International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhanced Cloud Security Model with Hybrid Encryption Approach for Advanced Data Security in Cloud Computing

[1]Jayachandran R., [2]Malathi D.

Submitted: 04/09/2023 **Revised**: 23/10/2023 **Accepted**: 06/11/2023

Abstract: Cloud computing (CC) is a typical paradigm that maintains, manages, and backs up statistics remotely using dynamic capabilities. It allows consumers and companies to access services on demand and as needed across a web network, and it increases the capabilities of physical resources by maximizing and sharing their utilisation. Cloud computing performance can be harmed by inefficient resource management. As a result, resources must be distributed fairly among many stakeholders without jeopardizing the organization's profit or user happiness. Information security and privacy, on the other hand, have surfaced as a major worry threatening CC's success. To begin with, storing data on the cloud increases the risk of data leakage and unauthorised access. Second, cyber-attacks and disruptions are increasingly targeting cloud systems, posing a danger to cloud security. It's It is a requirement for the advancement of distributed computing. As a consequence, in this paper, a hybrid task-based security method has been developed. A secure and safe environment for distributed computing operations has been built using the improved Cat Swarm algorithm for Task Scheduling with Quantum Key Distribution ICSTS-QKDP for CC, which employs quality-based encryption. To begin, an improved cat swarm optimization algorithm-based short scheduler for task scheduling (ICSTS) reduces make-span time while increasing throughput. The suggested design provides cloud users peace of mind when it comes to data security. Quantum Key Distribution Protocol (QKDP) incorporates quantum key cryptography to provide cloud storage security and control data dynamics. A large quantity of data is collected from a variety of computing devices in the distributed computing paradigm, which may be monitored and limited by the framework. The strategy is primarily concerned with data access, storage, and management. The secured keys are transferred across a trusted channel when the model is used. The suggested approach outperforms the present one in terms of resource usage, energy consumption, reaction time, secure key transfer, and so on. Its goal is to prevent unauthorised client access and ensure that only authorised clients have access to the same data.

Keywords: *Task scheduling, Cloud computing, Key agreement, QKDP, time consumption.*

1. Introduction

The cloud paradigm has indeed been thought out to help users [1]. The cloud model is a hereditary one that was created by combining the efficacy of existing and new ways to supply services depending on user requests. Furthermore, the paradigm offers Software services, Platform as a Service, Cloud infrastructure, and other services [2]. In particular, private, public, community, and plug - in hybrids are used to distribute services. When data is outsourced to the cloud, considerations such as cloud responsibility, data integrity, and security must be taken into mind [3]. Data security, which is critical in a variety of applications, is the largest challenge in the cloud for the owner who exposes their own information.

Furthermore, because the cloud is based on the bedrock of two fundamental pillars, namely cloud computing and networking, Internet connectivity and infrastructure are critical. The network may be utilised for CC and other applications in numerous cloud apps [3]. As either a result, more application service providers (ASPs) [4] understand the difference amongst actual usage and maintenance. In terms of the demand prediction schedule, the ASP examines the renting services on a regular basis, makes suitable decisions concerning objective and resource allocation [5,6].

Data security and job planning are the most common concerns in cloud computing. Task planning, on the other hand, is generally a primary focus of CC research. Many jobs in CC need great performance, a fast accomplishment time, a quick reaction time, and the ability to utilise available resources. The jobs must be assigned appropriately because of the allocation plan's many aims. It may give services to clients utilizing a variety of resources through the Internet [7]. Amazon has built various cloud computing systems since introducing the notion of cloud computing. Small, big, and extremely large events are separated into three groups based on their size [8]. The IT industry is significantly impacted by CC [9], and there is fierce competition among enterprises in terms of service delivery efficiency [10]. Companies are also attempting to develop or update their services using a variety of resources in order to attract more clients to the cloud [11]. As a result, resource allocation and SLA [12], which measures customer happiness, are two of the most critical criteria that influence service quality. Dimensions

[1,2]*Department of Computing Technologies,*
S.R.M Institute of Science and Technology,
Kattankulathur-603203

and bounds must be established, and achieving upper parameters is challenging [13].

Security in cloud computing is a difficult issue nowadays. Because secret keys are transferred as photons across a Fibre optics connection through quantum-based channels. It's difficult to launch communication while moving from a fibre optic connection to a cloud environment. It is assumed that without fibre optic connection, communication will take place in the cloud. Quantum communication technology is critical for safeguarding communication channels [14] against unauthorised users. Quantum cryptography [15] has received a great deal of attention in previous studies, and the QKD is derived from quantum cryptography. The random key is generated amongst two authorised users in the remote area using this QKD [16]. Recently, some novel QKD advancements and strategies have been proposed [17].

The resulting are some noteworthy contributions made by this study:

- To deal with resource constraints in the cloud, we recommended using the sophisticated Cat optimization algorithm to schedule user workloads.
- To optimize the work, the recommended resource allocation and protection with intelligent computer strategy development employ hybrid machine learning.
- To improve passive capabilities, ICS-TS splits the cloud environment into workspace and state space. GO-DNN-based planning process further reduces resource utilisation in a massive cloud system with several servers handling numerous user requests each day.
- QKD has been presented as a way to improve security.

The remainder of the paper is organised as follows. Introduction is depicted in the first part. Section 2 explains the themes of related work. The suggested framework with algorithm is shown in Section 3. The execution and outcomes are described in Section 4. To conclude, section 5 discusses the conclusion and references.

2. Related Work:

Over the past two decades, CC has become more and more popular as a distributed system that relies on the Internet. It has drawn a lot of interest since it can swiftly provide and unload resources from shared pools based on requests [18]. The volume of request that require to be processed in the cloud increases along with the increase in cloud users. The performance of a work will be diminished if the scheduling is inappropriate [19]. The scheduling algorithm is in charge of distributing work requests from cloud users to cloud resources [20].

Initially, people looked at task scheduling with an emphasis on quality of service. He et al. [21] were pioneers, analysing and executing the next schedule using QoS parameters as evaluation criteria. The proposed solution is a general method that incorporates QoS into the Min-Min heuristic algorithm and considerably increases performance. A cloud-based QoS-driven job task scheduling is developed [22] that line up tasks based on their uniqueness, assigning resources and allocates resources. It was put to the test and found to perform well in terms of load balancing and performance. S et al. [23] improves resource consumption efficiency, reduces costs, and delays by using the recommended and distributed queue based on active demand. To limit energy usage the workload to calculate the number of VMs to employ, as well as the control of incoming requests is done [24].

The authors of [25] proposed and asserted the effectiveness of a two-three party QKD prototype. The use of QKDP to protect the data from the dense-coding attack is well established [26]. The QKDP is reportedly faster than existing Cloud security techniques, according to [27]. The model was validated using fibre optic channels for data transmission and a novel QKDP model to manage weak consistent states in connection [28]. Furthermore, the work presented in [29] has categorized cloud service providers in order to ensure the security of cloud private data using an enhanced cloud security model based on QKDP (ECSM-QKDP). A cloud-based security paradigm based on erasure codes has been developed.

[30] created a Provable Data Possession (PDP) concept with a hash index hierarchy approach for cloud data security. The findings suggest that the proposed model outperforms current models in terms of effectiveness.

3. Proposed Work:

Numerous experts have tried to achieve superior results in asset allocation, asset arranging, and asset appropriation based on the review [21–31]. Clients did not need assets during previous evaluations, and because assets were distributed, clients did not organize. Distributed computing faces a big problem with assignment scheduling. An efficient use of resources will result from proper job planning.

Additionally, one-time pad communication is used to ensure data security. The attempt of the attacker to obtain the data can be recognized. The quantum channel is used by the BB84 protocol to understand and share the qubits between two entities. Additionally, different polarizations are used to represent the quantum states.

This section describes the working procedure of the proposed ICSTS-QKDP for CC, which employs quality-based encryption.

3.1 Network Model

The service provider receives a request from the cloud user asking for access to various cloud resources. Loads are used to illustrate this necessity. There are four divisions of the workload. The task manager receives the workload and divides it into various categories. To shorten workdays and increase production, a work plan based on the sophisticated cat live algorithm is used. To create a loaded virtual machine (VM), the centers of each cluster's loads are determined and aggregated. The formation of the C1, C2, C3, and C4 clusters. In Figure 1, a detailed model is displayed. There are several task managers, and there are various clusters for the workload. Task scheduling and resource management are managed using the ICS-TS and GO-DNN scheme. Each VM's RAM, CPU, and bandwidth usage of each allotment are calculated, and the virtual machines are organised according to their best VM value.

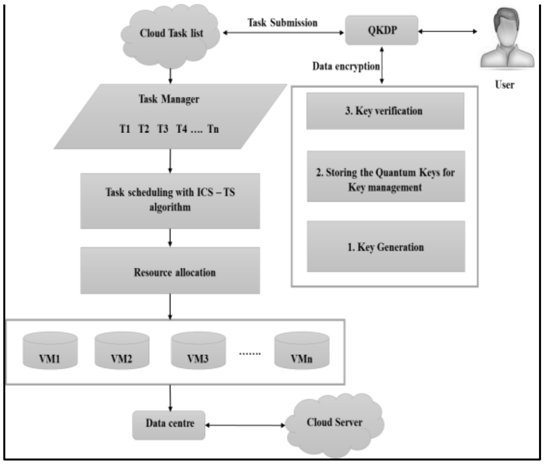


Fig 1: Proposed model of ICTS-QKDP

In order to optimize task scheduling, the proposed system's ICS-TS algorithm receives inputs including user request, Task Type, Task Dependency, and Bandwidth and returns multiple service providers. In order to maximise resource usage, it employs the Group Optimized Deep Neural Network (GO-DNN) technique. The system uses the QKDP encryption technique to boost security.

3.2 Using the ICS-TS method for task scheduling

The following are the variables that numerous service providers can use to optimize scheduling:

User request (U_r): A collection of user requests made up of 1 to n task items.

Task Type (T_t): The task type is specified, and it ranges from 1 to m. The Tm specifies the maximum number of tasks that may be performed within the task unit.

Task dependency (T_d): Task unit dependencies are shown as U_r. $T_{d\ ij} = 1$ is the data retrieved from U_{ri}, and this data is utilised by $T_{d\ ij}$. Otherwise, $T_{d\ ij} = 0$ is taken into account.

Input Data (D_{in}): The activity unit's data input size is expressed as input information.

Output Data (D_{out}): The errand unit's yield information size is referred to as D_{out}. The asset pool is considered heterogeneous in this case, and the benefit is obtained from the real machine, a person, or a PC at the remoteness that makes up the information centre. The same assets are assigned to several arrangements. R = (PM, P_c, CP, R, CE, N_{bw}, E_{com}).

Physical Machines (PM): It is denoted as PM = (PR1, PR2, PR3,..., PRn) and denotes the collection of real machines present in a data centre.

Computing Power (P_c): The matrix of the dispensation power of the real computers is denoted by the letters pc. $P_{c\ ij}$ denotes the finishing of task unit type I on a PM_j, with $P_{c\ avg,j}$ being the average power of PM_j. The power utilization is calculated by averaging the entries in a matrix $P_{c\ j}$'s column.

Bandwidth (BW): BW_{ij} indicates the frequency band between PMs and the transfer speed between PM_i and PM_j.

In the cloud services, it is initially assumed that there are k-subtasks for users. R1, R2,..., Rm indicates computational resources. Each resource, Rj, is assumed to have a fixed costs price, which is denoted by pj. p = {p1, p2,..., pm} is the price vector. ti is the time allotted for Ri to complete the subtask. t = t1, t2,..., tm denotes the execution time vector.

ICS are one-of-a-kind social insects that live in the services they produce. The queen, a few of the planes, and the workers are indeed the three most frequent bee components. Because of the royal jelly, the queen bee is bigger than ordinary bees. A queen's usual lifespan is five to six years, during which time she can lay up to 1500 eggs. The aircraft attempts to join the queen in the air when she travels inside the bee. Equation (1) depicts a queen-controlled drone crossing.

$$P(D) = e^{\frac{-\Delta(f)}{S(t)}} \qquad (1)$$

where P(D) denotes the likelihood, and $\Delta(f)$ indicates the importance of the distinction between the spermatheca of the queen as well as the sperm of the drone. S(t) is speed at time 't'. The speed and energy drop with each iteration, are given respectively:

$$S\,(t+1) = \langle S(t) \qquad (2)$$

$$E(t) = \langle E(t) \qquad (3)$$

where the randomly produced factor ‘ ⟨’ ranges between [0, 1]. At each cycle, it estimates the lowered energy and speed. The letters 'E' and 'S' stand for energy and speed, respectively. The complete algorithm may be found below.

Algorithm:

1. D_{in}, U_r, T_t, and BW should all be initialized.
2. Determine the U_r and D_{in} (using it eqn)
3. Determine the T_d.
4. Eliminate the data that is dependent from the vector
5. Get the starting value of P (D)
6. If (P (D) = = 1)
7. U_r that has a higher importance is carried out.
8. P_c,CE should be calculated.
9. Maintain the finest solution.
10. Else
11. Pause pending P (D) reaches a high level.
12. If (P (D) == 0) after some iteration
13. Replacing the queen with brood.
14. End

The difficulty of the ICS-TS approach is O(n), where n is the quantity of occurrences. The most significant goal is to improve resource allocation. The efficiency of cloud systems is enhanced via resource utilisation. Another factor is minimizing the cost of utilizing existing resources. As a result, GO-DNN is used to allocate resources.

3.3 QKDP framing:

BB84 is a procedure that is described as a protected QKDP and is developed for network amenities. The photon attribute is also used by the protocol. The bit series for quantum data is prepared by entity A. In light of this, entity A generates a quantum state that is thereafter randomly chosen and saved. During the creation of the quantum state, Entity A chose a data bit that is dispersed. The entity at the other end does the same for recording the results and verifying the bit order. Just after post-processing, the quantum keys have been distributed. The next stage employs the Safeguard Authentication Protocol to secure key distribution and key sharing (SAP). Figure 1 shows the flow of work for the proposed system.

The reliable nodes transfer the quantum secret keys, which are then transmitted through Near Field Connectivity to other users. The technology's maximum communication range is 10 cm, which is sufficient to shield shared data from eavesdroppers. Moreover, a distance bounding model is used to frame the SAP, preventing relay assaults.

The following are the requirements for proximity limiting in SAP:

Initialization: The round-trip duration is supplied as 'Δt_{max}', and the startup is done to exchange the baseline quantum secret key q_x and q_y with the hash function HS.

Phase of reaction: A random number 'r_a', a message, and the hash rate are calculated as a sending response from mobile entities. The encrypted answer is returned by the mobile entity. In another manner, the mobile entity only transmits a single answer every round.

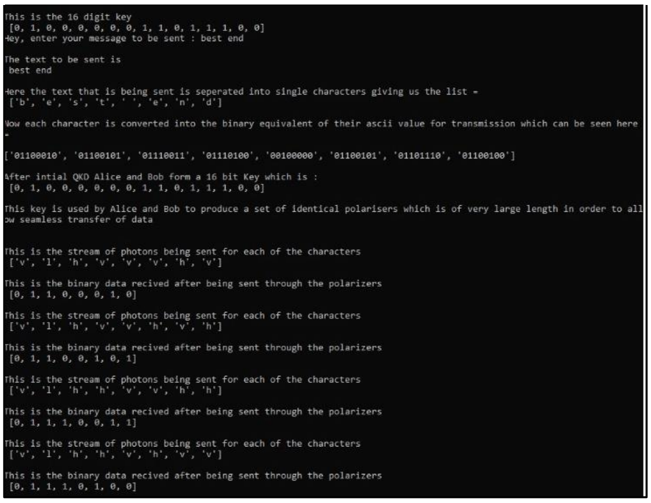
Phase of verification: The channel verifies the verification round trip time as well as the encrypted material.

Using the HASBE technique, the quantum secret keys are exchanged with the protected quantum keys in a secure storage area. Thus, the secure and safe environment with scheduled task is implemented effectively.

4. Experimental Results:

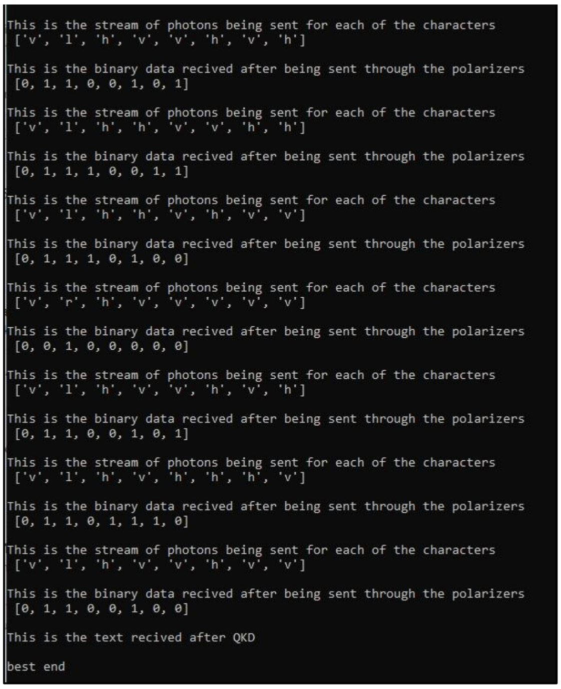
With the aid of the simulation programme known as CloudSim, the suggested model is assessed and tested. The results and comparisons between the suggested model and the current models are presented in this section.

Additionally, evaluations of the results are done based on aspects like calculation time, key generation time, memory usage, and the maximum services offered to consumers.



```
This is the 16 digit key
 [0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0]
Hey, enter your message to be sent : best end

The text to be sent is
 best end

Here the text that is being sent is seperated into single characters giving us the list -
 ['b', 'e', 's', 't', ' ', 'e', 'n', 'd']

Now each character is converted into the binary equivalent of their ascii value for transmission which can be seen here
-

['01100010', '01100101', '01110011', '01110100', '00100000', '01100101', '01101110', '01100100']

After intial QKD Alice and Bob form a 16 bit Key which is :
 [0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0]

This key is used by Alice and Bob to produce a set of identical polarisers which is of very large length in order to all
ow seamless transfer of data


This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'v', 'v', 'v', 'h', 'v']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 0, 0, 0, 1, 0]

This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'v', 'v', 'h', 'v', 'h']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 0, 0, 1, 0, 1]

This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'h', 'v', 'v', 'h', 'h']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 1, 0, 0, 1, 1]

This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'h', 'v', 'h', 'v', 'v']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 1, 0, 1, 0, 0]
```

Fig 2a: Execution window



```
This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'v', 'v', 'h', 'v', 'h']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 0, 0, 1, 0, 1]

This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'h', 'v', 'v', 'h', 'h']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 1, 0, 0, 1, 1]

This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'h', 'v', 'h', 'v', 'v']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 1, 0, 1, 0, 0]

This is the stream of photons being sent for each of the characters
 ['v', 'r', 'h', 'v', 'v', 'v', 'v', 'v']

This is the binary data recived after being sent through the polarizers
 [0, 0, 1, 0, 0, 0, 0, 0]

This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'v', 'v', 'h', 'v', 'h']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 0, 0, 1, 0, 1]

This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'v', 'h', 'h', 'h', 'v']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 0, 1, 1, 1, 0]

This is the stream of photons being sent for each of the characters
 ['v', 'l', 'h', 'v', 'v', 'h', 'v', 'v']

This is the binary data recived after being sent through the polarizers
 [0, 1, 1, 0, 0, 1, 0, 0]

This is the text recived after QKD

best end
```

Fig 2b: Execution window

In Fig. 2, the execution window is displayed. The results of the time calculations of secured keys with respect to the stages in HAT are shown in the graph in Fig. 3. Table 1 provides the corresponding values. The suggested model requires more time to commutate secure keys as the HAT gets larger, as illustrated in the picture.

Fig. 4 shows the outcomes of the evaluation of the general processing time dependent on the size of the shared data files. This provides evidence of the proposed model's storage efficiency. The suggested model, among others, successfully secures the shared data using the QKDP execution

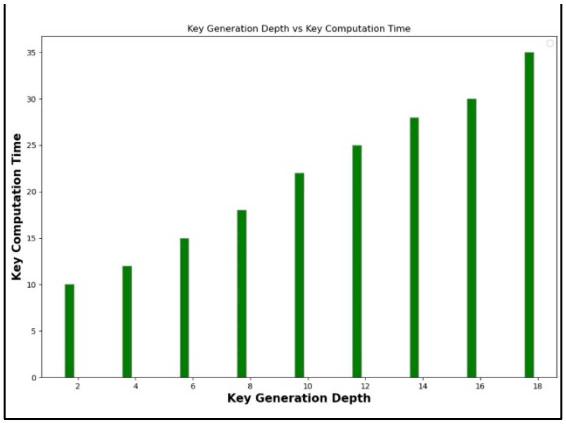


Fig 3: Time computations of secured keys

Table 1: The essential computation time analysis's findings

Key Generation Depth	Key Computation time (mS)
2	9.8
4	12
6	13.1
8	14.5
10	21.1
12	24.3
14	26.4
16	28
18	34

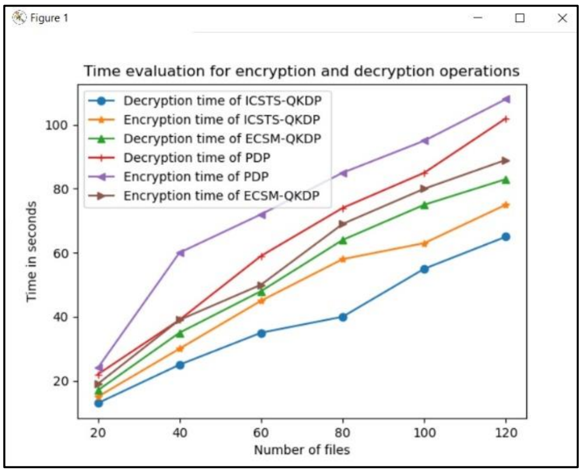


Fig 4: Time evaluation

In this case, the suggested cloud model offers users with secure services up to 99.2% of the time, which is the most effective outcome compared to other models. The time factor is used to analyse this component.

5. Conclusion:

The enhanced Cat Swarm method for Task Scheduling with Quantum Key Distribution ICSTS-QKDP for CC, which uses quality-based encryption, is presented in this study. We introduced a hybrid machine learning approach that organises jobs and distributes resources efficiently in cloud settings in this paper. When comparing our suggested technique to the present PDP, ECSM-QKDP systems for CPU consumption and response, we noticed that our methodology produces good results. The suggested approach employs HASBE technique. Through the QKD channel, the keys to authorised users. Users, on the other hand, can communicate with cloud apps using quantum cryptography after completing the authentication procedure.

The experimental findings reveal that the suggested paradigm improves data security when shared via the cloud by utilizing quantum cryptography's improved security enforcement. In the future, a safe quantum computing technique for massive data processing might be created. Furthermore, for analysis, the employments are carried out in a real-time context.

References

[1] Scott, A.: The limits of quantum computers. In: Proceedings of the second international conference on computer science: theory and applications, CSR'07. pp. 4–4. Springer-Verlag, Berlin, Heidelberg(2007). https://doi.org/10.1186/s13635-016-0051-2.

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: a Berkeley view of cloud computing, University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, (2009).

[3] Wang, C., Wang, Q., Ren, K.: Towards secure and dependable storage services in cloud computing. IEEE Trans. Serv. Comput. 2(2), 220–232 (2012).

[4] Son, S.; Jung, G.; Jun, S.C. An SLA-based cloud computing that facilitates resource allocation in the distributed data centers of a cloud provider. J. Supercomput. 2013, 64, 606–637.

[5] Wei, G.; Vasilakos, A.V.; Zheng, Y.; Xiong, N. A game-theoretic method of fair resource allocation for cloud com-puting services. J. Supercomput. 2010, 54, 252–269.

[6] Buyya, R.; Yeo, C.S.; Venugopal, S.; Broberg, J.; Brandic, I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Futur. Gener. Comput. Syst. 2009, 25, 599–616.

[7] Almeida, J.; Almeida, V.; Ardagna, D.; Cunha, Í.; Francalanci, C.; Trubian, M. Joint admission control and resource allocation in virtualized servers. J. Parallel Distrib. Comput. 2010, 70, 344–362.

[8] Mei, H.; Wang, K.; Yang, K. Multi-Layer Cloud-RAN With Cooperative Resource Allocations for Low-Latency Computing and Communication Services. IEEE Access 2017, 5, 19023–19032.

[9] Khasnabish, J.N.; Mithani, M.F.; Rao, S. Tier-Centric Resource Allocation in Multi-Tier Cloud Systems. IEEE Trans. Cloud Comput. 2015, 5, 576–589.

[10] Bal, P.K.; Pradhan, S.K. Privacy Preserving Secure Data Storage scheme based on Adaptive ANN and Homomorphic ReEncryption Algorithm for Cloud. In Proceedings of the 2019 International Conference on Intelligent Computing and Remote Sensing (ICICRS), Bhubaneswar, India, 19–20 July 2019

[11] Bal, P.K.; Pradhan, S.K. Multi-level authentication-based secure aware data transaction on cloud using cyclic shift transposition algorithm. In Advances in Intelligent Computing and Communication; Springer: Singapore, 2020.

[12] Das, T.K.; Tripathy, A.K.; Srinivasan, K. A Smart Trolley for Smart Shopping. In Proceedings of the 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 3–4 July 2020

[13] A. Winter, Coding theorem and strong converse for quantum channels, IEEE Trans. Inform. Theory 45(7) (1999)

[14] Z. Sakhi ; R. Kabil ; A. Tragha ; M. Bennai,"Quantum cryptography based on Grover's algorithm",IEEE,Second International ConferenCE,18-20 Sept. 2012

[15] Mitch Leslio "Quantum Cryptography via satellite". 2017.

[16] Mahdi H. A l Hasani Kais A. Al Naimee "Impact security enhancement in chaotic quantum cryptography", Volume 119, November 2019, 105575.

[17] Keshanchi, B.; Souri, A.; Navimipour, N.J. An improved genetic algorithm for task scheduling in the cloud environments using the priority queues: Formal verification, simulation, and statistical testing. *J. Syst. Softw.* 2017, *124*, 1–21.

[18] Liu, C.Y.; Zou, C.M.; Wu, P. A Task Scheduling Algorithm Based on Genetic Algorithm and Ant Colony Optimization in Cloud Computing. In Proceedings of the 2014 13th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, Xi'an, China, 24–27 November 2014; pp. 68–72.

[19] Alhaidari, F.; Balharith, T.; AL-Yahyan, E. Comparative Analysis for Task Scheduling Algorithms on Cloud Computing. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–6.

[20] He, X.; Sun, X.; Von Laszewski, G. QoS guided min-min heuristic for grid task scheduling. *J. Comput. Sci. Technol.* 2003, *18*, 442–451.

[21] He, X.; Sun, X.; Von Laszewski, G. QoS guided min-min heuristic for grid task scheduling. *J. Comput. Sci. Technol.* 2003, *18*, 442–451.

[22] Potluri, S.; Rao, K.S. Optimization model for QoS based task scheduling in cloud computing environment. *Indones. J. Electr. Eng. Comput.* 2020, *18*, 1081–1088.

[23] Hanini, M.; Kafhali, S.E.; Salah, K. Dynamic VM allocation and traffic control to manage QoS and energy consumption in cloud computing environment. *Int. J. Comput. Appl. Technol.* 2019, *60*, 307–316.

[24] Shih, H., Lee, K., Hwang, T.: New efficient three-party quantum key distribution protocols. IEEE J. Sel. Top. Quant. Electron. 15, 1602–1606 (2009).

[25] Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Dense-coding attack on three-party quantum key distribution protocols. IEEE 10(10), 1–6 (2010).

[26] Cotler, J.S., Shor, P.W.: A New relativistic orthogonal states quantum key distribution protocol. Arxiv, pp. 1–6 (2013).

[27] Chuan, W., Wan-Ying, W., Qing, A., Gui-Lu, L.: Deterministic quantum key distribution with pulsed homodyne detection. Chin. Phys. Soc. IOP Publ. Ltd. 53(1), 67–70 (2010).

[28] Moritoh, Y., Imai, Y., Inomo, H., Shiraki, W.: A cloud service on distributed multiple servers for cooperative learning and emergency communication. Commun. Comput. Inf. Sci. 188, 377–390 (2011)

[29] Ateniese, G., Burns, R.C., Curtmola, R., Herring, J., Kissner, L., Peterson, Z.N.J., Song, D.X.: Provable data possession at untrusted stores. In: Ning, P., di Vimercati, S.D.C., Syverson, P.F., (eds.) ACM conference on computer and communications security, ACM, pp. 598–609 (2007)

[30] Shen, J., Zhou, T., He, D., Zhang, Y., Sun, X., Xiang, Y.: Block design-based key agreement for group data sharing in cloud computing. IEEE Trans. Dependable Secure Comput. 16, 996–1010 (2017)

[31] Pasha, M. J. ., Rao, C. R. S. ., Geetha, A. ., Fernandez, T. F. ., & Bhargavi, Y. K. . (2023). A VOS analysis of LSTM Learners Classification for Recommendation System. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 179–187. https://doi.org/10.17762/ijritcc.v11i2s.6043

[32] Prof. Madhuri Zambre. (2016). Automatic Vehicle Over speed Controlling System using Microcontroller Unit and ARCAD. International Journal of New Practices in Management and Engineering, 5(04), 01 - 05. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/47

[33] Kumbhkar, M., Shukla, P., Singh, Y., Sangia, R.A., Dhabliya, D. Dimensional Reduction Method based on Big Data Techniques for Large Scale Data (2023) 2023 IEEE International Conference on Integrated Circuits and Communication Systems, ICICACS 2023

[34] Gummadi, A. ., & Rao, K. R. . (2023). EECLA: A Novel Clustering Model for Improvement of Localization and Energy Efficient Routing Protocols in Vehicle Tracking Using Wireless Sensor Networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 188–197. https://doi.org/10.17762/ijritcc.v11i2s.6044

[35] Mr. Dharmesh Dhabliya, Prof. Ojaswini Ghodkande. (2016). Prevention of Emulation Attack in Cognitive Radio Networks Using Integrated Authentication . International Journal of New Practices in Management and Engineering, 5(04), 06 - 11. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/48

[36] Molla, J. P., Dhabliya, D., Jondhale, S. R., Arumugam, S. S., Rajawat, A. S., Goyal, S. B., Raboaca, M. S., Mihaltan, T. C., Verma, C., Suciu, G. Energy Efficient Received Signal Strength-Based Target Localization and Tracking Using Support Vector Regression (2023) Energies, 16 (1), art. no. 555, .