2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS) | 978-1-6654-6275-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICPECTS56089.2022.10047356

An Efficient Task scheduling and Data security in Heterogeneous Cloud Computing using Hybrid Meta-Heuristic Algorithm and Block Chain based Key Aggregate Cryptosystem

Devi.D
Department Of Computer Science and Engineering
SRM Institutes of Science and Technology
Chengalpattu-603203
ddevi2006@gmail.com

S.Godfrey Winster
Department Of Computer Science and Engineering
SRM Institutes of Science and Technology,
Chengalpattu - 603203
godfreys@srmist.edu.in

***Abstract*— Cloud computing is a rapidly growing technology which is hugely used in various fields and it offers a strong and fashionable corporate environment. However, cloud computing environment faces many challenges in scheduling and securing the huge amount of data provided by various users. To overcome the conventional performance limitations in resource scheduling and data security various optimization and encryption models are evolved in recent times. However, the performances can be improved if hybrid models are employed. Thus, a hybrid Ant Colony Optimization-Variable Neighborhood Search(ACO-VNS) metaheuristic algorithm is presented in this research work to improved task scheduling. Furthermore, to handle user data security and privacy a combination of Attribute Based Encryption (ABE) with (BKAC) blockchain based key aggregate cryptosystem technique is presented. simulation analysis includes standard benchmark datasets and the performances are compared to existing techniques such as Energy –Efficient Dynamic Scheduling Scheme (EDS), Cross Entropy based Virtual Machine (CEVP), Meta-Heuristic Crow Search Algorithm (H3CSA), PPSO (Parallel Particle Swarm Optimization) and Block Chain based CP-ABE Scheme with Partially Hidden Access Policy (BCP-ABE-PHAS) to validate the superior performance. The experimental result demonstrates the performance of the proposed meta-heuristic and ABE-BKAC model in terms of completion ratio, response time, make span , energy consumption, keygen time, Encryption Time and Decryption Time.**

Keywords*—- *Non Deterministic Polynomial(NP) hard Problem, Ant Colony Optimization (ACO), Varaible Neighborhood Search (VNS), Attribute Based Encryption (ABE), Blockchain based Key Aggregate Cryptosystem(BKAC)

I. INTRODUCTION

Cloud computing is represented as a service method which distributes various computing service to user through internet. cloud offers various services as IaaS, PaaS and SaaS models. generally the computing environment of cloud is categorized into homogeneous and heterogeneous cloud computing. Homogeneous cloud computing is the environment which use complete software stack from the same vendor, whereas heterogeneous cloud computing is the environment which use complete software stack from the different vendors. Since heterogeneous environment uses different vendors, it faces some major challenges and it is shown in the following fig.1.

Due to the requirement of variety of processors for various corporation's heterogeneous cloud computing is most widely adopted in every domain. Providing optimal resources to the tasks is a complex process in cloud computing as it requires to analyze different kinds of processors with different execution time from different vendors. Since, cloud handles numerous processes, tasks will be created frequently. So, an appropriate mapping of corresponding task to the allocated resources becomes hard to achieve. This research work introduces a hybrid meta-heuristic algorithm to overcome this problem.

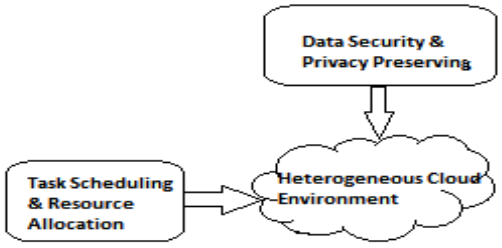

Fig. 1. Major problem faced in heterogeneous Cloud Computig Environment

Various heuristic and meta- heuristic algorithm had been constructed to solve this task scheduling and resource allocation problem. However, the performance of those algorithms is not efficient. In order to overcome the problem, this research work introduces a hybrid meta-heuristic algorithm. Meta-heuristic algorithm is a process of identifying the better solution for hard problems. The research motive is to attain better scheduling performance by decreasing the make span and energy consumption during the process of task scheduling. At the same the data security is also an essential factor in cloud. To resolve data security problem, an efficient encryption method should be used. Since, to enhance the data security at different service level, this work introduces an Attribute Based Encryption method, which uses different scheme for different services. This technique encrypts and decrypts the data based on the user attributes. This algorithm provides better security than other conventional methods since the encrypted data have the attributes instead of original data. Additionally, to ensure the probity and privateness of cloud

data. Since, this research work, introduces a block chain based key aggregation cryptosystem technique to improve the performance of privacy preserving public auditing method. Blockchain-based public auditing technique offers a better result for the issue of conflicting in contrast to the harmful auditors or cloud server providers. With the objective to reduce the energy consumption and make span the following contributions are made in this research work as follows.

- An efficient task scheduling and Resource Allocation in heterogeneous cloud computing environment using hybrid optimization model is presented.
- Data security and Privacy Preserving Public Auditing method using the combination of Attribute
- Based Encryption and Blockchain based Key aggregation Cryptosystem technique is presented.
- Simulation analysis of proposed technique is presented using benchmark datasets and compared with existing techniques.

The remaining discussions are presented in the following sequence. Detailed literature review to present the existing methodologies and its features are included in section II. The proposed optimization and encryption models are formulated and discussed in detail in section III. Simulation analysis and performance evaluation are presented in section IV. The observations are concluded in the last conclusion section.

II. Related Works

A detailed literature review of existing methods proposed by research community for task scheduling and data security in cloud computing is presented based on the methodology, feature merits and demerits. Resource allocation model reported in [5] includes genetic algorithm and random forest classifier as a hybrid model to attain better performance in resource allocation process. Here the training dataset for Random forest technique is created using genetic algorithm. From the dataset created, RF model will get trained to map virtual machine to physical machine. Further Load balancing process is also conducted using IQR technique and maximum correlation policy. Metrics like execution time, average start time, resource utilization, energy consumption, and average finish time are used to evaluate the performance and the result demonstrates better performance. The two level meta-heuristic model reported in [13] adopts lower level Algorithm(LOLA) and upper level Algorithm(UPLA) for the purpose of scheduling the jobs. Here, LOLA generate parameterized – active schedule using decoding procedure and UPLA is used to control the parameters of LOLA. Based on the parameters like direction of scheduling and time limit which is prescribed the user, scheduling is performed for the tasks. Here, make-span is used as an evaluation metrics to analyze the performance.

The method adopted in the report [18] utilizes adaptive probabilistic scheduler to schedule the task in local mobile clouds. The minimizing of the energy consumption is taken as the main objective in this work. Here task completion rate, average task waiting time and average energy are considered to validate the performance. In the article [19] four types of bag-of-task scheduling methodologies. Shortest Job first, Min-Min, Round-robin and Max-Min algorithms were compared and the performance were evaluated using the metrics like Make span ,Throughput ,waiting time, resource utilization and failed tasks due to low battery failure and low memory failure. The result demonstrates that none of the method obtains better performance in minimizing energy consumption. The model reported in [7] uses a HP-CP-ABE Hidden –Policy -Ciphertext-policy Attribute Key Encryption method for cloud data security. Considering the problem of decisional n-BHDE and decisional linear assumption, selective security is achieved. This method utilizes performance like Secret key size, time cost of keyGen, time cost in decryption and time cost in decryption to demonstrate the performance. The method reported in article [10] utilizes a crypto currency based Ethereum blockchain network to ensure the data integrity and security in cloud environment. Result analysis was performed compared with bitcoin. based on the cost associated with generating hash value and cryptocurrency.

From the above survey, it was analyzed that most of the existing task scheduling system are failed to minimize the energy consumption and make span. Thus to attain enhanced performance a hybrid optimization model and encryption model is presented for task scheduling and data security using ant colony optimization, variable neighborhood search method and ABE-BKAC techniques.

III. Proposed Work

The proposed work adopts two stages .The first stage formulates the hybrid optimization model for resource allocation and task scheduling and the second stage involves combination of Attribute Based Encryption and Block chain based Key aggregation Cryptosystem technique for Data security and Privacy Preserving Public Auditing method

A. Task scheduling and Resource Allocation

The proposed hybrid optimization model incorporates ant colony optimization and variable neighborhood search for efficient task scheduling and resource allocation process. The process flow of the task scheduling and resource allocation model is shown in Figure-2.

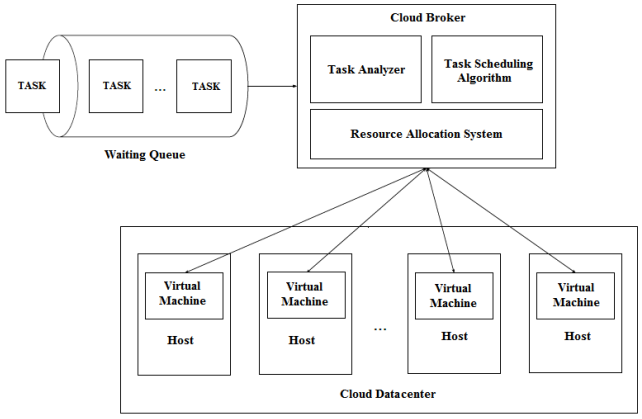

Fig. 2. Proposed model overview

The cloud broker is in charge for the scheduling of tasks, and a waiting queue carries the entire prepared task to be presented for the further implementation. The enquiry of the status of every available resource of virtual machines are performed by cloud broker and based on the status enquiry they

introduces and processes the all available resources. The appropriate processing order of the given tasks is computed using the proposed scheduling algorithm. After the completion of scheduling algorithm, the broker will allocate the tasks to the selected computing resources accordingly.

B. Proposed Ant Colony Optimization and Variable Neighborhood Search Technique

Ant Colony Optimization (ACO) is a nature inspired optimization model algorithm which provides optimal solution based on the food searching behavior of ant. In the proposed work, ACO gives solution to the optimization problem by using pheromone trail and heuristic function. The pheromone trail is a technique used by the ants to share and find required knowledge about better solutions. In this proposed method, assuming P as the pheromone matrix, which contains 'n' number of tasks and 'r' number of machines and P[j][h] represents the allocation of assigning task j to machine h. Next, to find the best solution ant uses heuristic function 'ßjh'and which is given by the following equation

$$\beta_{jh} = \frac{1}{\text{empty[h]}} \quad (1)$$

Where, empty(h) denotes the time by which the machines get empty. When empty(h) is small, then ßjh will become high. The machine is considered to be more efficient if it gets empty soon. The quality of the solution can be given by the fitness function. In this proposed work minimization of make span and energy consumption is taken in account, which denotes the required throughput of the heterogeneous system. The less value of make span and minimum energy consumption represents the scheduling model is producing a good-quality schedule (i.e, the model is efficiently mapping the task to its allocated resource). After every iteration, pheromone matrix is updated using the following equation.

$$P_{jh} = \begin{cases} \sigma \times P_{jh} + \Delta_{P_{jh}} \; if \; h \leftarrow j \; in \; lgood\_ant \\ \sigma \times P_{jh} \qquad\qquad else \end{cases} \quad (2)$$

Where, represents $\sigma(0 < \sigma \leq 1)$ is the decay parameter utilized by the ants to forget poor knowledge and $\Delta_{\beta_{jh}}$ represents the quantity of pheromone accumulated on the way and it is calculated using the following equation.

$$\Delta_{P_{jh}} = \frac{makespan(lgood_{ant})}{makespan(ggood_{ant})} \quad (3)$$

The ant uses two lists to generate solution for task scheduling. One is the scheduled list, which is empty in the beginning and another is unscheduled list which contains j number of tasks at the beginning. The initial allocation of task to the machine is selected arbitrarily. From the pheromone trail Pxy every ant will get benefit of understanding knowledge about scheduling corresponding task x to the allocated machine y. Through the heuristic function ßxy in condition of earliest emptiness, the best available machine is identified. After this, task x from the unscheduled list is process and allocated to the identified available machine. Along with this, proposed model uses one more heuristic function called ETC(x,y) , which is used in the transition rule. According to the rule, task x is stochastically selected to be assigned to a machine y . The transition rule used here is given using the following equation

$$s_{xy} = \frac{[p_{xy}]^{\alpha} \times [\beta_{xy}]^{\gamma} \times \frac{1}{ETC[x,y]}}{\sum [p_{xy}]^{\alpha} \times [\beta_{xy}]^{\gamma} \times \frac{1}{ETC[x,y]}} \quad (4)$$

Where α denotes the pheromone relative weight parameter and γ denotes heuristic relative weight parameter and ETC is the expected execution time to complete task j on machine h. The process of scheduling and allocation will get continues until the entire task in the unscheduled list gets completed.(i.e, unscheduled list becomes zero). All the ant in the colony follows this and construct their best solution. The ant which is having the minimum make span is obtained as the good local ant. For every iteration, the pheromone trail condition will get updated using equation (3) and the entire process will get repeated until it reaches defined ending condition.

C. Variable Neighborhood Search

In order to improve the ultimate solution of ACO technique, this proposed work combines VNS to the ACO algorithm. VNS utilize several neighborhood designs to examine a number of neighborhoods for the existing necessary solution. A well represented neighborhood designs will definitely provide better examination of improved solution. The methodical modification of neighborhood structures is the basic purpose of the VNS metaheuristic. This modification takes place in the two phases, one is descent phase in this the meta-heuristic search to identify a local minimum; and another is the perturbation phase in this the meta-heuristic try to run away from the local minimum. VNS includes three steps to search the variable Neighborhood and those are Quake step, Development Step and Neighborhood variable step. Quake step contains the submission of a set of operators in a specific order. The problem of local minimum trapping is resolved using these operators .Then, in development step the improvement of the solution found in quake step is obtained by performing local search using Problem Aware Local Search (PALS) search. The process of this step generally involves two basic process called Initial development and best development. In the Initial development, the local seek process will get stops, when it identifies the development solution for existing solution, whereas in the best development ,the local search process will continue until it find the all possible solutions and then it selects the best from those identified possible solutions. Lastly variable neighborhood step will takes place, which helps to take a decision for accepting or rejecting the existing solution as a new necessary solution. These three steps will continue to process until it reaches some ending condition.

D. Data Security and Preserving Privacy Public Auditing

To secure data in cloud a combination of Attribute Based Encryption (ABE) with (BKAC)blockchain based key aggregate cryptosystem technique is presented in this section. The work flow of the proposed data security and privacy preserving model is shown in the figure-3. The proposed structure consist of the following proprietor of data (POD),User of data(UOD). Attribute In charge, Interplanetary File System(IPFS) and a Block chain.

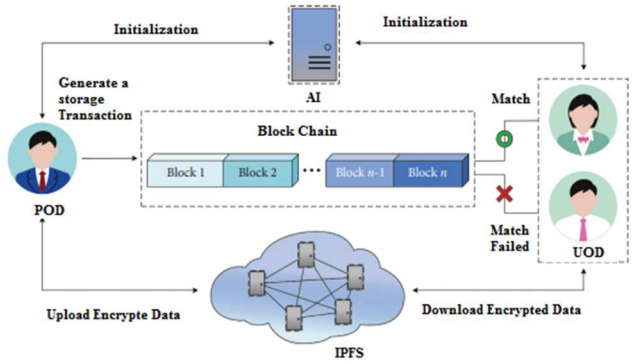

Fig. 3. Data Security and Privacy Preserving Model

The proposed scheme uses following steps:

1. Setup (1α): This method is executed using AI.It take 1α as the security parameter and gives public parameter (param)as output.

2. Keygen(param,pk,msk): It is utilized by AI.It takes public parameter as input t and gives Master secret key and public key as output.

3. Encrypt (pk,m,($\overline{ap}$,g):It is utilized by POD .It contains ConstructGBF and GenCT function.

ConstructGBF,($\overline{ap}$,g): It takes access policy($\overline{ap}$) and set of wildcard position(g) as input and gives GBF as output.

GenCT(pp,m,($\overline{ap}$,g)):It takes public parameter(pk),message(m),access policy $\overline{ap}$ and set of wildcard position(g) as input and gives ciphertext(CT) as output.

4. Extract(msk): It is utilized by POD..It takes Master Secret Key (msk) as the input and gives aggregate key associated weight as an output (skw).

5. Decrypt (pk,skw,GBF,CT): it is utilized by UOD . It consist of QuesGBF and Decr functions

6. QuesGB.(w,GBF): Here attribute vector of UOD (w) is taken as the input and question GBF to determine set of wildcard position(g).

7. Decr(pk,skw, CT,g) : Here public parameter(pk), secret key with associated weight(skw), wildcard position(g) and ciphertext CT are taken as input and gives an message(m) as output. When the attribute vector of the UOD has follows the given access policy $\overline{ap}$ then the user will receives the message m from decrypt algorithm and the user is considered as an authorized person to open the file , otherwise decrypt algorithm will gives a random message as an output and the user is considered as an unauthorized person and he cannot able to open the file.

IV. Results and Discussion

The proposed model performance is evaluated in this section using JPBC library dataset, The proposed methods are implemented on a on a Windows 10 PC with 16GB RAM. The performance of the proposed hybrid meta-heuristic model is demonstrated using Make span, Response time, Completion Ratio and Energy consumption and compared with other conventional algorithms like EDS,CEVP and H3CSA. Similarly the performance of the proposed ABE-BKAC technique is validated using Keygen time, Encrypt time and Decrypt time and compared with other CP-ABE scheme. Energy consumption analysis of proposed model and existing models are presented in fig.4. Results demonstrates the better performance of proposed model which has minimum energy consumption compared to EDS and CEVP methods.

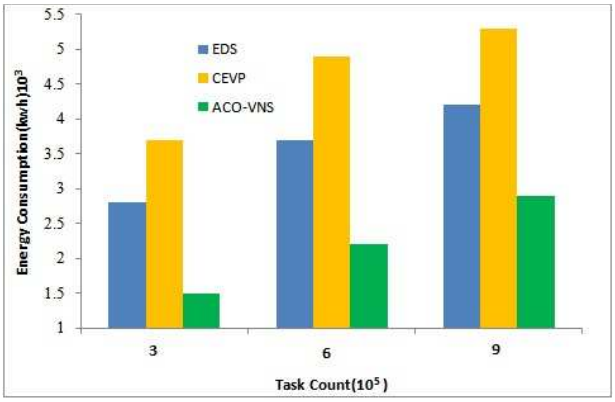

Fig. 4. Comparison of Energy comparison(kwh)

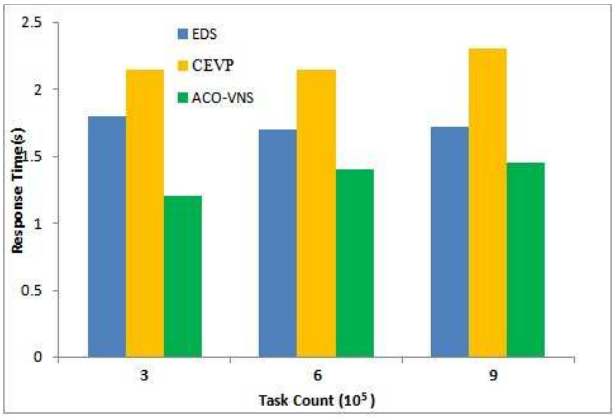

Fig. 5. Comparison of Response Time(s)

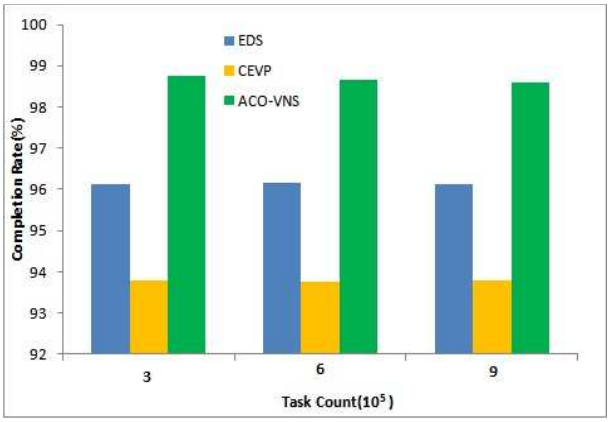

Fig. 6. Comparison of Completion Rate (%)

The analysis of response time is shown in figure-5.From the figure it is noted that the response time of the proposed ACO-

VNS is 0.3% less than EDS and 0.63% lesser than CEVP. The analysis of completion time is shown in figure-6. From the figure it is noted that the completion ratio of the proposed ACO-VNS is 2.53% less than EDS and 4.89% lesser than CEVP.

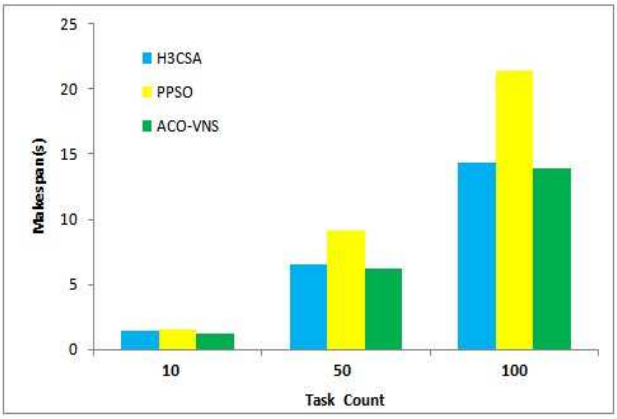

Fig. 7. Comparison of Makespan(s)

The analysis of Make span is shown in figure-7. From the figure it is noted that the response time of the proposed ACO-VNS is 0.82% less than H3CSA and 4.74% lesser than PPSO.

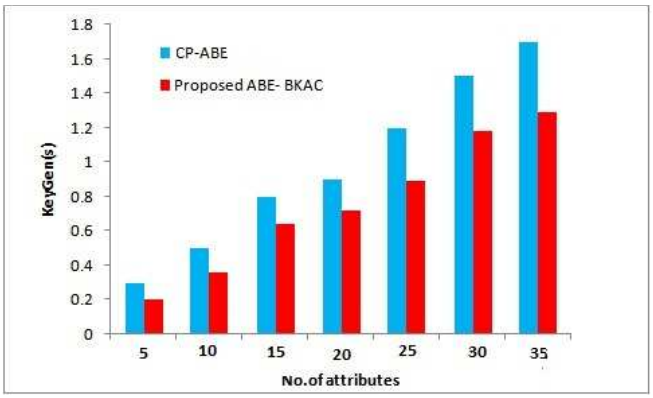

Fig. 8. Comparison of KeyGen time (ms)

The analysis of KeyGen time of proposed ABE-BKAC is shown in figure-8. Results confirms the better performance of proposed model in terms of keyGen time over existing CP-ABE model.

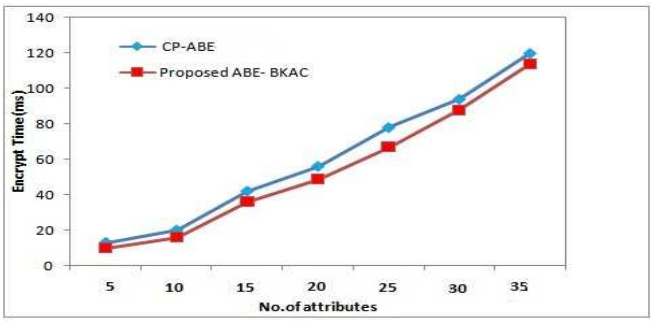

Fig. 9. Comparison of Encryption time (ms)

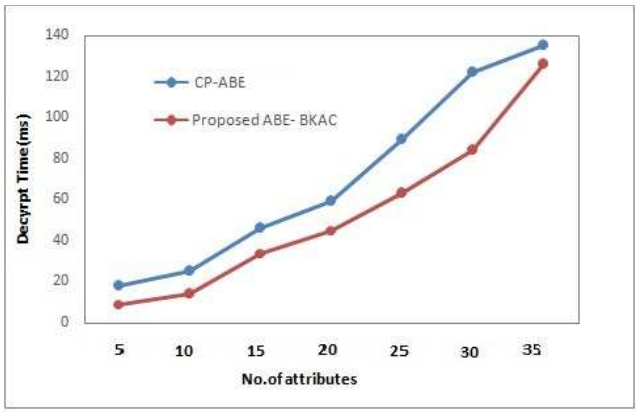

Fig. 10. Comparison of Decryption time (ms)

Figure 9 and 10 depicts the comparative analysis of proposed model and existing models for encryption and decryption time respectively. Results demonstrate the better performance of proposed model over existing technique like CP-ABE in encryption and decryption time. From the above result analysis, it was clear that the proposed ACO-VNS task scheduling technique provide better performance than other conventional methods like EDS,CEVP,H3CSA and PPSO. Similarly ,the proposed ABE-BKAC data security and privacy preserving technique provide better performance than CP-ABE conventional technique.

V. Conclusion

The proposed work presented a hybrid ACO-VNS meta-heuristic for task scheduling and resource allocation process and presented a ABE-BKAC technique for effective data security and privacy. The proposed multi-objective attains better performances compared to existing methods. Most of the existing model concentrate only either on task scheduling or security, but this proposed work concentrated on both the task scheduling and security hybrid meta-heuristic model used in the proposed work achieved effective task scheduling using optimization process . This model achieves minimized amount of energy and make span than other existing methods. The ABE-BKAC scheme used in the proposed work provides efficient data security and privacy preserving of cloud data.

References

[1] Belal Ali Al-Maytami , Pingzhi Fan, Abir Hussain , Thar Baker, Panos Liatsis"A Task Scheduling Algorithm With ImprovedMakespan Based on Prediction of TasksComputation Time algorithm for Cloud Computing," IEEE Access, vol. 7, pp. 160916-160926, 2019, doi: 10.1109/ACCESS.2019.2948704.

[2] Keke Gai ; Meikang Qiu; Hui Zhao; Xiaotong Sun, "Resource Management in Sustainable Cyber-Physical Systems Using Heterogeneous Cloud Computing," IEEE Transactions on Sustainable Computing, vol. 3, pp. 60 - 72, 2018, doi: 10.1109/TSUSC.2017.2723954.

[3] Fadl Dahan , Wojdan Binsaeedan , Meteb Altaf ,Mahfoudh Saeed Al-Asaly Mohammad Mehedi Hassan, "An Efficient Hybrid Metaheuristic Algorithm for QoS-Aware Cloud Service Composition Problem,IEEE Access, vol. 9, pp. 95208 - 95217, June. 2021, doi: 10.1109/ACCESS.2021.3092288

[4] Hadi Naghavipour ,Tey Kok Soon ,Mohd Yamani Idna Bin Idris, Morteza Namvar ,Rosli Bin Salleh , Abdullah Gani, "Hybrid Metaheuristicsfor QoS-Aware Service Composition: A Systematic Mapping Study" IEEE

Access, vol. 10, pp. 12678 - 12701, 2021, doi: 10.1109/ACCESS.2021.3133505.

[5] Madhusudhan H S ,Satish Kumar T , S.M.F D Syed Mustapha ,Punit Gupta ,Rajan Prasad Tripathi, "Hybrid Approach for Resource Allocation in Cloud InfrastructureUsing Random Forest and Genetic Algorithm,"Sceintific Programming,pp. 1-10, 2021, https://doi.org/10.1155/2021/4924708.

[6] Zhenwei Chen , Axin Wu , Yifei Li ,Qixuan Xing , Shengling Geng, "Blockchain-Enabled Public Key Encryption with Multi-Keyword Search in Cloud Computing,Security and Communication Networks, pp. 1-11, 2019, https://doi.org/10.1155/2021/6619689

[7] Leyou Zhang, Yilei Cui , and YiMu, " Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing,"IEEE System Journal, ,vol.14,no.1,pp. 387 - 397, May. 2019, doi: 10.1109/JSYST.2019.2911391.

[8] Hongmin Gao ,Zhaofeng Ma ,Shoushan Luo ,Yanping Xu ,and Zheng Wu, "BSSPD: A Blockchain-Based Security Sharing Scheme for PersonalData with Fine-Grained Access Control,"Wireless Communications and Mobile Computing,pp.1-20, 2021, https://doi.org/10.1155/2021/6658920.

[9] Deafallah Alsadie, "A Metaheuristic Framework for Dynamic Virtual Machine Allocation With Optimized Task Scheduling in Cloud Data Centers" IEEE Access vol. 9, pp. 74218 - 74233, May 2021, doi: 10.1109/ACCESS.2021.3077901.

[10] Ruba Awadallah , Azman Samsudin , Je Sen Teh , And Mishal Almazrooie, "An Integrated Architecture for MaintainingSecurity in Cloud ComputingBased on Blockchain," IEEE Access, vol. 9, pp. 69513-69526,Feb 2021, doi: 10.1109/ACCESS.2021.3077123.

[11] Xiaodong Yang ,1 Aijia Chen ,1 Zhisong Wang,1 and Shudong Li, "Cloud Storage Data Access Control Scheme Based on Blockchainand Attribute-Based Encryption," Security and Communication Networks, pp. 1-12, 2020, https://doi.org/10.1155/2022/2204832.

[12] Tianqi Zhou ,1 Jian Shen ,1,2 Yongjun Ren ,1 and Sai Ji, "Threshold Key Management Scheme for Blockchain-BasedIntelligent Transportation Systems,"Security and Communication Networks, pp. 1-8, 2021, https://doi.org/10.1155/2021/1864514.

[13] Pisut Pongchairerks, "A Two-Level Metaheuristic Algorithm forthe Job-Shop Scheduling Problem," Complexity, pp. 1-11, 2019,https://doi.org/10.1155/2019/8683472.

[14] Debabrata Samanta , Ahmed H. Alahmadi, Karthikeyan M. P,Mohammad Zubair Khan , Amit Banerjee , Goutam Kumar Dalapati, Seeram Ramakrishna, "Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture,"IEEE Access, vol. 9, pp. 98013 - 98025, July 2021, doi: 10.1109/ACCESS.2021.3095297.

[15] Ying Miao1, Qiong Huang 1,2, Meiyan Xiao1, And Hongbo, "Decentralized and Privacy-Preserving PublicAuditing for Cloud Storage Based on Blockchain," IEEE Transactions on Affective Computing, vol. 8, no. 3, pp. 139813-139826, Aug.2020, doi: 0.1109/ACCESS.2020.3013153.

[16] Chunhua Li, Jinbiao He, Cheng Lei, Chan Guo, Ke Zhou, "Achieving Privacy-Preserving CP-ABE Access Control with Multi-Cloud," in Intl Conf on Parallel & Distributed Processing with Applications, vol. 29, pp. 801-808, 2018, doi: 10.1109/BDCloud.2018.00120.

[17] Pooja More. "Cloud Data Security using Attribute-based Key-Aggregate Cryptosystem." International Conference on Research in Intelligent and Computing in Engineering (RICE), Oct 2018,doi: 10.1109/RICE.2018.8509077.

[18] Ting Shi1, Mei Yang, Xiang Li, Qing Lei, YingtaoJiang, “An energy-efficient scheduling scheme for time-constrained tasks in local mobile clouds” , Pervasive and Mobile Computing, vol-27,pp-90-105, 2019, https://doi.org/10.1016/j.pmcj.2015.07.005.

[19] Roxana-Gabriela Stan , Lidia B˘ajenaru , C˘at˘alin Negru .Florin Pop “ Evaluation of Task Scheduling Algorithm in Heterogeneous Computing Environment” Sep 2021, https://doi.org/10.3390/s21175906

[20] Samuel Manoharan, J.: A Novel user layer cloud security model based on chaotic Arnold Transformation using fingerprint biometric traits. Journal of Innovative Information Processing. 3(1): 36 – 51. (2021.