International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

# OPTIMIZED ENCRYPTION-INTEGRATED STRATEGY FOR CONTAINERS SCHEDULING AND SECURE MIGRATION IN MULTI-CLOUD DATA CENTERS

**ADALA AMARNATH [1], CHIGURUPATI SAI VENKATA SRIJA [2], NAGAM RISHIKA [3], KARINGULA PRACHOTHAN [4], VOVALDAS SRIDHAR [5]**

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

**ABSTRACT—** Containers are recognized for their lightweight and virtualization efficiency, making them a vital element in modern application orchestration. In this context, the scheduler is crucial in strategically distributing containers across diverse computing nodes. This paper presents a novel two-stage container scheduling solution that addresses node imbalances and efficiently deploys containers. The proposed solution formulates the scheduling process as an optimization problem, integrating various objective functions and constraints to enhance server consolidation and minimize energy consumption. The confidentiality of migrated containers is ensured through encryption, and the associated costs are incorporated into the optimization constraints. This approach ensures security in container scheduling, considering container attributes as input features in our proposed attributes-based encryption model. By carefully selecting containers and destination nodes, this work seeks to establish balance within cloud-based clusters. This contributes to the improvement of container orchestration systems and their effectiveness in real-world scenarios. The proposed solution's efficacy is demonstrated in its ability to efficiently deploy containers in multi-data center cloud environments and seamlessly migrate them between hosts within the same data center or across different data centers. Our results show

optimal consolidation with a reduction in the number of running hosts, ranging from 4% to over 18%. Additionally, the solution promotes minimal total power consumption with savings ranging from 3.5 to 16.25 megawatts, while also ensuring balanced server loads.

*Index Terms* – Container scheduling, cloud computing, server consolidation, energy efficiency, load balancing, container migration, multi-data center cloud, Attribute-Based Encryption (ABE), secure scheduling, power consumption minimization.

## I. INTRODUCTION

Over the past few years, containers have become popular for simplifying application deployment and management. This virtualization technology provides a consistent runtime environment, enabling seamless application mobility across diverse systems. Additionally, containers are lighter than traditional virtual machines, translating to faster initiation and termination and superior resource utilization.

Container technology is a virtualization method that provides a runtime environment for applications and their dependencies at the process level [1]. The container is composed of two primary layers: the application layer and the base image layer. These layers work in tandem to ensure the smooth operation of the application or microservice [2]. The application layer contains the code for the application itself, and dependencies include codes, binaries, system libraries, and any configuration files needed for the application to run. The base image consists of these files and common system files. The container's ability to run relies on the necessary binaries and libraries in the base image layer. A container engine must be installed on the machine for the container to work. Docker, LNX, OpenVZ, and Containerd are some examples of container engines. Containers can function on bare metal servers or virtual machines, and multiple containers with similar dependencies can be utilizing a common base image. The container platform architecture makes it possible to quickly deploy, migrate, terminate, and replicate containers, boosting the adaptability and scalability of computing systems [3]. Figure 1 illustrates the architecture of the container virtualization platform and its position within a host machine.

Security of containers is important for cloud system providers and end users. There are three levels of data protection for containers: securing the saved container base image (data at rest), securing the running container

memory (data in-use), and securing the container data while being migrated (data in-transit). In this research, we specifically focus on ensuring the security of container data while being migrated by encrypting it prior to the migration process at the source host, and decrypting it upon its arrival at the destination.

When migrating between hosts within the same data center or across different ones with varying resource capabilities, it's crucial to have an adaptive encryption algorithm and key size. We are utilizing attribute-based encryption, encompassing attribute-based access control (ABAC) and attribute-based encryption (ABE). In our proposed approach, a customized ABE method has been effective for our needs, as we rely on the cloud management portal to handle authorization control between cloud data centers. To clarify, we cannot consider a static portal configuration for the container migration data block using one encryption type and key size due to the diversity in data center hardware and running container characteristics with user SLA requirements. This highlights the need for an on-the-fly system to set a key size and encryption method type as needed.

Attribute-based access control (ABAC) is an access control approach that authorizes users based on their specific attributes. Attribute-Based Encryption (ABE) is an encryption technique that allows data owners to set access control policies for encrypted data. This method ensures that only individuals with the necessary attributes can decrypt the protected data. As a result, ABE is considered a promising access control mechanism [5]. There are two types of Attribute-Based Encryption (ABE): Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) [6]. KP-ABE limits access to encrypted data to a chosen few users with keys. It uses policies in users' private keys. On the other hand, CP-ABE is a type of public-key encryption that defines a user's private key using attributes. The ciphertext is tied to an access policy, and decryption is only possible if the policy and user attributes match. This access control is based on user attributes, which can be issued by attribute authorities in one or multiple domains [7]. CP-ABE schemes are advantageous as they can cover a large number of users. Multi-authority CP-ABE schemes are well-suited for applications like e-health and e-government where users have attributes from multiple domain authorities.

## II. RELATED WORK

### A. *Container-based virtualization for real-time industrial systems-A systematic review*

Industrial Automation and Control systems have matured into a stable infrastructure model that has been kept fundamentally unchanged, using discrete embedded systems (such as Programmable Logic Controllers) to implement the first line of sensorization, actuation, and process control and stations and servers providing monitoring, supervision, logging/database and data-sharing capabilities, among others. More recently, with the emergence of the Industry 4.0 paradigm and the need for more flexibility, there has been a steady trend towards virtualizing some of the automation station/server components, first by using virtual machines and, more recently, by using container technology. This trend is pushing for better support for real-time requirements on enabling virtualization technologies such as virtual machines and containers.

This article provides a systematic review on the use of container virtualization in real-time environments such as cyber-physical systems, assessing how existing and emerging technologies can fulfill the associated requirements. Starting by reviewing fundamental concepts related to container technology and real-time requirements, it goes on to present the methodology and results of a systematic study of 37 selected papers covering aspects related to the enforcement of real-time constrains within container hosts and the expected task latency on such environments, as well as an overview of container platforms and orchestration mechanisms for RT systems.

### B. *Container placement and migration in edge computing: Concept and scheduling models*

Containers are a form of software virtualization, rapidly becoming the de facto way of providing edge-computing services. Research on container-based edge computing is plentiful, and this has been buoyed by the increasing demand for single digit, milliseconds latency computations. A container scheduler is part of the architecture that is used to manage and orchestrate multiple container-based applications on heterogenous computing nodes. The scheduler decides how incoming computing requests are allocated to containers, which edge nodes the containers are placed on, and where already deployed containers are migrated to. This paper aims to clarify the concept of container placement and migration in edge servers and the scheduling

models that have been developed for this purpose. The study illuminates the frameworks and algorithms upon which the scheduling models are built. To convert the problem to one that can be solved using an algorithm, the container placement problem in mostly abstracted using multi-objective optimization models or graph network models. The scheduling algorithms are predominantly heuristic-based algorithms, which are able to arrive at sub-optimal solutions very quickly. There is paucity of container scheduling models that consider distributed edge computing tasks. Research in decentralized scheduling systems is gaining momentum and the future outlook is in scheduling containers for mobile edge nodes.

### *C. A survey of state-of-the-art multi-authority attribute based encryption schemes in cloud environment*

Cloud computing offers a platform that is both adaptable and scalable, making it ideal for outsourcing data for sharing. Various organizations outsource their data on cloud storage servers for availing management and sharing services. When the organizations outsource the data, they lose direct control on the data. This raises the privacy and security concerns. Cryptographic encryption methods can secure the data from the intruders as well as cloud service providers. Data owners may also specify access control policies such that only the users, who satisfy the policies, can access the data. Attribute based access control techniques are more suitable for the cloud environment as they cover large number of users coming from various domains. Multi-authority attribute-based encryption (MA-ABE) technique is one of the propitious attribute based access control technique, which allows data owner to enforce access policies on encrypted data. The main aim of this paper is to comprehensively survey various state-of-the-art MA-ABE schemes to explore different features such as attribute and key management techniques, access policy structure and its expressiveness, revocation of access rights, policy updating techniques, privacy preservation techniques, fast decryption and computation outsourcing, proxy re-encryption etc. Moreover, the paper presents feature-wise comparison of all the pertinent schemes in the field. Finally, some research challenges and directions are summarized that need to be addressed in near future.

### *D. A systematic literature review of attribute based encryption in health services*

The widespread adoption of cloud technology in the healthcare industry has achieved effective outcomes in sharing health records and sensitive data. In recent years, many organizations have prioritized E-Health as their primary goal for advancement in health services. As a result, Attribute Based Encryption (ABE) has emerged as a reliable model for health information exchange across cloud settings. Eventually, it leads to provide acceptable solutions for challenging scenarios like fine-grained access control. Despite ABE significance and its breadth of applications, no systematic and comprehensive survey exists in the literature that covers every variation of ABE in healthcare, highlighting its past and present status.

This paper presents a systematic and comprehensive study of ABE works concerning E-Health as the authors rigorously investigate healthcare-focused ABE frameworks and examine them based on various descriptive criteria, along with categorizing them systematically in 10 distinct domains and sub-domains, ultimately offering observations and potential recommendations. The descriptive research design, significant findings along with the suggested future works will help future research in ABE to secure the existing E-Health data sharing more effectively. The present study will also facilitate researchers and practitioners to comprehend the past trends and current state of ABE architectures in secure health data-sharing scenarios, as well as the prospect of ABE deployment in most recent technological evolutions.

## III. PROPOSED METHODOLOGY

To solve the data privacy, integrity and correctness problems, this paper proposes a Privacy-Preserving Searchable Encryption (PPSE) scheme with an access control mechanism based on private and public blockchains. The PPSE uses the blockchain to replace the central server and outsources the search query to a smart contract, which produces a correct and unchangeable result without verification of the DO. In addition, an access control mechanism is introduced through smart contracts to restrict DUs' access to the private blockchain, which can protect data privacy and eliminate malicious attacks.

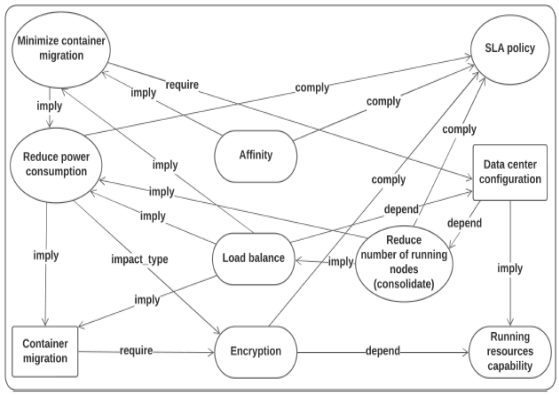
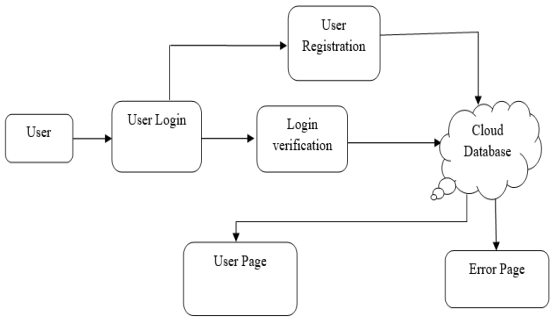



Fig. 1: System Overview

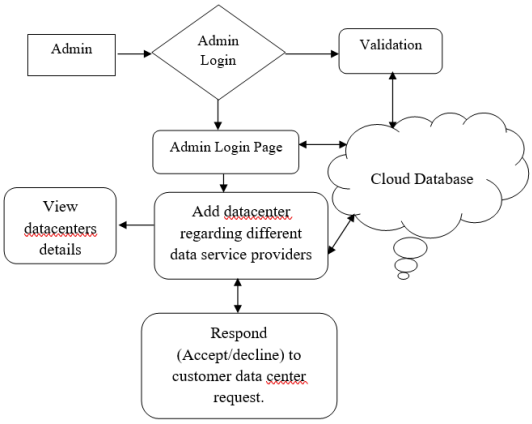
### 3.1 User Interface Design

In this module we design the windows for the project. In this module mainly we are focusing the login design page with the Partial knowledge information. Application Users need to view the application they need to login through the User Interface GUI is the media to connect User and Media Database and login screen where user can input his/her user name, password and password will check in database, if that will be a valid username and password then he/she can access the database.




### 3.2 Admin

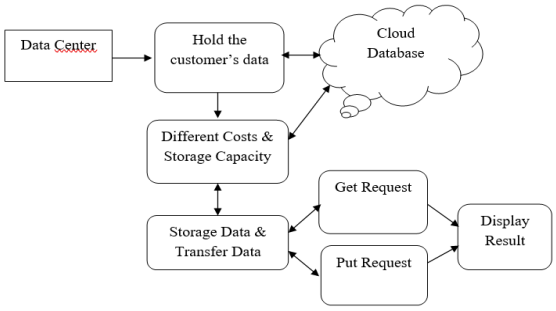
In this project the admin was done handling the data centers. In containers are deployed on the minimum number of running hosts, without factoring in additional optimization objectives. This facilitates rapid deployment and immediate customer service. Involves a conservative optimization model that balances load on running hosts, with minimal increases in power consumption and migration. Containers are migrated to other hosts, either within the same data center or in different data centers, with encryption to guarantee data confidentiality. The encryption and decryption schemes' processing is combined with scheduling optimization constraints to provide the best possible QoS for running containers and their scheduling.




### 3.3 Data Center

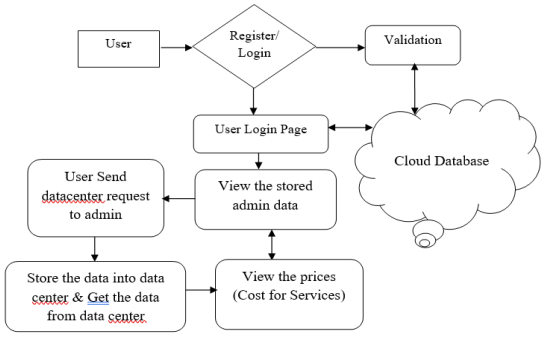
In this project data centers will store the store (Hold) the customer's data and each data center will have different costs as well as

capacity for storage, transfer, get requests and put requests. During stage two, the focus shifts towards container scheduling, with the primary goals of minimizing container migrations, power consumption, and running hosts. Different events are taken into consideration when determining scheduling actions, including SLA terms, affinity, load balance, encryption cost, data-center configuration, and capabilities. In the orchestration stage, the workload on data-center resources is redistributed according to the best possible data center hardware reconfiguration while keeping the aforementioned goals in mind. This process ensures that all conditions are met while prioritizing optimization goals and compliance with the SLA requirements.



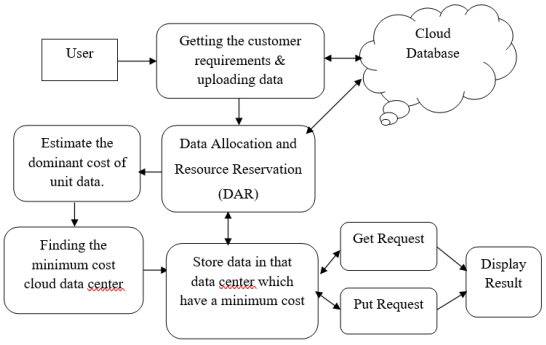

### 3.4 Customer (User)

In this project the customers or users will store the data into the cloud across multiple cloud providers. Encryption algorithms, along with KP-ABE, has gained significant attention in the field of security. Therefore, matching system and user requirements to the resources' capabilities by optimizing the security key size with the encryption algorithm is an area of active research.




### 3.5 Data Allocation and Resource reservation (DAR)

DAR (Data Allocation and Resource reservation) is a mechanism in our project to minimize the cost of cloud service across multiple cloud providers. The scheduling algorithm in our proposed scheme has prior knowledge of the migration encryption overhead that matches the source host's encryption cost requirement. The optimized scheduler takes into account the encryption cost each time a container is migrated to a destination host.




## IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed container scheduling strategy improves resource utilization, load balancing, and energy efficiency in multi-cloud environments. It reduced the number of active hosts by 4% to over 18% and achieved power savings of 3.5 to 16.25 MW. The integration of attribute-based encryption also ensured secure container migration. Overall, the method is both efficient and secure for cloud-based container management.




Fig. 2: Home Page

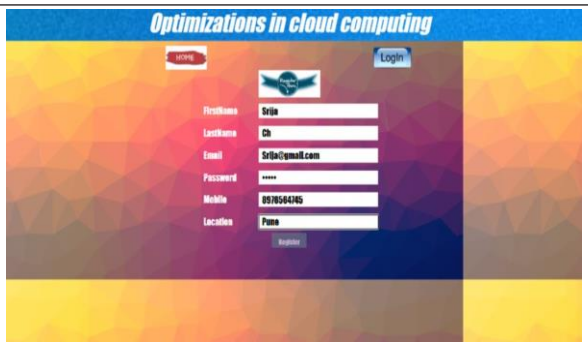



Fig. 3: Registration




Fig. 4: Login




Fig. 5: Upload Image




Fig. 6: Login to Site

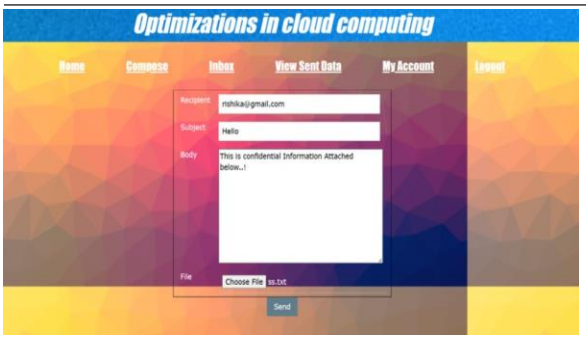



Fig. 6: Send Data

## V. CONCLUSION

This paper introduced a two-stage container scheduling solution that efficiently deploys containers and addresses imbalances across nodes through migration. The solution formulates the scheduling process as an optimization problem and incorporates various objective functions and constraints to improve server consolidation and reduce energy consumption. Encryption is used to ensure the confidentiality of containers during migration. The cost of encryption and decryption has been included in the optimization constraints of the proposed solution. The solution has been shown to be effective in multi-data center cloud environments, contributing to the improvement of container orchestration systems in real-world scenarios.

## REFERENCES

1. "Docker" in What is a Container?—Docker, USA, Sep. 2023, [online] Available: https://www.docker.com/resources/what-container/.

2. R. Queiroz, T. Cruz, J. Mendes, P. Sousa and P. Simões, "Container-based virtualization for real-time industrial systems—A systematic review", ACM Comput. Surv., vol. 56, no. 3, pp. 1-38, Oct. 2023.

3. O. Oleghe, "Container placement and migration in edge computing: Concept and scheduling models", IEEE Access, vol. 9, pp. 68028-68043, 2021.

4. "Weaveworks" in Docker Vs Virtual Machines (VMS): A Practical Guide to Docker Containers and VMS, USA, Sep. 2020, [online] Available: https://www.weave.works/blog/a-practical-guide-to-choosing-between-docker-containers-and-vms.

5. R. Gupta, P. Kanungo and N. Dagdee, "A survey of state-of-the-art multi-authority attribute based encryption schemes in cloud environment", KSII Trans. Internet Inf. Syst., vol. 17, no. 1, pp. 145-164, 2023.

6. R. Imam, K. Kumar, S. M. Raza, R. Sadaf, F. Anwer, N. Fatima, et al., "A systematic literature review of attribute based encryption in health services", J. King Saud Univ.-

Comput. Inf. Sci., vol. 34, no. 9, pp. 6743-6774, Oct. 2022.

7. P. S. K. Oberko, V.-H.-K. S. Obeng and H. Xiong, "A survey on multi-authority and decentralized attribute-based encryption", J. Ambient Intell. Humanized Comput., vol. 13, no. 1, pp. 515-533, Jan. 2022.

9. "Kubernetes The Linux Foundation" in Kubernetes: Production-Grade Container Orchestration, USA, Sep. 2023, [online] Available: https://kubernetes.io/.

**AUTHORS Profile**



**Mr. ADALA AMARNATH** has received his B.Tech - Computer Science and Engineering from JNTUH, Hyderabad in 2010, M.Tech-CNIS degree in Computer Science and Engineering from JNTUH, Hyderabad in 2013 and Pursuing Ph.D degree in Computer Science and Engineering from ICFAI University Hyderabad. He is dedicated to teaching field from the last 12 years. His research area Quantum Computing and Aptitude Computing. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



**Ms. CHIGURUPATI SAI VENKATA SRIJA** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



**Ms. NAGAM RISHIKA** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



**Mr. KARINGULA PRACHOTHAN** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



**Mr. VOVALDAS SRIDHAR** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.