DOI: 10.21917/ijct.2021.0360

SECURE AND ENERGY AWARE TASK SCHEDULING IN CLOUD USING DEEP LEARNING AND CRYPTOGRAPHIC TECHNIQUES

S. Rekha[1] and C. Kalaiselvi[2]

[1]*Department of Computer Science, Tiruppur Kumaran College for Women, India*
[2]*Department of Computer Applications, Tiruppur Kumaran College for Women, India*

Abstract

Cloud Computing is one amid emerging technology greatly necessitated aiding computing on demand services by letting users for subsequent pay-per-use-on-demand scheme. The service cloud providers have non insignificant impacts on ideal resources exploitation and cost benefit in case of Energy aware task scheduling in cloud. Presently Minimum Migration Time (MMT) policy was employed for Virtual Machines migration and offering an energy proficient cloud service. Nonetheless prevailing methodologies never concentrated on any security for cloud. The confidential data protection is highly demanded now-a-days due to increasing users for cloud computing. Hence robust security system for cloud computing is greatly demanded by various cloud researchers. An enhanced approach is presented for mitigating these concerns in which Artificial Bee Colony Optimization (ABC) is deployed for queuing all incoming tasks into multi-level. Shortest-Job-First (SJF) buffering and Min-Min Best Fit (MMBF) scheduling algorithms are checked initially. The SJF buffering and Extreme Learning Machine (ELM)-based scheduling algorithms integration is done for evading job starva¬tion probability in SJF-MMBF. The over utilized host detection is achieved through Adaptive Neuro Fuzzy Inference System (ANFIS) and Virtual Machines (VMs) migration is attained via Minimum Migration Time (MMT) policy from over-utilized hosts to other hosts for energy consumption reduction. Also, security in cloud is greatly achieved by presenting a novel cryptographic technique. There are several advantages such as sharing hardware, software and losing data fear deficiency and due to which current demand for cloud computing is greatly necessitated. The significant information on cloud is maintained by business person, hence data security is vital concern as there is hacking and unauthorized access probability. Here cloud data encryption is attained through elliptic curve cryptography, hence successful and secure storage on cloud is accomplished thereby. The authorized user might access cloud data via key in the suggested system.

Keywords:

Energy Consumption, Cloud Computing, Migrate Virtual Machines, Data Security, Unauthorized Access, Elliptic Curve Cryptography

1. INTRODUCTION

Due to the elasticity and flexibility, Cloud Computing grasped a huge momentum in recent times. As an Internet-based computing strategy, Cloud Computing facilitates the users with shared data and processing resources as a service, which enables the users that they do not require to have it on their infrastructure, and they can access the services as per their requirement and pay accordingly, namely pay-as-you-go model. Since the cloud framework is proved to be smart service and redefining the path, where IT hardware is designed and purchased, cloud is capable of transforming and influencing almost all segments of IT domain. To handle the massively increasing need of Quality of Experience (QoE) and Quality of Service (QoS), the cloud system targets at empowering the next generation data centers with the help of both applications delivered services through Internet, hardware as well as software [1] [2].

In the services provided through cloud system, the software development platforms, storage and computing resources, and computer applications are included. According to the feature of services, they are categorized into three categories, namely Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), which make billions of users to continuously access cloud services, like web hosting, streamed contents, content delivery, scientific applications, online gaming and social networking. Different features, like configuration and deployment requirements, are provided by each of these applications. On the other hand, the constant requirement for the innovative methods are always remain with cloud providers for facilitating the consumers with consistent services, and increasing the turnover, whereas providing an optimal QoS/QoE [3].

Besides, the concept of virtualization, specifically virtual machines (VMs) play a significant role in cloud systems. In the cloud infrastructure, scheduling the tasks towards VMs is highly necessitated, since the computer and storage are heterogeneous. Such that, it is crucial to explore the strategies that helps diminishing the process time to accomplish the task of users, and reducing the utilization of resources. Whereas, a set of policies, referred as scheduling, tends to regulate the order of computation process that needs to be carried out by a computer/set of computers [4] [5].

The VMs are migrated by using Minimum Migration Time (MMT) strategy in recent study, through which a task scheduled cloud service. Though considerable energy efficiency is obtained in the previous work, yet it lacks in terms of cloud security, since the increasing quantity of cloud users gradually escalates the risk in confidential data protection in cloud. Therefore, the researchers are mandated to explore a solid security system for cloud computing. In this study, an improved system is presented for resolving the aforementioned issues. As such, Artificial Bee Colony Optimization (ABC) method will be employed initially, for queuing each incoming task into multi-level.

Besides, the scheduling task is validated through scheduling algorithms. The over-utilized host is detected through Adaptive Neuro Fuzzy Inference System **(**ANFIS**),** whereas VMs are migrated from over-utilized hosts to other hosts by Minimum Migration Time (MMT), through which the energy consumption is greatly reduced. In addition, an unconventional approach is presents in this work, as regards cloud security. At this point, encryption of cloud data is carried out through elliptic curve cryptography, thereby the data storing process is accomplished in a secured manner. During the process of proposed framework, solely authorized users are allowed for cloud data access by using the key.

2. RELATED WORKS

In this segment, several secure cloud systems are comprehensively reviewed.

Baalamurugan and Bhanu [7] tend to efficiently structuring and classifying the secure wallet files, for which they designed a QoS framework. The extension is being proposed as the security methodology in CCEM2016 that employs automation process, by which the efficiency of cloud security is augmented. Nevertheless, some security issues that corresponds to cloud user community and enhancement of end user experience are existed in the Classifier-QoS. On the basis of Machine Learning (KNN-Learning), this Classifier-QoS is designed.

Chkirbene et al. [8] suggested a novel firewall strategy called Enhanced Intrusion Detection and Classification (EIDC) approach that aims at secure cloud computing environment. Received traffic packets are identified and classified through this EDIC, where a novel combination method, namely most frequent decision is utilized, in which the nodes' 11 in this document might interchangeably use words “node” and “user”. Accordingly, the decisions from past are merged to current one from ML algorithm that detects final attack category classification. Consequently, performance of learning as well as model accuracy get maximized. Using the available UNSW-NB-15 dataset, the results are generated, which depicts the efficiency of EICD to increase the anomalies detection by 24% than complex tree.

Makkaoui et al. [9] presented a novel cloud security and privacy model (CSPM) into layers that can be consideredvia cloud providers at all phases of constructing as well as observing the cloud services. This system can enable one and all to surpass the barrier adoption of cloud service. Subsequently, the level of reliability and security is increased, concerning cloud services. Eventually, some security threats and attacks will be occurred, for which some countermeasures can be proposed according to CSPM.

Wang, et al. [10] presented a novel secure cloud storage model accompanied by access control using Ethereum blockchain mechanism, in which Ethereum blockchain and ciphertext-policy attribute-based encryption (CP-ABE) are combined together. By decentralizing the proposed model, untrusted third parties are cleared off from this model, thereby only trusted third-party remains. There are three key features in this system, i.e. i) Ethereum blockchain technology that enable data owner for ciphertext storage of data by using smart contracts involved in a blockchain network; ii) owner of data is able to assign valid access periods for data practice, through which solely ciphertext is allowed to be decrypted at the time of valid access periods. Empirical findings and assessments clearly depict the capability of proposed strategy.

Zhang et al. [11] focused on addressing the problems of huge volume of heterogeneous data, for which they developed a MapReduce-based distributed HOPCM method. Accordingly, devise a privacy-preserving HOPCM algorithm (PPHOPCM) for safeguarding private data on cloud through BGV encryption system to HOPCM. Aimed at BGV model’s secure computing, the functions that update the membership matrix as well as cluster centers are estimated by means of polynomial functions in PPHOPCM. The final outcomes represent the efficiency of the PPHOPCM to cluster a huge volume of heterogeneous data by employing cloud computing deprived of private data revelation.

Marwan, et al. [12] intended for secure cloud-based medical image storage, for which they suggested a model on the basis of Shamir's Secret Sharing (SSS) technique as well as multi-cloud platform. Accordingly, the recommended method is exploitd to a gray-level image. Empirical findings exhibit that the solution provided by the proposed method improves the data security through splitting of secret image into various parts. Besides, it can be considered as an efficient approach for enabling healthcare organizations to efficiently and securely archive and share the healthcare information of patients across healthcare practitioners.

Gu et al. [13] projected a secure data query model for fog and cloud computing. At the time of providing the queried data to users through fog network, queried data is validated by using cloud services. During the process of this model, a few data aggregation topology trees are pre-designated for network fogging using cloud server. Subsequently, in accordance with pre-designated data aggregation trees, associated data may procured by fog network from fog nodes. Besides, associated data can be fed back to the cloud server through some fog nodes that are designated as sampled nodes. The proposed model’s security level is assessed on the basis of fog computing’s security requirements. The application of this model assures the dependability of required data as well as effective protection of data in contradiction of man-in-the-middle attack, single node attack and collusion attack of malicious users, which are proved by the empirical findings.

3. PROPOSED METHODOLOGY

The suggested secure cloud model is elaborated with different stages in detail comprising of six stages. An enhanced approach namely which Artificial Bee Colony Optimization (ABC) is deployed for queuing all incoming tasks into multi-level initially. Shortest-Job-First (SJF) buffering and Min-Min Best Fit (MMBF) scheduling algorithms are checked in second stage. The SJF buffering and Extreme Learning Machine (ELM)-based scheduling algorithms integration is done for evading job starvation probability in SJF-MMBF. In third stage, over utilized host detection is achieved through Adaptive Neuro Fuzzy Inference System (ANFIS) and Virtual Machines (VMs) migration is attained via Minimum Migration Time (MMT) policy from over-utilized hosts to other hosts for energy consumption reduction. Also, data storage security in cloud is greatly achieved by presenting a novel cryptographic technique namely curve cryptography in subsequent stage. Only authorized user has the proficiency in accessing cloud data using the key. The Fig.1 illustrates suggested model complete architecture.

3.1 MULTI QUEUING USING ARTIFICIAL BEE COLONY (ABC)

For attaining multi-level queuing task, an artificial bee colony (ABC) is predominantly utilized in this study, which is known as a population-based stochastic optimization method. It is inspired by a food foraging activities of real honey bees, where the food source for bees is signified as solutions. In ABC, there are three kinds of bees, i.e. employed, onlooker and the scout, where number of employed and onlooker bees are equal. In the process,

employed bee go to food sources and retort to hive and information exchange with onlooker bee through dancing on dance area. By observing dances, Onlooker bee takes the food sources according to the dance moves. The employed bee that sources the food have been abandoned turns out to be a scout and begins to explore for a new food source [13] - [15].

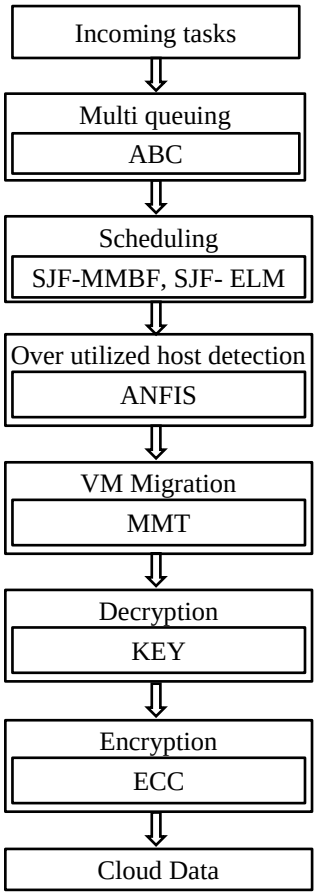

Fig.1. Proposed model Overall architecture

At first, in place of food source, the features in the cervical cancer data is initialized by ABC as an input. Each solution X_i (i=1,2,…,SN) denotes a D-dimensional vector in which D signifies number of parameters that needs to be optimized. Iteration of positions population (employed search process, onlooker and scout) will be continued up to the convergence of Maximum Cycle Number (MCN), C=1,2,…,MCN.

Applying Eq.(1), the position is modified by an employee bee. This work takes nectar amount as a classification accuracy. On the source position in employed bee's memory, she makes a modification, through which a new feature position is discovered. If the new one's classification accuracy is greater than the earlier one, then the old position of bee is replaced by a new one in her memory; or else, the old one remains in her memory [16] [17].

$$v_{ij} = x_{ij} + \varnothing_{ij}(x_{ij}\text{-}x_{kj}) \tag{1}$$

where, $k \in \{1,2,\ldots,SN\}$ and $j \in \{1,2,\ldots,D\}$ are the indexes that are arbitrarily selected; k is estimated arbitrarily and might vary from i, and $\varnothing_{ij}$ is a arbitrarily produced number amid [−1,1].

Post-accomplishing the search process done by every employed bee, information of their corresponding food sources is shared with onlooker bees by waggle dances. The classification accuracy is evaluated by an onlooker bee, and features accompanied by a probability p_i is selected that associates to the corresponding classification accuracy as follows,

$$p_i = \frac{fit_i}{\sum_{n=1}^{SN} fit_n} \tag{2}$$

In which solution fitness value i is denoted by fit_i; number of features in the cervical cancer data is signified by SN. The position modification is created, and the candidate source's classification accuracy is validated by the employed bee. In the memory of onlooker bee, she replaces the old position with a new one, if the accuracy is greater than the earlier one [18].

If the position is unable to be enhanced more, the following Eq.(3) is applied to replace the feature of which accuracy is abandoned through bees with the new features via scouts. As a control parameter, the parameter "limit" is deployed to identify the features' abandonment between the predefined number of cycles.

$$x_i^j = x_{\min}^j + rand\,(0,1)\left(x_{\max}^j - x_{\min}^j\right) \tag{3}$$

Algorithm 1: Multi queuing using ABC

Input: Number of incoming tasks

Output: Multi level queues

1. Initialize the number of tasks x_i, i = 1…SN
2. Initialize feature position
3. Estimate tasks completion time
4. Assign cycle to 1
5. Redo
6. FOR each employed bee
7. Create new solutions v_i by using Eq.(1)
8. Compute the completion time
9. Execute the greedy selection process
10. Determine probability p_i for the solution x_i using Eq.(2)
11. For every onlooker bee
12. Choose a solution x_i depending on p_i
13. Create new solutions v_i
14. Estimate the completion time
15. Execute the greedy selection process
16. If there is an abandoned solution for scout bees then
17. Switch it with a new solution
18. Memorize best solution (optimal queues) achieved so far
19. cycle = cycle+1
20. Until cycle = MCN
21. Terminate

The tasks are slashed into multi queues on the basis of aforementioned strategy. Besides, in accordance with the scheduling algorithms called SJF-MMBF and SJF-ELM, the divided task will be scheduled in their corresponding queue.

3.2 SCHEDULING POLICY FOR MIN-MIN BEST FIT AND SHORTEST-JOB-FIRST BUFFERING

The forthcoming resource necessities prediction is a challenging task as well too costly for accurate traffic features prediction (for instance arrival predicted level along with job medium size) for the reason of strong heterogeneity besides dynamism in task.

3.2.1 SJF-MMBF

Step 1: **Buffering Algorithm (SJF Buffering)**: Various type-v jobs that reached in time intervals [t;t+1) are buffered in v^{th} queue according to buffering policy as precise in Algorithm 1, for v V.

Step 2: **Scheduling Algorithm (MMBF Scheduling)**: In result epoch t, do

a. Estimate resource array N $A_t v$.

b. Choose action a_t*A_t such that Nal*NA_tV is determined.

Step 3: **Scheduling Process**: In a time interval [t; t+1), $Nv_p(t)$ type-v jobs endure to be served, and Na_t*vNv_pt type-v jobs are de-queued from v^{th} queue in an HOL approach then start to be aided for v V. The number of jobs to arise in queue and acquisitive workload constraint are proficient, correspondingly.

3.3 SJF-ELM

Step 1: Algorithm of Buffering (Buffering in SJF): A range of [t; t+1] are buffering time of sort of v jobs accordingly on queue as well as buffering policy. It is deployed in Algorithm SJF as SJF-ELM, $v \in V$.

Step 2: **Scheduling Algorithm (ELM Scheduling)**: In t_j of decision epoch, perform

- $S_t \leftarrow \left(N_v^p(t)\right), Q_v(t), W_v(t)$ state is intellect.
- Huge X actions are computed viably and N $A_s \times v$ as array resource.

Step 3: **Scheduling Process**:

a. **Scheduling**: Jobs of $N_v^p(t)$ type 1 are being supported in queue along $v \in V$, as well as de-queue $\left(N\left(a_t^*, v\right) - N_v^p(t)\right)$ type-1 jobs from 1th queue and start serving function. Queue holding plenty of waiting jobs and update necessary workload in accumulation are from

$$Q_v(t+1) = Q_v(T) - \left(N\left(a_t^*, v\right) - N_v^p(t)\right)$$

$$w_v(t+1) = W_v(T) - N\left(a_t^*, v\right) \quad (4)$$

b. Time computation of job completion in time-averaged as follows:

$$E\left[\breve{T}(t)\right] = \sum_{v=1}^{V} \alpha E\left(\breve{T}(t-1)\right) + (1-\alpha) T_v(t) \quad (5)$$

where $\alpha \in (0,1)$ denotes weight parameter.

c. If $E\left[\breve{T}(t)\right] T_j > E\left[T^*\right], \omega^*$,vector of parameter are updated

d. The final number of arrived traffic T gets stored as

$$\{j_v(t\text{-}T\text{+}1), \ldots, j_v(t)\}. \quad (6)$$

3.4 OVER UTILIZED HOST DETECTION USING ANFIS

Mostly, service to all requests allotted to it cannot be serviced by over-utilized host. In this circumstance, requests response times will be increased. Accordingly, in any cloud service provider, it is crucial for handling over-utilized hosts. In this system, ANFIS is greatly exploited for CPU utilization prediction.

3.4.1 Adaptive Neuro Fuzzy Inference System (ANFIS):

ANFIS input is all hosts CPU utilization information. ANFIS network is regarded as one of the neural networks which is on the basis of neuro fuzzy network. ANFIS architecture is utilized for two rules implementation as represented in Fig.2.

All nodes are adaptive nodes in first layer. The layer 1 outputs are fuzzy membership input grades are specified as:

$$O_i^1 = \mu_{A_i}(x) \quad \text{for } i=1,2 \quad (7)$$

where x and y denotes input nodes, A and B are represented as linguistic labels, (x) and (y) signifies membership functions which recurrently assume a bell shape using highest and lowest values equivalent to 1 and 0, respectively.

$$\mu(x) = \frac{1}{1 + \left(\frac{x - c_i}{a_i}\right)^{2b_i}} \quad (8)$$

where, a_i, b_i, and c_i denotes premise parameters set.

In second layer, nodes are fixed nodes. Labeled with M is done, representing that they accomplish as a simple multiplier. This layer outputs can be indicated as:

$$O_i^2 = w_i = \mu_{A_i}(x) \mu_{B_i}(y) \text{ for } i=1,2 \quad (9)$$

The output w_i represents rule firing strength. Every node result denotes the firing strength of a rule

In third layer, nodes are also fixed nodes. They are labeled with N, signifying that y a normalization role is played to firing strengths from previous layer [21] [22]. This layer outputs are characterized as:

$$O_i^3 = w_i = \frac{w_1}{w_1 + w_2} \text{ for } i=1,2 \quad (10)$$

The results are termed as normalized firing strengths.

In fourth layer, adaptive nodes are considered as nodes. Each node output in this layer is merely normalized firing strength and a first order polynomial product (for a first order Sugeno model). Consequently, this layer outputs are specified by:

$$O_i^4 = w_i f_i = w_i \left(p_i x + q_i y + r_i\right) \quad (11)$$

where w denotes layer 3 output, and $\{p_i, q_i, r_i\}$ represents parameter set. These parameters are known as ensuing parameters

In fifth layer, there is merely one fixed node labeling is done with S. This node accomplishes all incoming signals summation [23] [24]. Therefore, overall model output is given by:

$$O_i^5 = \sum_{i=1} w_i f_i = \frac{\sum_{i=1} w_i f_i}{\sum_{i=1} w_i} \quad (12)$$

The over-utilized host will be found at this stage,

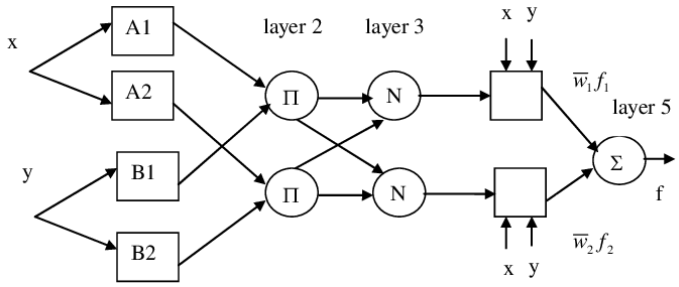

Fig.2. ANFIS Architecture

3.5 HOST UNDER LOADING DETECTION

The host is said to possess very low load as well limited requests allocations are done to it whenever a host is in underutilized mode. Therefore, in contrast to its energy consumption abundant requests are not responded. Also, a simple policy is necessitated for handling underutilized hosts in which all host but over utilized hosts are represented as underutilized hosts. Subsequently, all VMs are migrated which are allocated to underutilized hosts to other hosts but any host cannot be over-utilized owing to this reason. This process is done for all underutilized hosts which helps in switching as numerous hosts as likely to sleep mode. Therefore, this process might reduce number of active hosts as well as energy consumption generally.

3.6 VIRTUAL MACHINE MIGRATION USING MINIMUM MIGRATION TIME (MMT)

One or more Virtual Machines (VM) are migrated from these hosts to others with a constraint whenever a host is represented as over utilized host and this process does not consider other hosts to over utilized mode. Minimum Migration Time (MMT) policy is utilized for VMs selection from over utilized hosts [25] [26] which supports in VMs migration necessitating least time for carrying out migration process. The migration time is projected as amount of RAM utilized by VM divided by spare network bandwidth existing for host *j*. If VM *v* has ensuing conditions, MMT policy is used to obtain:

$$v \in \frac{V_j}{\forall V_j} \quad (13)$$

$$\frac{RAM_U(v)}{NET_j} \leq \frac{RAM_U(a)}{NET_j} \quad (14)$$

where V_j denotes set of VMs presently allotted to host *j*. NET_j represents spare network bandwidth available for host *j*; and $RAM_u(a)$ denotes amount of RAM presently exploited via VM.

Algorithm

Input: host List

For every host in host List do
  If host is over loaded then //Part A
    Get VMs to migrate from this host // Part B
    For every host in host List do
      If host is under loaded then // Part C
        If it is possible to migrate all VMs which is allocated to host to the other hosts then
          Migrate all VMs
        Else
          Keep host active
        End
      End
    End
  End

3.7 INTRUSION PREVENTION USING ELLIPTICAL CURVE CRYPTOGRAPHY

Elliptical Curve Cryptography (ECC) is greatly utilized in this research for cloud data encryption in which elliptical curves theory [19]-[21] forms the basis for public key encryption method. Elliptic curve properties are exploited for generating keys rather than using customary keys generation approach through two very large prime numbers product. At first elliptic curves for cryptography was employed in H.W. Lenstra's elliptical curve factoring algorithm. This erratic elliptic curve use greatly inspires for suggesting this elliptical curve cryptography.

ECC has benefit of exploiting smaller keys so long as same security level. ECC might offer similar security with 164-bit key that other schemes afford with 1024- bit key. High level security with low computing power and battery resource are the key abilities which is quite useful for further applications. ECC is a public key cryptosystem for public key and the private key generation so that data encryption and decryption can be attained. It is mainly on basis of mathematical complexity of solving elliptic curve discrete logarithm problem which handles with calculating number of steps or hops issue it proceeds to interchange from one point to another point on elliptic curve [22] [23].

Elliptic curves are binary curves besides symmetrical over x-axis specified by:

$$y^2 = x^3 + ax + b \quad (15)$$

where *x* and *y* denote standard variables defining function while as *a* and *b* signifies constant coefficients for curve definition. As *a* and *b* change values, elliptical curve also gets altered. For elliptical curves, $\Delta = 4a^3 + 27b^2$ discriminant is non zero. The operations used on elliptical curves in cryptography are point addition, point multiplication and point doubling.

The significant elliptic curve characteristic is finite field concept inferring that there is a manner for limiting curve values. This *max* value established on x-axis is characterized by *p*. It is also termed modulo value for any ECC cryptosystem. This point describes finite length upon which operations can be implemented on curve. In ECC, modular value represents system key size.

Thus, parameters that help in complete ECC cryptosystem description are:

P - Finite field Specification

a,*b* - Coefficients for describing curve

G - Generator point on curve where operation starts

n - Order of *G*

h - total points division on curve and order of *G*.

3.8 STEPS INVOLVED IN ECC ALGORITHM:

ECC is a public key cryptosystem where each user comprises two keys: public key and private key. Public key is deployed for encryption and signature verification while as private key is utilized for decryption and signature generation.

3.8.1 Key Generation:

Key Generation is one mainly meant for producing both public and private keys through an algorithm. The message data encryption is done using receiver's public key and data decryption is done through its private key.

Step 1: The sender chooses an arbitrary number *dA* amid the range [1, *n*-1]. This is the sender private key.

Step 2: Then sender creates public key through $PA = dA*G$

Step 3: Likewise, receiver chooses a private key *dB* and produces its public key $PB = dB*G$.

Step 4: The sender creates security key $K = dA*PB$ and receiver also constructs security key $K = dB*PA$

3.8.2 Encryption Algorithm:

Let sender desires to send a message *m* to receiver

Step 1: Assume m has any point M on elliptic curve

Step 2: The sender chooses a arbitrary number k from [1,*n*-1]

Step 3: The cipher texts produced will be pair of points (B_1,B_2):

$$B_1 = k*G \quad (16)$$

$$B_2 = M+(k*G) \quad (17)$$

On the basis of above process in cloud, data encryption is done and stored. Suppose any authorized user decides for processing those data then it can be accessed via known key to decrypt.

3.8.3 Decryption Algorithm:

To decrypt the cipher text, following steps are performed:

Step 1: The receiver computes B_1 and its private key product

Step 2: Then receiver subtracts this product from second point B_2

$$M = B_2 - (dB * B_1) \quad (18)$$

where, *M* notates original data sent through sender

4. RESULTS AND DISCUSSION

Experimentation and its outcomes are elucidated for the suggested model for which Java platform is greatly utilized. Various performance metrics comparison is done for validating recommended MQ-ECC with that of prevailing single queuing SJF-RL (SQ-SJF-RL), Single queuing SJF-MMBF (SQ-SJF-MMBF), PLBA, Multi Queuing SJF-ELM (MQ-SJF-ELM) and MQ-SJFELM-MMT pertaining to Throughput, Delay and cost.

The Fig.3 reveals prevailing SQ-SJF-RL, SQ-SJF-MMB, MQ-SJF-ELM method and SJFELM-MMT and suggested MQ-ECC system in which Scheduling methods throughput performance comparison which are plotted in x-axis and throughput values are plotted in y-axis. It is thereby validated that greater throughput of 0.87 (Kbps) is utilized by suggested MQ-ECC method which is considered to be an improved result since prevailing SQ-SJF-RL, SQ-SJF-MMBF, MQ-SJF-ELM and SJFELM-MMT technique delay values are 0.32 (Kbps), 0.56 (Kbps), 0.74 (Kbps) and 0.85 (Kbps) respectively.

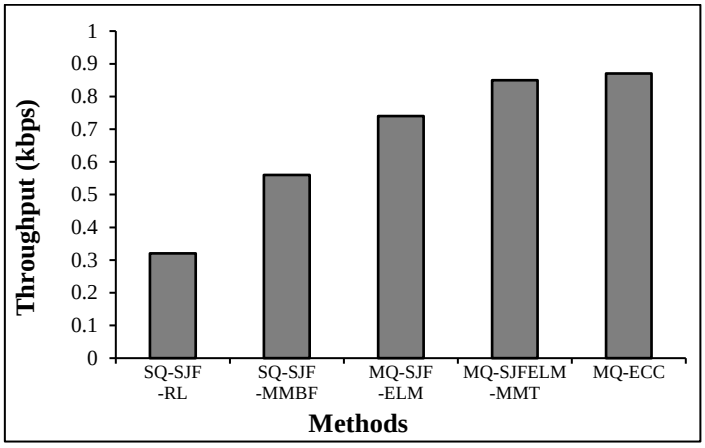

Fig.3. Scheduling approaches vs. Throughput

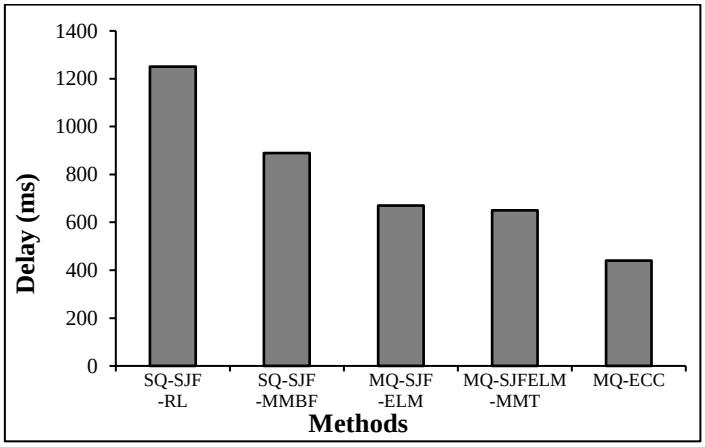

Fig.4. Delay vs. scheduling methods

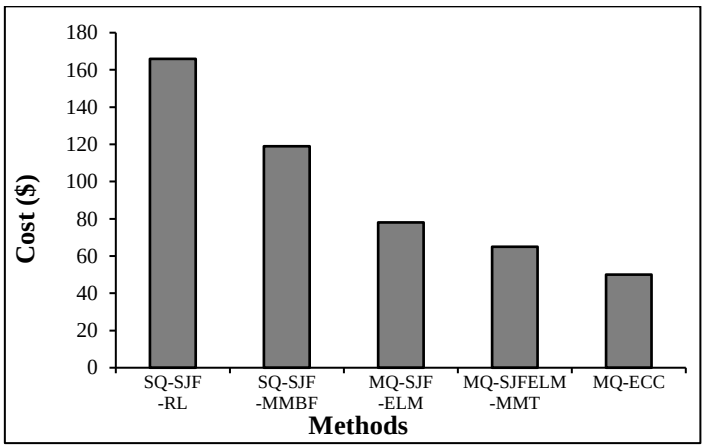

Fig.4. Cost results vs. Scheduling methods

The Fig.4 illustrates delay comparison of the prevailing SQ-SJF-RL, SQ-SJF-MMBF, MQ-SJF-ELM method and SJFELM-MMT and suggested MQ-ECC system in which Scheduling methods are plotted in x-axis and delay values are plotted in y-axis. It is thereby validated that lesser delay of 440 (ms) is utilized by suggested MQ-ECC method which is considered to be an improved result since prevailing SQ-SJF-RL, SQ-SJF-MMBF, MQ-SJF-ELM and SJFELM-MMT technique delay values are 1250 (ms), 890 (ms), 670 (ms) and 650 (ms) respectively.

The Fig.5 illustrates Cost metric comparison chart of the prevailing SQ-SJF-RL, SQ-SJF-MMBF, MQ-SJF-ELM method and SJFELM-MMT and suggested MQ-ECC system. It is thereby validated that lesser cost of 50$ for scheduling is utilized by suggested MQ-ECC method which is considered to be an improved result since prevailing SQ-SJF-RL, SQ-SJF-MMBF, MQ-SJF-ELM and SJFELM-MMT technique cost values are 166$, 119$, 78$ and 65$ respectively.

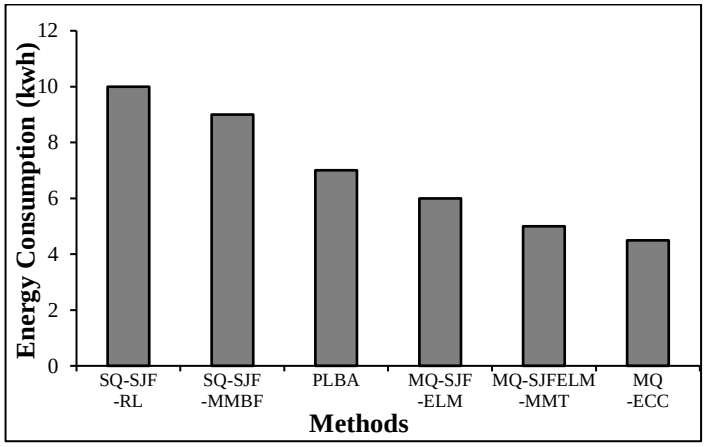

Fig.6. Energy consumption results vs. Scheduling methods

The Fig.6 illustrates energy consumption metric comparison chart of the prevailing SQ-SJF-RL, SQ-SJF-MMBF, PLBA, MQ-SJF-ELM method and SJFELM-MMT and suggested MQ-ECC system. The over utilized hosts for VM migration are detected by ANFIS Gaussian radial basis kernel and thereby increasing energy consumption in cloud environment. It is thereby validated that energy consumption of 4.5(kwh) for scheduling is utilized by suggested MQ-ECC method which is considered to be an improved result since existing SQ-SJF-RL, SQ-SJF-MMBF, PLBA, MQ-SJF-ELM and SJFELM-MMT technique offers only 10(kwh), 9(kwh), 7(kwh), 6(kwh) and 5(kwh) respectively.

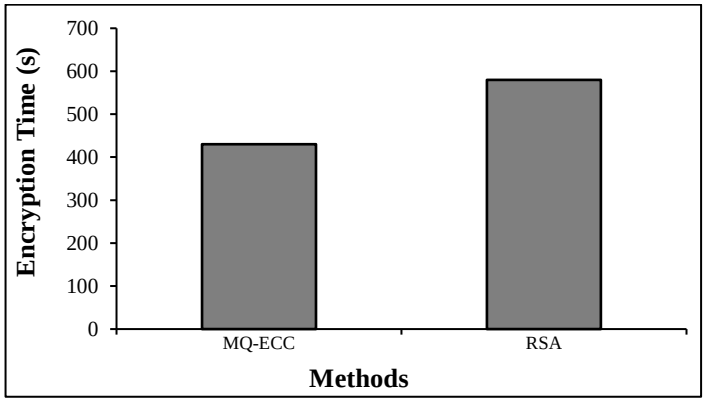

Fig.7. Encryption time vs. methods

The Fig.7 reveals the comparison chart of encryption time of suggested MQ-ECC method and prevailing RSA method. It is thereby validated that encryption time of 430s is utilized by suggested MQ-ECC method which is considered to be an improved result since 580s is required for prevailing RSA method

5. CONCLUSION AND FUTURE WORK

An enhanced methodology is presented for secured cloud services in which Artificial Bee Colony Optimization (ABC) is deployed for queuing all incoming tasks into multi-level. The over utilized host detection is achieved through Adaptive Neuro Fuzzy Inference System (ANFIS) and Virtual Machines (VMs) migration is attained via Minimum Migration Time (MMT) policy from over-utilized hosts to other hosts for energy consumption reduction. Also, security and data storage in cloud is greatly achieved by presenting a novel cryptographic technique namely elliptic curve cryptography for data encryption. The authorized user might access cloud data via key in the suggested system. The suggested model outperforms well which is validated through experimental outcomes pertaining to throughput and encryption time. Nonetheless, intrusion detection is not considered in this work and preferred for forthcoming research.

REFERENCES

[1] T. Zhao, S. Zhou, X. Guo and Z. Niu, "Tasks Scheduling and Resource Allocation in Heterogeneous Cloud for Delay-Bounded Mobile Edge Computing", *Proceedings of IEEE International Conference on Communications*, pp. 1-7, 2017.

[2] X.L. Zheng and L. Wang, "A Pareto based Fruit Fly Optimization Algorithm for Task Scheduling and Resource Allocation in Cloud Computing Environment", *Proceedings of IEEE Congress on Evolutionary Computation*, pp. 3393-3400, 2016.

[3] H. Cui, Y. Li, X. Liu, N. Ansari and Y. Liu, "Cloud Service Reliability Modelling and Optimal Task Scheduling", *IET Communications*, Vol. 11, No. 2, pp.161-167, 2017.

[4] K.M. Baalamurugan and S.V. Bhanu, "An Efficient Clustering Scheme for Cloud Computing Problems using Metaheuristic Algorithms", *Cluster Computing*, Vol. 22, No. 5, pp. 12917-12927, 2019.

[5] M. Chen, Y. Hao, C.F. Lai, D. Wu, Y. Li and K. Hwang, "Opportunistic Task Scheduling Over Co-Located Clouds in Mobile Environment", *IEEE Transactions on Services Computing*, Vol. 11, No. 3, pp. 549-561, 2016.

[6] R.S.V. Venkatesh, P.K. Reejeesh, S. Balamurugan and Charanyaa, S. "Future Trends of Cloud Computing Security: An Extensive Investigation", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, No. 1, pp. 246-253, 2015.

[7] K.M. Baalamurugan and S.V. Bhanu, "Analysis of Cloud Storage Issues in Distributed Cloud Data Centres by Parameter Improved Particle Swarm Optimization (PIPSO) Algorithm", *International Journal on Future Revolution in Computer Science and Communication Engineering*, Vol. 4, pp. 303-307, 2018.

[8] Z. Chkirbene, A. Erbad and R. Hamila "A Combined Decision for Secure Cloud Computing based on Machine

Learning and Past Information", *Proceedings of IEEE International Conference on Wireless Communications and Networking*, pp. 1-6, 2019.

[9] K. El Makkaoui, A. Ezzati, A. Beni-Hssane and C. Motamed, "Cloud Security and Privacy Model for Providing Secure Cloud Services", *Proceedings of International Conference on Cloud Computing Technologies and Applications*, pp. 81-86, 2016.

[10] S. Wang, X. Wang and Y. Zhang, "A Secure Cloud Storage Framework with Access Control based on Blockchain", *IEEE Access*, Vol. 6, pp.112713-112725, 2019.

[11] Q. Zhang, L.T. Yang, Z. Chen and P. Li, "PPHOPCM: Privacy-Preserving High-Order Possibilistic C-Means Algorithm for Big Data Clustering with Cloud Computing", *IEEE Transactions on Big Data*, Vol. 9, No. 2, pp. 1-14, 2017.

[12] M. Marwan, A. Kartit and H. Ouahmane, "Secure Cloud-based Medical Image Storage using Secret Share Scheme", *Proceedings of IEEE International Conference on Multimedia Computing and Systems*, pp. 366-371, 2016.

[13] K. Gu, N. Wu, B. Yin and W. Jia, "Secure Data Query Framework for Cloud and Fog Computing", *IEEE Transactions on Network and Service Management*, Vol. 17, No. 1, pp. 332-345, 2019.

[14] Y. Wang, J. You, J. Hang, C. Li and L. Cheng, "An Improved Artificial Bee Colony (ABC) Algorithm with Advanced Search Ability", *Proceedings of International Conference on Electronics Information and Emergency Communication*, pp. 91-94, 2018.

[15] F. Xie, F. Li, C. Lei, J. Yang and Y. Zhang, "Unsupervised Band Selection based on Artificial Bee Colony Algorithm for Hyperspectral Image Classification", *Applied Soft Computing*, Vol. 45, No. 1, pp. 428-440, 2019.

[16] R.A. Vazquez and B.A. Garro, "Crop Classification using Artificial Bee Colony (ABC) Algorithm", *Proceedings of International Conference on Swarm Intelligence*, pp. 171-178, 2016.

[17] A.V. Reddy, C.P. Krishna and P.K. Mallick, "An Image Classification Framework Exploring the Capabilities of Extreme Learning Machines and Artificial Bee Colony", *Neural Computing and Applications*, Vol. 14, No. 2, pp. 1-21, 2019.

[18] Banharnsakun, "Hybrid ABC-ANN for Pavement Surface Distress Detection and Classification", *International Journal of Machine Learning and Cybernetics*, Vol. 8, No. 2, pp.699-710, 2017.

[19] F.H.A. Vieira and A.C.P. De Leon Ferreira, "Deep Learning for Biological Image Classification", *Expert Systems with Applications*, Vol. 85, pp. 114-122, 2017.

[20] K. Kedarisetti, R. Gamini and V. Thanikaiselvan, "Elliptical Curve Cryptography for Images using Fractal Based Multiple Key Hill Cipher", *Proceedings of International Conference on Electronics, Communication and Aerospace Technology*, pp. 643-649, 2018.

[21] L. Sujihelen and C. Jayakumar, "Inclusive Elliptical Curve Cryptography (IECC) for Wireless Sensor Network Efficient Operations", *Wireless Personal Communications*, Vol. 99, No. 2, pp. 893-914, 2018.

[22] S. Selvi, M. Gobi, M. Kanchana and S.F. Mary, "Hyper Elliptic Curve Cryptography in Multi Cloud-Security using DNA (Genetic) Techniques" *Proceedings of International Conference on Computing Methodologies and Communication*, pp. 934-939, 2017.

[23] X. Duan, D. Guo, N. Liu, B. Li, M. Gou and C. Qin, "A New High-Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network", *IEEE Access*, Vol. 8, pp. 25777-25788, 2020.

[24] V. Chang, B. Gobinathan, A. Pinagapani and S. Kannan, "Automatic Detection of Cyberbullying using Multi-Feature based Artificial Intelligence with Deep Decision Tree Classification", *Computers and Electrical Engineering*, Vol. 92, pp. 1-16, 2021.

[25] K.M. Baalamurugan and S.V. Bhanu, "A Multi-Objective Krill Herd Algorithm for Virtual Machine Placement in Cloud Computing", *Journal of Supercomputing*, Vol. 76, No. 6, pp. 4525-4542, 2020.

[26] S. Eswaran, D. Dominic, J. Natarajan and P. B. Honnavalli, "Augmented Intelligent Water drops Optimisation Model for Virtual Machine Placement in Cloud Environment", *IET Networks*, Vol. 9, No. 5, pp. 215-222, 2020.