A Review on Resource Allocation with Security in different Computing Environments

L. Karuppasamy [a*] V. Vasudevan [b]
[a] Department of Computer Science and Engineering Kalasalingam Academy of Research and Education, Krishnankoil, India
Corresponding author email id: karuppas@gmail.com

ABSTRACT

The new age development in technology comes with the growth of a number of devices in a computing environment. This resulted in the continuous demand for resources from the client's end. Also, the presence of malicious nodes in the network are subjected to theunauthorized access to the resources and information as well. And hence it has been necessaryto allocate resources in a secured way. Therefore, the presented study reviewed the research studies based on resource allocation with appropriate security or in a secured environment. The study included the resource allocation using blockchain chain, deep reinforcement learning in terms of algorithm. And additionally, the studies used optimized resource allocation with security in different computing environments. The empirical review on these included studies revealed the challenges, and advantages in the resource allocation in different computing environments.

Keywords: Resource allocation, Security, Computing environment, Deep reinforcement learning, Blockchain

1 Introduction

Rapid development of technology results in the usage of more devices in our environment than before [1]. The more devices in the network it becomes more complex to manage the network.However, the recent surge in the user level created more complexity in the network-based systems. Resource Utilization and resource allocation [2] are two major factors that holds thekey responsible for the effective usage of the resource and power consumption. The resource allocation becomes one of the prominent factors in managing the resources [3]. The scheme adopted in the resource allocation makes the difference in the distribution of the resource according to the user's request. The resource allocation and the computation resources are critical in Industrial based systems. The schemes that are currently followed was not able to meet the demands of user dynamically. Moreover, the security and the creditability of the systems are subjected to risks [4].And conventionally, the resource allocation was associatedwith the system policy and it relies on the device information.

This makes the systemvulnerable and prone to malicious attacks as the device information can be acquired by the demanding devices. If the attack could be possible, then the industrial system becomesunsafe [5, 6]. Also, the efficiency of the overall system would be reduced. Resource allocation with security becomes one of the challenging issues while designing for a large-scale cloud application. Many research studies explored the challenges in the resource allocation and connectivity makes the developers are complex to control. However, the studies are need to be focused on the resource allocation with security [7]. The complexity of the system makes the third party to access the resource and often ends up in the loss of resource. Hence the study aimed to review the studies that are focused on the resource allocation with security in the computer network systems and its application.

The study included the research studies basedon deep reinforcement learning, and blockchain in terms of algorithm and techniques adoptedand studies based on type of computing environments such as cloud computing, fog computing,and Edge computing.

2 Recent Trends in Resource Allocation Security

Swarm Optimization is widely used for optimization problems in various fields, leveraging the power of collective intelligence to explore complex solution spaces and find optimal outcomes efficiently. The proposed method makes use of the SO algorithm specifically for resource allocation in cloud computing environments. By tapping into the collective intelligence of swarms, the aim is to improve resource allocation efficiency and enhance system performance. The experimental evaluation of this approach demonstrates its effectiveness in terms of resource utilization and response time when compared to existing methods. This highlights the potential of the approach to significantly improve resource allocation in cloud computing environments.

For managing the resource allocation evenly to different stakeholders, the authors [3] hybrid approach using RATS-HM was used. This approach initially uses cat swarm optimization algorithm as a short scheduler for improving the task scheduling which reduces the make-spantime. And followed by group optimization-based deep neural network for allocating the resources effectively using constraints such as resource load and bandwidth. And finally the NSUPREME scheme used for authentication which is used for encrypting the data storage. Authors [8] presented resource allocation and computation offloading model for the multi userwith data security. For the efficient utilization of shared resource, authors have combined radioand computation resources. The Advanced Encryption System (AES) is adopted for security here. They have also used integrated model to optimize the time and energy consumption of the entire system. At last to optimize the offloading decision for Memory Unit (MU), an optimized algorithm is used. Similar to the earlier study, another study [2] have demonstratedthe resource utilization, resource allocation with security. From the simulation, it was revealedthat by using the JPEG and MPEG4 for reducing the system over head the system able to savesystem over-head consumption for about 46%.

Several studies [9] have adopted deep reinforcement learning in resource allocation with security. The study [9] have used the blockchain framework for resource allocation and segmented the formulation problem into two sub-problems for the action space reduction. Thedeep reinforcement learning particle swarm optimization is then used to resolve sub-problems.Here, to optimize the gradient search, the PSO is used. The trust computing becomes the termto indicate the security of the system and often explores the detection of malicious nodes. Theresearch study [4] presented a new perception on the need of honesty in the devices used in theindustrial system and adopts the Vickrey-Clarke-Groves auction for resource allocation and utilization. And it was found that if the devices have become more trustful, the utilities are maximized. The conventional offloading [10] policies allows the user to share their tasks to thebase station. This increases the latency in the communication and also the security issue in thecommunication is not properly evaluated. So the authors used a combined computational offloading and load balancing. And for the security, the advanced encryption based on the electrocardiogram encryption and decryption is used. Results shows the hybrid approach was effective.

3 Deep Reinforcement Learning in Resource Allocation with Security

The fundamental concepts of reinforcement learning are depicted in Fig. 2, which include agents, environment, states, actions, and rewards. The agent is responsible for taking actions, which are the set of all possible moves that the agent can make, but it must choose among a limited number of possibilities. Additionally, there is a discount factor that multiplies the reward to diminish accumulated rewards based on the agent's actions. The surroundings are the world with borders that restrict the agent, and the surroundings inputs are the agent's current state and its action. It returns the agent reward and state, and the state may be the immediate configuration that the agent discovers or what is returned from the surroundings. The reward is the feedback that measures the success or failure of the agent's actions.

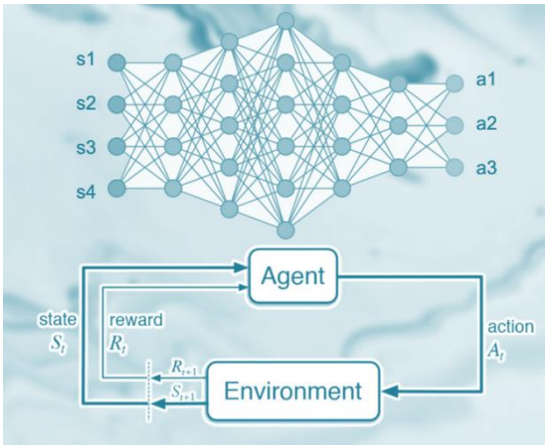

Fig.-1: Deep Reinforcement Learning

The deep reinforcement learning has been used for the resource allocation optimization by many studies and also used for the data offloading as well. The model used in the research study [11] is to optimize resource allocation and energy consumption. The deep learning optimization was adopted here mainly for the dimensionality challenge. And for the security scheme advanced encryption system is used. The experimental results showed the optimizationand the security was effective for the data offloading model. The study [12] explored the Quality of Service and security using the deep reinforcement learning. The agent in the deep reinforcement learning was constructed based on attributes such as bandwidth, CPU, security and delay. Mapping of virtual links are done by Breadth first strategy, based on the deduce the resource is different. The maximum cost and map probability. The experimental results show that the algorithm could bale to effectively solve the problem of the multi user demand.

The study [1] on the dynamic authentication using the novel watermarking algorithm showed the necessity of securing the IoT devices from the third party attacks. And the study used the LSTM and devices for the extraction of stochastic features based on the generated signal and apply watermark to the signal dynamically. This watermarking makes the signals are effectivein the communication. And furthermore, the game theory was adopted to boost the decision making process. To overcome the incomplete information, the deep reinforcement learning algorithm is used and assists the system to make decisions on the unauthenticated devices. Thesimulation shows the delay in third party attacks and therefore effective communication was achieved using the scheme.

The research study [13] adopted the Markov decision process to optimize the weighted sum, bandwidth resources, computation and power consumption. The deep reinforcement learning is used for the optimization of the resource allocation. The study adopted the deep reinforcement learning to avoid the dimensionality curse in the secured mobile edge computingnetwork. The dimensionality curse raise form the state and action space are controlled by decision making optimal policy. The numerical results showed that the scheme had been effective for the optimization of the resource. The devices in the traffic and roadside units based on the mobile edge computing are subjected to dynamic environment. The resource allocation becomes complex during such an environment. And hence the research study [14] presented the deep reinforcement learning approach for the optimization of resource allocation and to improve the system based on the secured edge computing network. The study adopts the blockchain based Internet-of-Vehicles system and the evaluation of the model shows the effectiveness of the optimization scheme.

4 Block Chain in Resource Allocation with Security

Blockchain technology has found widespread use in various industries such as IoT and healthcare. It employs blockchain data structures to verify and store data, and distributed node consensus algorithms to generate and update data. Cryptography is used to ensure the security of data transmission and access. The crux of the technology is a decentralized database. The key challenge lies in solving mining puzzles. Blockchain users or miners need to run a mining puzzle to solve the proof of work problem, which is a computing process that requires intensive computing resources.

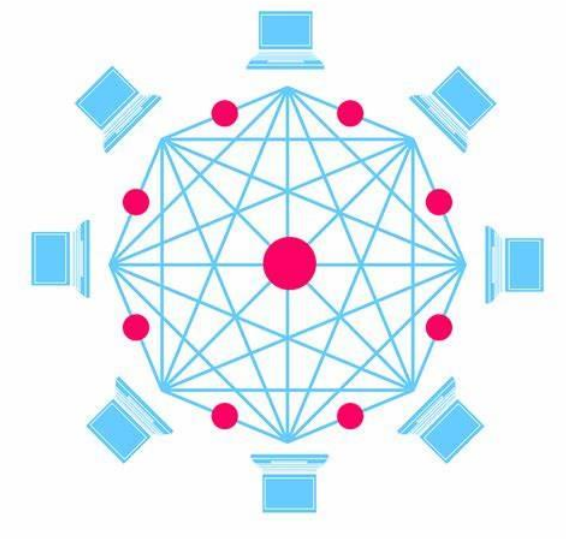

Fig.2: Blockchain Network Security

Blockchain are being adopted in the resource allocation for distributed allocation. And severalresearch studies have demonstrated the usage of blockchain in resource allocation. Likewise, the study [15] demonstrated the practice of reward and punishment mechanisms and boosting the fog nodes to actively distribute resources. This mechanism and process will be stored in theblockchain and become unmodifiable index. Furthermore, the index provides better service inlonger run and with mechanism of credible consensus the security protection is improved.

In the virtual environment, the key resource allocation with high security is often required. Theresearch study adopts [16] the blockchain technology on the basis of security. The blockchainbased virtual networking embedding algorithm is used for secured and optimized resource allocation. The results for the model validation makes the algorithm effective usage for the secured resource allocation in the virtual network system. The block chain networks used in the video streaming cannot sustain the computing capacity for longer transaction. The researchstudy [17] was aimed to resolve the problem in mobile edge computing, where the base stationsare used for the resource allocation for the video streaming. And smart contracts are used to improvise the efficiency of the operations for transcoding and delivery. The study has shown impressive results for the secured transmission of video files using the block chain network.

The research study [18] presented the block chain network with two auction mechanism in theedge computing service to maximize the social welfare of the miners. And one of themechanisms is employed when the miners demand for resources is same and another mechanismis employed when the miners demand for maximum-flow algorithm is used for the allocation of the resource while the demand for the resource is same. The heuristic algorithm is used for the allocation of the resource while the demand for the resource is different. The study shows the auction mechanism could provide the improved resource allocation in a secured block chain network. The Unmanned Aerial vehicle networks can be deployed in a large-scale network are subjected to security threats andprivacy. The research study [19] explored the above-mentioned problem and adopted the blockchain framework for the

network development. The drones in the network will be treatedas miners and gets resource from other edge computing node when it was required. Also the study recommends to utilize the game theory-based resource allocation for other researchers. The performance of the system was evaluated and shown how it can be employed.

5 Resource Allocation with Security in Cloud computing

In cloud computing due to the rapid development, there is a surge in the number of data centresutilized globally. And as a result of this surge, the energy consumption has become a major issue among the cloud computing. And to overcome the problem, the resource allocation werefocused by researchers to improve the consumption of energy during the computation. And studies [20] have adopted multi-objective-optimization method to improve the resource allocation. The simulation results showed that the allocation policy was effective without affecting the operations in the data center. Similar to the earlier study, another study adopted the multi objective function for the task scheduling and efficient resource allocation. Furthermore the study [21] initially to reduce the complex of the system, used Kernal Fuzzy C-means clustering algorithm. After the cluster formation, the artificial fish swarm optimization algorithm is used for the task allocation. This hybrid approach made the resourceallocation optimal.

The research study [22] presented the optimized resource allocation for the users that can be continuously available. The security was improved to ignore the inappropriate utilization of resource in the mobile station which was earlier accessed by malicious devices. And the simulation results showed that the system was shown better resource allocation with security. In another research study [4] the authors used STARK model for resource allocation with security. And the model was to prevent Remote to local, Denial of Service and User to Root attacks in cloud networks.

The research study [23] explored the resource allocation with migration from application to thecloud. The utility maximization model was adopted for the allocation of resource. Thegeneralization form of the optimization problem is difficult as it becomes complex to separate.The gradient based resource allocation scheme is used to optimize the problem. The numericalanalysis showed that the model was effective for the resource allocation.

6 Resource Allocation with Security in Fog Computing

Fog computing gives the advantage of computing directly at the edge of the network. The fognodes exists between the cloud and the end device. And as a matter of fact the resource allocation by fog nodes are not effective as the cloud.

The constant message [24] expansion adopted in the study provides a secured resourceallocation for the fog computing. It also secures the devices from the eavesdropper. Here the authors used a smart gateway to allocate the resources for the devices. This method becomes a robust system as it encompasses a full-key compromise resistance which ensures the security even if the god nodes and system are corrupt. In another research study [25], the authors have made the fog server as responsible for the tasks to be performed in the network. And with thisscheme of approach, the network becomes prone to malicious node attack and shown effectivein the experimental scenario. Also, the scheme were able to manage the computational cost forthe scientific computing. The research study [26] was aimed to allocate the bandwidth which reduces the time for the four different services in a fog computing network. The study took a two-step approach, in the first step lagrangian algorithm was used to generate the sub-optimalsolutions. And in the second step, the appropriate optimal solutions are selected and analyzed. Finally, the solutions are evaluated through the numerical simulation.

7 Resource Allocation with Security in Edge Computing

In Edge computing, the computation and the storage are placed at a close range to the source of data. For example, monitoring of oil rigs, monitoring of crop management using UAVs andoptimized video live streaming. Irrespective to the type of computing the resource allocation and security for the data is much required for the Edge computing. Likewise, the resource allocation [27] in edge computing between station and UAVs resources was optimized by usingpricing and trading dynamically. In pricing method, the edge computing units allocate the resource with pricing and the UAVs makes the optimal decision on the basis of pricing. In order to protect the security, the resource trading is preserved by the integration of blockchain.And the scheme was effective under simulation conditions.

The research study [28] explored the security defense system in the edge computing network environment. And one of the prominent challenges discussed was the optimized resource allocation for the secured edge computing system. And the study used computing intrusion detection system, with deterministic differential equation model to overcome the challenge. Also, the Lyapunov stability theory was adopted for the model to produce uniqueness and stability. And the simulation results have shown the model was effective in terms of security. In edge computing there will be physical layer to act as a security for the data transmission assurance. And hence the research study [29] explored the edge computing system using the access point, malicious eavesdropper and multiple mobile devices. The study adopted a difference of convex algorithm for the resource allocation and adopted Karush Kuhn Tucker conditions for the optimization problem. The results showed that the scheme was able to provide secure data transmission, optimized resource allocation and reduced power consumption.

The research study [30] have taken the combined UAV, and VANET in edge computing and analyzed the computation ability of the system. And moreover, the study adopted multi- objective optimization for the resource allocation and the security. And to resolve the computation utility the study divided the problem into two sub-problems and adopted Lagrangien dual decomposition for the offloading optimization and the resource allocation andproduced efficient results during the simulation. The research study [31] aimed to resolve the multiple user demand problem using the Stackelberg game for the optimized resource allocation in edge computing. And adopted one to many matching schemes for the resource allocation. Then, one-to many matchings is established to handle resource allocation problems.From the results it was shown the scheme was effective in the optimization of the resource allocation.

8 Challenges in Resource Allocation with Security

In computing environment, the resource allocation problem is often discussed but the recent developments have developed new set of challenges to overcome and are discussed here. The challenges in the resource allocation shows the importance of the resource allocation in a computing environment.

8.1 Resource Problem

The nodes in the environment and the number of users in the system determine the demand forthe resource[32]. And in certain cases, the resources become insufficient and cannot meet theclient's request or end up in delay. The surge in the technology makes the user and demand forthe resource allocation optimization it is likely to grow more.

8.2 Dynamic Resource Allocation

The rapid development results in new mobile devices that are connected to the systems. Also,in some applications the device will be mobile and are subjected to connect with different systems [5]. For example, UAVs deployed needs additional resources dynamically such as computing power.

8.3 Time Latency

Although at several cases, the resources allocated from different sources ends up in time latencymeaning delayed transmission [33]. The latency depends on the physical system as well. However, the latency creates a delayed sharing of resources which ends in load unbalancing and disruptions in load scheduling [34].

8.4 Power Consumption

Power consumption is one of the highly discussed challenges [35]. For an efficient system, the power consumption should be reduced than average system usage. Many studies have indicatedthe power consumption, and one of the major cause of the high power consumption is inappropriate allocation of resources. The sudden surge of the users or clients, the lack of communication, and extensive load causes more power consumption.

8.5 Malicious Nodes

The studies on the detection of malicious nodes in the network shows that the
presence of malicious nodes can cause several problems. One of the major problems is the information leakage through the unauthorized access of the nodes. The malicious nodes could affect the overall system by utilizing the scheduled resources.

8.6 Traffic Surge

Several studies indicated the load in the network leads to further issues in the network [36]. And therefore, the communication between the node and the station lagged. The traffic surge might be due to the increase in the users and the devices that are connected to the network.

8.7 Multiple User

The sudden surge in the multiple users do have impact on the overall system resource allocation.And several studies [37]evaluated their models for the multiple user configuration. Themultiple user problem is subjected to the type of applications, and the size of the network.

8.8 Multi-Tenancy Security and Privacy

In cloud computing, the multi-tenancy is adopted to manage the hardware resource and makesthe system more efficient and effective without any expansion. But it comes with the consequences in terms of security [38]. The virtual environments share some of the functionalities with the physical system, and are subjected to the security threat. This has beenrarely discussed by the research studies and shows the importance of security [39]during the resource sharing.

8.9 Trust Device / Computing

The trust factor for the devices is a crucial element in resource allocation. Information [7] security is a critical aspect and plays a significant role in protecting an organization's business.Organizations are required to safeguard their information and assets to sustain their value andreputation. The literature exploration done in the research study, reveals the challenges in the information security. The end devices and users are connected to the network and share information about the device and utility continuously for the efficient utilization of resources.But the malicious devices or nodes in the network could collect the information that are crucial.

9 Advantages of Resources Allocation with Security:

From the research studies, several observations are made that are found to be advantageous forthe modern computing environment if the resource allocation has been applied appropriated ina secured manner.

Optimized resource allocation: The techniques used for the resource allocation [35, 40] makesthe system to optimize the resources and improve the effectiveness of the overall system. Moreover, the queue for the load can be managed if the resources are allocated appropriately.

Dynamic resource allocation: The dynamic resource allocation [5, 6] shown in the studies indicated the effectiveness in the overall system. And recently, the systems are engaged more towards the mobile computing environment, the need for the dynamic resource allocation has grown faster.

Reduced Power consumption: the optimized resource allocation [41]makes the system to use the power in a controlled manner. Because the optimized resource allocation prevents the unnecessary usage of the resources that are consumed in an unauthorized manner.

Secured transmission: The security scheme adopted along with the resource allocation [36] assure the transmission of any sort of data or communication in the environment. The privacyof the data is preserved which would be the major threat in today’s scenario.

10 Experiments and Analysis

It is essential to evaluate the performance of the proposed resource allocation method that uses SSO in cloud computing environments. This evaluation is necessary to assess the effectiveness of the approach and compare it with other existing methods. Performance evaluation involves conducting experiments and analyzing various metrics to measure the efficiency and efficacy of the SO-based resource allocation approach.

During the experiments, it's important to collect data by monitoring resource usage, response times, and other relevant metrics. Statistical analysis techniques can be used to analyze the data collected and draw meaningful conclusions about the performance of the SSO-based allocation method. By thoroughly evaluating the proposed approach, it's possible to assess its strengths, limitations and overall effectiveness, providing valuable insights for future enhancements and optimizations in resource allocation for cloud computing environments.

Table.1. Resource Utilization

Task	ACO	PSO	Proposed SO
10	70%	75%	85%
20	75%	75%	84%
30	72%	78%	82%
40	68%	74%	80%
50	75%	85%	88%

Table.2. Response Time

Task	ACO	PSO	Proposed SO
10	115	110	100
20	112	105	98
30	120	115	105
40	125	120	108
50	110	100	98

Table 3. Throughput

Task	ACO	PSO	Proposed SO
10	500	550	580
20	450	520	560
30	480	530	590
40	510	560	600
50	470	540	590

11. Comparison with Other Algorithms

Algorithms state that the average waiting delay is directly proportional to the average queuing time. Therefore, the average waiting delay can be calculated by adding up the time spent waiting in the task queues of both users and Cloud servers. This relationship between task arrival rate and end-to-end delay is applicable to all four algorithms.

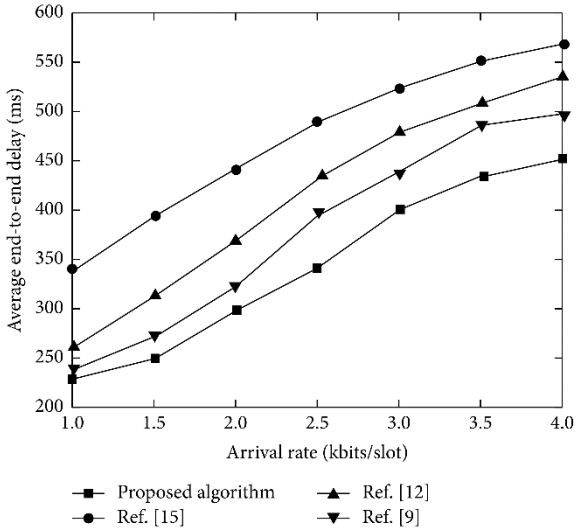

Fig. 3: Comparison of average end-to-end delay of different algorithms.

The proposed algorithm's main optimization objective is to minimize the average network delay, which has a direct impact on the algorithm's performance. The average network delay represents the time it takes for each service request to access the required service. Different algorithms can result in varying average network delays.

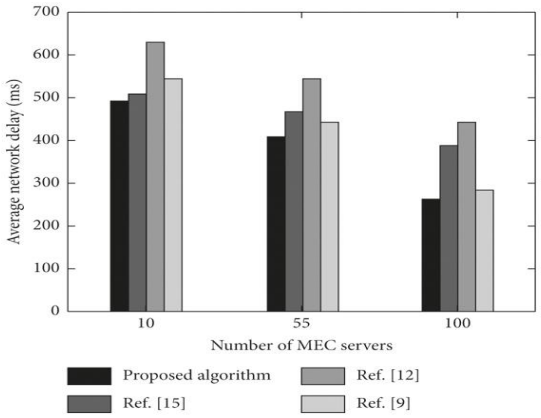

Fig. 4: Effect of different numbers of MEC servers on average communication delay.

The algorithm's performance is evaluated by the maximum user delay metric. The relationship between the number of user terminals and the maximum user delay is compared across different algorithms.

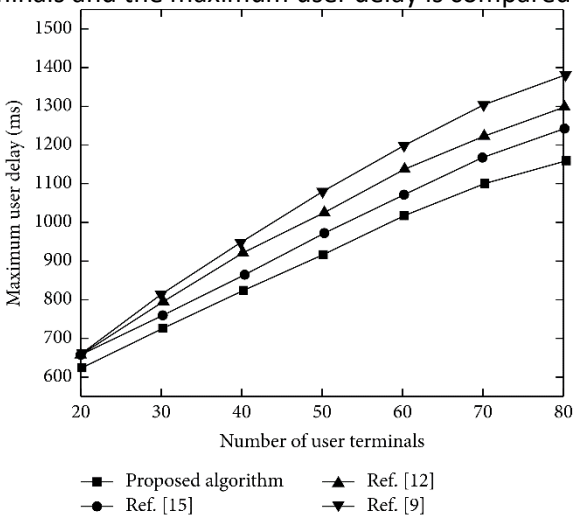

Fig. 5: Relationship between the number of terminals and the maximum user delay.

11 Summary

The research studies based on the resource allocation in the computing environment had revealed the challenges in the recent developments. As it has been observed that the challengesare grown from 2013 to 2021, but yet the problems try to shift into new directions. Earlier thestudies were much focused on the power consumption and optimized resource allocation. Butrecently, the focused were shifted towards the dynamic resource allocation, secured transmission, malicious node detection and latency. Among the research studies the security concerns while sharing the resources are rarely discussed. Moreover, the use of a combined approach with the security and resource allocation scheme are not widely seen. However some studies have taken the hybrid approach and try to solve the resource optimization and security issues in the environment.

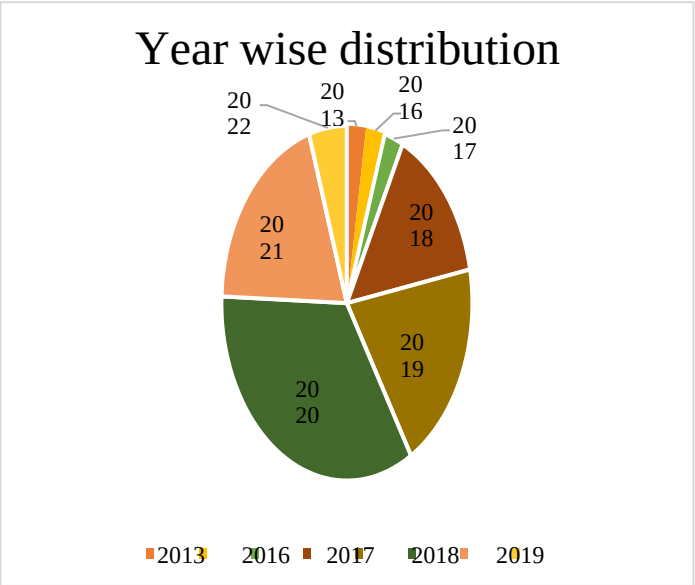

Fig. 6: Year-wise distribution of the articles

The number of articles per year for the current study reveals the studies are covered from the year 2018, 2019, 2020, and 2021. The study explored the recent developments, challenges in the resource allocation and security concerns in the system. This findings from the study wouldshow the appropriate direction for the researchers to explore.

12 Conclusion

The study shows the importance of the resource allocation in the modern computing environment. Although the research studies have explored and try to resolve the challenges inthe resource allocation, the problems still persist. And also, the factors that influences the resource allocation problem changes due to the rapid development. However, the matter of security is well discussed for the different computing environments. Moreover, the studies rarely discussed both and need to explore the significance of the security in the resource allocation. The study focused on studies that used deep reinforcement learning and block chain for resource allocation and the schemes that are followed by the studies are discussed. Also, the study selected the studies on the basis of computing environment and the schemes applied forthe resource allocation and the security.

The study has observed the shift in the problems that are encountered in the resource allocation from 2013 to 2021. Like earlier, the energy and resource optimization were the keyterm to explore for the research studies but recently it shifted into dynamic resource allocation,and secured transmission. However, the study didn't focus on the influence of the resource utilization on the resource allocation and security, and future studies could explore further on it to see the significance. And additionally, deep exploration of individual computing environment could reveal further challenges for the specific application as the present study discussed the common challenges that was observed from the recent studies.

References:

1. *Ferdowsi and W. Saad, (2018). "Deep learning for signal authentication and security in massive internet-of-things systems," IEEE Transactions on Communications, vol. 67, pp. 1371-1387.*
2. *A. Elgendy, W.-Z. Zhang, Y. Zeng, H. He, Y.-C. Tian, and Y. Yang,(2020). "Efficient and secure multi-user multi-task computation offloading for mobile-edge computing in mobile IoT networks," IEEE Transactions on Network and Service Management, vol. 17, pp. 2410-2422.*
3. *P. K. Bal, S. K. Mohapatra, T. K. Das, K. Srinivasan, and Y.-C. Hu, (2022). "A Joint ResourceAllocation, Security with Efficient Task Scheduling in Cloud Computing Using HybridMachine Learning Techniques," Sensors, vol. 22, p. 1242.*
4. *S. S. Gill and A. Shaghaghi, (2020). "Security-aware autonomic allocation of cloud resources:a model, research trends, and future directions," Journal of Organizational and End User Computing (JOEUC), vol. 32, pp. 15-22.*
5. *J. Cui, Y. Liu, and A. Nallanathan, (2019). "Multi-agent reinforcement learning-based resourceallocation for UAV networks," IEEE Transactions on Wireless Communications, vol. 19, pp. 729-743.*
6. *J. Wan, B. Chen, M. Imran, F. Tao, D. Li, C. Liu, et al., (2018). "Toward dynamic resources management for IoT-based manufacturing," IEEE Communications Magazine, vol. 56,pp. 52-59.*
7. *S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, (2020). "Information security governancechallenges and critical success factors: Systematic review," Computers & Security, vol.99, p. 102030.*
8. *I.A. Elgendy, W. Zhang, Y.-C. Tian, and K. Li, (2019). "Resource allocation and computationoffloading with data security for mobile edge computing," Future Generation Computer Systems, vol. 100, pp. 531-541.*
9. *Z. Ning, S. Sun, X. Wang, L. Guo, G. Wang, X. Gao, et al., (2021). "Intelligent resource allocation in mobile blockchain for privacy and security transactions: a deep reinforcement learning based approach," Science China Information Sciences, vol. 64,pp. 1-16.*
10. *W.-Z. Zhang, I. A. Elgendy, M. Hammad, A. M. Iliyasu, X. Du, M. Guizani, et al., (2020). "Secure and optimized load balancing for multitier IoT and edge-cloud computing systems," IEEE Internet of Things Journal, vol. 8, pp. 8119-8132.*
11. *I.Elgendy, A. Muthanna, M. Hammoudeh, H. A. Shaiba, D. Unal, and M. Khayyat, (2021). "Security-aware data offloading and resource allocation for MEC systems: a deep reinforcement learning,"*
12. *Jiang and P. Zhang,(2021). "VNE Solution for Network Differentiated QoS and Security Requirements from the Perspective of Deep Reinforcement Learning," in QoS-Aware Virtual Network Embedding, ed: Springer, pp. 61-84.*
13. *H. Ke, H. Wang, H. Zhao, and W. Sun, (2021). "Deep reinforcement learning-based computation offloading and resource allocation in security-aware mobile edge computing," Wireless Networks, vol. 27, pp. 3357-3373.*
14. *H. Xiao, C. Qiu, Q. Yang, H. Huang, J. Wang, and C. Su, (2020). "Deep reinforcement learningfor optimal resource allocation in blockchain-based IoV secure systems," in 2020 16th International Conference on Mobility, Sensing and Networking (MSN), pp. 137-144.*
15. *H. Wang, L. Wang, Z. Zhou, X. Tao, G. Pau, and F. Arena, (2019). "Blockchain-based resourceallocation model in fog computing," Applied Sciences, vol. 9, p. 5538.*
16. *H. Cao, Y. Hu, Q. Wang, S. Wu, and L. Yang, (2020). "A blockchain-based virtual network embedding algorithm for secure software defined networking," in IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1057-1062.*
17. *Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, (2019). "Decentralized resource allocation forvideo transcoding and delivery in blockchain-based system with mobile edge computing," IEEE Transactions on Vehicular Technology, vol. 68, pp. 11169-11185.*
18. *J. Zhang, W. Lou, H. Sun, Q. Su, and W. Li, (2022). "Truthful auction mechanisms for resourceallocation in the Internet of Vehicles with public blockchain networks," Future Generation Computer Systems, vol. 132, pp. 11-24.*
19. *Z. Chang, W. Guo, X. Guo, T. Chen, G. Min, K. M. Abualnaja, et al., (2021). "Blockchain- empowered drone networks: Architecture, features, and future," IEEE Network, vol. 35,pp. 86-93.*
20. *Shrimali and H. Patel, (2020). "Multi-objective optimization oriented policy for performance and energy efficient resource allocation in Cloud environment," Journal of King Saud University-Computer and Information Sciences, vol. 32, pp. 860-869.*
21. *P. Albert and M. Nanjappan, (2020). "An efficient kernel FCM and artificial fish swarm optimization-based optimal resource allocation in cloud," Journal of Circuits, Systemsand Computers, vol. 29, p. 2050253.*

22. *M. Rath, (2019). "Resource provision and QoS support with added security for client side applications in cloud computing," International Journal of Information Technology, vol. 11, pp. 357-364.*
23. *S. Li and W. Sun, (2021). "Utility maximisation for resource allocation of migrating enterpriseapplications into the cloud," Enterprise Information Systems, vol. 15, pp. 197-229.*
24. *L. Zhang and J. Li, (2018). "Enabling robust and privacy-preserving resource allocation in fogcomputing," IEEE Access, vol. 6, pp. 50384-50393.*
25. *J. Jiang, L. Tang, K. Gu, and W. Jia, (2020). "Secure computing resource allocation frameworkfor open fog computing," The Computer Journal, vol. 63, pp. 567-592.*
26. *F. Lin, Y. Zhou, G. Pau, and M. Collotta, (2018). "Optimization-oriented resource allocation management for vehicular fog computing," IEEE Access, vol. 6, pp. 69294-69303.*
27. *H. Xu, W. Huang, Y. Zhou, D. Yang, M. Li, and Z. Han, (2021). "Edge computing resource allocation for unmanned aerial vehicle assisted mobile network with blockchain applications," IEEE Transactions on Wireless Communications, vol. 20, pp. 3107- 3121.*
28. *H. Hui, C. Zhou, X. An, and F. Lin, (2019). "A new resource allocation mechanism for securityof mobile edge computing system," IEEE Access, vol. 7, pp. 116886-116899.*
29. *J.-B. Wang, H. Yang, M. Cheng, J.-Y. Wang, M. Lin, and J. Wang, (2020). "Joint optimizationof offloading and resources allocation in secure mobile edge computing systems," IEEETransactions on Vehicular Technology, vol. 69, pp. 8843-8854.*
30. *Y. He, D. Zhai, F. Huang, D. Wang, X. Tang, and R. Zhang, (2021). "Joint task offloading, resource allocation, and security assurance for mobile edge computing-enabled UAV-assisted VANETs," Remote Sensing, vol. 13, p. 1547.*
31. *S. Guo, X. Hu, G. Dong, W. Li, and X. Qiu, (2019). "Mobile edge computing resource allocation: A joint Stackelberg game and matching strategy," International Journal of Distributed Sensor Networks, vol. 15, p. 1550147719861556.*
32. *H. Ren, C. Pan, Y. Deng, M. Elkashlan, and A. Nallanathan, (2020). "Resource allocation for secure URLLC in mission-critical IoT scenarios," IEEE Transactions on Communications, vol. 68, pp. 5793-5807.*
33. *M.-N. Nguyen, L. D. Nguyen, T. Q. Duong, and H. D. Tuan, (2018). "Real-time optimal resource allocation for embedded UAV communication systems," IEEE WirelessCommunications Letters, vol. 8, pp. 225-228.*
34. *Q. Zeng, Y. Du, K. Huang, and K. K. Leung, (2020). "Energy-efficient radio resource allocationfor federated edge learning," in 2020 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1-6.*
35. *J. Zuo, Y. Liu, Z. Qin, and N. Al-Dhahir, (2020). "Resource allocation in intelligent reflectingsurface assisted NOMA systems," IEEE Transactions on Communications, vol. 68, pp.7170-7183.*
36. *M. Peng and K. Zhang, (2016). "Recent advances in fog radio access networks: Performance analysis and radio resource allocation," IEEE Access, vol. 4, pp. 5003-5009.*
37. *X. Li and L. Da Xu, (2020). "A review of Internet of Things—resource allocation," IEEE Internet of Things Journal, vol. 8, pp. 8657-8666.*
38. *J. Guo, Z. Song, Y. Cui, Z. Liu, and Y. Ji, (2017). "Energy-efficient resource allocation for multi-user mobile edge computing,(2017) in GLOBECOM IEEE Global Communications Conference, pp. 1-7.*
39. *S. Jeong, W. Na, J. Kim, and S. Cho, (2018). "Internet of Things for smart manufacturing system: Trust issues in resource allocation," IEEE Internet of Things Journal, vol. 5, pp. 4418-4427.*
40. *M. S. Alam, J. W. Mark, and X. S. Shen, (2013). "Relay selection and resource allocation for multi-user cooperative OFDMA networks," IEEE Transactions on Wireless Communications, vol. 12, pp. 2193-2205.*
41. *X. Hong, P. Liu, F. Zhou, S. Guo, and Z. Chu, (2019). "Resource allocation for secure UAV- assisted SWIPT systems," IEEE Access, vol. 7, pp. 242*

Received 11 October 2023
Revised 31 December 2023
Accepted 09 January 2024