Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 3 (2023)

An Advanced Cloud Data Streaming Framework for Optimized Container Resource Allocation, Job Scheduling, And Security Enhancement

R. Kokila
Research Scholar, Dr.M.G.R Educational and Research Institute, Maduravoyal, Chennai-600 095, Mail id: kokilamgr2019@gmail.com

Dr. S. Radha Rammohan
Professor, Dr. M.G.R Educational and Research Institute Maduravoyal, Chennai-600 095 Mail id: radharammohan1969@gmail.com

Abstract:
In the realm of cloud data streaming, the central concerns are Container resource allocation and job scheduling. Cloud infrastructure relies on container virtualization to facilitate construction and migration processes. Previous models have employed migration techniques to manage cloud container allocation and resource scheduling, but these come at the cost of increased response time and network traffic. To address these challenges, a novel approach is introduced, the Reduced Optimal Migration model (ROM). This model selectively triggers migration processes based on recommendations, optimizing resource allocation through a Machine Learning (ML) Algorithm. Job scheduling is enhanced through a dedicated Task Scheduling Algorithm. For robust data security during migration, a security-based technique is implemented in the 'Security-based Container Scheduling Model,' which ensures data integrity and safeguards against attacks. This system operates seamlessly online and offline, utilizing Edge Computing. During offline periods, defensive containers maintain data security until the system owner restores online connectivity. This holistic framework proves highly effective in resolving complex issues associated with large-scale optimization of resource allocation, migration, and security. Empirical results confirm its efficiency and security enhancements. The proposed work introduces an advanced cloud data streaming framework that optimizes container resource allocation and job scheduling while enhancing security during migration. It proves effective in addressing the challenges inherent in large-scale cloud data streaming processes.

Keywords- Containers, Migration, High security, streaming, machine Learning (ML), resource allocation, defensive containers.

1. INTRODUCTION

Generally, Cloud computing as the service-oriented theory contains three main services namely Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS). IaaS acts as a hardware layer containing storage, servers and NW devices in data centre. Software-as-a-Service deliberates a singleor combined application to the user according to the need. PaaS provides end user with development, testing and applications along with the operating system [1]. Recently, the cloud container usage for resource optimization has achieved a drastic rise. Based on the demand of cloud container some of the cloud-based engines (Docker, Mesosphere, kubernetes etc..,) [2] are used for utilization purpose. In cloud, the container performs a continuous allocation of incoming data, which is named as streaming process. Data streaming is a rapid motion approach where a continual steam of data are processed at a time. Stream processing and batch Processing are the two operational modes in big data streaming [3]. In stream process the data are defined as streams, where the data are analyzed right away

and the allocation done immediately. Whereas, in batch processing a batch of data are sent to database foranalysis and then the results are produced.

The existing system follows a migration process, where the data followsa streaming allocation. In case if the data exceeds the container size, then the data immediately shifted to the next maximum size and so on. The streaming process selection for container resource allocation is shown in the below figure 1. In stream processing the data are allocated before any verification. Moreover, in batch processing the data is analysed first and then sent for allocation. When the data are not produced to the suitable container for allocation then the system seeks 'migration process' (moving the data to bigger size container).

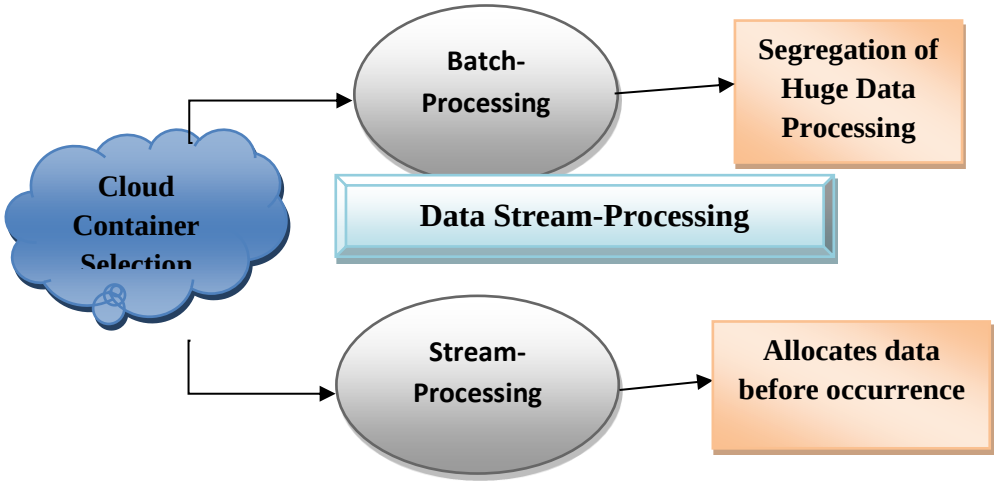

Figure.1 Streaming Process Resource Allocation

There are many algorithmic technique followed for processing a perfect container resource allocation. The proposed system aims to provide a secured container resource allocation providing a secured storage and transactionin cloud [4].

The contributions of the method are as follows:

1) Initially, the system uses a novel machine learning (ML) algorithm to analyze the incoming data initiating a proper container allocation. The most sensitive data are validated, encrypted and produced with extra space container for resource allocation to maintain confidentiality.
2) Further, the system proposes a reduced optimal migration technique to handle the volatile data. As to mitigate the migration time the system uses the migration technique, which is used only if required.
3) This reduced usage of migration process saves the computational time and consumes energy.
4) The system implements a task Scheduling Algorithm that helps in producing optimal container-based job scheduling. Further the algorithm reduces the processing time, improves reliability and in energy consumption.
5) Further to enhance the security even when the local system is offline, the system setupsome defensive containers. These defensive containers are active forms containers detecting and eliminates attacks even when the system is offline.
6) After every migration there are chances of data loss or attack. To provide an enhanced security to the container data a 'security based container scheduling model is followed. The model followsa set of rules to enhance the security. The rules of the model are Data Replacement with junk values, Auto Deletion After migration, and cross-verification.
7) The paper presents empirical results analysis, conveying that the proposed algorithm can efficiently produce a securedcontainerizes services in cloud.

The remainder of the paper are as follows. In Section 2 a summary of previous studies on container-basedmigration and some security measuresare discussed. The proposal implementation on secured container resource allocation, defensive containers mechanismwith some security measures are introduced in Section 3. Then following by section 3 the overall methodology used in this work are detailed. In Section 4 the empirical evaluation results are presented and discussed. Finally in section 5 the paper is concluded.

I. LITERATURE SURVEY

2.1 CONTAINER SCHEDULING STRATEGIES

In cloud computing the resource management, job scheduling is the key concern. The scheduling related strategies are:

Garg et al. [5] stated a boosting utilization for resource allocation. To enhance the profit of Virtual Machines in the CDC, the prediction model of the artificial neural network (ANN) with a multi-objective optimization theory is built. The boosting algorithm fulfils the QoS necessities for users in the service-level agreement. Adhikari et al. [6] established a new resource allocation strategy along with task optimization with help of the bat Theory and K-means for the Virtual Machines of the IaaS layer. The bat algorithm and k-means helps to minimize the computational time and task execution. Guerrero et al. [7] used the sorting genetic model II (NSGA-II) for the optimized resource management of cloud containers; acontainer allocation strategy is projected that targets to maintain container workload balance, improvise application reliability and reduce network communication overhead.Kaur et al. [8] produced a multi-objective scheduling model implementing a fuzzy Particle Swarm Optimization. FSO system aims to reduce transmitting time, energy consumption and power consumption processing a maximum resourceutilization of Virtual Machine. A container-based scheduling strategy for microservices and an allocation strategy is conferred by Lin et al. [9].

There are several migration related container allocations is processed by several preceding systems. T. Kim et al., in [10] introduced an Optimal Container Migration to process allocation in Edge Computing. The migration system is opted to reduce the network traffic occurs during allocation. M. Ouyang et al., [11] proposed a band area application with artificial Fish Swarm algorithm for appropriate resource utilization of the server.

I. METHOD IMPLEMENTATION

The system model implementation focuses on Container Resource Allocation and security towards the user data.

3.1 MACHINE LEARNING FOR RESOURCE ALLOCATION

In this paper a machine learning algorithm is used to study the incoming user data. When the user data enter the ML performs a validation on size, sensitivity and requirement of the user are well-analysed. Then, according to the requirement of the user a container is requested from the cloud for allocation. Also, complete client routine behaviour in cloud is examined by Machine learning algorithm. By matching the previous behaviour of the client, the new data can be analysed, the pattern matching helps in predicting the client data type earlier itself. In between the sensitive and normal data of the client are analysed and segregated for easy implementation.

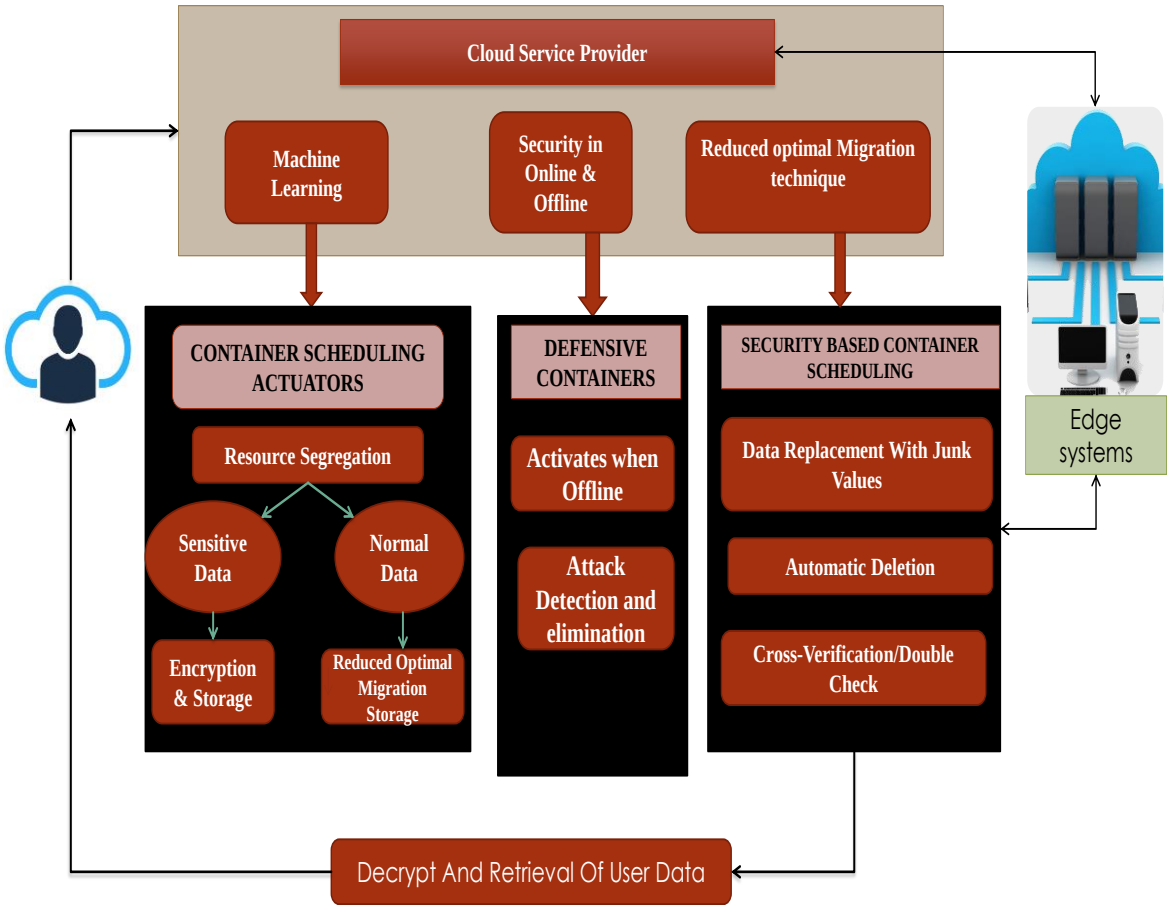

Figure.2 System Optimization Architecture

- *Sensitive data*: The sensitive data are chosen and sent for high-level encryption. The data once encrypted is then sent for container allocation. To maintain the confidentiality of the sensitive data extra container spaceallocation for the resource are assigned and maintained securely in cloud container itself.
- *Normal Data*: the segregated normal data of the client are taken separately and sent for migration storage.

3.2 DEFENSIVE CONTAINERS FOR SECURITY

- The system proposes a new defensive containers mechanism to validate the process when the system is offline. From the cloud containers some containers are allocated for defensive purpose and named as defensive containers. There are possibilities of edge systems or local systems being offline and also there are chances of attacks at that particular time. To prevent the resource form attacks and to provide protection in offline the defensive containers are used.

- The proposed defensive containers are established to detect and eliminate attacks when the local system is offline. The defensive containers are normal containers that generally perform minor tasksand keep loads of space to process the defensive mode. The defensive mode will be activated only in emergency at time of interruption.

3.3 REDUCED OPTIMAL MIGRATION TECHNIQUE

The main aim of the paper is to mitigate the migration process. Though migration helps in allocation it occupies more time and energy. To overcome the issue the system initializes a reduced optimal migration technique that is used only if required. For every data a threshold limit is set, if the data exceeds the ‘threshold’ limit then the datais

processed for migration container storage process. The resource allocation strategy is completely negligible processed only if the immense data is detected.

3.4 EDGE SYSTEM FOR RESOURCE ALLOCATION

The system uses edge systems for allocation. The edge systems act as local systems provided from the data centres for data storage purpose.Normally, the container process resource allocation but when there are more dependencies and need for Containers the suitable allocation becomes a complex task. So, the system adapts some edge systems and utilizes them for resource allocation. Here Nnumbers of edge systems are created and set for resource allocation.When data enters and the container is full then the resource are shifted to edge systems for allocation. The data centres buy a server and connect them with cloud.Then, the data are transferred to the server and the process is handled by the local edge systems.The edge systems slowly process the allocation step-by-step and provide suitable data allocation.

- **ELASTICITY THROUGH EDGE SYSTEM**

In the proposed system, when the process of the cloud server is overloaded then automatically the local edge systems are activated.The resource are scheduled and allocated in the edge system according to the availability basis.

- **EDGE SYSTEM OVERCOMING TENANT SERVER DRAWBACK**

When the process of the cloud server is overloaded, automatically the process is shifted to the tenant servers.But the usage of tenant servers may cost a lot and is not affordable.The edge systems are local systems and can be used for user data storage.Hence, edge system is cost-Effective as it can be used in place of tenant system.Incase if the edge system is full and cannot be used the tenant system are used. Then in that case according to the user requirement the tenant systems areadapted and used for storage.

- **EDGE SYSTEM FOR DOS ATTACK ELIMINATION**

Generally, all the initiated edge system will perform their regular process. In time of any attack all the edge system forms together and support attack elimination.Hence the edge system helps in detecting and eliminating attack.The edge system plays major role in eliminating Denial-of-service attack. Also, theExternal server is triggered and the blockage due to DOS attack is eliminated easily.

3.5 SECURITY BASED CONTAINER SCHEDULING MODEL

While performing migration process there are more chancesfor data loss or leakage. The main goal of the paper is to produce a high-level security while performing migration process in cloud for container resource allocation. To avoid the above mentioned defect during allocation process some major implementation methods are opted in the proposal.

- **DATA REPLACEMENT WITH JUNK VALUES**

There are chances that the flushed data can be retrieved from the container easily after migration. To avoid such circumstance the system implies a fake data replacement to the migrated container. The data from the user are allocated in the main server. After the migration storage the data are filled with some random Fake Values and the data is flushed. Even if the data is opted from the container only the deleted fake values can be recovered not the original user data. For instance, if any attacker recovers the data the person will get only the fake replaced dataset not the original data this way a high-level security is maintained.

- **CROSS VERIFICATION/DOUBLE CHECK:**

Before allocating the user resources the system initializes a detailed cross verification about the data completely. This verification makes the allocation simpler as the data are verified and a right choice of container can be deliberated to the user according to the size.

The system implementation in the figure 2 ensures an exact smart way of container resource allocation by reducing the migration time. Fish Swarm Optimizationis a multi-layer optimized allocation strategy helps in choosing the appropriate container validating the exact size of the user data previously. By implementing the fake data replacement, a secure resource allocation after migration process is guaranteed. Then, at last a double check operation is executed to verify the data and preceded for container allocation. Hereby, a secured user data with formal encryption and decryption is proposed, stored and retrieved providing a better user convenience.

II. RESULT ANALYSIS

In result analysis, a comparison of the existing migration models with the proposed reduced migration model is done in figure 3. The comparison of existing migration algorithms such as BAC migration approach and Container migration model is done with the proposed Reduced Migration model. In the comparison Reduced Migration model is proved to be best in task scheduling and resource allocation providing speed, reliability, minimal time and energy.

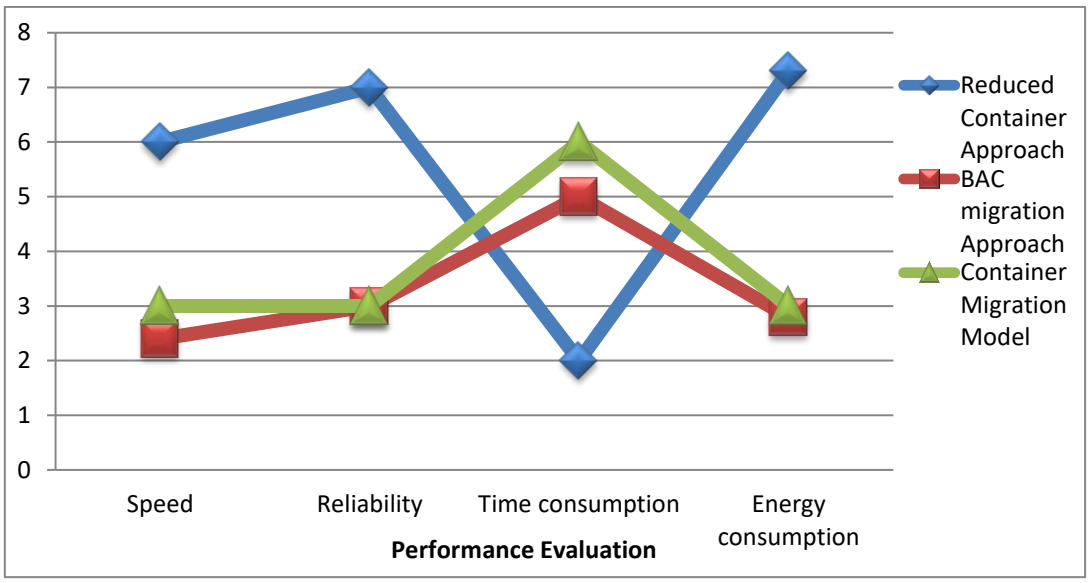

Figure.3 Migration model: Reduced Container model VS existing BAC and container migration model

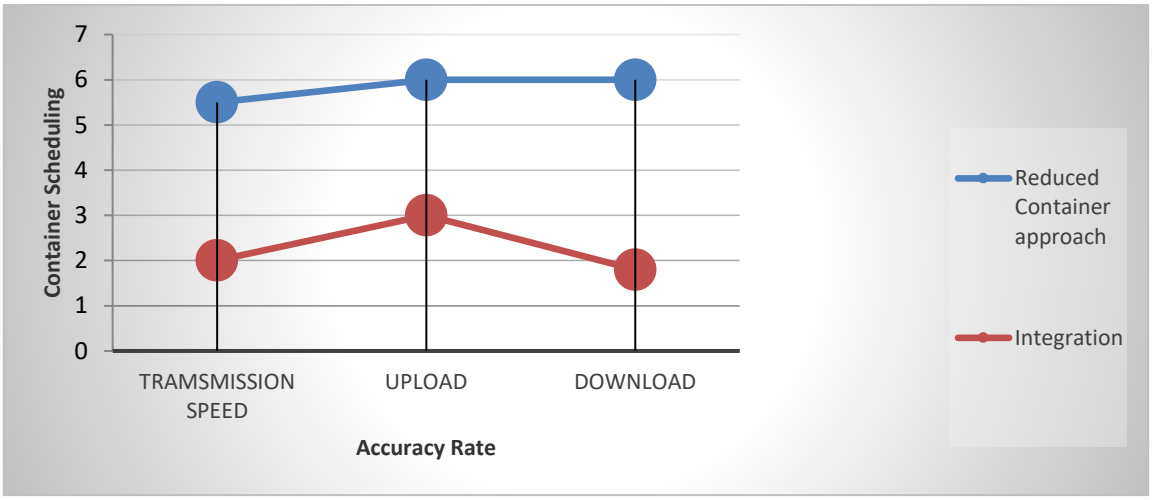

Figure.4 Accuracy Rate RCA approach Vs integration model

In Figure 4, the scheduling and accuracy rates are compared accounting the comparison with the integration model, the proposed reduced container approach proves to be better in accuracy.

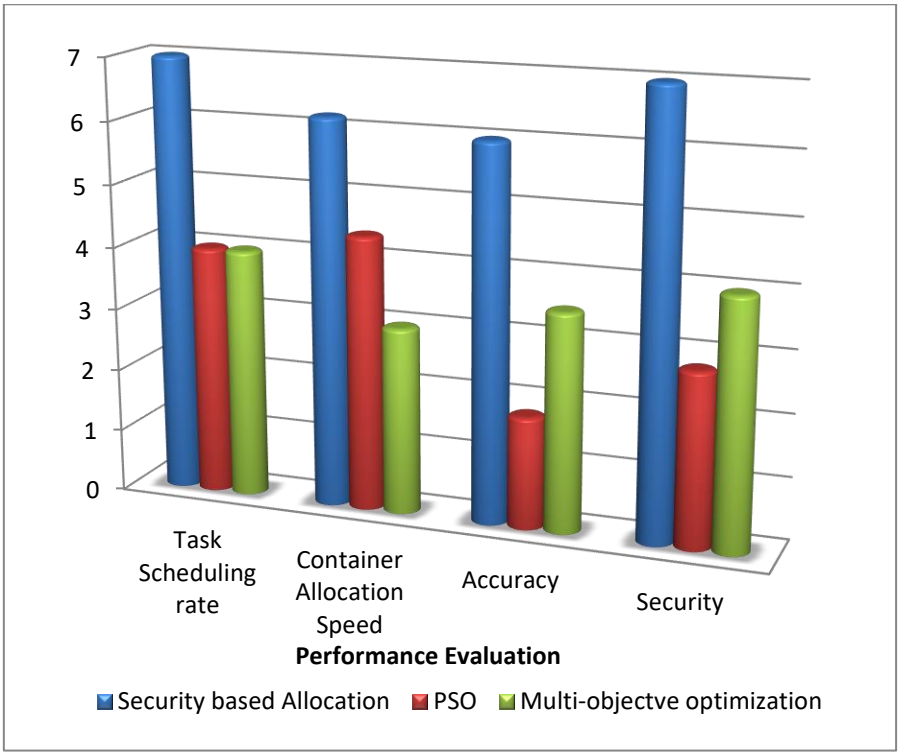

Figure.5 Security based Allocation VS existing PSO and multi-objective optimization model

In result analysis, a comparison of all the existing algorithms with the proposed model is done in figure 5. The comparison of existing algorithms such as PSO approach and multi-objective optimization is done with the proposed Security-based allocation algorithm. In the comparison theproposed algorithm is proved to be best in task scheduling, security maintenance, accuracy and resource allocation.

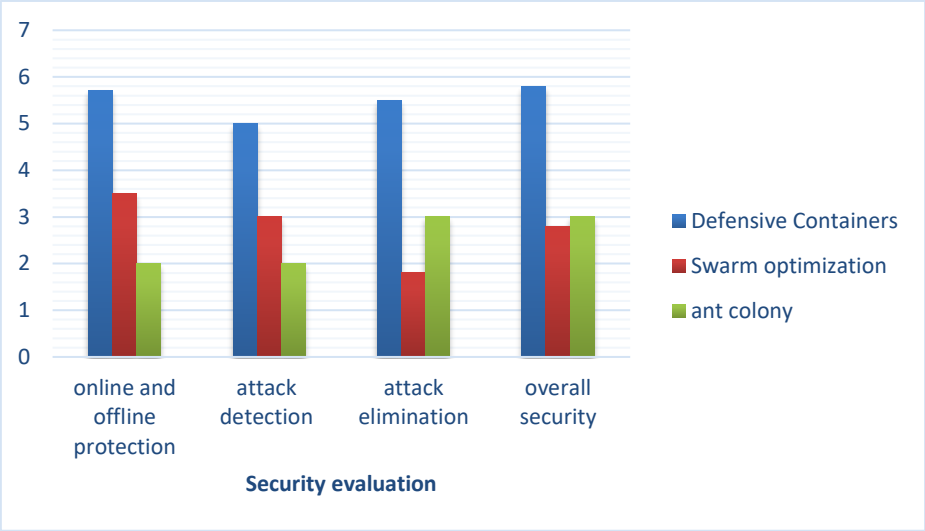

Figure.6 Security: defensive containers vs Swarm and Ant colony model.

In figure 6 a security evaluation is made where the proposed defensive containers is compared with other existing models such as Swarm and Ant colony model. The proposed model proved to be better in attack detection and eliminationeven offline.

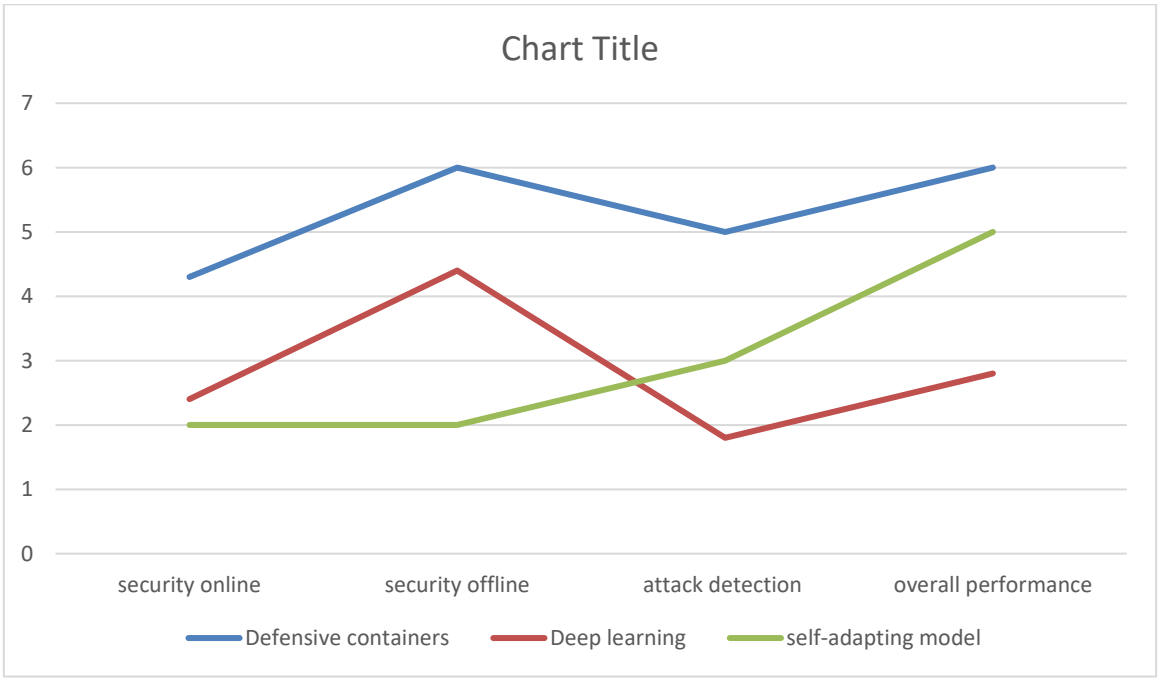

Figure.7 Security: defensive containers vs DL and Self-adapting model.

In figure 7 a security evaluation is made where the proposed defensive containers are compared with other existing models such as DL and Self-adapting model**.** The proposed model proved to be better in attack detection and elimination even offline.

III. CONCLUSION

In cloud container allocation streaming process is executed where a machine learning algorithm is used to analyze the user data and perform optimized allocation according to the data sensitivity. To perform an appropriate allocation the system uses a reduced optimal migration (ROM) process is used to allocate the normal data. The paper introduced a Security-based container scheduling modelthat performs a fake data replacement and cross verification to enhance the security of the container storage.to enhance the security the system proposed a defensive container mechanism to detect and eliminate attacks. Hence, the resources are maintained confidentially and the original data is produced to the user.The implementation model maintains the efficiency, speed, accuracy, security of task scheduling and resource allocation in cloud container.

Future enhancement

As a future enhancement the migration process allocation is completely take and a new optimization strategy is used to produce zero-time consumption.

REFERENCES

[1] R. Tang, ``Research on resources scheduling strategy of container cloud platform based on Kubernetes," M.S. thesis, Dept. Elect. Eng., UESTC Univ., Si Chuan, China, 2017.

[2] A. C. Zhou, B. He, X. Cheng, and C. T. Lau, “A declarative optimization engine for resource provisioning of scientific workflows in geo-distributed clouds,” IEEE Transactions on Parallel and Distributed Systems, vol. 28, no. 3, pp. 647–661, 2016.

[3] H. Zhang, X. Geng and H. Ma, "Learning-Driven Interference-Aware Workload Parallelization for Streaming Applications in Heterogeneous Cluster," in IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 1, pp. 1-15, 1 Jan. 2021, doi: 10.1109/TPDS.2020.3008725.

[4] X. Zhang, T. Wu, M. Chen, T. Wei, J. Zhou, S. Hu, and R. Buyya, “Energy-aware virtual machine allocation for cloud with resource reservation,” Journal of Systems and Software, vol. 147, pp. 147–161, 2019.

[5] S. K. Garg, A. N. Toosi, S. K. Gopalaiyengar, and R. Buyya, ‘‘SLAbased virtual machine management for heterogeneous workloads in a cloud datacenter,’’ J. Netw. Comput. Appl., vol. 45, pp. 108–120, Oct. 2014.

[6] M. Adhikari, S. Nandy, and T. Amgoth, ‘‘Meta heuristic-based task deployment mechanism for load balancing in IaaS cloud,’’ J. Netw. Comput. Appl., vol. 128, pp. 64–77, Feb. 2019.

[7] C. Guerrero, I. Lera, and C. Juiz, ‘‘Genetic algorithm for multi-objective optimization of container allocation in cloud architecture,’’ J. Grid Comput., vol. 16, no. 1, pp. 113–135, Mar. 2018.

[8] M. Kaur and S. Kadam, ‘‘A novel multi-objective bacteria foraging optimization algorithm (MOBFOA) for multi-objective scheduling,’’ Appl. Soft Comput. J., vol. 66, pp. 183–195, May 2018.

[9] M. Lin, J. Xi, W. Bai, and J. Wu, ‘‘Ant colony algorithm for multi-objective optimization of container-based microservice scheduling in cloud,’’ IEEE Access, vol. 7, pp. 83088–83100, 2019.

[10] T. Kim, M. Al-Tarazi, J. -W. Lin and W. Choi, "Optimal Container Migration for Mobile Edge Computing: Algorithm, System Design and Implementation," in IEEE Access, vol. 9, pp. 158074-158090, 2021, doi: 10.1109/ACCESS.2021.3131643.

[11] M. Ouyang, J. Xi, W. Bai and K. Li, "Band-Area Application Container and Artificial Fish Swarm Algorithm for Multi-Objective Optimization in Internet-of-Things Cloud," in IEEE Access, vol. 10, pp. 16408-16423, 2022, doi: 10.1109/ACCESS.2022.3150326.