

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152



Enhancing Kubernetes Cloud Bursting Security with Attribute-Based Management

P. Chandra Sekhar¹, Dharavath sai kumar², Dobba Sai³, Gangala chandu⁴

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India¹

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, Telangana, India²⁻⁴

ABSTRACT: In modern cloud computing, the demand for flexible and scalable service orchestration, coupled with robust security measures, is essential. This paper introduces an innovative approach to secure cloud bursting in Kubernetes by integrating Attribute-Based Encryption (ABE) with Kubernetes labelling. Our model tackles key challenges such as complexity, cost, and data protection compliance by leveraging both Kubernetes and ABE. We propose an attribute-based bursting mechanism that utilizes Kubernetes labels for efficient orchestration, alongside an encryption component that applies ABE to safeguard data. This unified management framework enhances data confidentiality while optimizing cloud bursting operations. By combining label-based orchestration with fine-grained encryption, our solution delivers a technologically advanced yet user-friendly approach to secure cloud bursting. We validate the feasibility and effectiveness of our model through a proof-of-concept implementation, demonstrating its ability to ensure compliance with security and privacy regulations while fulfilling the demands of modern cloud-based systems.

KEYWORDS: Attribute-Based Access Control (ABAC), Kubernetes, Cloud Bursting, Hybrid Cloud, Secure Cloud Computing

I.INTRODUCTION

In recent years, the proliferation of virtualization and containerization technologies has led to a significant increase in the complexity of distributed systems, as cloud computing systems. As organizations strive to achieve efficient resource management and scalability, Kubernetes has emerged as the most popular solution for orchestrating resources in such complex systems. For example, it is integrated into platforms such as Amazon Elastic Kubernetes Service, Google Kubernetes Engine, Azure Kubernetes Service IBM Cloud Kubernetes Service, and Oracle Container Engine for Kubernetes (OKE). This paper aims at exploring the challenges associated with cloud bursting, which allows private cloud services to use public cloud resources when local resources are exhausted or for any other reasons. Specifically, we address the configuration issues associated with service request load management over a hybrid cloud system including both private and public components. The orchestration of such a heterogeneous system presents a number of challenges, such as optimal management of typically large volume of resources, variable operating conditions, security issues, and compliance with local regulations. In order to address these challenges, resorting to attribute-based management policies is regarded as a valid approach. Attributes are intrinsic characteristics or properties related to the entities, workload, or resources to manage. They can refer to different aspects, such as computational requirements, security levels, data location, and other relevant information. Recent findings indicate that the related management challenges can be effectively addressed through the utilization of an attribute-based approach, which has been found to be preferred over the conventional role-based methods. Rather than depending solely on pre-defined roles, attributes can include a broader array of qualities and attributes associated with users, resources, or data. This level of flexibility, adaptability, and precision in access control renders them more suitable for scenarios characterized by a diverse, dynamic, and intricate range of access requirements. In particular, in this paper, we leverage the attribute-based approach to easily orchestrate load distribution and resource allocation between private and public clouds during the cloud bursting process. Attribute-based policies can be enforced by different technologies. In this paper we make use of Kubernetes, since today it is one of the most appreciate tools for managing distributed systems, especially in the context of cloud computing. It provides flexibility through different built-in components and tools. Among them, the usage of labels and label selectors can be exploited to simplify cloud bursting operations. While Kubernetes best practices recommend that labels be assigned semantic meanings before being used there is currently no standardized method for enforcing this practice. Our goal is to develop a systematic approach in the context of cloud bursting that

ensures semantic meaning associated with the generic Kubernetes label concept. Furthermore, it emerged that Kubernetes management does not suitably address all the security aspects related to data confidentiality and access controls, which are central in cloud bursting. Kubernetes incorporates access management, but it requires separate configuration processes that are decoupled from the logic of the orchestrated functions. Moreover, the existing access management mechanisms in Kubernetes have certain limitations in terms of managing complex authorization scenarios and are constrained by their policy scope. Hence, these limitations are challenging for achieving comprehensive and secure resource management in the context of cloud bursting. To overcome these limitations, in this paper we propose an architectural solution to address the security challenges of cloud bursting that integrates the Kubernetes orchestration with attribute-based encryption. When it is necessary to move data to the cloud, it is critical to ensure security and flexible, granular control over file access. This can be efficiently done through ABE. However, user revocation is a significant issue in ABE. In, the authors propose a ciphertext-policy ABE (CP-ABE) scheme with efficient user revocation for cloud storage system. User revocation is handled by introducing the concept of user group, with the rule of updating private keys of the users remaining in the group when any other user leaves it. In addition, since the computation cost of CP-ABE grows linearly with the complexity of the access structure, in order to mitigate it they propose to offload high computation demand to cloud service providers without leaking file content and secret keys. They prove that the proposed scheme can withstand collusion attack performed by the revoked users cooperating with the remaining ones. A similar approach, which requires the update of the unrevoked users' keys, is proposed in It is based on the use of a group manager to accomplish this task. It also applies re-encryption technology to prevent the revoked users from decrypting ciphertexts. However, since the correctness of outsourcing computing results is difficult to guarantee, this approach often requires resorting to the blockchain technology for obtaining such guarantees.

II.LITERATURE SURVEY

Title: The evolution of Kubernetes clusters in multi cloud and hybrid cloud.

Author: B. Ghosh.

Year: 2023.

Description

As a core technology, Kubernetes has become the foundation of modern application architecture, and more and more enterprises use Kubernetes as the container orchestration system. The following data comes from the raw data of the 2022 CNCF Survey. It can be seen that the proportion of enterprises using Kubernetes has reached 80%. Applications in enterprises are often complex and require different environments for development, testing, and production deployment. To avoid interference and crossover between applications, it is often necessary to deploy and manage applications separately in different Kubernetes clusters. After deploying independent Kubernetes clusters in different environments in the same data , the cluster scale, management methods, reliability, and security in different environments are different. From development, testing to production, the cost investment is also gradually increased to ensure Better performance, increased reliability and security. This is also a form of multi-Kubernetes clusters (note that multi-Kubernetes clusters are mentioned here).

Title: Revocable blockchain-aided attribute based encryption with escrow-free in cloud storage.

Author: Y. Guo, Z. Lu, H. Ge, and J. Li.

Year: 2023

Description

The massive amount of data generated by the Internet of Things (IoT) and the need to store that data presents a huge challenge for storage. However, meeting this challenge has also driven the development of storage technologies, especially those related to cloud storage. Although attribute-based encryption (ABE) schemes are commonly used to achieve data confidentiality and fine-grained access control in cloud storage, there is still an inherent problem with ABE schemes, namely the key escrow problem. In this paper, we propose a revocable blockchain-aided ABE with escrow-free (BC-ABE-EF) system that resolves the key escrow problem by replacing the traditional key authority with a consortium blockchain. The keys are generated between the blockchain and the data user through a secure key issuing protocol, and the blockchain cannot obtain the user's full key alone. Furthermore, utilize the decryption cloud server to schedule pre-decryption operations in cloud and introduce a group manager to update the group keys of unrecovered users and generate re-encryption keys. The security analysis shows that our scheme is secure under the Decisional Computation Diffie Hellman (DCDH) assumption. The effectiveness of the scheme is demonstrated by simulating the BC-ABE-EF scheme and comparing it based on performance analysis.

Title: Offloading using traditional optimization and machine learning in federated cloud–edge fog systems: A survey.

Author: B. Kar, W. Yahya, Y. Lin, and A. Ali.

Year: 2023

Description

The huge amount of data generated by the Internet of Things (IoT) devices needs the computational power and storage capacity provided by cloud, edge, and fog computing paradigms. Each of these computing paradigms has its own pros and cons. Cloud computing provides enhanced data storage and computing power but causes high communication latency. Edge and fog computing provide similar services with lower latency but limited capacity, capability, and coverage. A single computing paradigm cannot full fill all the requirements of IoT devices and a federation between them is needed to extend their capacity, capability, and services. This federation is beneficial to both subscribers and providers and also reveals research issues in traffic offloading between clouds, edges, and fogs. Optimization has traditionally been used to solve the problem of traffic offloading. However, in such a complex federated system, traditional optimization cannot keep up with the strict latency requirements of decision-making, ranging from milliseconds to sub-seconds. Machine learning approaches, especially reinforcement learning, are consequently becoming popular because they could quickly solve offloading problems in dynamic environments with some unknown information. This study provides a novel federal classification between cloud, edge, and fog and presents a comprehensive research roadmap on offloading for different federated scenarios. We survey the relevant literature on the various optimization approaches used to solve this offloading problem and compare their salient features. We then provide a comprehensive survey on offloading in federated systems with machine learning approaches and the lessons learned as a result of these surveys. Finally, we outline several directions for future research and challenges that have to be faced in order to achieve such a federation.

III. EXISTING SYSTEM

- Ciphertext-policy ABE (CP-ABE) scheme with efficient user revocation for cloud storage system. User revocation is handled by introducing the concept of user group, with the rule of updating private keys of the users remaining in the group when any other user leaves it.
- CP-ABE grows linearly with the complexity of the access structure, in order to mitigate it they propose to offload high computation demand to cloud service providers without leaking file content and secret keys.
- They prove that the proposed scheme can withstand collusion attack performed by the revoked users cooperating with the remaining ones.

EXISTING SYSTEM DISADVANTAGES

- Cost Management
- Data Security and Compliance.
- Disaster Recovery and Backup.

IV. PROPOSED SYSTEM

- In this paper we propose an architectural solution to address the security challenges of cloud bursting that integrates the Kubernetes orchestration with attribute-based encryption.
- Our goal is to develop a systematic approach in the context of cloud bursting that ensures semantic meaning associated with the generic Kubernetes label concept.
- Leveraging the Attribute-Based Encryption (ABE) technology, deployed through a cloud service, to improve security levels, in terms of data privacy, confidentiality, and access control, through fine-grained policies.

PROPOSED SYSTEM ADVANTAGES

- Data Confidentiality.
- Flexibility.
- Improves both efficiency and security.

➤ V. SYSTEM ARCHITECTURE

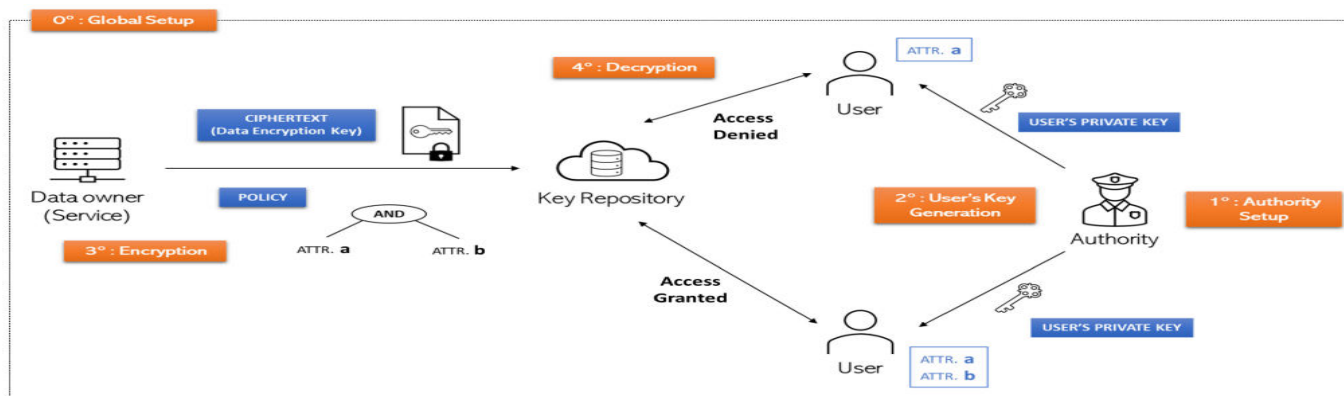


Fig:1 System Architecture

In the previous sections, we mentioned that our objective is not only to propose a unified orchestration, but also to offer a solution able to address some security issues, such as confidentiality, access control, and compliance to General Data Protection Regulation (GDPR) rules [35]. For example, when bursting is carried out using the infrastructure of a public cloud provider, it is important to protect user data, in order to avoid privacy issues for those services that require them. In this regard, ABE natively supports the decoupling of encryption keys from third parties (i.e., the infrastructure provider), thus ensuring that only users with the right attributes can access the protected service data, even if hosted on public clouds and regardless of local regulations that may affect the cloud service provider policies. Thus, the joint management of labels for both security and orchestration management can help mitigating confidentiality leakage for critical data. In addition, since ABE allows accessing contents through policies based on the owned attributes and not on the identity, the proposed approach can be used not only to ensure confidentiality, but also to protect anonymity while accessing data outside the private cloud deployment. The level of this protection depends on several factors, such as user population, number of attributes, derived policies, and so on.

VI. METHODOLOGIES

Modules Name:

This project having the following 4 modules:

1. User Interface Design
2. Key Repository
3. Authority
4. Cloud

1. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.

2. Key Repository

Key Repository is the second module in our project, where crucial functional requirements of the project will be carried out. KR first login with name and password then verify all user request for data. Key Repository will share keys to user to access the plain data. When Owner uploads data the keys will be shared Key Repository.

3. Authority

This is the third module in our project where Authority plays the main part of the project role. Authority login first then its checks User Registration data, if Authority approve keys for user then he access data or perform an remaining operation

4.Data Owner

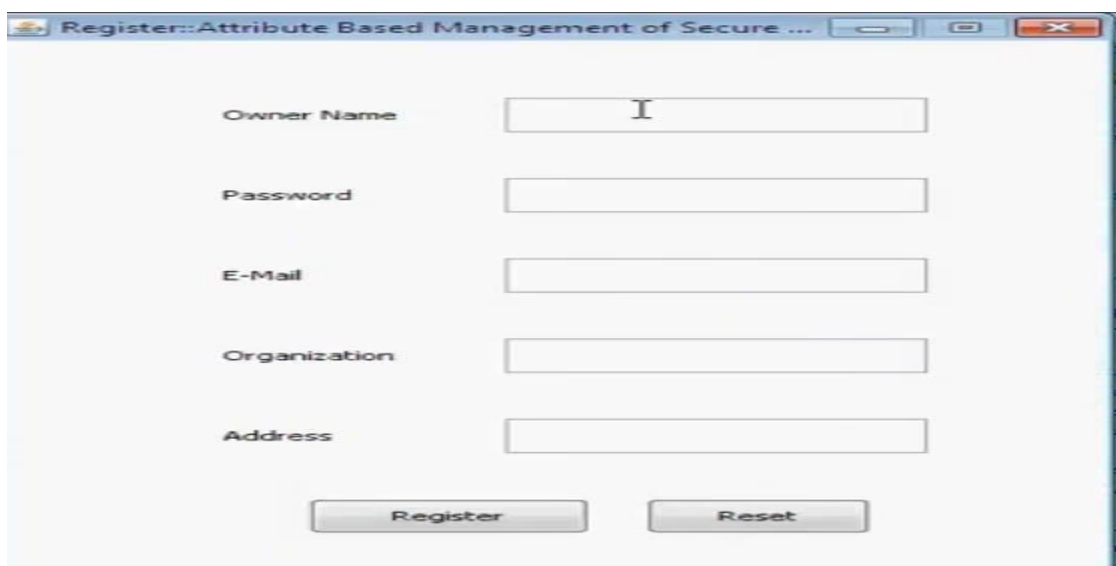
This is the fourth module in our project where data owner plays the main part of the project role. Owner register and then login in to the application, the registration details are stored inside database. After Owner Login he will directly navigate owner home page and Upload data. When data owner upload data the data will be encrypted the encrypted keys will be stored inside database and keys will shred with key repository.

VII. ALGORITHM USED**Attribute based encryption(ABE)**

Attribute-Based Encryption (ABE) is a sophisticated form of public-key encryption that enables fine-grained access control. Unlike traditional public-key encryption where a message is encrypted for a specific recipient, ABE allows for flexible encryption based on attributes or policies. There are two main types of ABE: Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, the sender encrypts a message with a set of attributes, while the decryption key is associated with an access policy. Decryption is only possible if the ciphertext's attributes satisfy the access policy of the decryption key. Conversely, in CP-ABE, the sender defines an access policy for encryption, and decryption keys are tied to sets of attributes; decryption is successful if the attributes of the key satisfy the policy. The core components of ABE include setup, key generation, encryption, and decryption. Setup involves generating system parameters and a master key. Key generation produces a private key based on an access policy or attributes, encryption uses a set of attributes or an access policy, and decryption verifies if the attributes meet the policy to allow access.

Cloud Bursting

Cloud bursting is a hybrid cloud computing strategy used to handle sudden spikes in IT demand by extending on-premises resources to a public cloud. When the demand for computational resources exceeds the capacity of a private data center, the excess workload is "burst" to a public cloud. This approach allows organizations to scale their resources dynamically and cost-effectively without over-provisioning their on-premises infrastructure for peak loads, which may only occur sporadically. Clustering, on the other hand, is a data analysis technique that involves grouping a set of objects or data points based on their similarities. The goal of clustering is to partition the data into subsets, or clusters, where data points within each cluster are more similar to each other than to those in other clusters. This technique is widely used in fields like machine learning, data mining, and pattern recognition to identify hidden patterns, categorize large datasets, and perform unsupervised learning. Common clustering algorithms include k-means, hierarchical clustering, and DBSCAN, each of which uses different methods to determine how data points should be grouped. Clustering can be applied in a variety of contexts, including customer segmentation, anomaly detection, and image processing.

VIII. EXPERIMENTAL RESULTS


The screenshot shows a web browser window titled "Register::Attribute Based Management of Secure ...". The page contains a registration form with the following fields and labels:

- Owner Name:
- Password:
- E-Mail:
- Organization:
- Address:

At the bottom of the form, there are two buttons: "Register" and "Reset".

Fig1: Registration Page

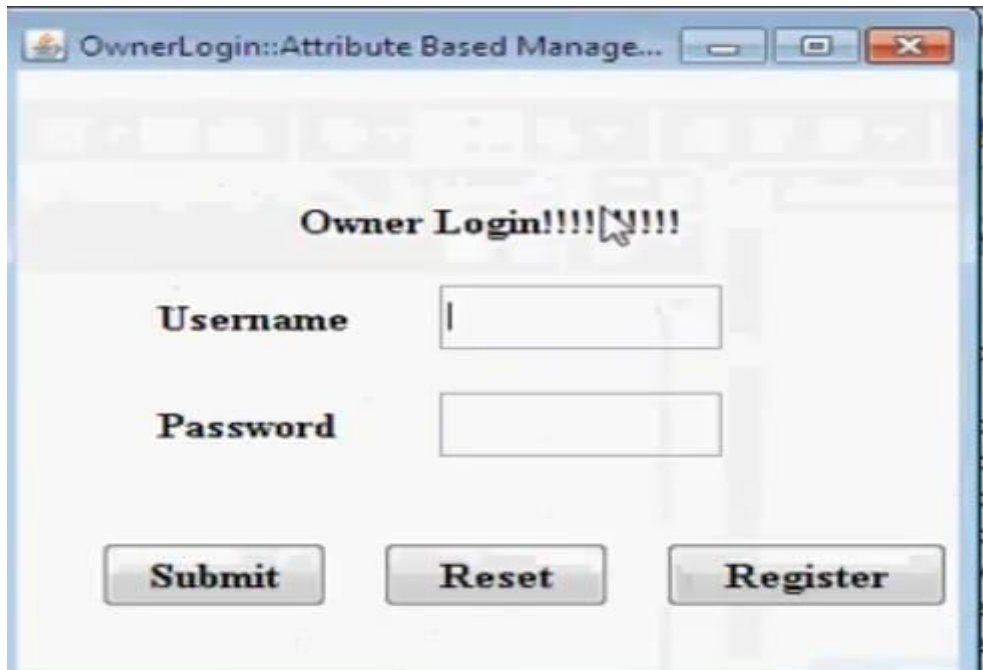


Fig2: Login Page

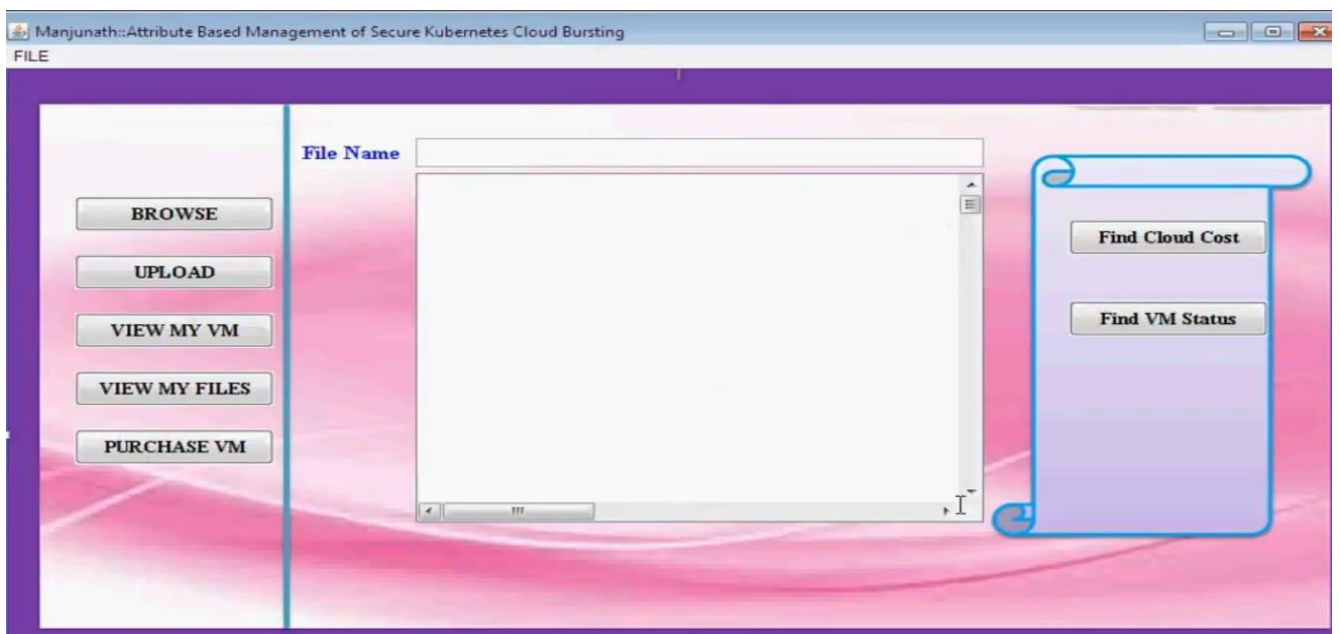
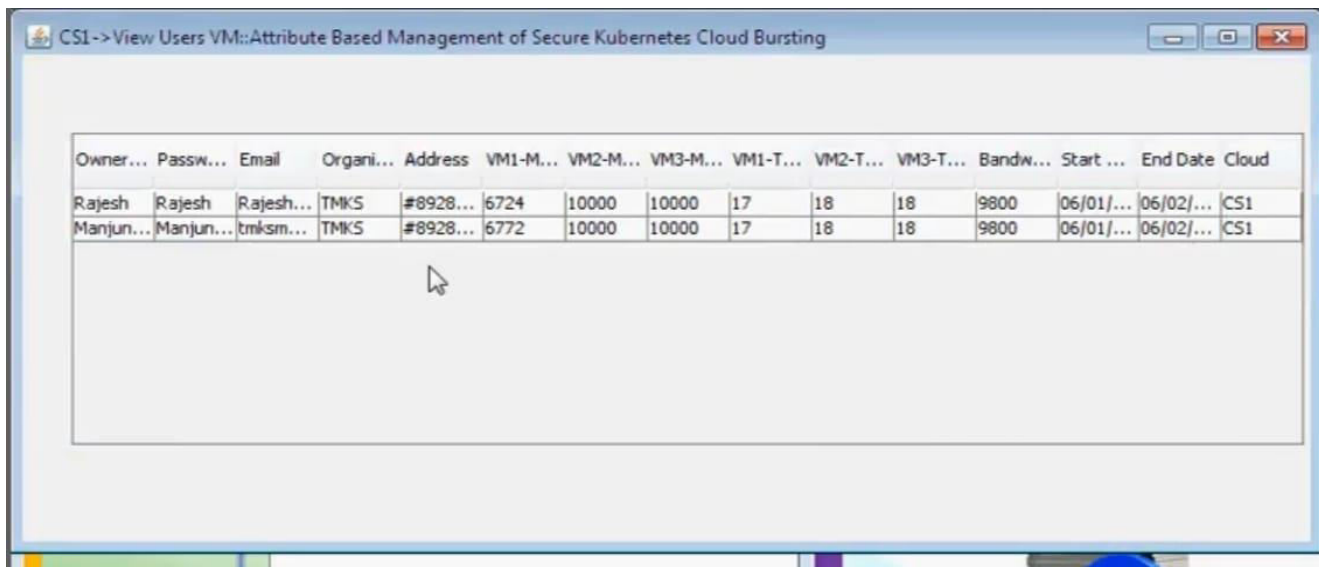


Fig3: Upload File



Owner...	Passw...	Email	Organi...	Address	VM1-M...	VM2-M...	VM3-M...	VM1-T...	VM2-T...	VM3-T...	Bandw...	Start ...	End Date	Cloud
Rajesh	Rajesh	Rajesh...	TMKS	#8928...	6724	10000	10000	17	18	18	9800	06/01/...	06/02/...	CS1
Manjun...	Manjun...	tmksm...	TMKS	#8928...	6772	10000	10000	17	18	18	9800	06/01/...	06/02/...	CS1

Fig4: Result

IX. CONCLUSION

In this paper, we introduce a robust orchestration scheme tailored for secure cloud bursting. This scheme addresses the complexities, cost challenges, and stringent data protection compliance requirements by harnessing the combined capabilities of K8s and ABE. By incorporating ABE, our approach achieves granular encryption and provides cloud resources with suitable confidentiality. At the same time, cloud bursting empowers the extension of computational tasks beyond the scope of a local primary cloud environment. The synergy of these two technologies establishes a cohesive management framework, guaranteeing secure access to bursting services and streamlined deployment of excess workloads to the cloud, all facilitated by Kubernetes.

X. FUTURE ENHANCEMENT

Future research will consider the integration of the proposed solution with artificial intelligence algorithms to proactively infer the need of resorting to bursting operations. In fact, purely relying on a reactive approach the latency of the process can either lead to temporary violation of service level agreements - loose approach - or allocation of excessive resources - conservative appromately.

REFERENCES

- [1] T.Kishore Babu, Raja Kiran Kolati, Pathipati Chandrasekhar, Nimmagadda MuraliKrishna, Sriharaha Vikruthi, B. Rajeswari Computer-Assisted Leukemia Detection and Classification using Machine Learning .“2024 International Conference on Expert Clouds and Applications (ICOECA)”,2024.
- [2] International Research Journal of Modernization in Engineering Technology and Science(irjmets) ,AUTHORIZED SEARCHABLE FRAMEWORK FOR E-HEALTHCARE SYSTEM, P.Chandra Sekhar*1, Kammala Vinay*2, Mogulla Ragender*3, Gouri Rohith*4
- [3] International Journal of Scientific Research in Engineering and Management (IJSREM),EFPB: Efficient Fair Payment Based on Blockchain for Outsourcing Services in Cloud Computing Pathipati Chandra Sekhar1 Assistant Professor, Guru Nanak Institute of Technology, Department of CSE, Hyderabad. K.Suresh Babu2Assistant Professor, PACE Institute of Technology and Sciences, Department of CSE,Ongole
- [4] International Research Journal of Modernization in Engineering Technology and Science, FASHION RECOMMENDATION SYSTEM USING SOCIAL MEDIA WEBSITE, P.Chandra Sekhar*1, Sania Mahereen*2, S.
- [5] Ram Prasad*3, S. Farhan AktherInternational Research Journal of Modernization in Engineering Technology and Science,USING MICROSERVICES PLANNING FOR ADDITIONAL CREATED HELP PARTAKING IN IOT EDGE CONDITIONS

- [6] P.Chandra Sekhar*1, G.Sravani*2, Ch.Deekshitha*3, G.Nandini*International Journal of Scientific Research in Engineering and Management (IJSREM),A Review of Machine Learning Strategies for Enhancing Efficiency and Innovation in Real-World Engineering Applications,
- [7] Mrs. Palagati Anusha1, Mr. S. Sujith Kumar2, Mr. Chandrasekhar Pathipati3 [1] (Amazon Web Serv., Inc., Seattle, WA, USA). Amazon Elastic Kubernetes Service (Amazon EKS). Accessed: Jun. 8, 2023. (google, Mountain View, CA, USA). Google Kubernetes Engine. Accessed: Jun. 8, 2023. (Int. Bus. Mach. Corp., Armonk, NY, USA). Kubernetes Service. Accessed: Jun. 8, 2023
- [9] "Module aw11 rabe." Accessed: Jan. 5, 2024
- [10] (Oracle Computer. Software. Co., Austin, TX, USA). Oracle Cloud Native Services—Container Engine for Kubernetes. Accessed: June 8, 2023.
- [11] "Security best practices for Kubernetes deployment." Mar. 2019. [Online]. Available: <https://kubernetes.io/blog/2016/08/security-bestpractices-kubernetes-deployment/>
- [12] "Anthos." Dec. 2023. [Online]. Available: <https://cloud.google.com/> author [8] (Palo Alto Networks, Inc., Santa Clara, CA, USA). Cloud Native Applications Protection Platform. Dec. 2023.
- [13] "Configuration best practices: Using labels." Jul. 2023. [Online].
- [14] (Cloud Bees Software. Co., San Jose, CA, USA). Configuring Cloud bees Build Acceleration for Agent Cloud Bursting. (Dec. 2023).
- [15] "Kubernetes auto scaler." Git hub. Dec. 2023.
- [16] (Microsoft Corp. Technol. Corp., Redmond, WA, USA). Securing Kubernetes Workloads In Hybrid Settings With Aporeto. (Dec. 2023)
- [17] (Amazon Web Serv., Inc., Seattle, WA, USA). TLS-Enabled Kubernetes Clusters With ACM Private CA and Amazon EKS, (Dec. 2023).
- [18] "Virtual kubelet." Dec. 2023
- [19] R. Ahuja and S. K. Mohanty, "A scalable attribute-based access control scheme with flexible delegation cum sharing of access privileges for cloud storage," IEEE Trans. Cloud Computer., vol. 8, no. 1, pp. 32–44, Mar. 2020.
- [20] S. Ameer, J. Benson, and R. Sandhu, "An attribute-based approach toward a secured smart-home IoT access control and a comparison with a role-based approach," Information, vol. 13, no. 2, p. 60, 2022.
- [21] D. Balouek-Thomert, E. G. Renart, A. R. Zamani, A. Simonet, and M. Parashar, "Towards a computing continuum: Enabling edge-to cloud integration for data-driven workflows," Int. J. High Perform. Computer. Appl., vol. 33, no. 6, pp. 1159–1174, 2019.
- [22] L. Baresi, D. F. Mendonça, M. Garriga, S. Guinea, and G. Quattrocchi, "A unified model for the mobile-edge-cloud continuum," ACM Trans. Internet Technol., vol. 19, no. 2, pp. 1–21, Apr. 2019.
- [23] M. Bellare, B. Waters, and S. Yilek, "Identity-based encryption secure against selective opening attack," Cry ptol. E Print Arch., IACR, Bellevue, WA, USA, Rep. 2010/159, 2010.
- [24] P. Benedetti, M. Femminella, G. Reali, and K. Steenhaut, "Reinforcement learning applicability for resource-based autoscaling in serverless edge applications," in Proc. IEEE Int. Conf. Pervasive Computer. Commun. Workshops Other. Events (Per Com Workshops), 2022, pp. 674–679.
- [25] S. Benitez. "Meet rocket." Accessed: Jan. 5, 2024. [Online].
- [26] S. Bera, S. Prasad, Y. Sreenivasa Rao, A. K. Das, and Y. Park, "Designing attribute-based verifiable data storage and retrieval scheme in cloud computing environment," J. Inf. Secure. Appl., vol. 75, Jun. 2023, Art. no. 103482.
- [27] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy (SP'07), 2007, pp. 321–334.
- [28] S. Böhm and G. Wirtz, "Cloud-edge orchestration for smart cities: A review of Kubernetes -based orchestration architectures," EAI Endorsed Trans. Smart Cities, vol. 6, no. 18, p. e2, May 2022.
- [29] D. Boneh, "Bilinear groups of composite order," in Proc. 1st Int. Conf. Pair.-Based Cryptography., 2007, p. 1.
- [30] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in Proc. Theory Cryptography. Conf., 2005, pp. 325–341.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152