Al-Aqsa University Journal (Natural Sciences Series),Vol.23, Pages 50 -68, Jan.2021
ISSN 2070-3155

Blockchain-Based AKA Scheme for Moodle System

Dr. **Zaher Haddad** *

مخطط مصادقة وتبادل مفاتيح القائم على تقنية البلوكتشين لنظام موودل

الملخص

الموودل عبارة عن بيئة التعلم الديناميكية المعيارية الموجهة للبشرية؛ إذ تعد أكثر أنظمة إدارة التعلم شيوعًا واستخدامًا في جميع أنحاء العالم؛ حيث تختار العديد من المعاهد التعليمية والمدارس والجامعات نظام الموودل؛ لتحقيق مرافق التعلم الإلكترونية الخاصة بها مثل: المحاضرات، والامتحانات، والواجبات، وما إلى ذلك. فنظام موودل يستخدم اتصال الإنترنت كقناة اتصال أساسية بين المستخدمين. ومع ذلك، تعتبر هذه التقنية غير آمنة على الرغم من وجود التسجيل والمصادقة وبروتوكولات اتفاقية المفاتيح التي تعد من أهم البروتوكولات في أي نظام إنترنت؛ فقد أشار العديد من الباحثين إلى أن هناك مشكلات أمنية كبيرة في نظام مصادقة موودل يجب حلها. ومن ناحية أخرى، فإن البلوكتشين عبارة عن تقنيات ناشئة ذات تأثير كبير على حياتنا في الأيام القادمة؛ لأنها تمنح البلوكتشين خصائصها الأمنية مثل: الأصالة، والنزاهة لمختلف التطبيقات مثل: البيتكوين، والعقود الذكية، وإنترنت الأشياء، وما إلى ذلك.

لذلك، في هذه الورقة، تقدم مخطط مصادقة آمن وفعال لنظام إدارة التعلم الموودل باستخدام تقنية البلوكتشين والبنية التحتية للمفتاح العام الجمال الذي يحقق التسجيل والمصادقة والاتفاقية الرئيسة. فيوضح تحليلنا الأمني أن النظام المقترح آمن، ويقاوم أنواعًا مختلفة من الهجمات؛ علاوة على ذلك، فإنه يوضح تقييم أدائنا أن المخطط المقترح أكثر كفاءة من المخطط الأكثر شيوعًا، إضافة إلى المخططات الأخرى؛ لأنه يحافظ على موارد المستخدمين، ويحافظ أيضًا على عرض النطاق الترددي للشبكة.

Zaher Haddad, PhD, Faculty of Computers and Information Technology, Al-Aqsa University, Gaza, Palestine
zj.haddad@alaqsa.edu.ps

Abstract

Moodle, Modular Object-Oriented Dynamic Learning Environment, is the most common learning management system being used around the world. many educational institutes, schools, and universities select Moodle system to achieve their electronic learning facilities such as lectures, exams, assignments and etc. Moodle as other Internet of thing systems uses Internet connection as the backbone communication channel between users. However, Security consideration is the most critical element facing the reliance on this technology. Registration, authentication, key agreement protocols are the most important protocols in any Internet of thing system since it is a well-known insecure channel. However, many researchers address that there are big security issues in the Moodle authentication system in need of being solved. On the other hand, blockchain is an emerging technology with great impact on our life in the coming days. Blockchain grants its security properties such as authenticity and integrity to various applications such as bitcoin, smart contracts, Internet of thing and etc.

Therefore, in this paper, we introduce a Secure and Efficient Authentication Scheme for Moodle Learning Management System using Blockchain Technology and Elgamal Public Key Infrastructure that achieves registration, authentication, and key agreement. Our security analysis illustrates that the proposed scheme is secure and withstands different types of attacks. Moreover, our performance evaluation shows that the proposed scheme is more efficient than the most common scheme and also other schemes since it preserves both the resources of users and the bandwidth of the network.

Keywords: Moodle, LMS, blockchain, registration, authentication, security, key management, public key, and signature.

Introduction:

Information Technology (IT) is the main feature of our modern age. Information technology is the study of developing and designing information system as software for computers, smartphones, and tablets in order to achieve a specific task such as maintaining, converting, processing, sending, receiving, retrieving or securing information (Alieyan, Almomani, Abdullah, Almutairi, & Alauthman, 2020). Therefore, Information technology has become an important element of our daily life as it coupled with many sectors such as political, economic, trading, money exchange, education and etc. (Alieyan, Almomani, Abdullah, Almutairi, & Alauthman, 2020). Corona Virus, the last suffocated situation that the world is suffering, is considered a live witness of the importance of information technology (World Health Organization (WHO), May 2020).

Among our life Fields, Education coupled information technology via number standard platforms called learning management systems (LMS). LMS is a software which enables instructors, educators, and students to execute their learning activities such as lectures, classes, evaluations, assignments, homework, and exams (Alomari, El-Kanj, Alshdaifat, & Topal, 2020).

LMS appeared in the late of 1990 in both asynchronous and synchronous-based shapes in order to offer classroom management for instructor led training or flipped classroom. Moreover, LMS is designed for analysis learning materials and concludes the recommendation to course. Thus, instructors can get feedback to make that course more accurate (Alomari, El-Kanj, Alshdaifat, & Topal, 2020) .

Moodle, an Internet of thing application, is a free open source LMS written in PHP programming language and distributed under general public license that allow end user to run, study, share and modify the software. Moodle is developed based on pedagogical principle that depends on theory and practice of learning and how the process influences and is influenced by (Anand & Eswaran, 2018). Moodle provides users with a number of standard features enabling them to create their own website and fill it with a dynamic course that extends at anytime/anywhere such as; modern and easy use interface, personalized dashboard, collaborative tools and activities; all-in-one calendar, convenient file management, simple and intuited test editor, notations, track process and etc. (De Medio, Limongelli, Sciarrone, & Temperini, 2020).

Authentication is a field of network security that allows users to access a specific network entity. As any field of Internet of thing, Moodle defines a number of authentication methods such as manual account, no login, email-based, control authentication service (CAS) external database, lightweight directory access protocol (LDAP), learning tool interpretability (LTI). However, Moodle suffers authentication problems since there is a weak vulnerability in the authentication handler that attacker can exploit to violate Moodle system (vuldb). Moreover, the uses of Internet

connection. It also constitutes a big security problem for Moodle authentication protocol since Internet connection is a well-known insecure channel (Kumar, Mitta, Thakur, & Srivastava, 2020).

Therefore, In this paper, we will introduce Secure and Efficient Authentication Scheme for Moodle Learning Management System using Blockchain Technology and Elgamal Public Key Infrastructure. The objective of proposed protocol is to withstand attacks such as modification, impersonating, man in the middle, and replay attacks. Therefore, in this scheme, we use elgamal public key cryptosystem to achieve authentication, signature, and key management. Also, we will use the blockchain technology to achieve integrity and distributivity.

The contribution of this paper is described as follows: first, it introduces secure authentication scheme to exchange keys and to verify signature by using standard key management algorithm such as elgamal public key infrastructure. Second, it provides efficient authentication scheme that consumes computation time and communication overhead less than the other schemes by using the blockchain technology. Third, it withstands different type of attacks since the Moodle system uses the Internet connection by using bilinear pairing for signature verification and timestamps to check the freshness of the messages.

The rest of this paper is organized as follows; section related work surveys the most common works of the Moodle authentication protocols that were proposed before. Section network model describes the network and threat model of Moodle authentication scenarios. Section preliminaries describes the elgamal public key infrastructure and blockchain technology since they are used in the proposed scheme. Section proposed scheme describes the proposed scheme that is introduced to achieve the authentication and key agreement protocol for Moodle learning management system. Section security analysis discusses the security analysis of the proposed scheme to illustrates how proposed scheme withstands the defined attacks. Section performance evaluation evaluates the performance of the proposed scheme compared with the most common schemes that were proposed before. Section conclusion concludes the works. Section future work introduces the future work of the proposed idea and the references

1. Related Works

In this section, we will survey the most common related works that target the security of Moodle system as follows:

(Ayyad, 2016), Ayyad et. al. considers the close relation between eLearning platform and The internet and interconnected network that make it a cyber-threatened. Therefore, they use some open-source tool to test the vulnerabilities of Moodle system by injection, cross-side, and brute-force attacks. However, this study is an analytical study which only introduces a recommendation to solve the problem.

In (Bucicoiu & Tapus, 2013), Bucicoiu et. al. regards the attendance of students to Moodle as a problem. Therefore, they use composite technique to solve this problem. The proposed scheme is composed of two stages; the first is a location-based authentication technique in order to determine the location of user. The second works on user photo to ensure double authentication. However, this scheme consumes long time and needs high processors while students are logging on the Moodle system by using mobile devices which have low processors and low batteries.

In (Gadhave & Kore, 2016), Gadhave et. al. considers the attendance of user a big problem in learning management systems such as Moodle. Therefore, they suggest granting an identity to each user to define user to Moodle system. However, the proposed scheme suffers from modification and replay attacks.

In (Gil, Sancristobal, Diaz, & Castro, 2011) (Gil, et al., 2013), Gil et. al. addresses a security risk in the higher education distance education system because the use of the internet, which is a well-known insecure channel. Therefore, they suggest to use biometric tool to achieve authentication in the learning management systems such as Moodle. However, the biometric is multimedia information, which is well-known for consuming a long time to verify. Moreover, replay attack is still a big problem since attacker could record a message and reuse it once again to overwhelm the system.

In (Zahid, Ali Zahoor, Khan, & Ali, 2016), Zahid et. al. considers the lack of student's awareness of the computer security can be a vulnerability that attacker can exploit to violate the security of the learning management system in Islamabad. Therefore, they use a hash function stored in database for each user identity. However, this system suffers in the middle attack,

In (Abd. Rahim, Mohd, Amin Sahari, Safie, & Bin Abd Rahim, 2018), Abd. Rahim et. al. claim that Moodle is the most widely learning management system around the world. and the large number of users who use Moodle system causes a big security problem. Therefore, they prepared a questionnaire to check the necessity to develop a special integrity system to Olympia college. However, this study is theoretical and did not consider the authentication protocol.

In (Amo-Filvà, Alier Forment, Peñalvo, & Fonseca Escudero, 2020), Amo-Filvà et. al. subject the fairness of student evaluation system that are followed by teachers in Moodle system suffers from a big problem since it may suffer from mood effect from the teacher toward the student. Therefore, authors suggest to develop a anonymity system to integrate with the Moodle system in order to preserves the privacy of student. However, this scheme did not consider the authentication protocol.

2. Network and Threat Model

Blockchain-Based AKA ….

Moodle learning management system supports a number of authentication scenarios that user could follow to access the learning management system, therefore, in this subsection, we will describe a general texture of Moodle network system and the authentication scenarios that Moodle defined to allow user accessing the learning management system. Moreover, we will describe the most common attacks that could violate the security of the Moodle authentication scenarios.

2.1. Network model

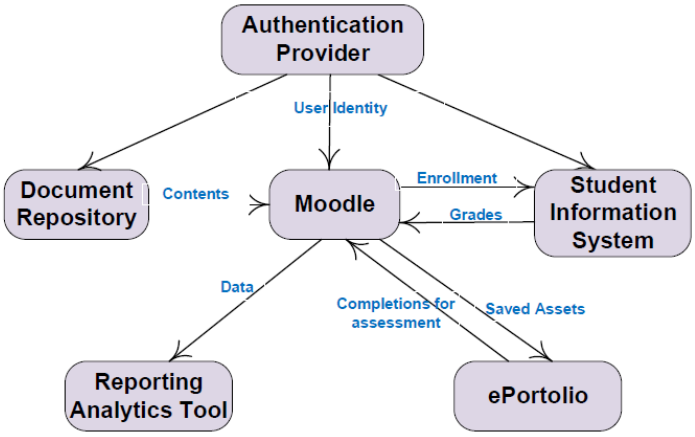

Figure 1: Moodle Network Architecture (Brown & Wilson, 2011)

Figure 1 describes the architecture of Moodle learning management system. Like other internet applications, Moodle system integrates a number of applications such as students' information system, document repository, reporting analytic tool, eportotio and authentication provider. The student information system holds information specified to the student such as profiles, course profiles, student course enrollment, and grads. Document repository holds files about course activities such as lectures, power point presentations, video's, audio, and pdf assignment files. the reporting analyst's tools hold some analytical applications to achieve the required statistics and computation that Moodle system need. The eprotolio integrates with Moodle to provide users with a template for different services such as creating a curriculum vitae (Brown & Wilson, 2011). Moreover, Moodle integrates with a number of authentication providers to allow users to log in Moodle site with a specific security permission such as username and passwords. However, Moodle developers defined a number of authentication schemes to achieve that purpose as follows (MoodleDocs):

1. Manual Account Authentication Scheme: In this scheme, Moodle system administrator is responsible for creating an account and grant permission for each user manually such as username, password, password expiry, lock user field, suspend options and atc.
2. Email Based Registration: In this scheme, Moodle administrator allows user to log in the Moodle system by using a specific email. This type of scenarios are followed by an organization that creates a formal email for their employees and considered this email an authorized identifier to user.
3. Central Authentication Service (CAS): CAS is a service provided over the internet that allows a number of predefined users to share number of different web applications.
4. External Database Authentication: In this method, Moodle system uses external database to check whether a given username and password is valid or not to log in the system.
5. Light-Weight Directory Access Protocol (LDAP) Authentication: In this scheme, Moodle system integrates with LDAP to allow user logging in the Moodle system. LDAP works over an Internet Protocol (IP) network to access and maintain distributed directory information services.
6. Learning Tool Interoperability (LTI): LTI is a tool developed by IMS Global learning consortium to establish a standard method for integrating rich learning applications and platforms in order to achieve authentication scenario.
7. MNet authentication: Moodle administrator can use Mnet software to establish peer to peer link between the LMS and a specific user.
8. Shibboleth: this kind of authentication scheme allows Moodle administrator to create an intermediate project to use identity-based authorization and logging in the Moodle system.

2.2. Threat Model

Moodle is a commonly used learning management system, where a lot of organizations, schools, universities, and students consider the platform to achieve their learning activities such as lectures, classes, exercises, exams, assignments, and grading. However, the widely used Moodle and their variation of users make it an attractive target to different attackers. Therefore, in this section, we will define the attackers that could violate the security of Moodle as follows (Idris Khan, Javed, & Alenezi, 2019) (Gayoso Martínez, Hernandez Encinas, Queiruga-Dios, Encinas, & Martin-Vaquero, 2013):

1. Modification Attack: in the Moodle system, modification attack may be a student target to modify his mark or extend the deadline of a specific assignment that was expired before.
2. Impersonating Attack: Also, in Moodle system, most commonly desired for persons who do not register a specific course to access and go to the course activities.
3. Man in the Middle Attack: in this case, attacker attempts to play as middle role between Moodle system and users in order to achieve a malicious task such as collecting information

about the security service and use this information to launch other attacks on illegal tasks such as Denial of Service (DoS) Attack and modification attack.

4. Replay Attack: in Moodle system, replay attack constitutes a big problem since all tasks are going online, therefore, replay attack attempts to record a specific message and resend this message many times in order to overwhelm the system and make it break down.

5. Preliminaries

In this section, we will describe the Elgamal public key cryptography and blockchain technologies since They are the core cryptographic algorithms that will be used in the proposed scheme.

5.1. Elgamal Public Key Cryptography

Elgamal (described by Taher Elgamal in 1985) is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. Elgamal encryption can be defined over any cyclic group G such as multiplicative group of integers modulo n (Stallings, 2013).

5.1.1. Elgamal Key generation algorithm

To generate private and public key, user follows steps as (Stallings, 2013) (Nofer, Gomber, Hinz, & Schiereck, 2017):

1. Party A generates a cyclic group G of order q with generator g.
2. Party A choose an integer x randomly, where, $(1 \leq x \leq (q-1))$.
3. Compute $h = g^x \bmod n$
4. The public key consists of the values (G, q, g, h).
5. A publishes this public key and retains x as her private key, which must be kept secret.

5.1.2. Elgamal Practical Use

The Elgamal cryptosystem is usually used as part of a hybrid cryptosystem where the message itself is encrypted using a symmetric encryption and the key is managed and exchanged by Elgamal algorithm. This is because asymmetric cryptosystems are usually slower than symmetric ones for the same level of security, so it is faster to encrypt the message, which can be arbitrarily large, with a symmetric cipher (Mahesh Kumar, V. N. K. Prasad, & Raju, 2020).

5.1.2. Elgamal Security

The security of the Elgamal scheme depends on the properties of the underlying group G. If the computational Diffie–Hellman assumption (CDH) holds in the underlying cyclic group G, then the encryption function is one-way. If the decisional Diffie–Hellman assumption (DDH) holds in G, then Elgamal achieves semantic security. Semantic security is not implied by the computational Diffie–Hellman assumption alone as if g is the generator of group G and r is a large prime number belong G, it is impossible for attacker to get r even if he knows g and g^r (K & Begam, 2020).

5.2. Blockchain Technology

Blockchain technology is a combination between cryptography and public ledger used to achieve trustiness between parties. Blockchain has number of properties as follows (Kim & Chandra Deka, 2019):

1. Distributivity: Build trust between strangers, each node of the network has a copy of blockchain with respect to that any new transaction is registered once it verified and could not be modified or rolled back.
2. Increase Connection: Create a peer-to-peer connection between two strangers without restrictions.
3. Raise Productivity: properties can use blockchain to exchange information without the need of third parties.
4. Security: Each transaction in the blockchain is held by the hash function of the previous block, therefore, it is impossible to modify or remove any transaction.
5.

6. Proposed Scheme

In this section, we will describe the proposed scheme that we will introduce to solve the defined problem in the Moodle authentication and key agreement protocol. The proposed scheme is composed of two components; initialization and authentication and key agreement protocol as follows:

6.1. Initialization

Initialization is the process that Moodle System Administrator (MSA) follows to bootstrap the security system. Table 1 describes the acronym being used in the proposed scheme:

Table 1: Proposed Scheme Acronym

Acronym	Description
q	Large prime number
Z_q	Finite Field
G	Cyclic Multiplicative Group
H, H_1\$, SHA256	hash function
Pr_m	Private key of MSA
Pk_m	Public key of MSA
Pr_u	Private key of user
Pk_u	Public key of user
B_{id_x}	block index of user x
TS	Timestamp
ĕ	Bilinear Pairings function
σ_x	Digital Signature of user x
ch	Challenge

Based on elgamal algorithm, MSA chooses a large prime number q and generate Z_q as a finite field with order q, Let G be a cyclic multiplicative group with generator g, whose order q. Consider H and H_1 are two hash functions (SHA256) where, H: $\{0,1\}^* \rightarrow G$ and H_1:$\{0,1\}^* \rightarrow Z_q$. The Moodle MSA uses Elgamal algorithm to generate public Pk_m and private Pr_m keys for MSA by choosing random element $Pr_m \in Z_q$ and computes $Pk_m = g^{Pr_m} \bmod q$. For each user of the network (u), MSA chooses random element $Pr_u \in Z_q$ and computes $Pk_u = g^{Pr_u} \bmod q$ as private and public key, respectively. Moreover, for each user, MSA create a block in the blockchain composed of Block Header, hash of the previous block, timestamp, Nonce, and public key. Finally, MSA distributes blockchain over clouds.

6.2. Authentication and Key Agreement Protocol

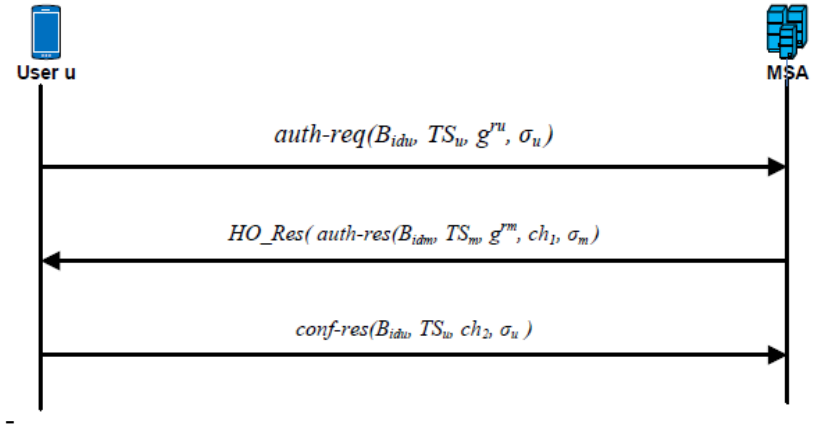

Figure 2: Proposed Authentication and Key Agreement Protocol.

Authentication and key agreement protocol are the scheme that Moodle users and MSA follow to mutually authenticate each other and shares a secret key. When users send an access request to MSA, MSA should execute authentication protocol that is illustrated in figure 2 as follows:

1. User (u) chooses a random number $r_u \in Z_q$, generate a timestamp TS_u, computes $\sigma_u = (H(B_{id_u}, TS_u, g^{r_u}))^{r_u}$ as a signature of the user, and sends authentication request, auth-req(B_{id_u} ,TS_u, g^{r_u} , σ_u) to MSA.
2. Once MSA receives the authentication request, it verifies the freshness of the message by timestamp, settled message will be dropped, and verified the signature of user as ĕ(σ_u, g) = ĕ((B_{id_u} ,TS_u, g^{r_u} , σ_u) , Pk_u), the proof of correctness is described below in equation 1, hence the public key of user u is stored in blockchain which infeasible to modified. If all verification is correct, MSA chooses a random number $r_m \in Z_q$ and timestamp TS_m and computes a shared key $K_{um} = H_1(g^{r_u})^{r_m} \bmod q$, and computes challenge $ch_1 = H(k_{um}, 1)$, Finally, MSA sends authentication response auth-res(B_{id_m}, TS_m, g^{r_m} , ch_1, σ_m), where $\sigma_m = (H(B_{id_m}, TS_m, ch_1, g^{r_m}))^{r_m}$

$$\begin{aligned} ĕ(\sigma_u, g) &= ĕ\,(H(B_{id_u}, TS_u, g^{r_u})^{r_u}, g) \\ &= ĕ\,(H(B_{id_u}, TS_u, g^{r_u}), g^{r_u}) \\ &= ĕ\,(H(B_{id_u}, TS_u, g^{r_u}),\ Pk\_u) \quad \ldots\ldots\ldots\ldots\ 1 \end{aligned}$$

3. Once the user receives the message, it checks the novelty of the message by using TS_m, and verifies the correctness of the σ_m. If all verification is correct, user u computes the shared key $K_{um} = H_1(g^{r_m})^{r_u} \bmod q$ and computes compares challenge ch_1, if it is correct, user u computes challenge $ch_2 = H(K_{mu}, 2)$ and sends confirmation response , conf-res(B_{id_u} , TS_u, ch_2, σ_u) to the MSA and exit the authentication protocol, otherwise, the user u will re-initiate a new authentication protocol

7. Security Analysis

In this section, we will investigate the robustness of the proposed scheme against the defined attacks. The proposed scheme is based on the blockchain and elgamal scheme. As mentioned in the preliminaries section, elgamal cryptosystem depends on discrete logarithm problem which is infeasible for attack to get a random number r even if he knows g^r and g. while blockchain technology has four proved properties such as integrity, distributivity, security and productivity. Therefore, we will show how the proposed scheme will use each of these properties to secure the Moodle system as follows:

1. Attack against authentication protocol: each member of the proposed scheme; instructor or student, has a public and private key that were generated by using elgamal cryptosystem. The private key is saved secure with the user and the public key id mentioned into the blockchain. therefore, attacker has no possibility to get the secret key by using the public key because of discrete logarithm problem and moreover, attacker has no ability to generate a new public because the only one who is responsible for a new block is the MSA.
2. Attack against key management: the shared key that is generated between each user and MSA after successful authentication is computed based on two fresh random number. The two random numbers; r_u and r_m, are exchanged securely based on the discrete logarithm problem that infeasible to attacker to break.
3. Attacks against modification message: each exchanged message in the proposed scheme is assigned by elgamal digital signature that is also well-known and infeasible to discover.
4. Attacks against integrity: each exchanged message is hash by using SHA256 hash function, which is still unbroken and irreversible function, therefore, any changes in the transmitted message will cause a signature failure and thus authentication failure.
5. Attacks against freshness and replication: each message has a timestamp. The settled message will be dropped. Therefore, the attacker has no ability to record a message and reuse this message to overwhelm the system.

Table 2: Security Attacks Comparison

Attack / Scheme	Bruteforce	Mathematical	Side Channel(Times)
Bucicoiu	2^{48}	2^{24}	52
Gadhave	2^{128}	2^{64}	443
Gil	2^{128}	2^{64}	443
Proposed	2^{160}	2^{80}	Infeasible

Table 2 illustrates a security comparison between the proposed scheme and other schemes, this comparison demonstrates that the proposed scheme is more secure and efficient to withstand attacks such as bruteforce, mathematical, and side channel attacks. In the bruteforce attacks, attackers attempts to get the secret key by trying all possible keys, the proposed scheme uses key size 160 bit, which require brute force attack to try 2^{160} compared to 2^{48}, 2^{128}, and 2^{128} that require bruteforce attack to try Bucicoiu (Bucicoiu & Tapus, 2013), Gadhave (Gadhave & Kore, 2016), and Gil (Gil, et al., 2013), respectively.

Moreover, the mathematical attacks require to try half of possible keys to get the secret key, however, the proposed scheme still provide more security and efficiency compared to the other scheme because of the use of 160-bit key. Furthermore, the proposed scheme withstands the side channel attacks who attempts to get the secret key by the numbers of times being used since the proposed scheme uses a fresh session key using new random number every session while the Bucicoiu (Bucicoiu & Tapus, 2013), Gadhave (Gadhave & Kore, 2016), and Gil (Gil, et al., 2013) use the same secret key and the side channel attack could violate the secret key of them each 48, 443, and 433 times, respectively.

8. Performance Evaluation

In this section, a comprehensive performance evaluation of our scheme is introduced compared with the most common three other schemes. This evaluation demonstrates the efficiency of the proposed scheme through two performance metrics such as communication overhead and computation overhead

8.1 Communication Overhead

In this sub section, we will distinguish the total bandwidth that the proposed scheme will consume compared with the other schemes. the communication overhead is computed by using the number of messages and the amount of data (in bytes) that need to be exchanged.

8.1.1 Number of exchanged messages

In order to achieve mutual authentication, the proposed scheme requires 3 messages, Bucicoiu) Bucicoiu و Tapus(2013 ، requires 10 messages, Gadhave (Gadhave & Kore, 2016) requires 8 messages and Gil (Gil, et al., 2013) requires 7 messages. It is clear that the proposed scheme requires number of messages less than the others, therefore less communication overhead in the network is needed as shown in Fig 3.

This gap of a number of messages that are needed to achieve mutual authentication referred to the use of blockchain technology since it is distributed via the internet including the public key of the user which is impossible to be fag while the other schemes need to exchange number of messages between moodle server and the user in order to ascertain the required authentication data.

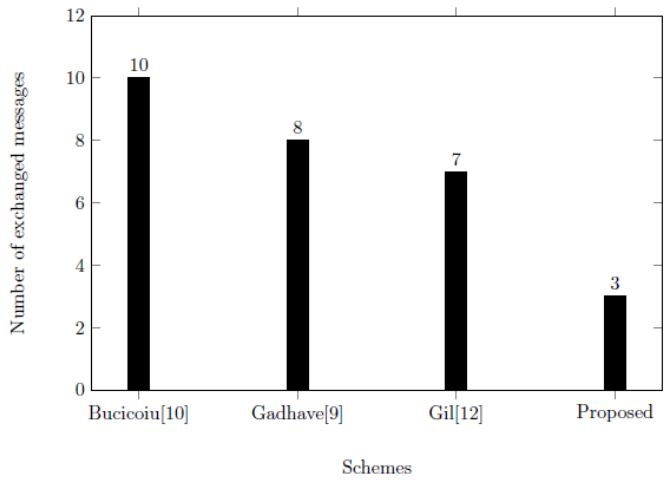

Figure 3 : Number of exchanged messages used in various Authentication Schemes

8.1.2. Amount of data

The amount of data is computed as the total bytes that the exchanged messages were composed of, therefore, we build each identifier by two bytes, the large prime number q as 20 bytes, elliptic curve point by 20 bytes for each, each signature by 20 bytes, and 5 bytes for each timestamp. According to these considerations, as demonstrated in fig 4, the proposed scheme requires amount of data less than the other schemes because it requires a smaller number of exchanged messages to perform AKA protocol.

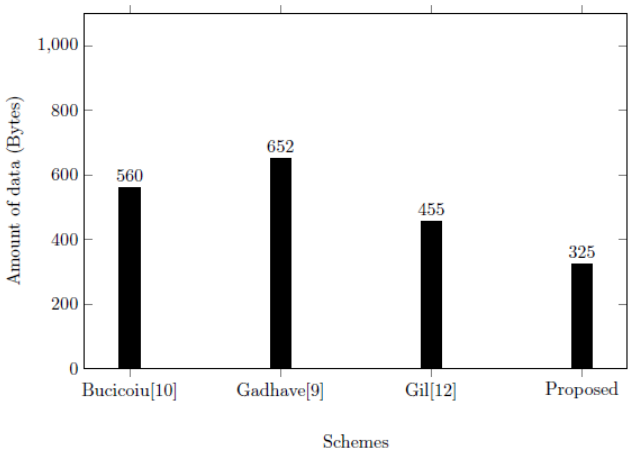

Figure 4 : Amount of data used in various Authentication schemes

Therefore, the decrease of the number of exchanged messages decreases the amount of data that are requireed to achieve the authentication and key agreement protocol, thus preserves the bandwidth of the whole network.

8.2. Computation Overhead

The process of achieving authentication and key agreement protocol consumes time called computation time, this is defined by the time required for the 5G node to compute the required functions that are used in the authentication and key agreement protocol.

According to the security cryptographic namespace coded in visual studio Net 2012, compiled with Microsoft Visual Basic .Net 2012 and run in a device with Intel(R) Core(TM) i7-4510U CPU@2.00GHz 2.60 GHz, 16 GB RAM and 46-bit operating system x64-based processor, the computation overhead of the cryptographic algorithm being used in our scheme are computed as cryptographic function, SHA256 hash function, AES, elgamal encryption/decryption, and modules operation consume 36, 5, 20, 1, 0.005 ms, respectively (Haddad, Taha, & Saroit, 2017). Moreover, according to (data.bitcoinity.org, 2019), the average time to mine a block is 120 ms. Furthermore, the elliptic curve point multiplication, point addition, and pairing consume 0.86, 0.58 and 4.14 ms, respectively.

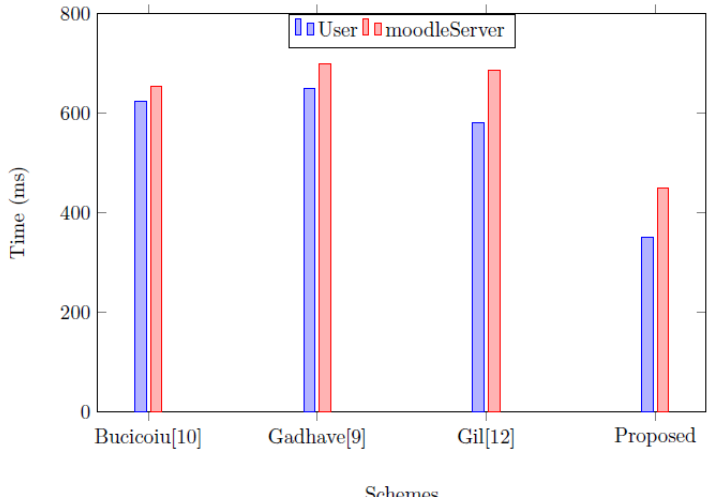

Figure 5: Authentication Computation Overhead for Various Schemes.

we compared in fig. 5 the computation overhead of the proposed scheme to the other existing schemes in order to achieve the authentication and key agreement protocol. The uses of blockchain decreases the time required to achieve authentication and key agreement protocol because the blockchain is considered a trusted distributed database and saves the time that the network mode needs to trust another network node. Therefore, the number of required messages needed to achieve authentication protocol are decreased, which save the required time.

In the user side, Moodle user, who uses mobile and tablet devices to access Moodle system gives a big attention to the battery consideration and how they will preserve their device batteries. Therefore, the decreases of the computation time required to achieve authentication and key agreement protocol by proposed scheme compared to other schemes is an attractive factor to these users.

9. Conclusion

In this paper, we propose a mutual authentication protocol for Moodle system using blockchain technology. The security analysis proves that the proposed scheme is secure because it withstands the defined attacks such as replay, man in the middle, and modification attacks. Moreover, the performance evaluation describes the efficiency of the proposed schemes comparing the most common scheme that were proposed to solve the authentication protocol in Moodle system.

10.Future Work

In the future work, we will implement the idea in the actual environment of Alaqsa University Learning Management System, Moodle system, since we need to prove the correctness and the efficiency of the idea and then go to test its implementation on a real system.

11. References

Gadhave, V., & Kore, S. (2016). Portable attendance system integrated with learning management system like moodle. *2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, (pp. 2042-2046).

Gil, R., Sancristobal, E., Diaz, G., & Castro, M. (2011). Biometric verification system in moodle their analysis in lab exams. *2011 IEEE EUROCON - International Conference on Computer as a Tool.* Lisbon, Portugal.

Abd. Rahim, Y., Mohd, O., Amin Sahari, M., Safie, N., & Bin Abd Rahim, Z. (2018). A Study On The Effects Of Learning Material Handling Procedures Towards Information Integrity In Moodle Learning Management System (LMS). *2018 2nd International Conference on Electrical Engineering and Informatics (ICon EEI)*, (pp. 81-85). Batam – Indonesia.

Alieyan, K., Almomani, D., Abdullah, R., Almutairi, B., & Alauthman, M. (2020). *Botnet and Internet of Things (IoTs): A Definition, Taxonomy, Challenges, and Future Directions.* doi:10.4018/978-1-5225-9742-1.ch013

Alomari, M., El-Kanj, H., Alshdaifat, N., & Topal, A. (2020). A Framework for the Impact of Human Factors on the Effectiveness of Learning Management Systems. *IEEE Access*, pp. 23542-23558.

Amo-Filvà, D., Alier Forment, M., Peñalvo, G., & Fonseca Escudero, D. (2020). Protected Users: A Moodle Plugin To Improve Confidentiality and Privacy Support through User Aliases. *Sustainability*.

Anand, A., & Eswaran, S. (2018, July). CASE STUDY MOODLE Approach to Learning and Content Management System (LCMS). *International Journal of Computer Sciences and Engineering*, pp. 1147-1152.

Ayyad, Y. (2016, Feb). Security Concerns in a Web-Based E-learning Platform. *Electronics and Systems Laboratory (LES)، Faculty of Sciences, Mohamed First University*. doi:10.13140/RG.2.1.4633.5763

Brown, A., & Wilson, G. (2011). *The Architecture of Open Source Applications: Elegance, Evolution, and a Few Fearless Hacks.* LULU International Publishing.

Bucicoiu, M., & Tapus, N. (2013). Easy attendance: location-based authentication for students integrated with moodle. In IEEE (Ed.), *2013 11th RoEduNet International Conference.* Sinaia, Romania. doi:10.1109/RoEduNet.2013.6511761

data.bitcoinity.org. (2019, Jan). Average time to mine a block in minutes.

De Medio, C., Limongelli, C., Sciarrone, F., & Temperini, M. (2020). MoodleREC: A recommendation system for creating courses using the moodle e-learning platform. *Computers in Human Behavior*, p. 104.

Gayoso Martínez, V., Hernandez Encinas, L., Queiruga-Dios, A., Encinas, A., & Martin-Vaquero, J. (2013, 09). Avoiding Sensitive Information Leakage in Moodle. *Literacy Information and Computer Education Journal*, pp. 1422-1432. doi:10.20533/licej.2040.2589.2013.0190

Gil, R., Orueta, G., Tawfik, M., Garcia-Loro, F., Pesquera Martin, A., Sancristobal, E., . . . Castro, M. (2013). Fingerprint Verification System in Tests in Moodle. *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje*, pp. 23-30.

Haddad, Z., Taha, S., & Saroit, I. (2017, Nov). Anonymous authentication and location privacy preserving schemes for LTE-A network. *Egyptian Informatics Journal*, pp. 193 - 203.

Idris Khan, F., Javed, Y., & Alenezi, M. (2019, 11). Security assessment of four open source software systems. *Indonesian Journal of Electrical Engineering and Computer Science*, pp. 860-881. doi:10.11591/ijeecs.v16.i2.pp860-881

K, M., & Begam, B. (2020). Enhancing the Security in ElGamal Cryptosystem using Paring Functions. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, pp. 165-177.

Kim, S., & Chandra Deka, G. (2019). *Advanced Applications of Blockchain Technology- Studies in Big Data 60.* Springer International Publishing.

Kumar, N., Mitta, N., Thakur, P., & Srivastava, R. (2020). Analysis of Different Detection and Mitigation Algorithm of DDoS Attack in Software-Defined Internet of Things Framework: A Review. In *Recent Trends and Advances in Artificial Intelligence and Internet of Things* (pp. 597--607). Springer International Publishing.

Mahesh Kumar, M., V. N. K. Prasad, M., & Raju, U. (2020). BMIAE: blockchain-based multi-instance Iris authentication using additive ElGamal homomorphic encryption. *IET Biometrics*, pp. 165-177.

MoodleDocs. (n.d.). *Moodle Docs 3.9.* Retrieved 2021, from https://docs.moodle.org/39/en/Authentication", addendum = "(Last Modified: 5 December 2018, at 14:15)"

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, pp. 183 - 187.

Stallings, W. (2013). *Cryptography and Network Security:Principles and Practice.* Addison-Wesley.

vuldb. (n.d.). *MOODLE UP TO 3.7.1 INFORMATION DISCLOSURE.* Retrieved 08 12, 2020, from https://vuldb.com/?id.150277

World Health Organization (WHO). (May 2020). *Considerations for public health and social measures in the workplace in the context of COVID-19.*

Zahid, Z., Ali Zahoor, M., Khan, F., & Ali, E. (2016). LMS NUST concurrent session impact and solution. *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, (pp. 305-311). Islamabad, Pakistan. doi: 10.1109/IBCAST.2016.7429847