http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

OPEN ACCESS Information Technology Journal

ISSN 1812-5638
DOI: 10.3923/itj.2016.77.83

Research Article
Elliptic Curve Diffie-Hellman Random Keys Using Artificial Neural Network and Genetic Algorithm for Secure Data over Private Cloud

Othman Alesawy and Ravie Chandren Muniyandi

Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

Abstract

Background: Achieving secure communication and safeguarding sensitive data from unauthorized access over public networks are major concerns in cloud servers. Unique and random encryption keys are vital for data security. **Methodology:** A public key cannot be derived from a random key generator because it can allow middlemen to attack the network easily and access sensitive data. Hence, to secure both data and keys, a system should be used to generate intermediate encryption and decryption keys that are unique, mixed and random. This study investigates how much time is needed to encrypt and decrypt the Elliptic Curve Diffie-Hellman (ECDH) key between cloud users and cloud servers, which are simulated as GUI tools. **Results:** Findings showed that the time consumed increases as the number of text files grows. **Conclusion:** Thus, this experiment demonstrates good improvement in time when an Artificial Neural Network (ANN) is applied to ECDH key exchanges. When the developed ECDH with ANN is applied to genetic algorithms, a high efficiency in terms of the time consumed, performance and accuracy is achieved.

Key words: Elliptic curve cryptography, Diffie-Hellman key, encryption algorithm, artificial neural network, genetic algorithm

Received: May 16, 2016 Accepted: May 31, 2016 Published: June 15, 2016

Citation: Othman Alesawy and Ravie Chandren Muniyandi, 2016. Elliptic curve Diffie-Hellman random keys using artificial neural network and genetic algorithm for secure data over private cloud. Inform. Technol. J., 15: 77-83.

Corresponding Author: Othman Alesawy, Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Cloud computing is the fundamental change occurring in the IT domain[1]. It is an internet-created progression that serves the concerning demand for a strong IT foundation, which includes programming, equipment and client applications. This progression facilitates the use of cloud-based applications and provides low apparatus requirements for clients. Using the internet, clients can secure or retrieve information from the cloud at any time and at any place[2].

Cloud suppliers offer cloud computing organization as an IT asset to clients. Three ordinary cloud computing organizations are as follows[1,3,4]. Infrastructure as a service (IaaS) gives clients excellent control over courses of action and the use of IT assets, such as virtual servers and points of confinement[5,2] Platform as a service, unlike IaaS gives clients a relatively low level of control over passed-on applications[6,3]. Software as a service (SaaS) gives client-compelled administrative control over SaaS execution, in which case the bolster, administration and utilization of cloud administration are fulfilled by the cloud administration supplier.

A cloud system provides comprehensive system access, interest-driven self-organization, metered organization, pay-as-you-gobble up organization, game plans of action and fast flexibility. Private information security is a major concern, especially in cloud computing[7]. Several studies have extensively investigated the use of public keys to increase data privacy[8]. However, public keys reduce the time efficiency between clients and cloud servers[9]. The drawbacks of cryptography algorithms include complexity and the need for data speed acceleration.

One related study adopted the Elliptic Curve Diffie-Hellman (ECDH) key to secure data in cloud computing architecture[10]. However, a significant drawback of the ECDH key is its intensive nature, which causes long execution times and complex computations[11]. Thus, in the present study, an Artificial Neural Network (ANN) to reduce the encryption and decryption time. Also, went beyond the challenge of applying the ANN to the ECDH key by using the ANN with a Genetic Algorithm (GA) on the ECDH key to improve data encryption and decryption speed over cloud servers. This study presents a detailed review of the most relevant study and explains the methodology through three phases[1] implementing the ECDH key and measuring the time consumed through the GUI tools between users and cloud servers based on MATLAB[2], developing the ECHD key time through the ANN and measuring the time[3] and achieving perfect time by implementing the ECDH key with the ANN and GA.

MATERIALS AND METHODS

Elliptic curve cryptography: Elliptic Curve Cryptography (ECC) is dependent on elliptic curve theory[12]. To plan public key cryptographic frameworks, Koblitz and Miller proposed the idea of ECC, which is described briefly below. The general type of elliptic curve E over a prime finite field Fp is:

$$y2 = x3+ax+b \quad (1)$$

where, a, b, Fp and the discriminate D = 4a3+27 b2 0. The points on elliptic curve E over a prime finite field Fp together with an extra point O is called the point at infinity or the zero point, which is denoted as:

$$A = \{(x, y): x, y\ Fp, E\ (x, y) = 0\}\ (1) \quad (2)$$

Let n be the order of A such that n g mod q = 0, where, g is the generator of A. Additionally, let A be an additive cyclic group under the point addition "+", which is defined as P+0 = P, where P An[11]. The point scalar multiplication over A can be defined as:

$$kP = P+P+\ldots\ldots..+P\ (k\ times) \quad (3)$$

If P, Q and A, then P+Q is point R. The line passing through P and Q intercepts the curve at point -R. The reflection of -R is R with respect to the x-axis. This condition is known as the point addition (Fig. 1).

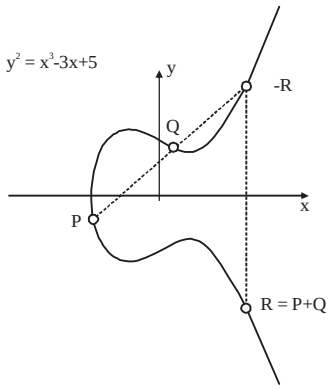

Fig. 1: Point addition

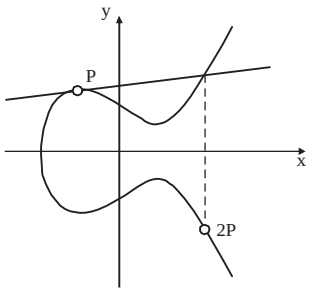

Fig. 2: Point doubling

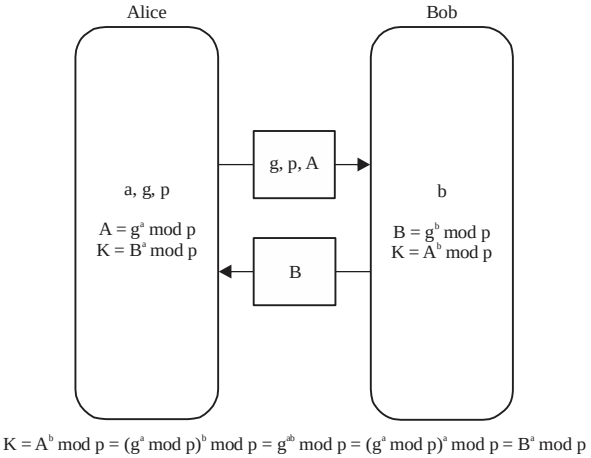

Fig. 3: ECDH

If two points overlap, i.e., P = Q, then R = P+P and becomes a tangent at P, which intersects the curve at -2P. The image of 2P on the changed sign of the y-coordinate is the result of P+P which lies on the curve E/FP. This condition is known as point doubling, as shown in Fig. 2.

Elliptic Curve Diffie-Hellman (ECDH) key exchanges: For the most part, the encryption/decryption of a large proportion of information requires the use of symmetric key (also called secret key) cryptosystems because of their faster calculations in comparison with public key cryptosystems[13]. To create a secret key between two clients for one session, the ECDH key trade method can be applied to an elliptic curve.

Assume that clients A and B need to concur on a secret key for secret key cryptography. Client A produces private key dA and public key PA = dAG, where G is the elliptic curve generator. Client A sends PA to client B. Similarly, client B produces private key dB and public key PB = dBG. Client B then sends PB to client A. Upon receipt of client A's message, client B processes dB (PA) = dAdBG. Upon the receipt of client B's message, client A figures dA (PB) = dAdBG. At this point, clients A and B can both utilize dAdBG, which is a point on the given elliptic curve serving as a typical secret key, as shown in Fig. 3.

Artificial neural network: The ANN is an information preparation paradigm that functions as an organic sensory system, similar to the human brain that processes information[14]. The key segment of this paradigm is the structure of information preparation system, which is composed of a large number of significantly interconnected segments (neurons) functioning as one to handle specific issues. The ANNs, similar to humans learn by illustration. An ANN organizes a specific application, such as design acknowledgment or data request, through a learning process. Learning in common structures incorporates acclimations to the synaptic associations that exist among neurons. The same could also be said for ANNs.

Genetic algorithm: A GA is an improved inquiry system, which can provide an ideal arrangement for the tedious operations of its base administrators, including determination, traverse and change[15]. The GA involves 6 main procedures.

- **Initialization:** The initial population is generated randomly across the search space or as defined by the user
- **Evaluation:** After the initialization of population, the fitness values of the candidate solutions are evaluated
- **Selection:** After the assessment, the fittest chromosomes are likely to be chosen for the cutting edge. To process fitness likelihood, it should register the fitness of every chromosome
- **Crossover:** Crossover combines two or more parts of parental answers to make new, potentially better arrangements. The crossover should be possible through various techniques. A position (single or numerous positions, which rely on the crossover technique) is randomly selected in the guardian chromosome and is then replaced with a sub-chromosome
- **Mutation:** Mutation randomly alters an answer after crossover works on two or more parental chromosomes. The strategy for mutation is diverse. This stage is completed by placing the generate at an irregular position with another of the same worth
- **Uniform crossover:** Uniform crossover takes the uniform fixed ratio between two parents, thus making the information complicated in this algorithm

Proposed approach: Neural cryptography depends on the impact of two neural systems that are fit for synchronization through common learning. In every progression of this online strategy, the neural systems receive a typical data design and ascertain their output.

The two neural systems utilize those outputs presented by their accomplice to change their weights. This process leads to fully synchronized weight vectors. The synchronization of neural networks is in fact, a complex dynamic process. Network weights perform random walks, which are driven by a competition of attractive and repulsive stochastic forces. Two neural networks can increase the attractive effect of their moves by cooperating with each other. However, a third network which is only trained by the other two, clearly has a disadvantage because it cannot skip some repulsive steps. Therefore, two bidirectional neural systems can expand the cooperation to promote the impact of their moves to each other. In any case, a third system which is trained by the other two, clearly has a disadvantage because it cannot skip some repulsive steps. Along these lines, bidirectional synchronization is much faster than unidirectional learning. More specifically, the application of the ANN with the GA should show high efficiency on the basis of three metrics: Time cost, performance and error rate.

Figure 4 shows the encryption process for the ANN with the ECDH key, that is how text files are sent from the client and then encrypted.

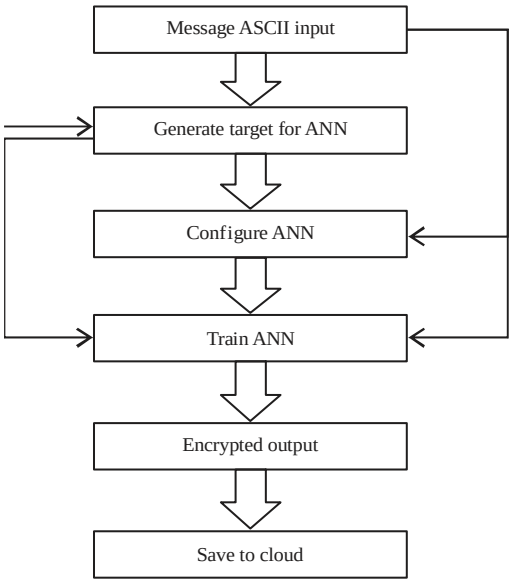

Fig. 4: ECDH+ANN

RESULTS

In this experiment based on MATLAB, it has used ECDH keys along with an ANN. The ANN replicates the randomness of nature, where a population of individuals adapts to its surroundings through a natural selection process and natural system behavior. The ANN produces a population with a high fitness value and this population is the intermediate cipher text that is used in encryption. This intermediate cipher is then used by the ANN to encrypt the original message. The ANN utilizes the error backpropagation algorithm, which uses its own key in the form of its weights and biases.

Nonetheless, it will run the text file on three scenarios based on time:

- ECDH
- ECDH+ANN
- ECDH with ANN-GA

Figure 5 shows the entire process of ECDH+ANN-GA. One important related work on data security in cloud computing architecture based on ECDH showed and claimed that their framework is secure enough for cloud data. However, the security efficiency measurement needs further investigation. As shown in Fig. 6, the ECDH with ANN-GA achieves the best interval time in comparison with the ECDH+ANN and ECDH scenarios because the ANN itself needs time when applied to the randomness of the ECDH. This study is realized by uploading 10 text files.

Considering the decryption process of all three scenarios, it can see improvements in both the encryption and decryption times, as shown in the time interval in Fig. 7.

The performance and error rate of the ANN and GA are issues in the combined application of the two algorithms to ECDH. Thus, in the performance stage, it perform encryption and decryption, as shown in Fig. 8 and 9, respectively.

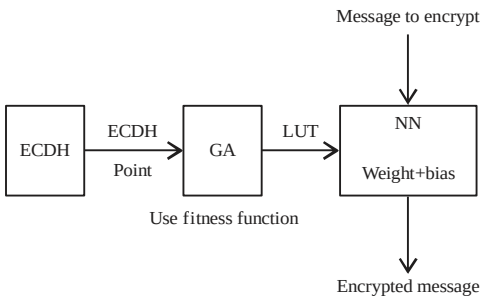

Fig. 5: ECDH+ANN-GA encryption

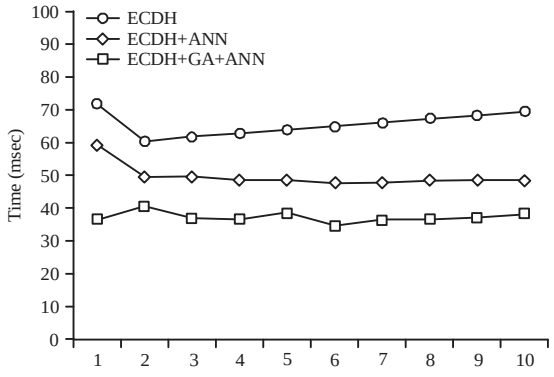

Fig. 6: Text encryption time over the cloud

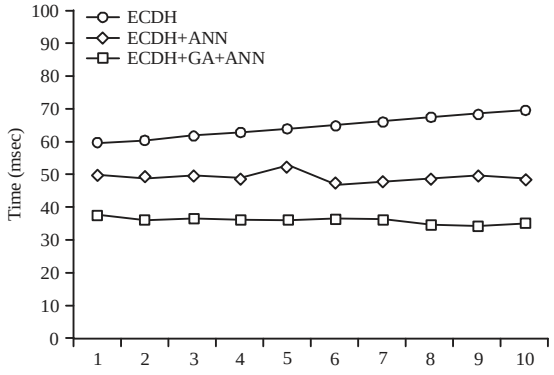

Fig. 7: Text decryption time over the cloud

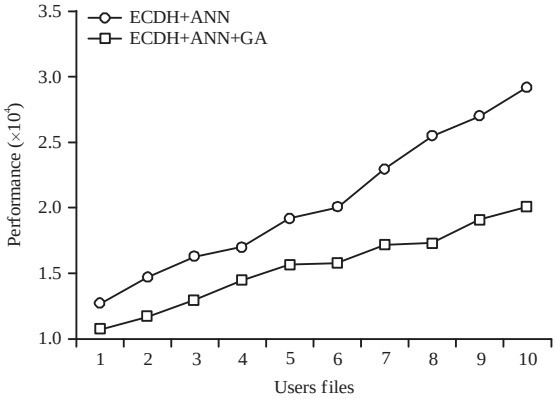

Fig. 8: Performance encryptions for ECDH+ANN and ECDH+ANN-GA

For the error metric, it also apply the encryption and decryption processes for the ANN and ANN-GA over the ECDH. In Fig. 10, the interval of the GA is better than that of the ANN by 20%, which indicates how the GA attempts to solve the error rate in the ANN through a hybrid combination. Figure 11 illustrates the error rates for both the GA and ANN over the ECDH for decrypting 10 text files.

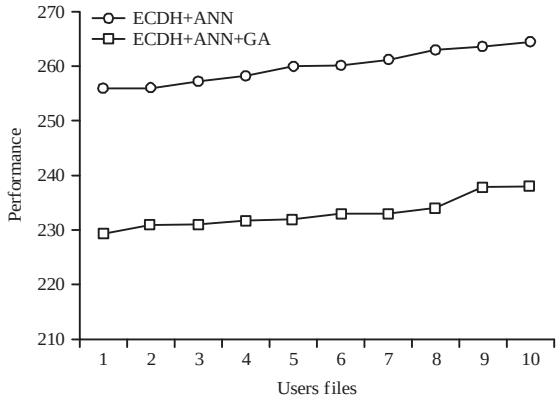

Fig. 9: Performance decryption for ECDH+ANN and ECDH+ANN-GA

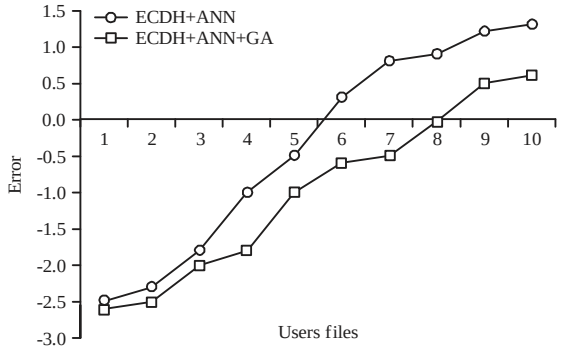

Fig. 10: Error encryption

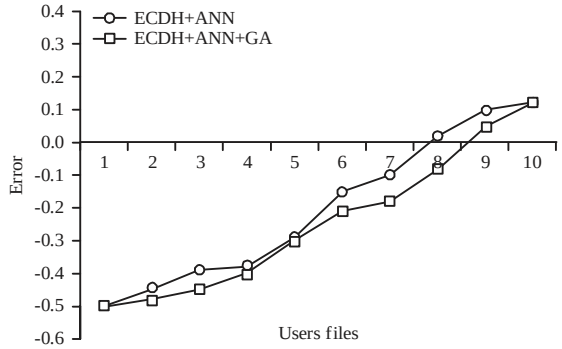

Fig. 11: ECDH+ANN and ECDH+ANN-GA

The main contribution of this study is to enhance the security by assessing and studying the performance of ANNs on the user data over elliptic curves with the high accuracy. Then, it simulate the proposed neural network model with genetic algorithm and ECDH. To simulate the usage of mixed keys from ECDH, GA and ANNs. The result has shown a feasible results based on time, performance and error.

DISCUSSION

These result shows better time efficiency rather than Genkin *et al.*[11] scheme. While combining the concept of ECDH key exchange. Authentication should be done by using Elliptic Curve Digital Signature Algorithm (ECDSA) in Gajra scheme shown high cost in term on comparison with this study[16]. Another related study proposed a novel tri-mechanism for cloud security against data breach, which provide all around security to the cloud architecture Gupta shame Gupta and Chourey[17] but also it take more time for ECDH key exchanges. While, a respected proposed scheme which allows users not only securely store and access data in the cloud but also share data with multiple users in a secured way via unsecured internet. They use ECC for cryptography and authentication operation which makes the scheme work in a less efficient way. Yin *et al.*[18] in the proposed solution gave a reason why to hybrid ANN with GA for less time cost with high performance and less error.

Achieving secure communication across insecure networks and safeguarding secret and sensitive data from unauthorized access over public networks is a major concern in cloud servers. In this study, an implemented asymmetric cryptography, which generates both public and private keys by implementing the ECDH with ANN (error backpropagation neural network) and GA for encryption and decryption processes. By using ECDH with ANN and GA, it will achieved data confidentiality, data integrity for the prevention of manipulations, sender and recipient authentication and prevention of the case in which either recipients or senders deny any of the messages. In this implementation, it used ECDH keys along with the GA. The GA replicates the randomness of nature, where a population of individuals adapts to its surroundings through a natural selection process and natural system behavior. The GA produces a population with a high fitness value and this population serves as the intermediate cipher text used in the encryption. This intermediate cipher is then employed by the ANN to encrypt the original message. The ANN utilizes the error backpropagation algorithm, which uses its key in the form of its weights and biases. It used ECDH, GA and ANN keys to generate unique, encrypted messages that could not be accessed without authorization. The keys generated also possess the randomness required for security and key strength. Hence, the implementation presented in this study enhances data security by assessing and studying the performance of ANNs and GAs on user data over elliptic curves with high accuracy.

CONCLUSION

This study aimed to achieve secure communication across unsecured networks and to safeguard confidential data from unauthorized access over public networks. This study has implemented a symmetric cryptography, which generates both public and private keys, using ECDH with ANN (error backpropagation neural network) for encryption and decryption processes. Using ECDH with ANN and GA, it achieved data confidentiality, data integrity for the prevention of manipulations, sender and recipient authentication and prevention of the case in which either recipients or senders deny any of the messages. It has presented an encryption system based on ECDH with ANN-GA. The latter was used to construct an efficient encryption system through a permanently changing key. Therefore, the main concern is encryption time. Thus, the time consumed as the main metric and considered the encryption-decryption performance and error ratio of the ANN and GA over the ECDH.

The proposed method with the addition of the ANN and ANN-GA was found to be better than the Tirthani and Ganesan scheme in terms of time consumed, performance and error rate in encrypting and decrypting text files.

ACKNOWLEDGMENT

This study was supported by Dana Impak Perdana (DIP-2014-037) of the Universiti Kebangsaan Malaysia (UKM).

REFERENCES

1. Armbrust, M., A. Fox, R. Griffith, A.D. Joseph and R. Katz *et al.*, 2010. A view of cloud computing. Commun. ACM, 53: 50-58.
2. Mohapatra, S. and L. Lokhande, 2014. Cloud Computing Strategy. In: Cloud Computing and ROI: A New Framework for IT Strategy, Mohapatra, S. and L. Lokhande (Eds.). Springer, New York, ISBN: 9783319086637, pp: 67-104.
3. Leimeister, S., M. Bohm, C. Riedl and H. Krcmar, 2010. The business perspective of cloud computing: Actors, roles and value networks. Proceedings of 18th European Conference on Information Systems, June 7-9, 2010, Pretoria, South Africa.
4. Voorsluys, W., J. Broberg and R. Buyya, 2011. Introduction to Cloud Computing. In: Cloud Computing: Principles and Paradigms, Buyya, R., J. Broberg and A. Goscinski (Eds.). John Wiley and Sons Inc., Hoboken, New Jersey, ISBN-13: 9780470887998, pp: 1-44.
5. Dawoud, W., I. Takouna and C. Meinel, 2010. Infrastructure as a service security: Challenges and solutions. Proceedings of the 7th International Conference on Informatics and Systems, March 28-30, 2010, Cairo, Egypt, pp: 1-8.

6. Beimborn, D., T. Miletzki and S. Wenzel, 2011. Platform as a service (PaaS). Bus. Inform. Syst. Eng., 3: 381-384.
7. Nair, N.K., K.S. Navin and C.S.S. Chandra, 2015. Digital signature and advanced encryption standard for enhancing data security and authentication in cloud computing. Int. J. Res. Applied Sci. Eng. Technol., 3: 240-244.
8. Rahaman, M. and M.M. Islam, 2015. A review on progress and problems of Quantum Computing as a Service (QCaaS) in the perspective of cloud computing. Global J. Comput. Sci. Technol., 15: 15-18.
9. Moon, C. and B. Black, 2015. Application monitoring for cloud-based architectures. United States Patent Application No. 20150358391. http://www.freepatentsonline.com/y2015/0358391.html
10. Tirthani, N. and R. Ganesan, 2014. Data security in cloud architecture based on diffie hellman and elliptical curve cryptography. International Association for Cryptologic Research. https://eprint.iacr.org/2014/049.pdf
11. Genkin, D., L. Pachmanov, I. Pipman and E. Tromer, 2016. ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs. In: Topics in Cryptology, Sako, K. (Ed.). Springer, New York, pp: 219-235.
12. Azad, S. and A.S.K. Pathan, 2014. Practical Cryptography: Algorithms and Implementations Using C^{++}. CRC Press, USA., ISBN: 9781482228892, Pages: 365.
13. Lang, J. and R. Haakegaard, 2015. The Elliptic Curve Diffie-Hellman (ECDH). November 2015. http://cs.ucsb.edu/~koc/ecc/project/2015Abstracts/Lang+Haakegaard.pdf.
14. Saied, A., R.E. Overill and T. Radzik, 2016. Detection of known and unknown DDoS attacks using Artificial neural networks. Neurocomputing, 172: 385-393.
15. Shankar, K. and P. Eswaran, 2016. An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm. In: Artificial Intelligence and Evolutionary Computations in Engineering Systems, Dash, S.S., M.A. Bhaskar, B.K. Panigrahi and S. Das (Eds.). Springer, India, ISBN: 978-81-322-2656-7, pp: 705-714.
16. Gajra, N., S.S. Khan and P. Rane, 2014. Private cloud security: Secured user authentication by using enhanced hybrid algorithm. Proceedings of the International Conference on Advances in Communication and Computing Technologies, August 10-11, 2014, Mumbai, pp: 1-6.
17. Gupta, A. and V. Chourey, 2014. Cloud computing: Security threats and control strategy using tri-mechanism. Proceedings of the International Conference on Control, Instrumentation, Communication and Computational Technologies, July 10-11, 2014, Kanyakumari, pp: 309-316.
18. Yin, X.C., N. Thiranant and H.J. Lee, 2014. An efficient and secure data storage scheme using ECC in cloud computing. J. Internet Comput. Ser., 15: 49-58.