Journal of Engineering and Applied Sciences 13 (10): 3525-3533, 2018
ISSN: 1816-949X

Attribute Based Authentication System using Homomorphic Encryption

Marwan Majeed Nayyef, Ali Makki Sagheer and Sarah Shihab Hamad
Department of Computer Science, University of Anbar, Al-Anbar, Ramadi, Iraq

Abstract: Authentication is the first defense line of user attributes protection and an important process to ensure basic security objectives such as confidentiality and integrity. Any user has specific attributes and all user's attributes (data) must be encrypted before stored in the database at the server, so that, no one can access to those attributes even service provider that are considered sensitive information, the difficulty lies in processing data without knowing its content to solve this problem, homomorphic encryption is proposed for authentication process because of it can deal with the encrypted text without the need for decryption and HE creates a common factor that is generated from the original text and its cipher text for matching common factor to access to the system. In this study, proposed elliptic curve algorithm based on HE to encrypt user's attributes.

Key word: Homomorphic encryption, authentication system, elliptic curve cryptography, HE, authentication process, common factor

INTRODUCTION

Information security is one of the most significant processes for protecting information and preventing unauthorized persons to reach the sensitive information in any form of attacks such as use, modification, disclosure, inspection or disruption) and this information must be accessed by the user who owned it only (Huda *et al*., 2015).

Therefore, there is a significant correlation between information security and cryptography in terms of exchange services for protection such information confidentiality, information integrity and information availability. Cryptography provides information security, especially for useful practical applications as well as involving encryption, digital signature, message digests and what added the biggest strength of encryption is the length and the strength of the encryption keys that are an important mechanism (Alia *et al*., 2014).

The encryption strength depends directly on the strength of the keys used in the encryption and decryption and those keys must be protected in a way to prevent unauthorized access to their in addition to making key available to the user when needed. If the key is short or weak this leading to produce weak encryption and vice versa. As well as the keys that have been generated must provide it the protection with the same importance to other confidential information it must be protected from disclosure and to be available when needed (Bethencourt *et al*., 2007). In this study, key generation depends on the elliptic curve, so, the key strength depends on the ECDLP. Cryptography enters and contributes in the field of computer science, especially in the field of computer and network security for access control and information confidentiality (Alia *et al*., 2014).

Literature review: By Tebaa *et al*. (2012) new scheme introduced for maintaining the confidentiality of the data in the cloud computing without knowing their meaning, so, it can be implemented using homomorphic encryption, in this study, a number of algorithms traditional proposed (Paillier and RSA) on the basis of homomorphic encryption which has been successfully implemented, according to information that has not been identified even by the service provider and deals with them in an encrypted form (Tebaa *et al*., 2012).

By Chauhan *et al*. (2015), proposed a method depending on solving the problem of traditional encryption method which provides security for data in transmission and storage state but when dealing with those data in order to processing and performing operation, data will be decrypted. This state is considered as problem because the data is available to the service provider to solve that problem, PHE methods are proposed in order to processing data without decryption, in this case, PHE provides high security for data stored in cloud because It prevents anyone including the service provider from knowing the original text (Chauhan *et al*., 2015).

Sharma (2016) creates a voter system in 2016 in order to solve the problem of the time consuming, obstruction and disruption which may happen, the development of Information Technology led us to propose e-Voting system to solve all these problems, e-Voting system

Corresponding Author: Marwan Majeed Nayyef, Department of Computer Science, University of Anbar, Al-Anbar, Ramadi, Iraq

helps us to vote from any place. In this study an e-Voting system proposed based on Paillier Homomorphic Encryption scheme in order to provide security for those systems through processing and transferring data in ciphertext form. The e-Voting system was executed successfully and contributed to data security which transfers over the internet and also ensures efficiency, privacy, universal verifiability and no vote duplication (Sharma *et al*., 2016).

By Suveetha and Manju (2016) proposed banking application for data security. The bank contains a large number of customer information that is confidential and must no one can access that information, so, it should preserve the confidentiality of the data. In this study, paillier HE is achieved to apply operation on encrypted banking information because HE allows performing a calculation on ciphertext without using a secret key. In this scheme, security and confidentiality of data is performed within the homomorphic encryption (Suveetha and Manju, 2016).

By Zamare and Phursule (2014) proposed a secure system based on password-based Authentication method to authenticate client and server, the key is distributed using DH and ElGamal algorithm, In the use of a single server structure, passwords are stored in one server. If the server is attacked by the intruder, the intruder may get passwords. To solve this problem, they suggested using two servers where the passwords are divided into two parts, each part stored in one of the two servers. This protocol is efficient and the cost effectiveness is the parallel execution of the servers which are during the registration and authentication stage, this system requires less execution time because of parallel execution of tow server and also increase efficiency due to the security against active and passive attack (Zamare *et al*., 2014).

By Burande and Kahate (2015) they suggest new system authentication based on password authentication protocol instead of using one server to store the data, two servers were used to avoid the breach that might occur. In this study, The ElGamal algorithm and DH are used. In two servers which are used for authentication, the backup services are provided for the purpose of continuing the service, the authentication of client information on the server one is kept with backup on server two and vice versa if one of the two servers shut down because of some reason, the other server must still provide services to the client. This protocol provides a safety against active and passive attack as well. Cryptography of Elgamal and DH algorithms are essential for a technique of encryption and decryption (Burande and Kahate, 2015).

By Sujatha *et al*. (2015), suggested new authentication system depends on speaker recognition. Security systems based on password must provide privacy and authentication privacy. So, the design of the system with high-security authentication and strong privacy protection is still an open problem due to weak passwords, in this study, voice password is depended as a password for authentication which done using neural network instead of using text-password. Biometric identification system focused around distinguish of automatic speaker is a security framework to allow clients to access machine frames (Sujatha *et al*., 2015).

Cryptography: Cryptography is one of the most important aspects in the field of computer security and it's a way for the transfer of confidential information and data during open network communication. Therefore who owns the secret key can read the message after converting it to the original text the information may be documents, images, phone conversations or any other data (Alia *et al*., 2014). Cryptography that is used for Information security to convert information to the form which is not readable by unauthorized user, this form is called encryption. While encrypted information can bring it back to the original text that can be read by the person allowed him and who owns the encryption key, this is called the decryption (Bethencourt *et al*., 2007).

Types of cryptographic algorithms (Fig. 1) Edited by Sen (2014) secret key cryptography: In private key both of encryption and decryption use one key and must be the same key which called symmetric encryption, so the sender can encrypt the message with a certain key while at the receiver the same key used to decrypt the ciphertext to get the original text.

Public key cryptography: This type of encryption depending on two keys, one for encryption that called public key and the other for decryption that called secret key which used for the purpose of confidentiality, non-repudiation, authentication and key exchange (Sen, 2014). The two keys are related mathematically and even if we know one of the keys it is difficult to know the other, so, the plaintext is encrypted with one key and the ciphertext is decrypted with the second key because of the cryptography required pair of keys, this process called asymmetric cryptography the public key must be available at any time for anyone while the secret key must be remain kept confidential and only authorized user can use it for decryption (view the message) (Suveetha and Manju, 2016).

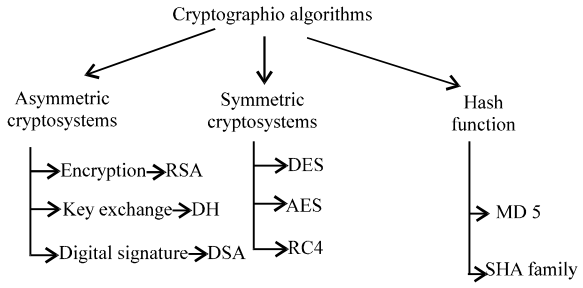

Fig. 1: Three types of cryptographic algorithms

Hash functions: It is generated by mixing a different data size to get a new output called message digest and cannot return the mixture to the original state, therefore changing any bit or bits in the input leading to the high change in the hash code and its purpose is to maintain the integrity of the data. There are many techniques of a hash function such as MD5 and SHA family.

MATERIALS AND METHODS

Attribute Based Encryption (ABE): ABE is dealing with multiple attributes, user attributes deemed sensitive data and need to be more secure when used for authentication, Attribute-Based Encryption (ABE) is a mechanism which working on the basis of the public key where the encryption and decryption process possible based on attributes of user, cipher text and user's secret key typically rely on the attributes, decrypted cipher text and obtain the original text occur only if the set of cipher text attributes equivalent to the set of secret key attributes of the user, so the process of decryption be possible if the number of matching is meets the threshold value (Suveetha and Manju, 2016). For example, ABE is more complex in the decryption process because of only who has a secret key that matches to name: = Marwan AND Age: <28 and address: = Baghdad" who can decrypt. ABE is suitable for many applications so that each user has a unique secret key which was obtained by the attributes associated with it (Huda *et al*., 2015). Table 1 shows the set of attributes.

Homomorphic encryption: By Rivest *et al*. (1978) are first researchers who suggest the Homomorphic Encryption (HE) on the basis of RSA algorithm which was homomorphically on the multiplicative operation. With progress in 1982 Goldwasser and Silvio another algorithm is suggested called Goldwasser that is homomorphic on. In 1999, Paillier also suggested a secure encryption system that was homomorphically with addition operation as well as other algorithms such as Elgamal which homomorphic on multiplication operation (Rivest *et al*., 1978; Benzekki *et al*., 2016; Chauhan *et al*., 2015). And continued in this case until 2005 when the researcher Dan Boneh, EU-Jin Goh and Kobbi Nissim perform the first homomorphic encryption scheme using two operations which have the unlimited number of additions and one multiplication (Dasgupta *et al*., 2016). HE allows for any persons to use a specific mathematical operation applied to the ciphertext to getting results to be the same results if the same operation has been applied to the original text. HE concept is shown in the following Fig. 2.

Table 1: Set of attributes

Attributes	Values
Full-name	First name, middle name, Last name
Identity number	AB-12345678
Phone number	071-12547158
Address	Baghdad-altajee 1-2-3 No. 2
Email	mmn@gmail.com
Place of birth	Baghdad, Basra
Age	30, 2
Birthdate	01-10-1992
Gender	Male, Female
Position	President, Director
Location	1st f4 D2 building

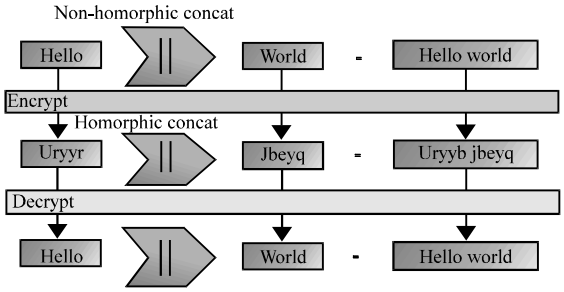

Fig. 2: Homomorphic encryption

Homomorphic encryption functions: Homomorphic encryption HE contains four functions, HE (key generation, encryption, decryption and evaluation.

Key generation: At client each of the secret an public-key are generated (sk, pk) = Key gen (k) where k is parameter security.

Encryption: It is the encryption function used to produce ciphertext© by using secret key sk and plain text (m), c = Enc (sk, m).

Evaluation: The server uses a function f for evaluating the ciphertext and it's doing by using f and pk, Eval (f, pk, c) where $c = (c_1, ..., c_{tn})$ and n refer to the number of inputs of the circuit (Chen *et al*., 2014; Gentry, 2009). Therefore, Dec (sk, Eval (f, pk, c)) = C (m_1, m_2, ..., m_t) where C is a computation which perform in the client.

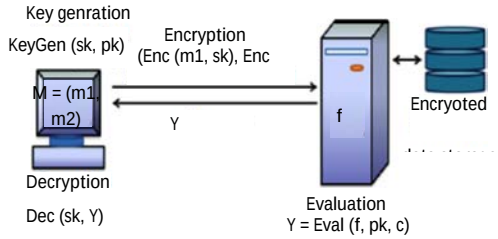

Fig. 3: Homomorphic encryption functions

Decryption: Is a function used to obtaine the original text by using secret key m = Dec (c, sk), Dec (sk, Eval (f, pk, c)) (Fig. 3).

Properties of homomorphic encryption: There are two properties of HE additive and multiplicative HE, therefore with Additive HE. Enc (pt_1+pt_2 mod n) = Enc (pt_1)+Enc (pt_2) mod n. With multiplicative HE, Enc (pt_1*pt_2 mod n) = Enc (pt_1)*Enc (pt_2) mod n (Filho *et al*., 2016).

Authentication system: The rapid development of the internet and the systems that run on the internet, there are many users who research on those systems which containing confidential information, require the authentication process and before entering into those systems must verify the identity their entity (may be a person, program, ..., etc.) for accessing system (Manjua *et al*., 2014).

Authentication is an important process to validate of user's identity whether is allowed to access or not in order to keep sensitive information that must be accessed by authorized users, so, the mechanism is that the credentials of a certain users are compared with other credentials on file in a database of user that we need to validated him, this comparison may be happening locally (in the operating system) or globally when credentials are stored in authentication server, if the credentials are matching, the system reply a value which represents authorization for the user (Lee *et al*., 2008).

Most of the research in the security authentication field must supply at least two elements in order to say that is a positive authentication and the best to be three elements, so the three classes of authentication with some elements are (Alia *et al*., 2014).

Something knowledge: This type depending on some factors that are remember such as (password or called a Personal Identification Number (PIN), the answer to the question (security question).

Something owner: Something possessed by the user, such as (smart card, security token, software token).

Something inherent: Many of characteristics are found such as (Biometric) face detection, fingerprint, DNA, voice, signature or retinal pattern) (Lee *et al*., 2008). Because of many of the risks associated with the certain system, we need different levels of protection, so we must build security levels commensurate with the levels of risk and finally the build of authorization system that worked on the specific needs of the application system (Manjua *et al*., 2014).

Password authentication method: At present, most systems rely on id/password in identification and authentication process (Alia *et al*., 2013). Password authentication is one of the common methods used for authentication of user. user authentication is an interaction take place between human to computer and the process used in systems that are relying on the attribute of users such as password, the application must provide registration (log in) form, user's attribute data are captured, then processed and stored in the database. After the registration process when a specific user wants to access the system, he must first verify the identity based on his password that is compared with the value stored in the system (Manjua *et al*., 2014). This type of authentication is easier because of the ease of memorizing. Recently, there have been two types of a password is that textual and graphical (Alia *et al*., 2012).

RESULTS AND DISCUSSION

Elliptic curve cryptography: Elliptic curve cryptography is a public-key cryptography algorithm which is based on the structure of algebraic and discrete logarithms of an elliptic curve over finite fields. When Elliptic Curves (EC) are defined, there are two types of a finite field is prime field Fp and binary fields F^2m where p is a large prime numbern our research, prime fields Fp is adopted (Sunuwar *et al*., 2015; Patel *et al*., 2014). It is known for the key sizes of ECC are smaller, faster encryption, better security and more efficient for the same level of security compared with other systems of public cryptography (such as RSA). There are several algorithms can be encrypted by using ECC (like Elgamal), a secure key exchange (Diffie-Hellman of ECC) and also digital signatures validation and authentication (Sunuwar *et al*., 2015).

Elliptic Curve Discrete Logarithm Problem (ECDLP): One of the very interesting open problems in cryptography is the understanding of a trapdoor on the discrete logarithm in order to solve the DLP is hard only if declared parameters are used while it is easy by using a private key (trapdoor key) (Sagheer *et al*., 2012).

Definition 1 (DLP): For specific group G, let x, y belongs to G, recall that in the DLP is how to find an integer a belong to Z, so that, $x^a = y$ (Sagheer *et al*., 2012). The DLP can be used on many finite groups as well as the multiplicative group over a prime filed Fq, this idea can be increased to arbitrary groups and especially for elliptic curve groups (Patel *et al*., 2014).

Definition 2: (ECDLP): An elliptic curve EC, let P, Q belongs to EC and in the ECDLP is how to find integer k where (0<k<n), if Q = kp (Sagheer *et al*., 2012). So that, EC is an elliptic curve over a specific finite field Fq, P is point of order n on EC. ECDLP on EC is how to find k where (1<k<n), if there is such a right, so (Chauhan *et al*., 2015). Q = kP. Where kP = P+P+, ..., +P K-time.

Elliptic curve over prime field

Definition 3: Let q refer to the prime number an elliptic curve EC over a prime field Fq is given in the following Eq. 1:

$$EC: y\ 2\ (mod\ q) = x3 + ax + b\ (mod\ q) \quad (1)$$

Where a, b∈Fq and must satisfy the equation that: $4a^3+27\ b^2 \neq 0$ (mod p), so, the group of elliptic curve points E(Fq) are generated when all points of (x, y) satisfy the Eq. 1 of elliptic curves with a point 8 (called the point at infinity) (Dawahdeh *et al*., 2015; Patel *et al*., 2014).

Arithmetic on elliptic curve

Addition and doubling point

Point addition: Assume that $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ where $x_1 \neq x_2$ means that P_1+P_2 and P_1, P_2 are two points on an elliptic curve EC defined in Eq.1. The summation of $(P1 + P_2)$ generates another point P_3 also on elliptic curves. Add two points on elliptic curve are depending on some conditions shown in the following (Sagheer *et al*., 2012): If $P_1 \neq P_2$ with $x_1 = x_2$ and $y_1 \neq y_2$ then $P_1+P_2 = O$. If $P_1 \neq P_2$ with $x_1 \neq x_2$ and then the sum of P_1 and P_2 is defined by:

$$P_1+P_2 = P_3 = (x_3, y_3) \quad (2)$$

Where:

$$\lambda = \frac{(y_1-y_1)}{(x_1-x_1)} \quad (3)$$

$$x_3 = \left(\lambda^2 - x_1 - _{x2}\right) \bmod p \quad (4)$$

$$y_3 = (\lambda(x_1-x_3)-y1) \bmod p \quad (5)$$

Point doubling: Suppose that $p = (x_1, y_1)$ is a point on EC, so adding any point with itself called doubling point on an EC which defined by Dawahdeh *et al*. (2015):

$$P_3 = P_1+P_1 = 2\ P_1 \text{ and } P_3 = (x_3, y_3) \quad (6)$$

Where:

$$\lambda = \frac{(3\ (2\ x_1)+a)}{(2y_1)} \quad (7)$$

$$x_3 = \left(\lambda^2 - 2x_1\right) \bmod p \quad (8)$$

$$y_3 = \lambda\ (x_1-x_3)-y_1 \bmod p \quad (9)$$

Point multiplication (scalar multiplication): Point multiplication considered as the dominant cost in the cryptography of elliptic curves and it controls the time of implementation of elliptic curve cryptography, particularly the representation ECDLP (Abbas *et al*., 2016) (Fig. 4).

Definition 4 (multiplying an integer number with a point on an EC): Let P_1, P_2 are two points on an EC, k∈Z then $P_2 = kP_1 = P_1\ P_1+, \ldots, +P_1$ (k times).

The proposed authentication system: The system is an authentication system that enables users to access the contents of the system in a secure manner and keep user's attributes from any breach or unauthorized access, so that, no one can access user attributes except service providers (access all attributes but with encrypted form) which are considered sensitive information to maintain privacy and only the user who owns the password (secret key) can access to the system.

The encryption is done by submitting user's attributes and sending them via. a secure channel (SSL) to the server to encrypt all user attributes and stored in server storage which are accessed during login phase by the user without decryption using the homomorphic encryption to be protected user's privacy.

The authentication process occurs when the client wants to login to the system as described in the following steps. When the client needs access to the system, the server asks authentication from a client, the client shows a dialog box asking for the username and password for the server. The client sends his identity username and password over the network (over the SSL connection). The server receives the username and password from the client and is given to the homomorphic encryption function to obtain the output and in the same time search for the encrypted username and password in the local

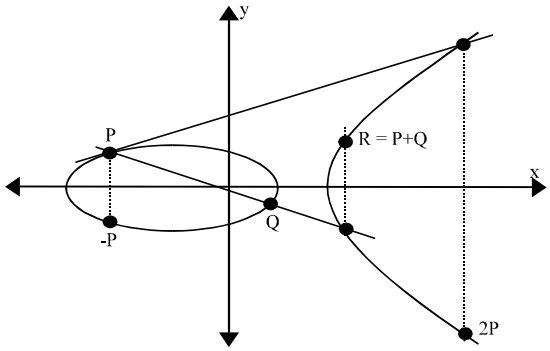

Fig. 4: An elliptic curve and the point addition and point doubling operations on this curve

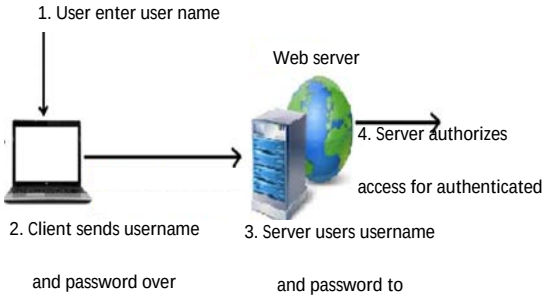

Fig. 5: General system model

database and given the encrypted results to the homomorphic encryption function to obtain the output, if the output is matched, the user's identity is accepted as evidence authenticating. The server shows whether the user is allowed access to the required resources or not if so, the client can access it. Figure 5 explain the general system model.

Registration phase: The system consists of a set of design interfaces and in order for users to access the system who is located on the server through the link, initially the user must enter to the registration page for the purpose of registration in the system (Greeshma *et al*., 2015) as shown in the following Fig. 6.

During the registration process, new users can be added to the user's table on the server. The registration process includes the recording of the user's attributes in this system some of attributes depended such as the user name, email, gender, address, phone number and password.

The proposed model: In this model, the key is generated depending on the combination of username and password then all user attributes are encrypted before storage except the password (pass) which get the output of SHA 1 then encrypted and store all encrypted attributes (C) at server storage as in Fig. 7.

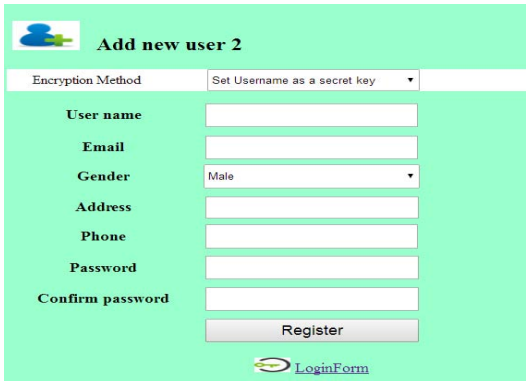

Fig. 6: Registration form

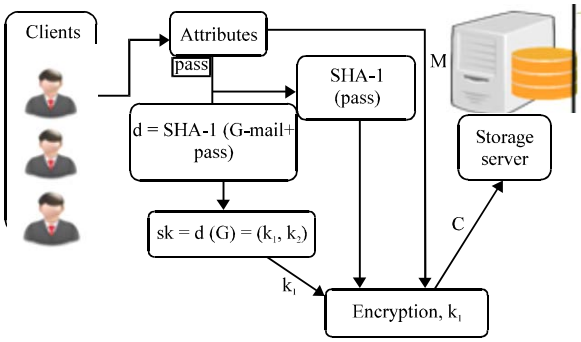

Fig. 7: The proposed model

Security model: The security of the authentication system depends on cryptography of elliptic curve which used Elliptic-Curve Discrete Logarithm Problem (ECDLP) for key generation.

Security model depends on the proposed algorithm

Key generation:

- d = SHA-1 (username+password)
- k = d (G) whe re G is the base point, so, G = (x, y)
- $k = (k_1, k_2)$
- We depend k_1 as the secret key, $sk = k_1$

Encryption:

- Convert attributes chars (M) and SHA-1 (password) to ASCII where $M = (m_1, m_2, \ldots, m_n)$
- $c_i = m_i k_1$
- C is the output of all encrypted attributes

Decryption:

- $m_i = c_i KI^{-1}$
- M is the output of all decrypted attributes

Login phase (authentication): The process of logging into the system is obtained when the user who previously registers in the system wants to access system resources by requesting the login page as in the following Fig. 8.

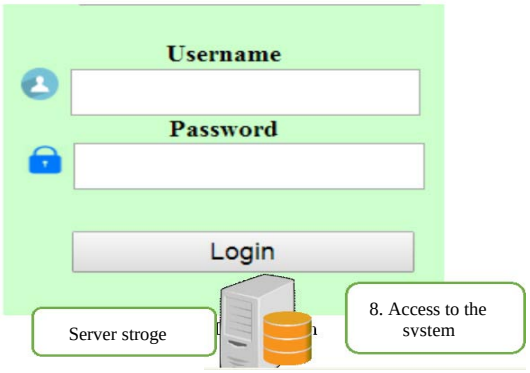

Fig. 8: Login form

Steps of user authentication:

- After user registration, a user logs on to the system through the login page
- After a dialog box appears, the user is required to enter the username and password to log in
- The username and password are sent to the server via. a secure channel SSL
- Secret Key (sk) is generated by using a password which combines with username to be passed through SHA-1 to get (d) that is multiplied with a Base Point G = (x, y) to get the secret key point (k_1, k_2), in this paper k_1 is depends as a private key
- This is authentication stage which is done according to Homomorphic encryption HE, the username and password are combined (UNpt+Ppt) then evaluated to obtain an output (outpt)
- The encrypted username and password (UNct, Pct) are retrieved from the database located at the server and combine (UNct+pct) then evaluated using HE to get another output (outct)
- Matching each of (outpt and outct) where the outpt is a value which refers to the plaintext of the combine (username+password) after computation, outct refers is a value which refers to the homomorphic computation of combined ciphertext (UNct+Pct), then finally matching (outpt and outct)
- Log in to the system if the values match else reject (Fig. 9)

Example of authentication system: If UserName(UN) = Marwan 90 and password = 19 Mmnr 90 the authentication process show as in the Fig. 10.

Algorithem:

Step 1: Generate a random number (d)
Step 2: generate a secret key
sk = d*G(gx, gy) = (k_1, k_2)
Set k_1 as a secret key used for encryption
Step 3: Encryption of username and password
Step 4: Authentication Process based on Homomorphic Encryption (APHE)
Step 5: Matching of outpt and outct for login
Step 6: If the matching is true, access to the system else reject

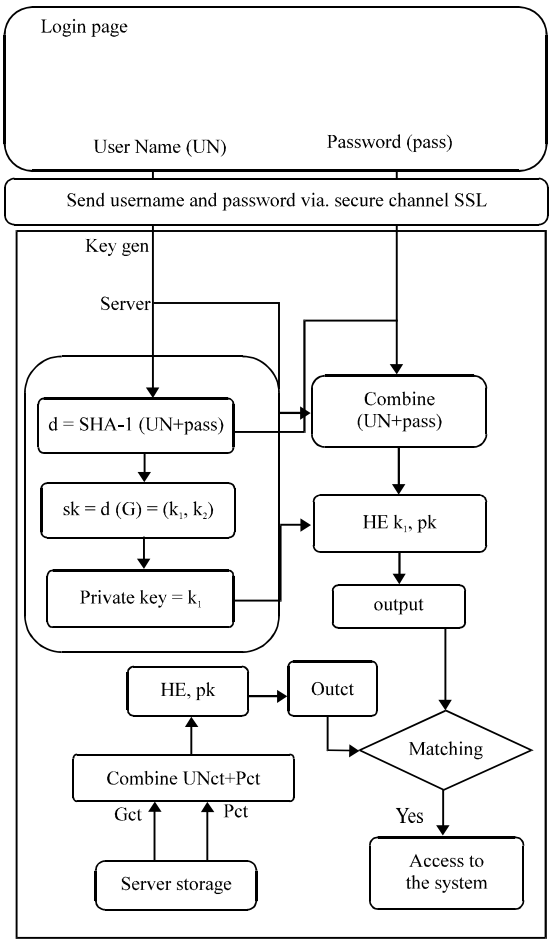

Fig. 9: Authentication model

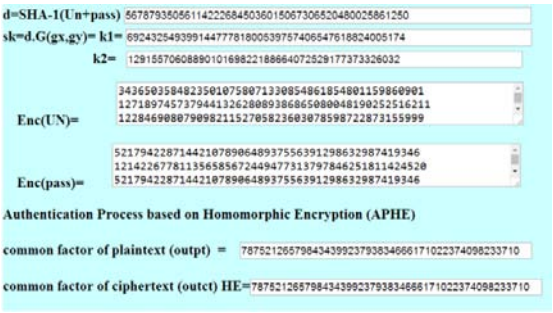

Fig. 10: Authentication Process Based on Homomorphic Encryption (APHE)

Implementation time: In this study, more than one implementation are doing, therefore, Table 2 represent number of implementation.

Security of elliptic curve cryptography: ECC is one of the powerful and efficient asymmetric algorithms for the given key length and it is attractive, particularly for security

Table 2: Execution time for authentication

Username (UN)	Password	Execution time (msec)
Marwan 90	19 Mmmm 90	22
Mohammedsalem70	Msalem 123123	30
OmerFalah 55	Mfmfmfl 23456	26
AhmedObiadNazzal 88	Ahmed 19881988	34

Table 3: Comparison between ECC and RSA

ECC(bits)	RSA (bits)	Key Size Ratio (ECC/RSA)
106	512	1:5
160	1024	1:6
256	2048	1:8
384	7680	1:20
512	15360	1:30

applications where it limited in power calculation and integrated circuit area, e.g., PC cards, wireless devices and smart cards.

The security of the ECC algorithm depends on the difficulty of ECDLP. ECC currently appears to be implemented on a 160 bit to provide nearly the same security level against the attacks of hackers compared with key length 1024 bit in RSA. This variation in the length of the keys has led to improve and speed in performance and less storage requirements, Table 3 present the comparison between ECC and RSA in terms of size of key length and strength (Abbas *et al*., 2016).

CONCLUSION

The use of Homomorphic Encryption (HE) in the authentication process provided great protection for user attributes that became completely encrypted and no one could know the information even if the server database was hacked by Hacker, since, they could not obtain known information except encryption and also homomorphic encryption is a true option in the process of authentication where it was implemented successfully and gave results and strong security to maintain the privacy of users.

REFERENCES

Abbas, S.A. and A.A.B. Maryoosh, 2016. Data security for cloud computing based on Elliptic Curve Integrated Encryption Scheme (ECIES) and Modified Identity based Cryptography (MIBC). Intl. J. Appl. Inf. Syst., 10: 7-13.

Alia, M., A. Tamimi and O. Al-Allaf, 2013. Integrated system for monitoring and recognizing students during class session. Int. J. Multimedia Applic., 5: 45-52.

Alia, M.A., A.A. Hnaif, H.K. Al-Anie and A.A. Tamimi, 2012. Graphical password based on standard shapes. Sci. Ser. Data Rep., 4: 71-79.

Alia, M.A., A.A. Tamimi and O.N. AL-Allaf, 2014. Cryptography based authentication methods. Proceedings of the World Congress on Engineering and Computer Science Vol. 1, October, 22-24, 2014, International Association of Engnring, San Francisco, California, USA., ISBN:978-988-19252-0-6, pp: 1-6.

Benzekki, K., A.E. Fergougui and A.E.B.E. Alaoui, 2016. A secure cloud computing architecture using homomorphic encryption. Intl. J. Adv. Comput. Sci. Appl. IJACSA., 7: 293-298.

Bethencourt, J., A. Sahai and B. Waters, 2007. Ciphertext-policy attribute-based encryption. Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07.), May 20-23, IEEE, New York, USA., ISBN:0-7695-2848-1, pp: 321-334.

Burande, N.S. and S.A. Kahate, 2015. Design model for two server password authentication protocol. Intl. J. Sci. Eng. Comput. Technol., 5: 383-384.

Chauhan, K.K., A.K. Sanger and A. Verma, 2015. Homomorphic encryption for data security in cloud computing. Proceedings of the 2015 International Conference on Information Technology (ICIT), December 21-23, 2015, IEEE, Bhubaneswar, India, ISBN:978-1-5090-0487-4, pp: 206-209.

Chen, L., H. Ben and J. Huang, 2014. An encryption depth optimization scheme for fully homomorphic encryption. Proceedings of the 2014 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), October 17-18, 2014, IEEE, Beijing, China, ISBN: 978-1-4799-8003-1, pp: 137-141.

Dasgupta, S. and S.K. Pal, 2016. Design of a polynomial ring based symmetric homomorphic encryption scheme. Perspect. Sci., 8: 692-695.

Dawahdeh, Z.E., S.N. Yaakob and A.M. Sagheer, 2015. Modified El-gamal elliptic curve cryptosystem using hexadecimal representation. Indian J. Sci. Technol., Vol. 8, 10.17485/ijst/2015/v8i15/64749

Filho, G.J., G.P. Silva and C. Miceli, 2016. A public key compression method for fully homomorphic encryption using genetic algorithms. Proceedings of the 2016 19th International Conference on Information Fusion (FUSION), July 5-8, 2016, IEEE, Heidelberg, Germany, ISBN:978-0-9964-5274-8, pp: 1991-1998.

Gentry, C., 2009. A Fully Homomorphic Encryption Scheme. Stanford University, Stanford, California, Pages: 199.

Greeshma, S. and R. Jayapriya, 2015. Securing Database Server Using Homomorphic Encryption and Re-encryption. In: Security in Computing and Communication, Abawajy, J., S. Mukherjea, S. Thampi and A. Ruiz-Martinez (Eds.). Springer, Berlin, Germany, ISBN:978-3-319-22914-0, pp: 277-289.

Huda, S., A. Sudarsono and T. Harsono, 2015. Secure data exchange using authenticated ciphertext-policy attributed-based encryption. Proceedings of the 2015 International Conference on International Electronics Symposium (IES), September 29-30, 2015, IEEE, Surabaya, Indonesia, ISBN:978-1-4673-9344-7, pp: 134-139.

Lee, Y.G., H.C. Kim, J.J. Kim and M.S. Jun, 2008. A design of home network security protocol using user authentication and access control technology. Proceedings of the International Conference on Convergence and Hybrid Information Technology ICHIT'08, August 28-30, 2008, IEEE, Daejeon, South Korea, ISBN:978-0-7695-3328-5, pp: 30-34.

Manjua, R., A.N. Shajin and A. Rajendran, 2014. Multimodal biometric authentication system based performance scrutiny. Intl. J. Soft Comput., 9: 246-254.

Patel, S.J., A. Chouhan and D.C. Jinwala, 2014. Comparative evaluation of elliptic curve cryptography based homomorphic encryption schemes for a novel secure multiparty computation. J. Inf. Secur., 5: 12-18.

Rivest, R.L., L. Adleman and M.L. Dertouzos, 1978. On data banks and privacy homomorphisms. Found. Secure Comput., 4: 169-180.

Sagheer, A.M., 2012. Elliptic curves cryptographic techniques. Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS'12), December 12-14, 2012, IEEE, Gold Coast, Queensland, Australia, ISBN:978-1-4673-2392-5, pp: 1-7.

Sen, J., 2014. Theory and Practice of Cryptography and Network Security Protocols and Technologies. INTECH Process Automation Inc., Lahore, Pakistan, ISBN:978-953-51-1176-4, Pages: 156.

Sharma, T., 2016. E-Voting using homomorphic encryption scheme. Intl. J. Comput. Appl., 141: 14-16.

Sujatha, K., P.N. Rao, A.A. Rao, K.R. Prasad and M.S.B. Deepthi, 2015. Biometric identity verification using automatic speaker recognition. Proceedings of the 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), January 24-25, 2015, IEEE, Visakhapatnam, India, ISBN:978-1-4799-7676-8, pp: 1-5.

Sunuwar, R. and S.K. Samal, 2015. Elgamal encryption using elliptic curve cryptography. Master Thesis, University of Nebraska-Lincoln, Lincoln, Nebraska.

Suveetha, K. and T. Manju, 2016. Ensuring confidentiality of cloud data using homomorphic encryption. Indian J. Sci. Technol., Vol. 9, 10.17485/ijst/2016/v9i8/87964.

Tebaa, M., S.E. Hajji and A.E. Ghazi, 2012. Homomorphic encryption applied to the cloud computing security. Proceedings of the World Congress on Engineering, July 4-6, 2012, WCE, London, UK., ISBN: 978-988-19251-3-8, pp: 4-6.

Zamare, R. and R. Phursule, 2014. Password authentication key exchange by two server password only in web applications. Intl. J. Recent Dev. Eng. Technol., 2: 113-117.