Volume: 8 Issue: IV Month of publication: April 2020
DOI:

Securing E-learning System using Hybrid Cryptosystem

Sahana V Torgal[1], Aditi Ravichandra[2]
[1]*Student, Department of Computer Science, Atria institute of technology, Bengaluru, India*
[2]*Asst. Professor, Department of Computer Science, Atria institute of technology, Bengaluru, India*

Abstract: E-learning is one of the foremost used approach to learn things and can be accessed easily through internet. Internet has now become a hotspot to many threats and attacks. As this system merely depends upon internet, securing this system from all types of threats has been a challenging factor. This paper presents about e-learning platform in which we aim to secure this platform. We implement the application of cryptographic techniques. By combining elliptic curve cryptography and Diffie-Hellman key exchange protocol, we introduce a new hybrid cryptosystem (3D Pake protocol). This cryptosystem is used for securing the e-learning system from all offline dictionary attacks and also provide a secure user authentication.

Keywords: E-learning, hybrid cryptography, information security, 3D pake protocol

I. INTRODUCTION

Now days people are easily being communicated with each other, specially through internet. With this growth, all other trending technologies can be accessed easily through internet. One among them is the education system which is also changing from their traditional practice to online education by introducing e-learning platform. Many organisations and institutions as introduced this platform so as to provide a promising learning for their employments and students. This platform provides a efficient learning to the beginners. It also makes use of audio and streaming videos to deliver the content to the learners.

E-learning system make use of large set of databases for storing study materials, course details and also user information. Privacy of this information is a concern these days as internet has been exposed to different types of threats and attacks. To put an end to these attacks cryptographic techniques has been used. Cryptography is an approach for hiding information from various third-party attacks.

Symmetric and Asymmetric key cryptography are the types of cryptography. Symmetric make use of same key for encryption and decryption but asymmetric make use of different keys i.e. public and private key. Hybrid cryptosystem is combination of two crypto techniques.

This combination enhances the overall security of the systems. It provides strong encryption and decryption methods. Therefore, this paper secures the information of e-learning system by using hybrid crypto algorithm which generates key, during the registration of each user.

II. LITERATURE SURVEY

In [1] Vijaya Patil, Aditi Vedpathak, Pratiksha Shinde, Vishakha Vatandar, Prof. Surekha Janrao published paper E-learning system using cryptography and data mining techniques which introduces a system which make use of elliptic curve cryptography for securing purpose and decision tree algorithm for classification purpose.

In [2] R. Krishnaveni, V. Pandiyaraju published paper A Secure E-Learning System and its Services which introduces securing e-learning system using elliptic curve cryptography and they suggested the use of vector machine algorithm for filtered web search engine.

In [3] Gaurav Yadav and Apana Majare published paper A comparative study of performance analysis of various encryption algorithms. Their paper discusses about the recent existing cryptographic techniques and also comparative analysis of the performance using different parameters in the algorithms.

In [4] M. M. Steven, and M. Bellovin, published paper Encrypted key exchange: Password-based protocols secure against dictionary attacks. They introduced the first pake protocol as Encrypted key exchange to secure the user passwords from vulnerable dictionary attacks.

In [5] K. Anitha Kumari, G. Sudha Sadasivam & L. Rohini published paper An Efficient 3D Elliptic Curve Diffie–Hellman (ECDH) Based Two-Server Password-Only Authenticated Key Exchange Protocol with Provable Security. This paper introduces about 3D pake protocol security analysis of the protocol which provides resistant to offline dictionary attacks.

III. CRYPTOGRAPHIC TECHNIQUES:

A. Elliptic Curve Cryptography

It is one among the public key cryptographic techniques. It is a practice based on algebraic structure of elliptic curves over finite fields. ECC generates smaller keys which provide an equivalent security compared to other non-EC cryptography. The advantages are speed and smaller keys.

B. Diffie-Hellman key Exchange

It is the first public key protocol. It is an approach of exchanging cryptographic keys securely over a public channel. The advantages are there is no requirement of prior knowledge about both sender and receiver. The sharing of the secret key is safe.

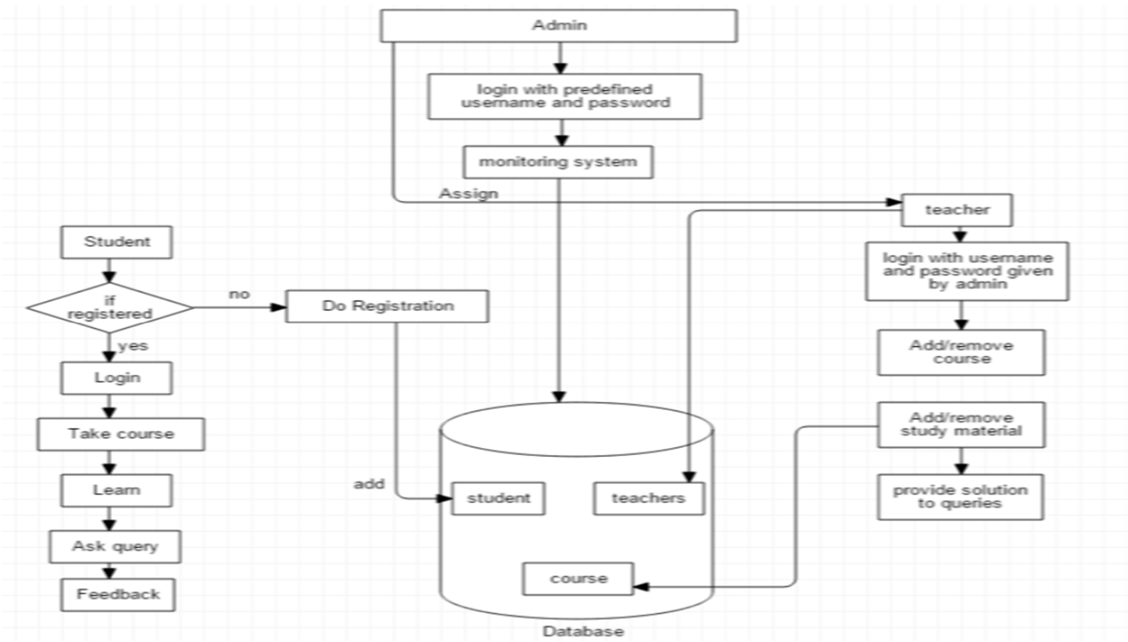


Fig 1. System design

IV. PROPOSED SYSTEM

The e-learning system design is depicted in figure 1. The overall system contains three important attributes student, admin and teacher. The security system for user authentication i.e. for student and teacher is as follows:

A. 3D Elliptic curve Diffie-Hellman Pake Protocol

The ECC encryption scheme interpretation under the decisional Diffie-Hellman assumption is more shielded as encrypting the same message a few times, produce unique cipher texts. Non identical plain texts at many cases in the similar manner will produce an identical cipher text for which the attackers/hackers may find difficulty in decrypting the cipher text to obtain the plain text.

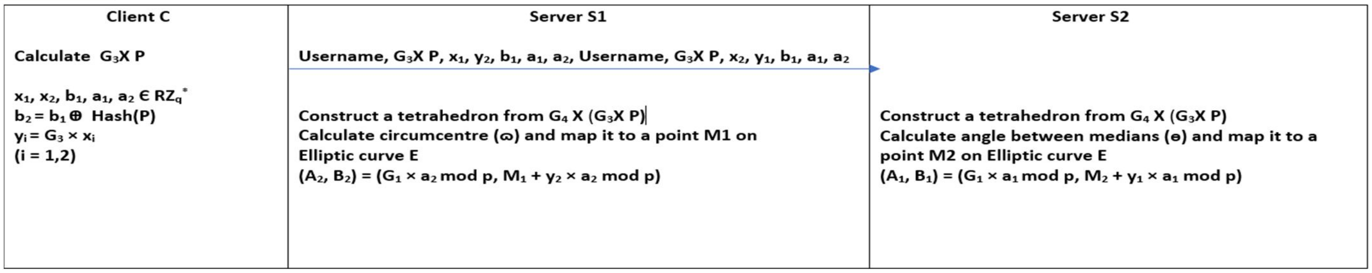
3D PAKE protocol is a hybrid cryptographic algorithm that requires two servers for authentication; one server engages with clients and the other is hidden from the clients [5].

B. Architecture

The proposed security system for e-learning involves three phases, namely initialization, registration, authentication and key exchange

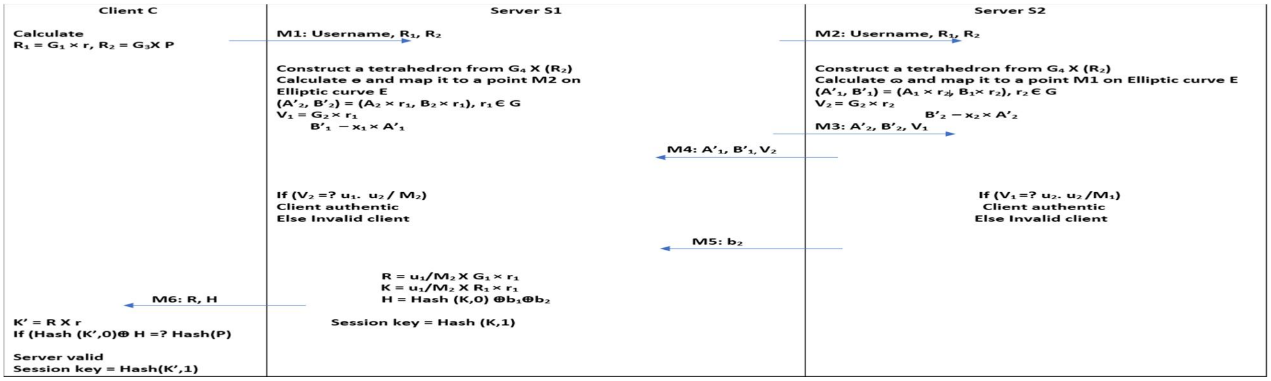
Commonly used notations in the 3D PAKE protocol are: [5]

1) Zq*-group G of large prime order q
2) E-elliptic curve defined over a finite prime field Fp
3) p-a large prime number
4) a, b-two parameters in Zp satisfying 4a3+27b2 mod q not equal to 0
5) Ep (a, b)-an elliptic curve over GF(p) containing a set of points (x, y) satisfying that y2 = x3 + ax + b (mod p)
6) G1; G2; G3; G4 -base points of order q over Ep (a, b), where q is a large prime number



Client C	Server S1	Server S2
Calculate G_3X P $x_1, x_2, b_1, a_1, a_2 \in RZ_q^*$ $b_2 = b_1 \oplus$ Hash(P) $y_i = G_3 \times x_i$ (i = 1,2)	Username, G_3X P, x_1, y_2, b_1, a_1, a_2, Username, G_3X P, x_2, y_1, b_1, a_1, a_2 Construct a tetrahedron from G_4 X (G_3X P) Calculate circumcentre (ϖ) and map it to a point M1 on Elliptic curve E $(A_2, B_2) = (G_1 \times a_2 \bmod p, M_1 + y_2 \times a_2 \bmod p)$	Construct a tetrahedron from G_4 X (G_3X P) Calculate angle between medians (ɵ) and map it to a point M2 on Elliptic curve E $(A_1, B_1) = (G_1 \times a_1 \bmod p, M_2 + y_1 \times a_1 \bmod p)$

Fig 2. Registration Module



Client C	Server S1	Server S2
Calculate $R_1 = G_1 \times r, R_2 = G_3X P$	M1: Username, R_1, R_2	M2: Username, R_1, R_2
	Construct a tetrahedron from G_4 X (R_2) Calculate ɵ and map it to a point M2 on Elliptic curve E $(A'_2, B'_2) = (A_2 \times r_1, B_2 \times r_1), r_1 \in G$ $V_1 = G_2 \times r_1$ $B'_1 - x_1 \times A'_1$	Construct a tetrahedron from G_4 X (R_2) Calculate ϖ and map it to a point M1 on Elliptic curve E $(A'_1, B'_1) = (A_1 \times r_2, B_1 \times r_2), r_2 \in G$ $V_2 = G_2 \times r_2$ $B'_2 - x_2 \times A'_2$ M3: A'_2, B'_2, V_1
	M4: A'_1, B'_1, V_2	
	If (V_2 =? u_1. u_2 / M_2) Client authentic Else Invalid client	If (V_1 =? u_2. u_2 /M_1) Client authentic Else Invalid client
	M5: b_2	
M6: R, H	$R = u_1/M_2 X G_1 \times r_1$ $K = u_1/M_2 X R_1 \times r_1$ $H = Hash (K,0) \oplus b_1 \oplus b_2$ Session key = Hash (K,1)	
K' = R X r If (Hash (K',0)$\oplus$ H =? Hash(P) Server valid Session key = Hash(K',1)		

Fig 3. Authentication and Key Exchange Module

a) x1; x2 -private keys belong to RZq*

b) y1; y2 -public keys

c) b1; a1; a2; r; r1; r2 belong to RZq*

d) P-user’s password

e) b2=b1 □Hash (P)

f) K - secret key

g) ɵ-angle between the medians of the tetrahedron

h) ϖ-circumcentre of the tetrahedron

i) Hash ()-secure one-way hash function [5]

i) *Initialization Phase:* An elliptic curve E_p (a, b) of order n and a base point p, which satisfy the Equation $4a^3+27b^2 \bmod p \neq 0$ [5] is chosen by the servers S1 and S2. Both servers mark a point (G_1) on the curve E_p and randomly selects an integers x_1 by S1 and x_2 by S2. Then S1 computes $G_1 \times x_1$ and S2 computes $G_1 \times x_2$. They also decide a hash function “Hash”. Then they are provided with the password shares b_1 and b_2. ϖ is circumcentre of tetrahedron whose ECC encryption is given to S1 and it is mapped on point M_1 on elliptic curve. ɵ is angle between medians of tetrahedron whose ECC encryption is given to S2 and it is mapped on point M_2 on elliptic curve. Thus, the servers publish all the public parameters which were calculated above.

ii) *Registration Phase:* At start, the client decides upon on a password P and then calculates G_3X P. It also chooses it decryption key x_i and compute the encryption key y_i for the server S_i where i=1,2. In addition to this it selects b_1 and computes b_2. Lastly it transfers its information i.e. username, G_3X P, x_1, x_2, b_1, b_2, a_1, a_2 to both servers S1 and S2 as shown in fig 2. Server S1 encrypts ϖ and server S2 encrypts ɵ with the encryption key of S2 and S1 respectively through equations as depicted in fig 2. Thus, S1 inputs the values A_2, B_2, x_1, a_1, b_1 in its database. Similarly, S2 also inputs the values A_1, B_1, x_2, a_2, b_2.

iii) *Authentication and Key Exchange Phase:* After the registration is successful, the client and the servers are ready for the mutual authentication process. Firstly, the client starts the process by sending a request message to server S1, which is then transferred to S2 by S1. Upon receiving the request, the S2 will transfer back the authentication information stored its database to S1. Both servers then construct a tetrahedron using the requested message. Therefore, S1 compute ϖ and S2 compute ɵ and verifies with their stored values in the database. After successful verification, S2 sends the parameters needed for generation of key to S1. Upon receiving the parameters, S1 computes its secret key and later send its parameters for key generation to the client. In similar manner, client justify its authentication with the servers and also compute its secret key comparable to key of S1. Thus, computation part of the authentication procedure is depicted in fig 3.

V. CONCLUSION

E-learning system is now a trending approach adopted by educational institutions and many other organisations.

As of rapid growth of this system, security concerns become a challenge as to secure the study materials, courses and user information. As internet is vulnerable to many threats and attacks. E-learning platform which can be accessed using internet can also to vulnerable to these attacks.

Security from such attacks is provided for the system using hybrid crypto methodology. Hybrid cryptosystem basically involves the combination of two crypto techniques. As mentioned, 3D Elliptic curve Diffie-Hellman pake protocol is

A hybrid cryptographic algorithm which uses two servers for authentication among which one is hidden from the clients.

This proposed system is invulnerable to offline dictionary attacks as it provides strong user authentication for system. As it a combined model it provides a very strong encryption and decryption methods. Thus, user can access the E-learning system with an invulnerable and strong user authentication.

REFERENCES

[1] Vijaya Patil, Aditi Vedpathak, Pratiksha Shinde, Vishakha Vatandar, Prof. Surekha Janrao “E-learning system using cryptography and data mining techniques”, International Research Journal of Engineering and Technology e-ISSN: 2395-0056 p-ISSN: 2395-0072 Volume: 05, Issue: 01, Jan-2018.

[2] R. Krishnaveni, V. Pandiyaraju “A Secure ELearning System and its Services”, International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106 Volume- 1, Issue- 4, June-2013.

[3] Gaurav Yadav and Aparna Majare “A comparative Study of Performance Analysis of Various Encryption Algorithms”, International Conference on Emanations in Modern Technology and Engineering 2017.

[4] M. M. Steven, and M. Bellovin, “Encrypted key exchange: Password-based protocols secure against dictionary attacks,” in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA,1992.

[5] K. Anitha Kumari, G. Sudha Sadasivam & L. Rohini “An Efficient 3D Elliptic Curve Diffie–Hellman (ECDH) Based Two-Server Password-Only Authenticated Key Exchange Protocol with Provable Security”, IETE Journal of Research, ISSN: 0377-2063 25 Apr 2016.