A CONCEPTUAL MODEL USING THE ELLIPTIC CURVE DIFFIE–HELLMAN WITH AN ARTIFICIAL NEURAL NETWORK OVER CLOUD COMPUTING

Aws Naser Jaber[1], Mohamad Fadli Zolkipli[2]
[1,2] Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang, Lebuhraya Tun Razak
26300 Gambang, Pahang
Malaysia
e-mail: awscomputer2009@gmail.com

Othman Hanshal[3]
[3]Universiti Kebangsaan Malaysia

Abstract - Cryptography makes taking a cipher and duplicating the original plain content difficult without the comparing key. With all-around outlined cryptography, messages are scrambled in a manner that savage power assaults against the calculation or the key are everything except unthinkable. A solid cryptography obtains its security from the utilization of staggeringly long keys and encryption calculations that are impervious to different types of assault. Neural net application represents the following advancement in great cryptography. This study manages the utilization of a neural system in cryptography, particularly, the configuration of a neural system that can be commonsense use in cryptography. This focus also incorporates an experimental demonstration.

Keywords: Cryptography key; encryption system; encryption algorithm; artificial neural network.

1. INTRODUCTION

Cloud computing is a primitive change happening in the field of information technology (IT) [1]. Cloud computing is an Internet-construct innovation that serves the IT infrastructure, which comprises programming, equipment, and client applications. This innovation gives its consumers ease in utilizing cloud-based applications and low gear prerequisites on the customer side. Information can be stored or obtained by clients over the cloud at any time and any place via the Internet [2]. This service has asset pooling, universal system access, on-interest self-administration, metered administration (measured assets utilization), pay-as-you-devour plans of action, and fast versatility (assets can be scaled here and there effortlessly).

2. LITERATURE REVIEW

Cloud suppliers offer purchasers cloud computing administrations as IT assets. Three normal cloud computing administrations are depicted below [1-2]. Infrastructure as a Service (IaaS): IaaS gives cloud buyers an irregular condition of control and commitment in the course of action and utilization of IT resources. Examples include virtual server events and limits, Application Programming Interface (APIs) hardware, composes, and operating systems [3]. Platform as a Service (PaaS): PaaS gives cloud customers an instant domain currently contained and designed IT assets. Consumers have a lower level of control over the conveyed applications than in IaaS [4]. Software as a Service (SaaS): SaaS provides cloud consumers cloud benefits that they can utilize and arrange. A cloud purchaser has exceptionally constrained regulatory control over SaaS execution. The support, administration, and usage of cloud administrations are completed by the cloud administration supplier (CSP) [5]. Figure 1 illustrates the three types of cloud services.

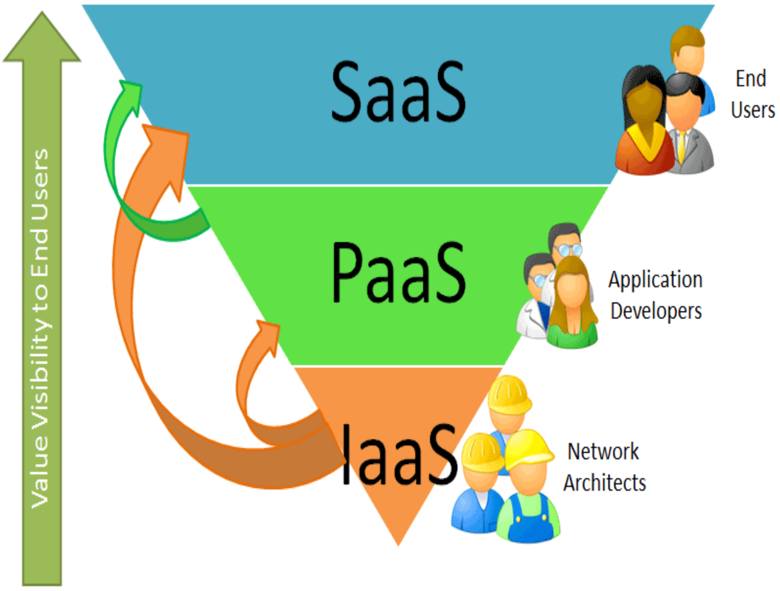

Figure 1: Cloud computing services

The deployment models of distributed computing depend on the foundation or environment made accessible to associations with regard to their needs. Four organization models are depicted below:

- Public cloud: A public cloud is a base or environment that is freely available and is claimed by a third-party CSP. The CSP gives the same base assets over the Internet to every one of the clients of the general population cloud but with restricted setups, security assurance, and element availability [6].
- Private cloud: A private cloud is a base or environment that is implied for a specific association. Information in a private cloud is more secured and controlled than that in a public cloud. A private cloud can be facilitated on-premises or by a remotely trusted third party [7].
- Community cloud: A community cloud is a base or environment that is implied for more than one association with particular communities. That is, it offers basic and particular needs, for example, policy compliance, security, and protection. A community cloud may be overseen by a CSP or by associations and may be facilitated on-premises or off-premises [7].
- Hybrid cloud: A hybrid cloud is shaped by the coordination of two or more clouds (private, community, or public). It meets the exceptional necessities of an association by performing diverse functions [8].

2.1 Elliptic curve cryptography

An elliptic bend cryptosystem (ECC) depends on elliptic curve theory [9]. To plan public key cryptographic frameworks, Koblitz and Miller proposed the idea of elliptic curve cryptography. A brief presentation on the ECC is given as follows. The general type of elliptic curve E over a prime finite field Fp is

$$y^2 = x^3 + ax + b \tag{1}$$

where a, b, Fp, and the discriminate $D = 4a^3 + 27b^2\ 0$. The points on elliptic curve E are over a prime finite field Fp together with an extra point *O* called the point at infinity or zero point, which is denoted as

$$A = \{(x, y)\text{: } x, y\ Fp, E(x, y) = 0\}\ \{O\} \tag{2}$$

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

$$kP = P + P +\text{……..} +P \text{ (k times)} \tag{3}$$

If P, Q, and A, then the addition P + Q is a point R. The line passing through P and Q intercepts the curve at a point called –R. The reflection of –R is R with respect to the x-axis, and this is known as point addition as shown in Figure 2.

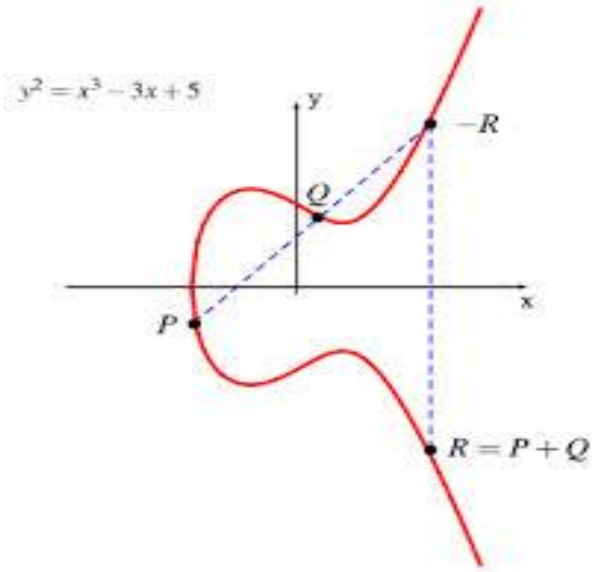

Figure 2: Point addition

If two points overlap, i.e., P = Q, then R= P + P and it 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 the addition of P+P, which lies on the curve E/FP. This situation is known as point doubling as shown in Figure 2.

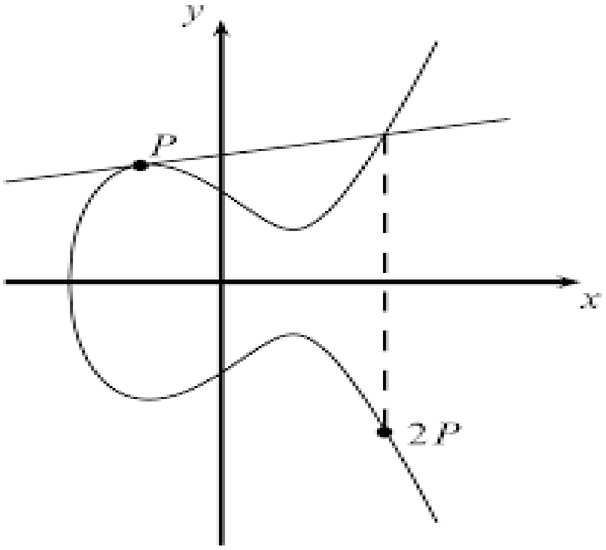

Figure 3: Point doubling

2.2 Elliptic curve Diffie–Hellman (ECDH) key exchange

To encrypt/decrypt the majority of information, symmetric-key (otherwise called secret key) cryptosystems are utilized because of their faster calculation in contrast to public key cryptosystems [10]. To create a secret key between two clients for a solitary session, the ECDH key trade method can be connected to an elliptic curve as depicted below.

Assume that clients A and B need to concur on a secret key, which will be utilized for secret key cryptography. “A” produces a private key dA and a public key PA = dAG, where G is the generator of the elliptic curve. “A” sends PA to “B.” Similarly, “B” produces a private key dB and a public key PB = dBG. “B” sends PB to “A.” Upon the receipt of A's message, B processes dB (PA) = dAdBG. Upon the receipt of B's message, A determines dA (PB) = dAdBG. Both A and B can utilize dAdBG, which is a point on the given elliptic curve, as a typical secret key as shown in Figure 3.

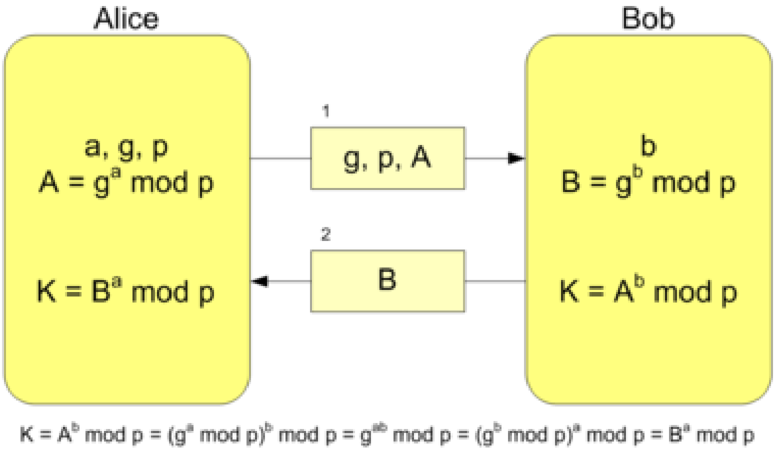
Alice
Bob
a, g, p
A = g^a mod p
K = B^a mod p
1
g, p, A
2
B
b
B = g^b mod p
K = A^b mod p
K = A^b mod p = (g^a mod p)^b mod p = g^ab mod p = (g^b mod p)^a mod p = B^a mod p

Figure 4: ECDH

2.3 Back propagation neural networks

An artificial neural network (ANN) is a data preparation paradigm that is implemented through organic sensory systems, for example, the mind and information processing [11]. The key component of this paradigm is the structure of the data preparation framework, which consists of an extensive number of interconnected handling components (neurons) working as one to address particular issues. ANNs, similar to people, learn by illustration. An ANN is arranged for a particular application, for example, design acknowledgment or information order, through a learning process. Learning in natural frameworks includes acclimations to the synaptic associations that exist among neurons. This situation is also valid in ANNs.

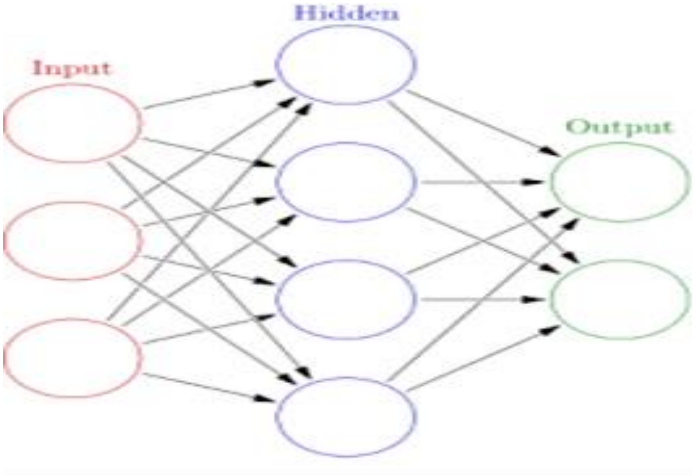

Figure 5: General neural network

The backpropagation system is a standout among the most complex neural systems for regulated learning [12]. With regard to topology, the system is included in a multilayer feedforward neural system. As shown in Fig. 1, a completely associated variation is generally utilized so that every neuron from the n-th layer is associated with all neurons in the (n+1)- th layer. However, this situation may be exaggerated. A few associations may also be lost. In any case, no associations exist among neurons in the same layer. A subset of data units has no information associations from different units as the states of the data units are settled by the issue. Another subset of units is assigned as yield units, the states of which are considered in the calculation results. Units that are neither data nor yield are known as hidden units.

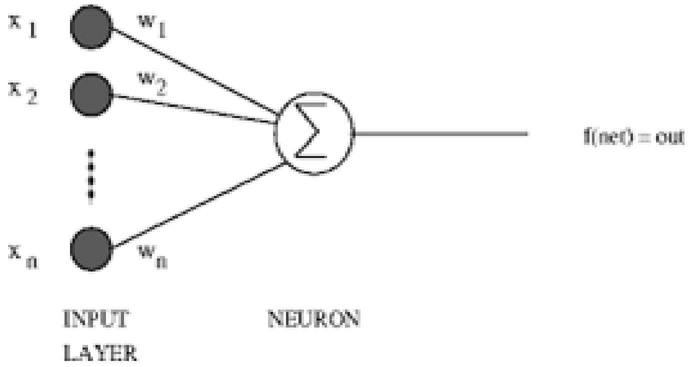

Figure 6: Simple artificial neuron

An essential computational component is called a neuron (Figure. 4), hub, or unit (Fausett 1994). It obtains information from different units or from an outside source. Every datum has a related weight w, which can be adjusted to demonstrate synaptic learning. The unit registers some capacity f of the weighted entirety of its inputs. Therefore, its yield can serve as information to different units. The weighted whole is known as the net information to unit i. Note that w_{ij} indicates the weight from unit j to unit i (not the other way around). The capacity f is the initiation capacity of the unit. Backpropagation calculation typically utilizes a logistic sigmoid actuation capacity (4) for estimations of t in the scope of genuine numbers from $-\infty$ to $+\infty$.

A backpropagation algorithm fits with a gathering called "gradient descent methods." An instinctive definition is a calculation that scans worldwide for the least weight scene by slipping downhill in the most abrupt bearing. The introductory position is set to arbitrarily select the weights of the system to some extent (usually from - 1 to 1 or from 0 to 1). Given the distinctive focus, backpropagation utilizing a fully connected neural network is clearly not a deterministic algorithm.

3. PROPOSED APPROACH

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

At this point, both systems utilize the outputs presented by their accomplice to change their own weights. This process leads to fully synchronized weight vectors. The synchronization of neural networks is, in fact, a complex dynamic process. The weights of the networks perform random walks, which are driven by a competition between 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, has a clear disadvantage because it cannot skip some repulsive steps. Therefore, two bidirectional neural systems can expand the cooperation to communicate the effect of their moves with one another. In any case, a third system, which is trained by the other two, has a clear disadvantage because it cannot avoid some appalling steps. Therefore, bidirectional synchronization is much faster than unidirectional learning.

Two partners, A and B, need to trade a secret message over a public channel. To ensure security against an aggressor T, who is listening in on the correspondence A, encrypts the message. However, B must obtain A's secret key over the general population channel. This goal can be accomplished by synchronizing two three-equality machines, one for A and one for B, separately. After synchronization, the framework creates a pseudorandom bit arrangement that passes through a test on arbitrary numbers. When another system is prepared on this bit succession, removing some data on the measurable properties of the grouping becomes unusual. The Current Trusted Platform Modules (TPMs) produce a mystery key and further encrypt and decrypt a secret message. Consequently, we utilize a multi-layer topology as our application is a calculation issue. In this paper, the backpropagation system is proposed for the encryption-and-decoding process. Neural systems offer a capable and general structure for speaking to a nonlinear mapping from a few information variables to a few yield variables. The procedure for deciding on the estimations of these parameters on the premise of an information set is referred to as learning or preparing. In this manner, the information set is referred to as a preparation set. A neural system can be considered a suitable decision because of its useful structures for encryption and unscrambling operations. Figure 5 illustrates this system.

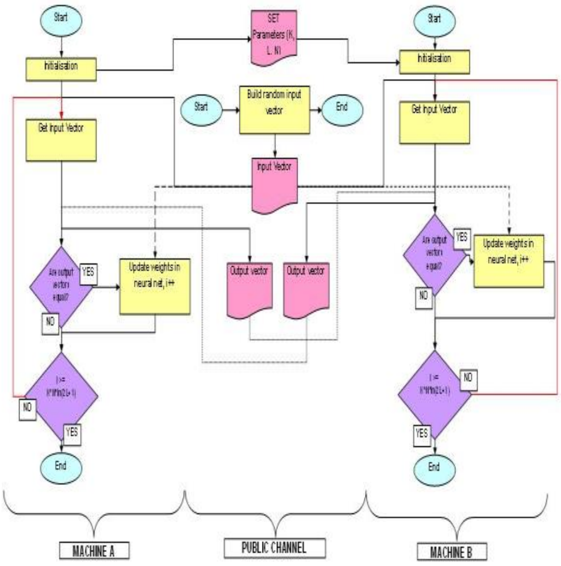

Figure 7: ANN architecture

4. EXPERIMENT AND RESULTS

We used MATLAB version 2015a to perform the experiment through an I7 processor. The starting run of MATLAB initiated the ANN to generate the balanced keys for the ECDH as shown in Figure 6.

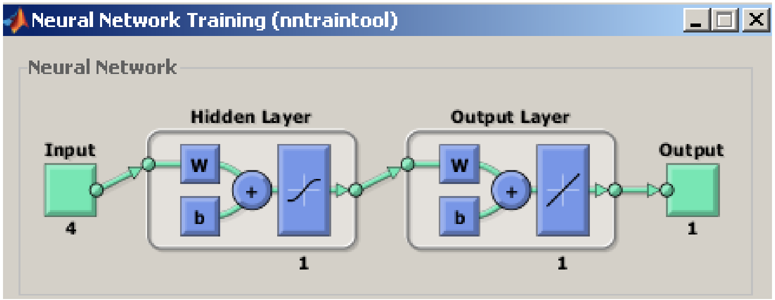

Figure 8: ANN-based ECDH

However, we ran our experiment through MATLAB and used the ECDH keys along with an ANN. An ANN replicates the randomness of nature. Populations of individuals adapt to their surroundings through natural selection processes and the behavior of natural systems. An ANN produces a population that has a higher fitness value, and this population is the intermediate cipher text that will be used in encryption. This intermediate cipher is then used by the ANN to encrypt the original message. The ANN uses the error backpropogation algorithm, which uses its own key in the form of its weights and biases.

We ran the two text file scenarios: before ECDH + NN and after ECDH + NN. Table 1 presents the operation of ECDH+NN before encryption in terms of a time metric and, table 2 shows the decryption process.

Table 1: Encryption before (With ECDH+NN)

Performance	Time	Error %
2183.4681	28	-0.0588
1842.9474	23	-0.0026
406.8916	22	-0.0588
404.1541	20	0.0026
2635.2167	21	0.0052
9026.2943	20	-0.0466
16725.6721	20	0.0060
638.7912	20	-0.1502
939.3597	20	0.01705
40592.6835	20	1.0181

Table 2: presents the operation after decryption.
Decryption → Before (With ECDH+NN)

Performance	Time	Error %
404.9120	33	-9.17984
617.5989	36	-9.17984
419.9209	44	-2.1280
436.9801	43	-0.1235
2776.0304	44	-0.4433
9109.7314	45	-1.6682
17505.2216	56	-1.4325
677.8595	59	-0.3477
886.09285	45	-0.4516
41167.5365	59	0.28506

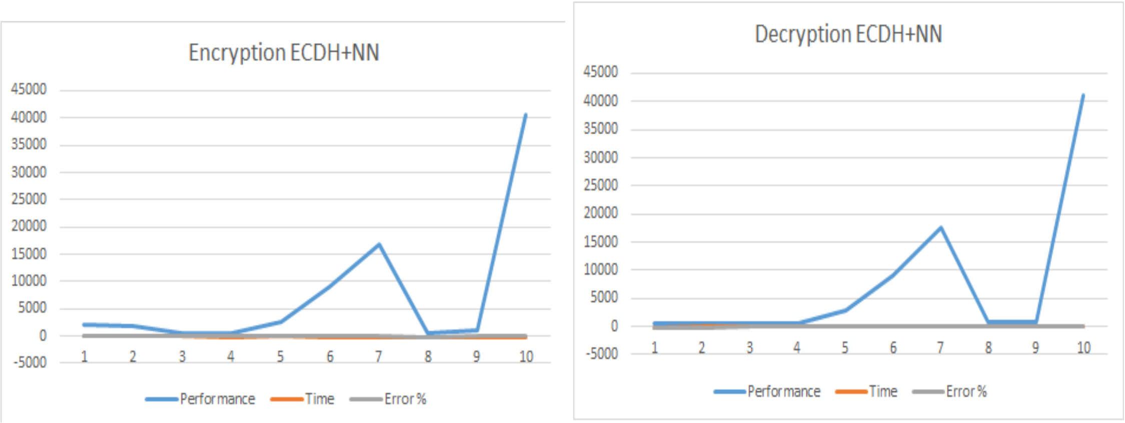

Figure 9: ECDH NN after encryption

5. CONCLUSION

This study aimed to achieve secure communication across unsecure networks and to secure secret and sensitive data from unauthorized access over public networks. We implemented symmetric cryptography, which generates both public and private keys, using ECDH with an ANN (error back propogation NN) for encryption and decryption processes. Using ECDH with an ANN and GA, we achieved confidentiality of data, data integrity that prevents any manipulations, authentication of both sender and recipient, and prevention of both recipient and sender from denying the messages. Nevertheless, we presented an encryption system based on an ANN. The ANN was used to construct an efficient encryption system through a permanently changing key. The ANN topology is an important issue because it has various uses depending on the application of the system it is designed for.

REFERENCES

[1] P. S. KUMAR, and B. T. RAO, “AN EFFICIENT CLOUD BASED KEY AGGREGATE DATA SHARING,” *Journal of Theoretical & Applied Information Technology*, vol. 83, no. 3, 2016.

[2] C. Huang, L. He, X. Liao, H. Dai, and M. Ji, “Developing a trustworthy computing framework for clouds,” *International Journal of Embedded Systems*, vol. 8, no. 1, pp. 59-68, 2016.

[3] S. S. Manvi, and G. K. Shyam, “Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey,” *Journal of Network and Computer Applications*, vol. 41, pp. 424-440, 2014.

[4] S. Pandey, and J. Varshapriya, “Using Platform-As-A-Service (Paas) for Better Resource Utilization and Better Quality Applications,” *International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN*, pp. 2349-2163, 2014.

[5] C. W. Brown, and K. Nyarko, “Software as a Service (SaaS),” *Cloud Computing Service and Deployment Models: Layers and Management: Layers and Management*, pp. 50, 2012.

[6] A. Li, X. Yang, S. Kandula, and M. Zhang, "CloudCmp: comparing public cloud providers." pp. 1-14.

[7] Y. Jadeja, and K. Modi, "Cloud computing-concepts, architecture and challenges." pp. 877-880.

[8] J. Li, Y. K. Li, X. Chen, P. P. Lee, and W. Lou, “A hybrid cloud approach for secure authorized deduplication,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 26, no. 5, pp. 1206-1216, 2015.

[9] D. Mukhopadhyay, A. Shirwadkar, P. Gaikar, and T. Agrawal, "Securing the Data in Clouds with Hyperelliptic Curve Cryptography." pp. 201-205.

[10] A. J. Menezes, *Elliptic curve public key cryptosystems*: Springer Science & Business Media, 2012.

[11] A. J. Maren, C. T. Harston, and R. M. Pap, *Handbook of neural computing applications*: Academic Press, 2014.

[12] T. Chen, and Y.-C. Wang, “A nonlinearly normalized back propagation network and cloud computing approach for determining cycle time allowance during wafer fabrication,” *Robotics and Computer-Integrated Manufacturing*, 2016.