, the members of high organizations and various institutions are concerned regarding the security and the authentication of mobile learning.

A safe and protected mobile learning system comprises various security characteristics, namely privacy and confidentiality of information, intrusion detection, entity authentication, secure routing and data aggregation, key management and distribution, and data integrity. It is necessary to consider these characteristic features to obtain complete learning materials that are highly secure when using various mobile devices. In addition, data integrity and confidentiality are the two significant security conditions satisfied by executing a simple link-layer mechanism that utilizes authentication codes by encrypting the data packets. In addition, authentication is the most significant privacy asset for ensuring the receiver that an appropriate sender sends the message or not [24].

On the contrary, in terms of security, the attackers can hijack the sessions, also referred to as cookie spoofing. In the proposed system, the cloud data comprises information on the data owner, data user, negotiator inspector and cloud server. Here the teacher or educator signifies the data owner, and the students are represented as the user. Initially, the user commences a file for storing it in cloud service, examining the type of data file and cloud server accessibility. In addition, the user has the capability to decide if the input file is significant (critical and sensitive) or insignificant. If the data file is sensitive, then the files are split and accumulated in a diverse virtual machine. If it is an ordinary file, then the data file will be accumulated in single virtual machine. Meanwhile, if the data owner stores the file that is at risk, then it needs to be encrypted. At this point, the hybrid optimal elliptic curve cryptography (HOECC) algorithm is employed in data encryption [23].

#### 4.3. Setup Processes

During the processes of encryption, the system parameters are initialized by the data proprietor for generating both the public and the private keys. This paper proposes a cloud-based mobile learning system using a hybrid optimal elliptic curve cryptography (HOECC) algorithm comprising public and private keys for data encryption. The proposed approach utilizes an adaptive tunicate slime-mold (ATS) algorithm to generate optimal key value. The steps involved in set up process and their respective mathematical expressions are discussed in the next section.

##### 4.3.1. HOECC Algorithm

The general form of the elliptic curve is expressed in Equation (1):

$$E^2 = F^3 + jX + k \quad (1)$$

From the Equation (1), E and F signify the standard variables, j and k denote the elliptical curves. It is well known that the elliptic curve is varied by varying j and k. In addition to this, the HOECC comprises two keys (i.e., private keys and public keys) for both encryption and decryption. The encryption processes employed in verifying the signature and the signals are generated using decryption processes [26].

##### 4.3.2. Key Generation Process

The optimal elliptical curve cryptography process is described for two pre-determined sectors. It is necessary to pick the field containing numerous points for various cryptographic-

based tasks. The prime sector chooses the prime number and the finite number generated on the elliptical curve. Therefore, the public key is generated by

$$P_K = r * P_C \quad (2)$$

From Equation (2), the public key and the point of curve are represented by  $P_K$  and  $P_C$ , respectively;  $r$  denotes the random number that ranges from  $r \rightarrow [1 \text{ to } n]$ . The proposed approach optimally selects the random value and the (ATS) algorithm is employed for generating the optimal key value [27].

### Tunicate Swarm Algorithm

Tunicates are an invertebrate marine animal that generate light of a pale bluish-green color that belongs to the subphylum Tunicate. Tunicates are radiant, cylindrical-shaped and glow in the dark place. The tunicates are small and contain a gelatinous tunic that assists in fusing all individuals. The tunicates are the only marine animal that generates jet-like propulsion from its atrial siphon [28]. Jet propulsion is more effective, and it has the capability to move around the tunicates perpendicularly deep in the sea. The size of tunicates may vary from few centimeters to 4m, and each tunicate differs from the other. Similarly, the tunicate swarm algorithm imitates the activities, manners and characteristic features of the tunicates. The tunicate algorithm, in other terms, is referred to as the swarm intelligence algorithm that solves diverse engineering-based problems. The following section provides the step-by-step process involved in the tunicate swarm algorithm.

*Step 1: Preventing disputes between various tunicates.*

The dispute among various tunicates (search agents) is avoided by employing a vector  $\vec{K}$ . Therefore, the position of new search agents is evaluated using Equation (3):

$$\vec{K} = \frac{\vec{\alpha}_F}{\vec{\beta}_F} \quad (3)$$

From this Equation,  $\vec{\alpha}_F$  and  $\vec{\beta}_F$  signify different forces, namely the gravity force and the social force among the tunicates.

From Equation (3),

$$\vec{\alpha}_F = \Re_3 + \Re_2 - \gamma; \text{ where } \gamma = 2\Re_1 \quad (4)$$

$$\vec{\beta}_F = [\lambda_{MIN} + \Re_1 \cdot \lambda_{MAX} - \lambda_{MIN}] \quad (5)$$

From Equations (4) and (5), the random value ranges from 0 to 1 and are represented as  $\Re_1$ ,  $\Re_2$ ,  $\Re_3$ , respectively. The flow of water in the deepsea is denoted by  $\gamma$ . The first and final subordinate speeds are represented as  $\lambda_{max}$  and  $\lambda_{min}$ .

*Step 2: Gesticulation towards the most excellent neighbor.*

This process describes the movement of tunicates to the best neighbor following conflict among the neighboring tunicates [29]. Hence,

$$\vec{\delta}_{FS} = \left| \vec{F}_P - \Re \cdot \vec{T}_P(z) \right| \quad (6)$$

From Equation (6), the distance among the food source and the tunicates is represented as  $\vec{\delta}_{FS}$ .  $\vec{F}_P$ ,  $\vec{T}_P$ , and  $\Re$  signifies the food position, tunicate position and random value that ranges from 0 to 1.

*Step 3: Converging towards the best search agents.*



Here, the tunicates uphold their position towards the food source. Thus, the mathematical expression in converging the tunicate towards the food source is represented in Equation (7):

$$\vec{T}_U(z) = \begin{cases} \vec{F}_P + \vec{K} * \vec{\delta}_{FS}; \text{if } \Re \geq \frac{1}{2} \\ \vec{F}_P - \vec{K} * \vec{\delta}_{FS}; \text{if } \Re < \frac{1}{2} \end{cases} \quad (7)$$

From this equation, the updated position of the tunicate with respect to the food position is denoted by  $\vec{T}_U(z)$ .

*Step 4: Updating processes.*

The positions of various search agents are updated in accordance with the best search agents' position. Therefore, the updated equation is

$$\vec{T}_P(z+1) = \frac{\vec{T}_P(z) + \vec{T}_P(z+1)}{2 + \Re_1} \quad (8)$$

From Equation (8), the updated tunicate's position is represented by  $\vec{T}_P(z+1)$ .

#### Slime-Mold Algorithm

At an initial stage, the slime-mold algorithm was categorized under the fungus family and it was said to be known as slime mold. In general, the slime molds are eukaryotic, surviving in both hot and cold localities. There are three significant phases in slime mold: plasmodium stage, dynamic and active stage, and research stage. In addition, the slime mold can adjust the search patterns based on the amount of available food. The slime mold employs a region-limited search approach when the food source quality is large. If the quality of the food is low, then the slime mold leaves and searches for other quality food sources. The slime-mold algorithm imitates the characteristic behavior and performances of the slime mold; the mechanisms involved [30] are discussed in the subsequent section.

*Step 1: Proceed towards food.*

The slime mold identifies as the food source by aroma floating in the air. The mathematical expression in searching for the food source is given in Equation (9):

$$\vec{\psi}(t+1) = \begin{cases} \vec{\psi}_y(t) + \vec{\vartheta}y \cdot \left( \vec{w} \cdot \vec{\psi}_X(t) - \vec{\psi}_Y(t) \right), a < x \\ \vec{\vartheta}z \cdot \vec{\psi}(t), a \geq x \end{cases} \quad (9)$$

From Equation (9),  $\psi$ ,  $\psi_X$  and  $\psi_Y$  signifies the location and randomly selected individuals of the slime mold. The weight of the slime mold in vector form is denoted as  $\vec{w}$ . The parameter  $\vec{\vartheta}y$  increases from  $[-k$  to  $k]$  and the parameter  $\vec{\vartheta}z$  linearly decreases from 1 to 0;  $\psi_Y$  signifies the high aroma location. The total number of current iterations is represented by  $t$ . Then, the  $x$  value is expressed as

$$x = \text{TanH} \left| f(j) - b_f \right| \quad (10)$$

From Equation (10), the fitness and the best fitness values are represented by  $f(j)$  and  $b_f$ , respectively. It is known that

$$\vec{\vartheta}y = [-k, k] \quad (11)$$

From Equation (11),

$$k = \text{arcTanH} \left( - \left( \frac{t}{t_{\max}} \right) + 1 \right) \quad (12)$$

The expression based on the weight of the slime mold in vector form is given by Equation (13). Therefore,

$$w(\vec{S}_I(j)) = \begin{cases} 1 + a \cdot \log\left(\frac{\text{Optimal fitness} - \text{best fitness}}{\text{Optimal fitness} - \text{worst fitness}} + 1\right), & \text{condition} \\ 1 - a \cdot \log\left(\frac{\text{Optimal fitness} - \text{best fitness}}{\text{Optimal fitness} - \text{worst fitness}} + 1\right), & \text{others} \end{cases}; \text{where } S_I = \text{sort}(S) \quad (13)$$

From Equation (13), the random value is represented by  $a$  which ranges from  $[0, 1]$ . The smell index is denoted by  $S_I$ .

*Step 2: Food wrapping process.*

This process imitates the food searching behavior of the slime mold. If the food quality is high, then the waves produced by the bio-oscillator are very strong, which further causes the cytoplasm to flow fast within a thick vein. The numerical expression in determining the food wrapping processes with reference to the location updating is obtained in Equation (14):

$$\vec{\Psi}^* = \begin{cases} \Re \cdot (U_L - L_L) + L_L, & \Re < b \\ \vec{\Psi}_y(t) + \vec{\vartheta}y \cdot \left( w \cdot \vec{\Psi}_X(t) - \vec{\Psi}_Y(t) \right), & a < x \\ \vec{\vartheta}z \cdot \vec{\Psi}(t), & a \geq x \end{cases} \quad (14)$$

From Equation (14), the upper and lower limits are represented as  $U_L$  and  $L_L$ , respectively. The terms  $\Re$  and  $a$  signify random values that have the range  $[0, 1]$ . The  $b$  value signifies the parameter setting experiments.

*Step 3: Oscillatory process.*

The slime mold relies significantly on waves of propagation generated by the biological oscillator for changing the flow of cytoplasm in the vein. Here we utilized  $w$ ,  $\vec{\vartheta}y$  and  $\vec{\vartheta}z$  to simulate the variations in the width of the slime mold.

- $w$ : The value  $w$  employs in simulating the frequency of oscillation at diverse food concentration for the quick approach of food when the food is obtained at high quality. Similarly, the approach of food is very low when the food quality is small.
- $\vec{\vartheta}y$ : The value  $\vec{\vartheta}y$  gradually reaches to zero and randomly oscillates among  $[-k$  to  $k]$  with respect to increase in iterations.
- $\vec{\vartheta}z$ : The value  $\vec{\vartheta}z$  eventually reaches to zero and randomly oscillates between  $[-1, 1]$  with respect to an increase in iterations.

#### Adaptive Tunicate Slime-Mold (ATS) Approach-Based Optimal Key Generation

Figure 2 provides the schematic flow diagram for the proposed adaptive tunicate slime-mold (ATS) approach based on optimal key generation. The proposed ATS approach is selected in such a way that performances in terms of encryption time, decryption time, computation time, success rate and convergence rate are better when compared with various other optimization algorithms. In addition, the step-by-step process for the proposed ATS approach is discussed in the following section.

The initial process involves generating the initial population of the tunicates followed by selecting the initial parameters. The condition is checked and if the criteria are satisfied, then the fitness values are evaluated for all respective tunicates. Then, the swarm behavior of the tunicates and the jet-like propulsions are determined using Equation (8). Finally, the position of every search agent (food source) is updated. Here, the conditions for the tunicate containing at least one neighboring tunicate are checked and the position of various search agents evaluated using Equation (14). The processes are iteratively repeated until the last iteration is used to find the optimal keys.

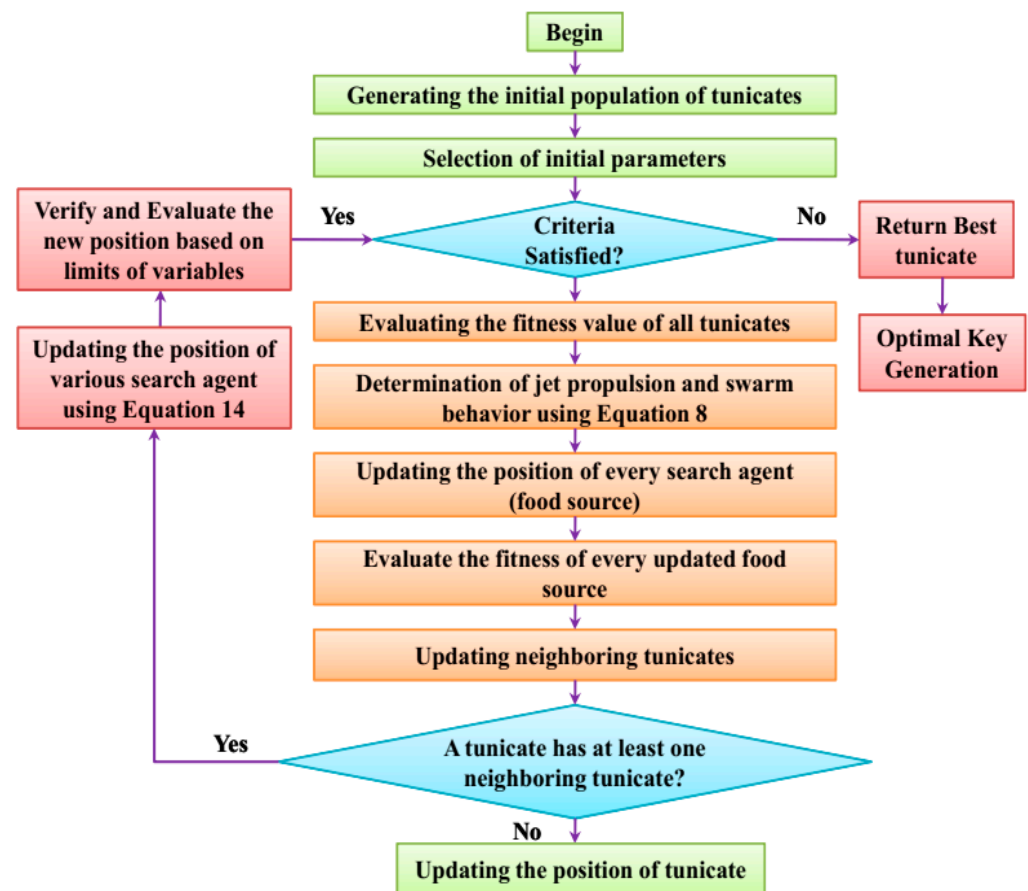


Figure 2. Flow diagram of the proposed ATS approach.

#### Computational Complexity

The computational complexity of the proposed ATS algorithm is expressed in Equation (15):

$$\text{Computation Complexity} = O(D * n_{pop} + obj * n_{pop}) \quad (15)$$

In this equation, the size of the population or the total number of search agents is represented as  $n_{pop}$ ,  $obj$  and  $D$  are the objective function and dimensions, respectively

#### 4.3.3. Encryption and Decryption Process

During the optimal generation of elliptical curve cryptography, the input data are encrypted and the output data are split into two various cipher texts, namely  $C_T^1$  and  $C_T^2$ . The multiplication and addition operation involved is determined in Equations (16) and (17):

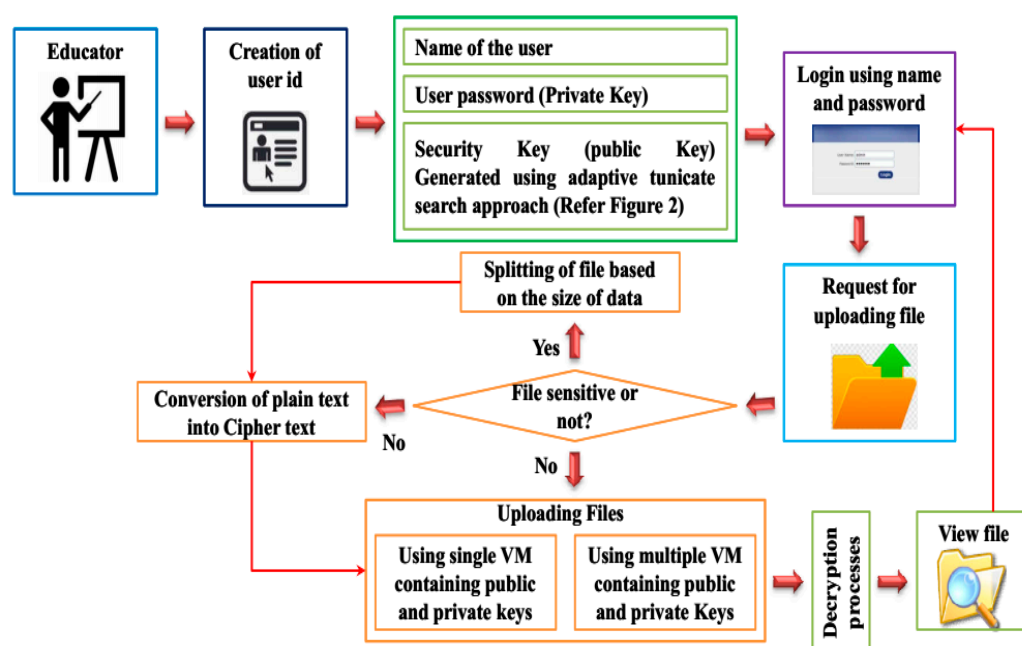
$$C_T^1 = \mathfrak{R} * P_C \quad (16)$$

$$C_T^2 = \text{Data} + \mathfrak{R} * P_C \quad (17)$$

From Equations (15) and (16),  $\mathfrak{R}$  signifies the random value that ranges from 1 to  $-(n-1)$ . The encrypted message  $C_T^1$  and  $C_T^2$  is transmitted to the receiver. Then, the data are decrypted by the receiver, followed by the transmission of cipher text. Thus,

$$\text{Data} = C_T^2 - \mathfrak{R} * P_C \quad (18)$$

In accordance with Equation (18), the input data are encrypted on the data proprietor side. Figure 3 provides a detailed understanding regarding the process of encryption and decryption, and how the data are secured with high authentication, data integrity and confidentiality.



**Figure 3.** Workflow based on the encryption and decryption process.

The advantages of the proposed HOECC-based mobile learning system are discussed as follows:

- Low power consumption;
- Low CPU utilization;
- Low memory usage;
- Fast encryption and decryption process.

## 5. Results and Discussions

When it comes to mobile application programming, this paper utilized a popular programming language named Java. The application is built by the J2ME Java family; it provides networking support and has API JSRO82 for Bluetooth technology.

### 5.1. Performance Measures

The performance measures, such as encryption time, decryption time, downloading time, uploading time and reputation, are discussed in the following section.

- Encryption time is the time taken for the encryption algorithm to create the cipher text from the plain text. It is employed to compute the throughput of an encryption method. It represents the speed of the encryption.
- Decryption time is the time taken to convert the encrypted data into the original data is called decryption time. It is the reverse scheme for the encryption. Decryption decodes the encrypted data so that the authorized user can only decrypt the data using a secret key or password.
- Uploading time is time taken to transmit the data from one computer system to another system through the network.
- Downloading time is the time taken to download any page linked with the services, including the entire content contained in the page.

### 5.2. Performance Evaluation

The degree to which the cloud-based m-learning assisted in controlling the infrastructural and technological challenges is computed by using the student's capability to admit the data uploaded into the cloud. Figure 4 depicts that 90% that the data increased entry to the content and more than 60% of the students decided data access is easy. Students

who identified the complexities in accessing the content recognized that these were due to poor network connection and the cost of the data for downloading and watching video. Students, who cannot be able to download the educator's data on their own, received the files from the classmates through Xender or Bluetooth. Whereas this describes the time for accessing the data, which took a long time for few students, the solution is to assure that all the participants accepted the data prior to class.

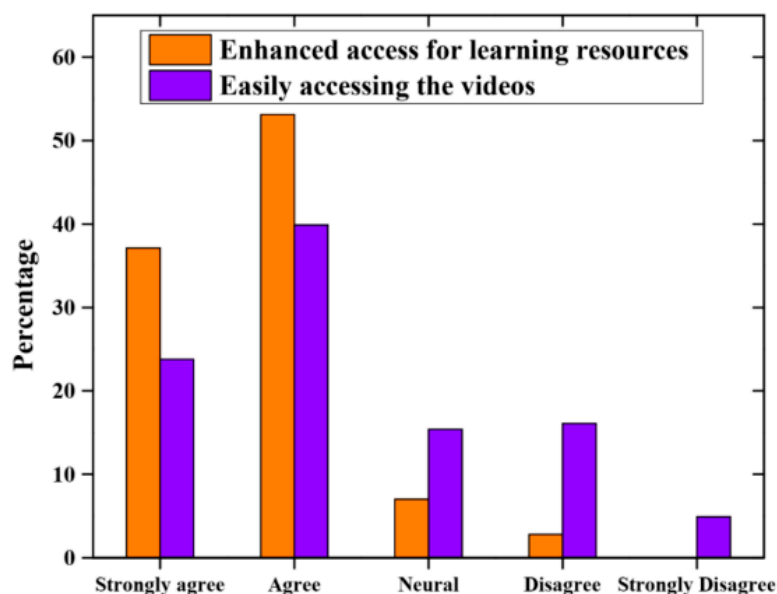


Figure 4. Consequences of cloud computing on m-learning.

The consequences of cloud computing-based m-learning on students learning experience are established by the two variables. The first variable is that asking students to compare the learning experiences before and after their commitment to m-learning. The second variable is with the help of comparing student attitudes to m-learning before and after the trial. Figure 5 depicts that about 90% of the students stated that m-learning prepared them faster and easier, whereas 73% of the students established it as useful.

Figure 6 depicts the damaging effects of m-learning security threats to students. The most frequent consequences are confidential ratio loss, psychological damage, loss of study hours, performance loss and no effects. Of the students, 85.71% indicated the confidential ratio loss, 47.62% indicated psychological damage, 71.93% perceived loss of performance, and 3.53% perceived no effects.

Figure 7 describes the security issues encountered when using mobile devices for m-learning. Most of the students agreed that theft is the concern when mobile devices are utilized for learning purposes, 67.18% of the students perceived theft of mobile device, 72.85% of the students responded that the malware attack is a major concern, 77.44% of the students indicated that their friends utilized their mobile device without their authorization, 35.24% of the students indicated the denial of service, and 3.82% indicated there were no security attacks.

The encryption time and decryption time for the various file sizes in KB for the proposed method is tabulated in Table 2. From the evaluation results, the proposed encryption and decryption scheme obtains lesser time when compared with other encryption schemes. The table describes the time required for the encryption and decryption time for the ATS scheme.



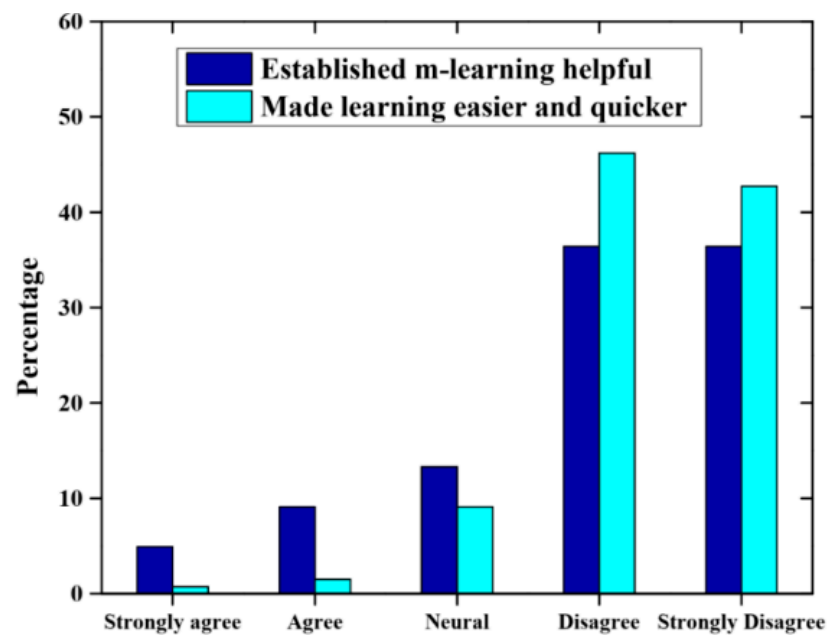


Figure 5. M-learning experience of the students.

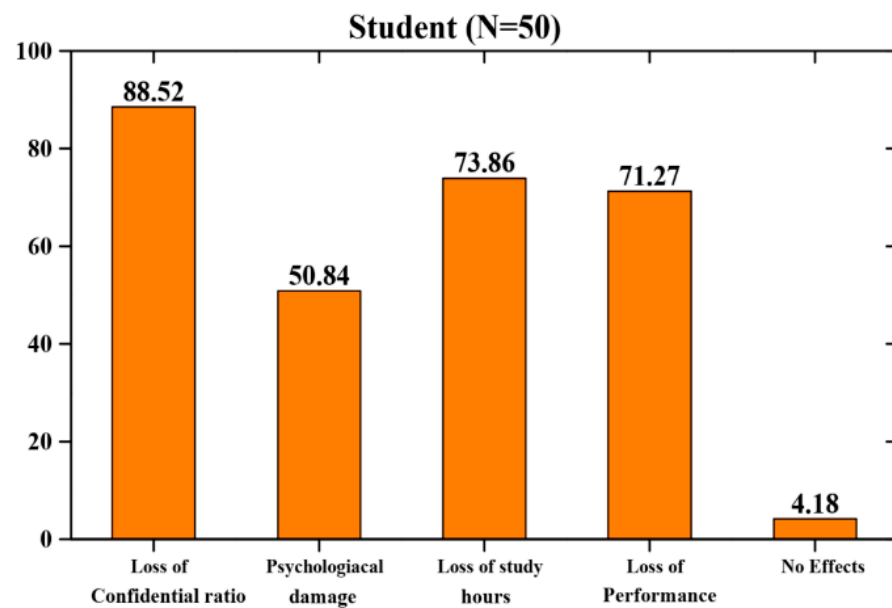
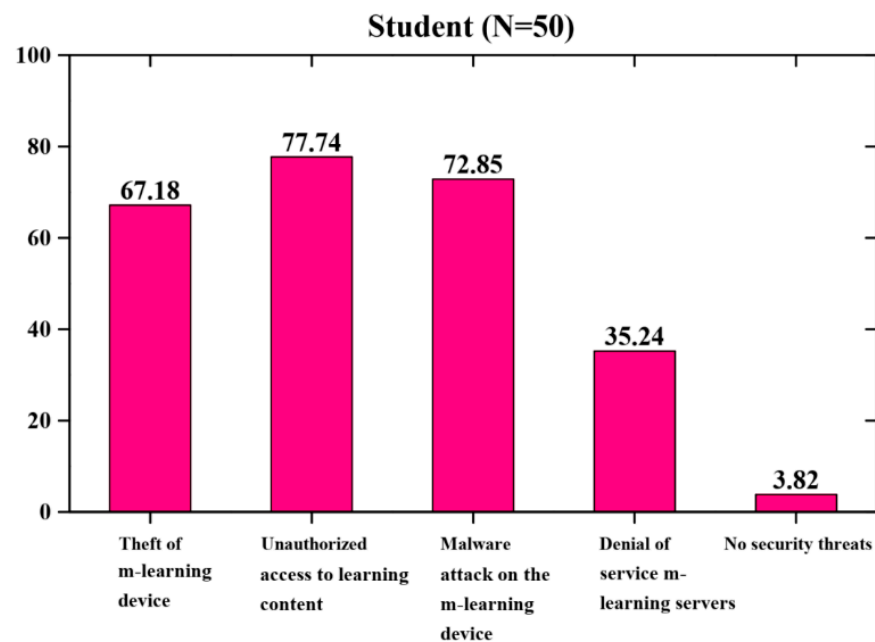


Figure 6. Damaging effects of m-learning security threats to students.

The time obtained for downloading and uploading is minimized, and it has low memory consumption. The time changed by altering the system configuration; thus, the average of the entire earlier work time was obtained as a reference. Table 3 demonstrates the downloading and uploading time for various file sizes.



**Figure 7.** Security issues encountered in m-learning.

**Table 2.** Encryption and decryption time from the proposed approach.

Size of the File (KB)	Encryption Time (ms)	Decryption Time (ms)
10	453	326
20	684	412
30	812	598
40	1120	782
50	1358	897

**Table 3.** Uploading and downloading time for the proposed approach.

Size of the File (KB)	Uploading Time (ms)	Downloading Time (ms)
10	1995	1266
20	3156	1988
30	4018	2146
40	5095	3084
50	5894	3982

Concerning the period for communication with the students in the lecture, students demand requesting questions that are listed on educator's screen; however, these questions are reacted due to the accessibility of time when the flow of the topic is completed. In the question time, students are provided access to allocate the data, text or file by the teacher. It is exposed to launch attacks by distributing malicious data from trustless students. Figure 8 describes the interaction of the average student's time per hour. The results describe that if 10 questions are asked, then the interaction of the student per hour is 13%, 20%, 26% and 32% for the average question number reacted as 2, 3, 4 and 5 questions in the existing method. In the proposed scheme, however, the interaction of the student's time per hour is 15%, 20%, 25% and 30%. If the interaction time is less, then the reputation and the trust are less than others, minimizing the attack chances by predictably malicious students.

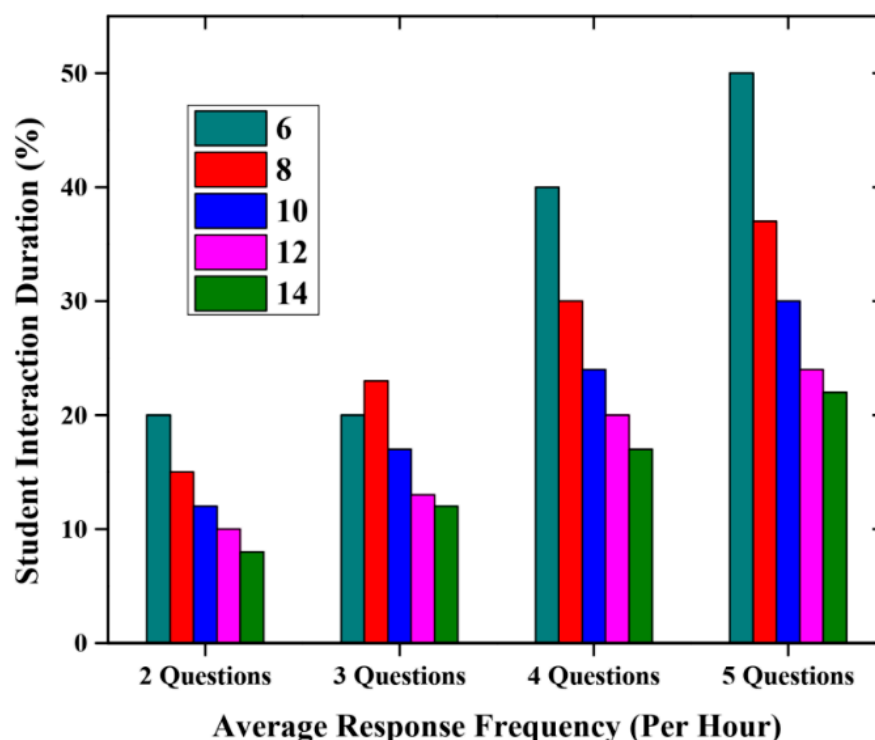


Figure 8. Duration of the student interaction and the responses.

The reputation and trust level score are sustained for the students once the action such as a lecture, quiz, examination and tests are over. The students who have a typical and disciplined nature allocate positive points, and the students who have a disobedient and dishonest affinity provide negative points, which remains the expectation. Figure 9 represents the reputation and the trust level of the students with respect to the academic actions. The results reveal that student in the beginning actions, believed to be involved in the deceptive and malicious actions, on the later stage such as students S2 and S7 for the proposed ATS scheme. In contrast, students like S3 and S8 for the proposed ATS scheme revived their reputation and trust level following primary objections and negative points.

### 5.3. Comparative Analysis

The comparative analysis of the proposed ATS with ECC encryption algorithm is compared with various algorithms such as the modified grasshopper optimization algorithm (MGOA) [26], cuckoo search (CS) [27] and ant-bee colony (ABC) [31]. The proposed algorithm is compared with the other algorithms for the measures such as uploading time, downloading time, encryption time and decryption time. Figure 10 describes the comparative analysis of the encryption time for the proposed method with other methods such as MGOA, CS and ABC. The proposed method consumes only less encryption time when compared with other methods of secure m-learning.

Figure 11 describes the comparative analysis of the decryption time for the proposed method with other methods such as MGOA, CS and ABC. The proposed method consumes only less decryption time when compared with other methods of secure m-learning.

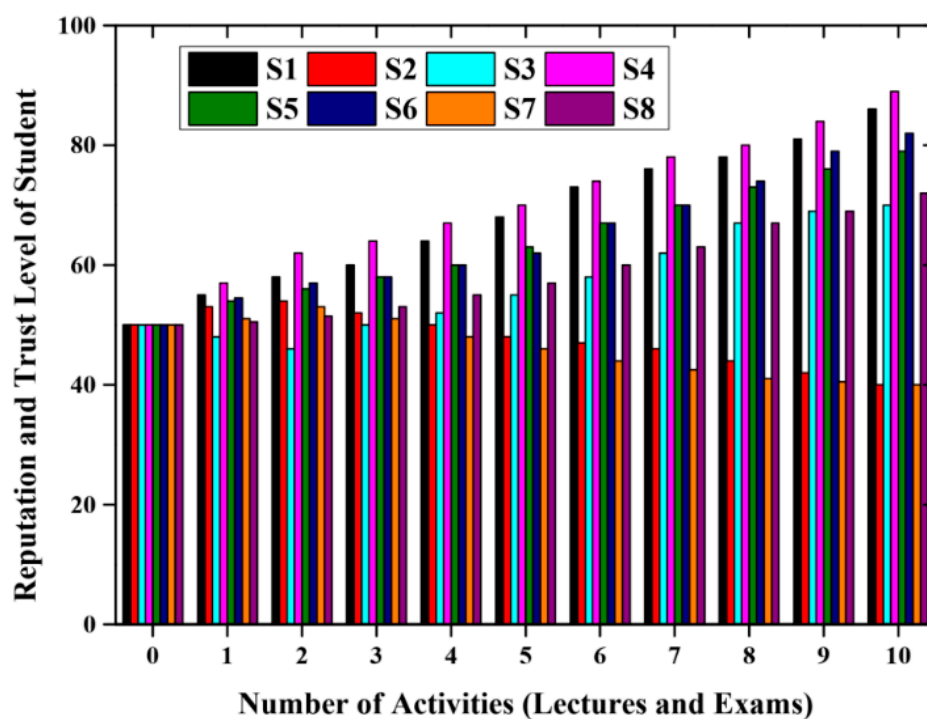


Figure 9. Reputation level and trust level of the students.

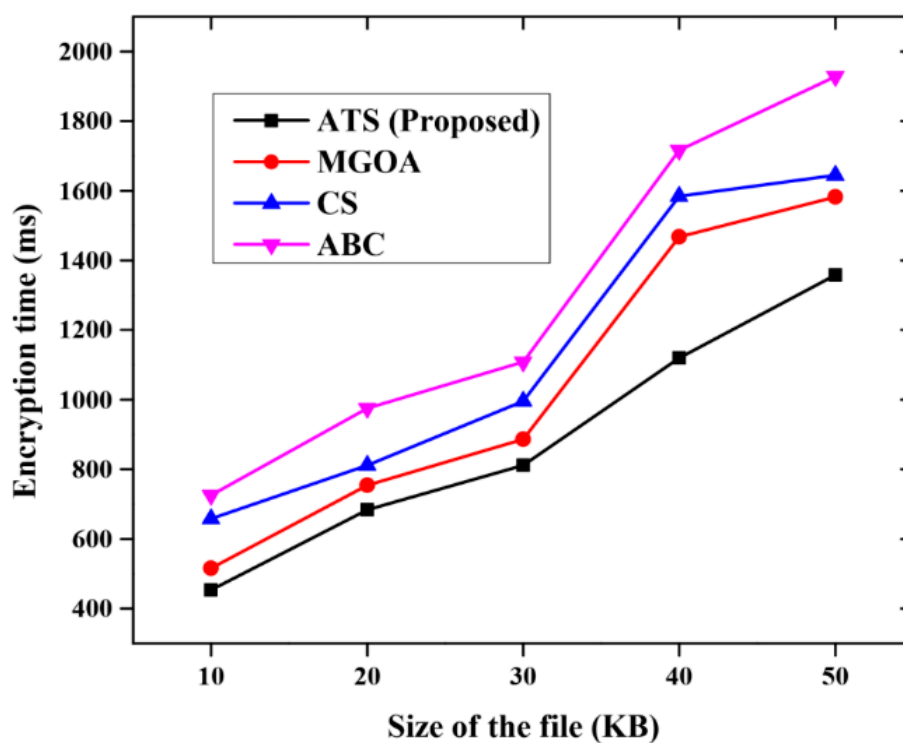


Figure 10. Comparative analysis for the encryption time.

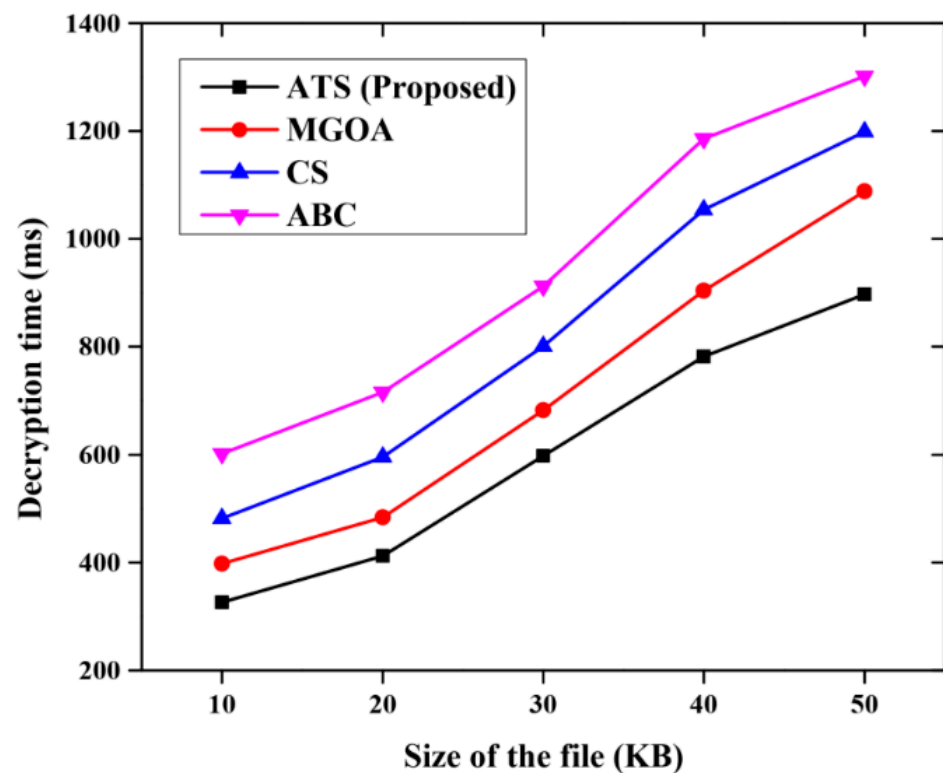


Figure 11. Comparative analysis for the decryption time.

Figure 12 describes the comparative analysis of the uploading time for the proposed method with other methods such as MGOA, CS and ABC. The proposed method outperforms other methods. The proposed method consumes only less uploading time when compared with other methods of secure m-learning.

Figure 13 describes the comparative analysis of the downloading time for the proposed method with other methods such as MGOA, CS and ABC. The proposed method outperforms other methods. The proposed method consumes only less downloading time when compared with other methods of secure m-learning.

Table 4 provides the comparative tabulation of the proposed ATS algorithm with various other optimization algorithms such as MGOA, CS and ABC. Various parameters like computation time, success rate and convergence rate are evaluated for various methods. From the tabulation, the results demonstrate that the proposed approach provides better performance when compared with other optimization algorithms.

Table 4. Comparative analysis for various parameters.

Approaches	Computation Time	Success Rate	Convergence Rate
ATS (Proposed)	0.35 s	96.7%	$5 \times 10^3$
MGOA	0.78 s	93%	$3.7 \times 10^3$
CS	1.2 s	87%	$2.8 \times 10^3$
ABC	1.18 s	85%	$2.6 \times 10^3$



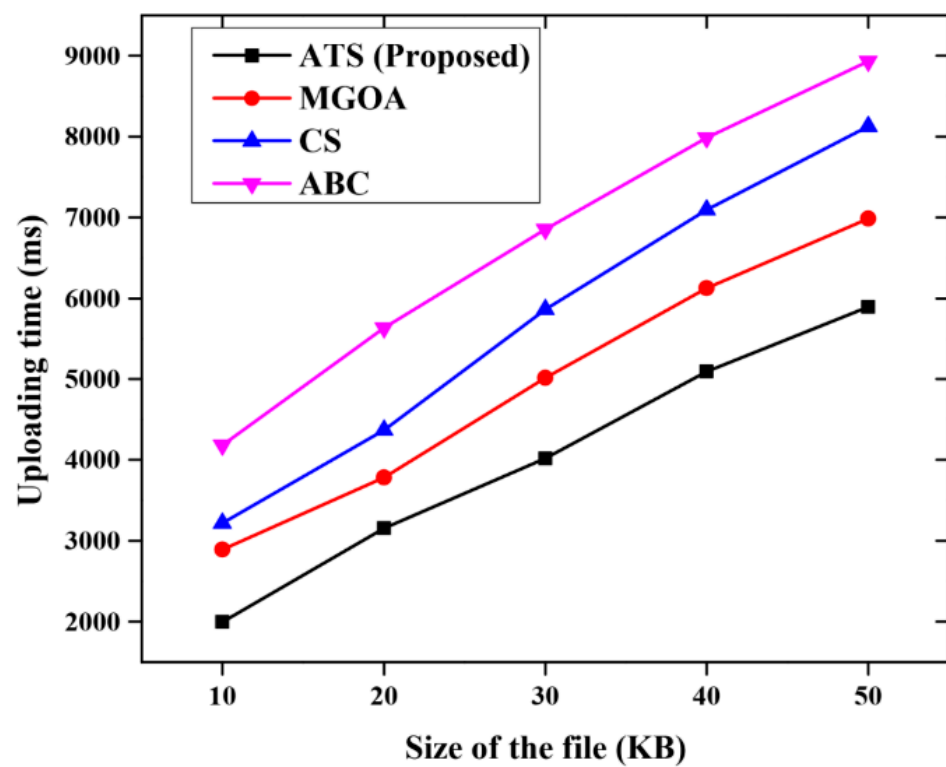


Figure 12. Comparative analysis for the uploading time.

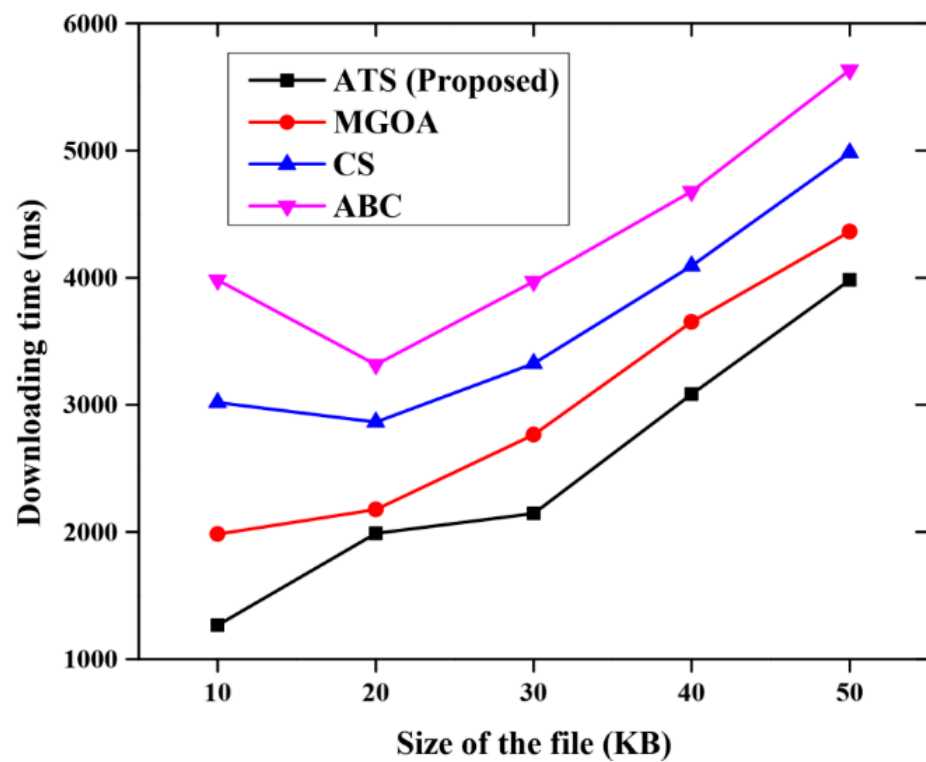


Figure 13. Comparative analysis for the downloading time.

## 6. Conclusions

The secure m-learning method is presented to assure consistent educational activities such as examinations, lectures, quizzes and other tests. This study states the merit of cloud computing and m-learning create benefits at Abdulaziz University. This paper discusses the student observations on security features of mobile learning that are increasing the potential for open and distance education. The mobile learning system is becoming more prevalent due to the presence of the Internet everywhere. In various cases, privacy and security during data sharing are considered the most significant issue. On the other hand, the mobile learning system is influenced directly by progressive technological advancements and the issues based on security and privacy are entirely different from the e-learning system. This paper proposes a cloud-based mobile learning system using the HOCC algorithm, comprising public and private keys for data encryption. The proposed approach selects optimally the random value and the ATS algorithm is employed for generating the optimal key value. Here, the survey was conducted among King Abdulaziz University sophomore students from the Faculty of Computing and Information Technology (FCIT). The inputs were used for selecting programming language and other factors in developing the tool. The study investigation employed a survey comprising 50 students, and the questionnaire was sent for all fifty students. In general, the initial phase involved the collection of indicators from the KA University for building the classification of platforms for selecting the technology, and to determine the usability and effectiveness of the system. In addition, various evaluation parameters, namely the encryption time, decryption time, downloading time, uploading time and reputation were evaluated. The analysis revealed that the proposed approach provided better results when compared with other techniques. In future research studies it will be necessary to focus on computational cost during the encryption process, which needs to be minimized.

**Author Contributions:** Conceptualization, D.M.A.; methodology, D.M.A. and S.H.H.; software, G.A., L.C. and M.A.; validation, D.M.A.; formal analysis, D.M.A. and G.A.; investigation, S.H.H.; data curation, D.M.A., G.A. and A.M.; writing—review and editing, M.A. and G.A.; visualization, A.M.; supervision, D.M.A.; project administration, D.M.A.; funding acquisition, D.M.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This project was funded by the National Plan for Science, Technology and Innovation (MAARIFAH), King Abdulaziz City for Science and Technology, the Kingdom of Saudi Arabia, award number 12-INF2259-03. The authors also acknowledge with thank the Science and Technology Unit, King Abdulaziz University, for technical support.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** The authors are thankful to all the associated personnel who contributed to this study in any way.

**Data Availability Statement:** The data supporting this research and that were used to build the system can be acquired from the corresponding author or second-to-last author upon request.

**Acknowledgments:** This project was funded by the National Plan for Science, Technology and Innovation (MAARIFAH), King Abdulaziz City for Science and Technology, the Kingdom of Saudi Arabia, award number 12-INF2259-03. The authors also acknowledge with thank the Science and Technology Unit, King Abdulaziz University, for technical support.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Buabeng-Andoh, C. Exploring University students' intention to use mobile learning: A research model approach. *Educ. Inf. Technol.* **2021**, *26*, 241–256. [[CrossRef](#)]
2. Butler, A.; Camilleri, M.A.; Creed, A.; Zutshi, A. The use of mobile learning technologies for corporate training and development: A contextual framework. In *Strategic Corporate Communication in the Digital Age*; Emerald Publishing Limited: Bingley, UK, 2021.
3. Mergany, N.N.; Dafalla, A.; Awooda, E. Effect of mobile learning on academic achievement and attitude of Sudanese dental students: A preliminary study. *BMC Med. Educ.* **2021**, *21*, 1–7. [[CrossRef](#)] [[PubMed](#)]

4. Vallejo-Correa, P.; Monsalve-Pulido, J.; Tabares-Betancur, M. A systematic mapping review of context-aware analysis and its approach to mobile learning and ubiquitous learning processes. *Comput. Sci. Rev.* **2021**, *39*, 100335. [\[CrossRef\]](#)
5. Liu, C.; Zowghi, D.; Kearney, M.; Bano, M. Inquiry-based mobile learning in secondary school science education: A systematic review. *J. Comput. Assist. Learn.* **2021**, *37*, 1–23. [\[CrossRef\]](#)
6. Qureshi, M.I.; Khan, N.; Gillani, S.M.A.H.; Raza, H. A Systematic Review of Past Decade of Mobile Learning: What we Learned and Where to Go. *Int. J. Interact. Mob. Technol.* **2020**, *14*, 67–81. [\[CrossRef\]](#)
7. Okai-Ugbaje, S.; Ardziejewska, K.; Imran, A. Readiness, roles, and responsibilities of stakeholders for sustainable mobile learning adoption in higher education. *Educ. Sci.* **2020**, *10*, 49. [\[CrossRef\]](#)
8. Hamidi, H.; Chavoshi, A. Analysis of the essential factors for the adoption of mobile learning in higher education: A case study of students of the University of Technology. *Telemat. Inform.* **2018**, *35*, 1053–1070. [\[CrossRef\]](#)
9. Chang, C.Y.; Lai, C.L.; Hwang, G.J. Trends and research issues of mobile learning studies in nursing education: A review of academic publications from 1971 to 2016. *Comput. Educ.* **2018**, *116*, 28–48. [\[CrossRef\]](#)
10. Sung, Y.T.; Lee, H.Y.; Yang, J.-M.; Chang, K.-E. The quality of experimental designs in mobile learning research: A systemic review and self-improvement tool. *Educ. Res. Rev.* **2019**, *28*, 100279. [\[CrossRef\]](#)
11. Pooranian, Z.; Shojafar, M.; Garg, S.; Taheri, R.; Tafazoli, R. LEVER: Secure Deduplicated Cloud Storage with Encrypted Two-Party Interactions in Cyber-Physical Systems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5759–5768. [\[CrossRef\]](#)
12. Ennouamani, S.; Mahani, Z.; Akharraz, L. A context-aware mobile learning system for adapting learning content and format of presentation: Design, validation and evaluation. *Educ. Inf. Technol.* **2020**, *25*, 3919–3955. [\[CrossRef\]](#)
13. Pensabe-Rodriguez, A.; Lopez-Dominguez, E.; Hernandez-Velazquez, Y.; Dominguez-Isidro, S.; De-la-Calleja, J. Context-aware mobile learning system: Usability assessment based on a field study. *Telemat. Inform.* **2020**, *48*, 101346. [\[CrossRef\]](#)
14. Romero-Rodríguez, J.-M.; Aznar-Díaz, I.; Hinojo-Lucena, F.-J.; Gómez-García, G. Mobile learning in higher education: Structural equation model for good teaching practices. *IEEE Access* **2020**, *8*, 91761–91769. [\[CrossRef\]](#)
15. Li, K.C.; Lee, L.Y.-K.; Wong, S.-L.; Yau, I.S.-Y.; Wong, B.T.-M. The effects of mobile learning for nursing students: An integrative evaluation of learning process, learning motivation, and study performance. *Int. J. Mob. Learn. Organ.* **2019**, *13*, 51–67. [\[CrossRef\]](#)
16. Bai, H. Pedagogical practices of mobile learning in K-12 and higher education settings. *TechTrends* **2019**, *63*, 611–620. [\[CrossRef\]](#)
17. Al-Emran, M.; Mezhyuev, V.; Kamaludin, A. Towards a conceptual model for examining the impact of knowledge management factors on mobile learning acceptance. *Technol. Soc.* **2020**, *61*, 101247. [\[CrossRef\]](#)
18. Mutambara, D.; Bayaga, A. Determinants of mobile learning acceptance for STEM education in rural areas. *Comput. Educ.* **2021**, *160*, 104010. [\[CrossRef\]](#)
19. Bernacki, M.L.; Greene, J.A.; Crompton, H. Mobile technology, learning, and achievement: Advances in understanding and measuring the role of mobile technology in education. *Contemp. Educ. Psychol.* **2020**, *60*, 101827. [\[CrossRef\]](#)
20. El-Sofany, H.; El-Haggar, N. The effectiveness of using mobile learning techniques to improve learning outcomes in higher education. *Int. J. Interact. Mob. Technol.* **2020**, *14*, 4–18. [\[CrossRef\]](#)
21. Troussas, C.; Krouska, A.; Sgouropoulou, C. Collaboration and fuzzy-modeled personalization for mobile game-based learning in higher education. *Comput. Educ.* **2020**, *144*, 103698. [\[CrossRef\]](#)
22. Korać, D.; Damjanović, B.; Simić, D. March. Information security in M-learning systems: Challenges and threats of using cookies. In Proceedings of the 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 18–20 March 2020; pp. 1–6.
23. Khairi, T.W.A. Secure mobile learning system using voice authentication. *J. Eng. Appl. Sci.* **2019**, *14*, 8180–8186.
24. Al Shehri, M. A secure mobile learning framework based on Cloud. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 7–11.
25. Lee, E.-Y.; Jeon, Y.J.J. The Difference of user satisfaction and net benefit of a mobile learning management system according to self-directed learning: An investigation of cyber university students in hospitality. *Sustainability* **2020**, *12*, 2672. [\[CrossRef\]](#)
26. Verma, O.P.; Jain, N.; Pal, S.K. Design and analysis of an optimal ECC algorithm with effective access control mechanism for big data. *Multimed. Tools Appl.* **2020**, *79*, 9757–9783. [\[CrossRef\]](#)
27. Malik, A.; Aggarwal, M.; Sharma, B.; Singh, A.; Singh, K.K. Optimal Elliptic Curve Cryptography-Based Effective Approach for Secure Data Storage in Clouds. *Int. J. Knowl. Syst. Sci.* **2020**, *11*, 65–81. [\[CrossRef\]](#)
28. Kaur, S.L.; Awasthi, K.; Sangal, A.L.; Dhiman, G. Tunicate Swarm Algorithm: A new bio-inspired based metaheuristic paradigm for global optimization. *Eng. Appl. Artif. Intell.* **2020**, *90*, 103541. [\[CrossRef\]](#)
29. Fetouh, T.; Elsayed, A.M. Optimal Control and Operation of Fully Automated Distribution Networks Using Improved Tunicate Swarm Intelligent Algorithm. *IEEE Access* **2020**, *8*, 129689–129708. [\[CrossRef\]](#)
30. Li, S.; Chen, H.; Wang, M.; Heidari, A.A.; Mirjalili, S. Slime mould algorithm: A new method for stochastic optimization. *Future Gener. Comput. Syst.* **2020**, *111*, 300–323. [\[CrossRef\]](#)
31. Malik, A.; Jain, V.K. Effective Renewal and Signing Method to Achieve Secure Storage and Computation Using Hybrid RSA-MABC Algorithm. *Int. J. Intell. Eng. Syst.* **2016**, *9*, 11–20. [\[CrossRef\]](#)