International Journal of
Human Computations & Intelligence
Vol. 04, Issue. 02, 2025

RESEARCH ARTICLE OPEN ACCESS

Attribute Based Management of Secure Kubernetes Cloud Bursting

Harsha Vardhan . Yousuf Khan . Venkata Nikhil . Jyoshna Priya . P Siva Lakshmi

Department of CSE,
Annamacharya Institute of Technology and Sciences,
Kadapa, Andhra Pradesh, India.

DOI: **10.5281/zenodo.15263369**
Received: 27 January 2025 / Revised: 21 February 2025 / Accepted: 27 March 2025
©Milestone Research Publications, Part of CLOCKSS archiving

Abstract – In contemporary cloud computing, ensuring flexible and scalable service orchestration alongside strong security measures is crucial. This paper presents a novel strategy for securely managing cloud bursting in Kubernetes by integrating Attribute-Based Encryption (ABE) with Kubernetes labelling. Our proposed model tackles challenges related to complexity, cost, and compliance with data protection regulations by leveraging both Kubernetes and ABE. The approach introduces an attribute-based bursting mechanism that utilizes Kubernetes labels for orchestration, alongside an encryption component that employs ABE to safeguard data. This integrated management framework enhances data confidentiality while optimizing cloud bursting efficiency. By merging label-based orchestration with fine-grained encryption, our model delivers a secure yet user- Venkata Nikhilsolution. A proof-of-concept implementation validates the practicality and effectiveness of our approach, demonstrating its capability to align with security and privacy regulations while addressing the demands of modern cloud environments.

Index Terms –Cloud bursting, orchestration, attribute-based encryption,Kubernetes.

I. INTRODUCTION

In recent years, the rapid advancement of virtualization and hybrid cloud management, incorporating both containerization technologies, has resulted in the integration of private and public components. The orchestration of these systems has traditionally relied on role-based methods. However, instead of solely depending on predefined roles, attributes provide a broader spectrum of qualities linked to users, resources, or data. This flexibility enhances adaptability and precision in access control, making it ideal for environments with diverse, dynamic, and complex access requirements [16],. In this paper, we

MILESTONE
RESEARCH.IN
OPEN ACCESS

ISSN (Online): 2583-5696
Int. Jr. of Hum Comp. & Int.

utilize an attribute-based approach to facilitate seamless load distribution and resource allocation between private and public clouds during the cloud bursting process.

Different technologies can enforce attribute-based policies. In this work, we adopt Kubernetes due to its popularity as a robust tool for managing distributed systems, particularly in cloud computing. Kubernetes offers flexibility through various built-in components and tools, including labels and label selectors, which can be leveraged to streamline cloud bursting processes. While Kubernetes best practices suggest assigning semantic meaning to labels before utilizing them [9], no standardized enforcement method currently exists. Our objective is to establish a structured approach within cloud bursting that ensures the association of semantic meaning with Kubernetes labels. Additionally, Kubernetes management does not fully address all security concerns related to data confidentiality and access control, which are crucial for cloud bursting [6]. While Kubernetes incorporates access management, it necessitates separate configurations that are disconnected from the logic of orchestrated functions. Furthermore, its existing access control mechanisms have constraints in handling complex authorization scenarios and exhibit policy limitations. These constraints pose challenges for achieving secure and comprehensive resource management within cloud bursting. To mitigate these issues, we introduce an architectural framework that enhances security in cloud bursting by integrating Kubernetes orchestration with Attribute-Based Encryption (ABE).

Our key contributions in this paper include:

1. Defining semantic meaning for key labels, transforming them into attributes that add context to cloud bursting configurations and improve label comprehension.
2. Incorporating ABE, deployed via a cloud service, to strengthen security through fine-grained policies that ensure data privacy, confidentiality, and access control. This ABE component integrates seamlessly within the Kubernetes environment, aligning with attribute logic and enhancing overall system security.
3. Introducing a unified management layer that streamlines configuration by managing all attributes holistically, including those used by Kubernetes and the ABE module. This unification simplifies administration, removes the need for separate configurations, and provides a more efficient experience.

In summary, we propose a secure cloud bursting framework that enhances both efficiency and security in resource management over traditional methods by integrating semantic labels, cryptographic technology, and a unified attribute-based configuration model. The remainder of this paper is structured as follows. Section II presents a review of related literature. Section III provides an overview of fundamental concepts. Our proposed methodology is outlined in Section IV. Section V details the results of our proof-of-concept implementation. Finally, Section VI concludes with our final observations and remarks.

II. LITERATURE SURVEY

Cloud computing has become essential for scalable resource management, with Kubernetes serving as a widely adopted tool for container orchestration. However, ensuring security in cloud bursting—where workloads shift between cloud environments—presents various challenges. Researchers have explored different solutions to address these concerns. Several studies have examined cloud bursting techniques, focusing on optimizing resource allocation while maintaining performance and cost efficiency. However, these approaches often overlook robust security mechanisms. Security risks such as unauthorized access, data leaks, and compliance issues remain critical challenges, prompting the exploration of Attribute-Based Access Control (ABAC) as a viable solution.

Kubernetes has been studied extensively for its efficiency in workload management across hybrid cloud setups. While its built-in security features help mitigate risks, ensuring strong authentication and policy enforcement in cloud-bursting scenarios is an ongoing research area. Some works propose integrating Attribute-Based Encryption (ABE) with Kubernetes to enhance data security, yet practical implementations remain limited. Although existing research contributes valuable insights into Kubernetes security and cloud bursting, a dedicated framework for managing security through attribute-based policies is still underdeveloped. This study aims to fill that gap by introducing an approach that strengthens access control in multi-cloud environments.

III. METHODOLOGY

To address the challenges of securely extending workloads from private to public cloud environments using Kubernetes, we propose a methodology that integrates Attribute-Based Encryption (ABE) with Kubernetes' native labelling system. This approach enhances data security and access control during the cloud bursting process.

Utilizing Kubernetes Labels for Resource Organization

Kubernetes employs labels—key-value pairs assigned to resources—to facilitate efficient organization and selection. In our framework, these labels are used to define attributes associated with specific workloads and data, enabling precise identification and management of resources.

Integrating Attribute-Based Encryption (ABE)

ABE is a cryptographic method that encrypts data based on a set of attributes, ensuring that only users possessing the required attributes can decrypt and access the information. By aligning ABE with Kubernetes labels, we establish a robust access control mechanism where data encryption corresponds to the attributes defined by these labels.

Secure Cloud Bursting Process

In our model, when a workload is designated for bursting to a public cloud, Kubernetes labels dictate the attributes associated with the involved data and resources. The data is encrypted using ABE according to policies derived from these labels. Upon reaching the public cloud environment, access to the data is restricted to users or services that meet the specified attribute criteria, thereby maintaining data confidentiality and integrity during the bursting process.

4. Implementation Steps

- Define Attributes: Establish clear attribute sets corresponding to access control requirements.
- Assign Labels: Apply appropriate labels to Kubernetes resources to reflect the defined attributes.
- Formulate Policies: Develop ABE policies that align with the labeling schema, specifying which attribute combinations grant access to encrypted data.
- Encrypt and Deploy: Encrypt data using the formulated ABE policies before initiating cloud bursting, ensuring that only authorized entities can decrypt and access the data in the public cloud environment.

This methodology offers a scalable and flexible solution for secure cloud bursting in Kubernetes environments, effectively combining Kubernetes' resource management capabilities with the robust access control provided by ABE

IV. RESULTS AND DISCUSSIONS

It enhance the coherence of your research paper by directly linking findings to their interpretations. This integrated approach allows for immediate analysis of each result, facilitating a seamless flow from data presentation to contextual understanding. To implement this effectively, consider organizing the section around key themes or research questions. For each theme, present the relevant findings succinctly, followed by an interpretation that connects these results to existing literature and theoretical frameworks. This method not only highlights the significance of your findings but also addresses any unexpected outcomes and acknowledges the limitations of your study. By weaving results and discussion together, you create a cohesive narrative that guides the reader through your research journey, emphasizing the contribution of your work to the broader field.

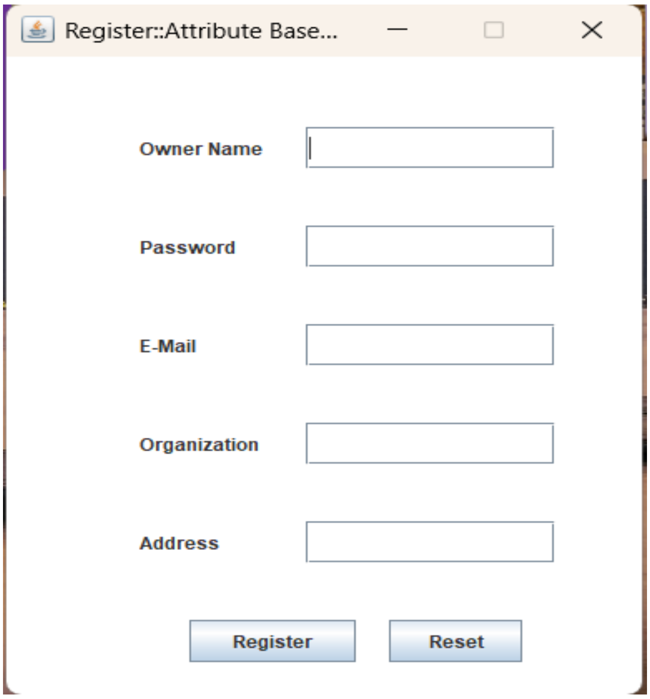


Fig 1:Registration page

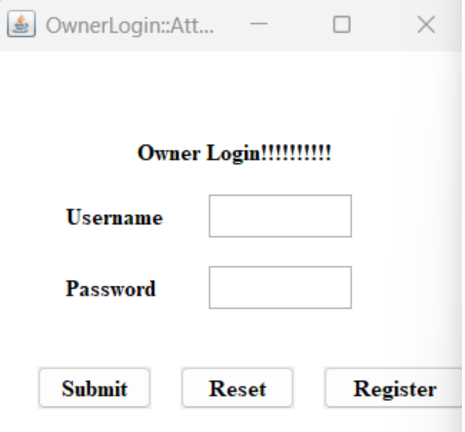


Fig 2: Login page

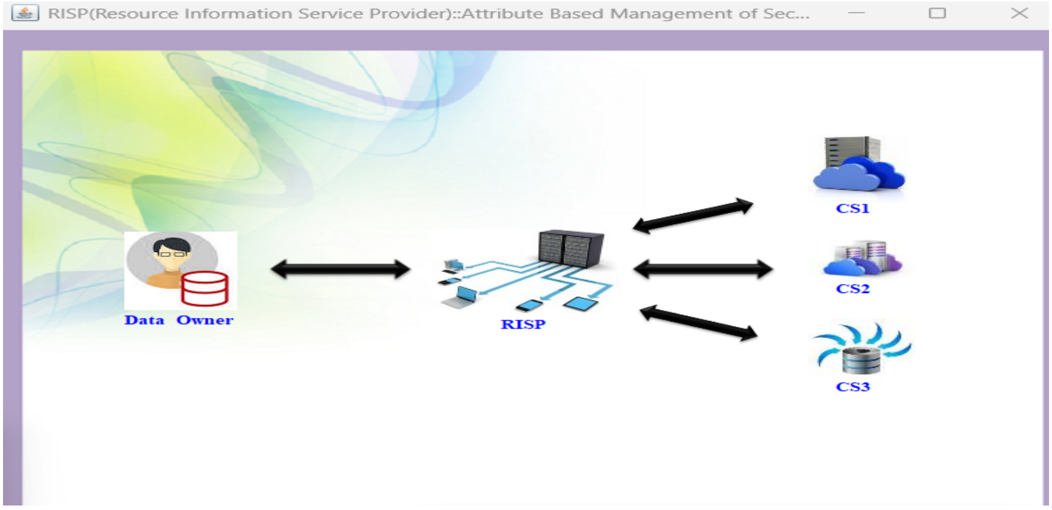

RISP(Resource Information Service Provider)::Attribute Based Management of Sec...
Data Owner
RISP
CS1
CS2
CS3

Fig 3: RISP(Resource Information Service Provider)

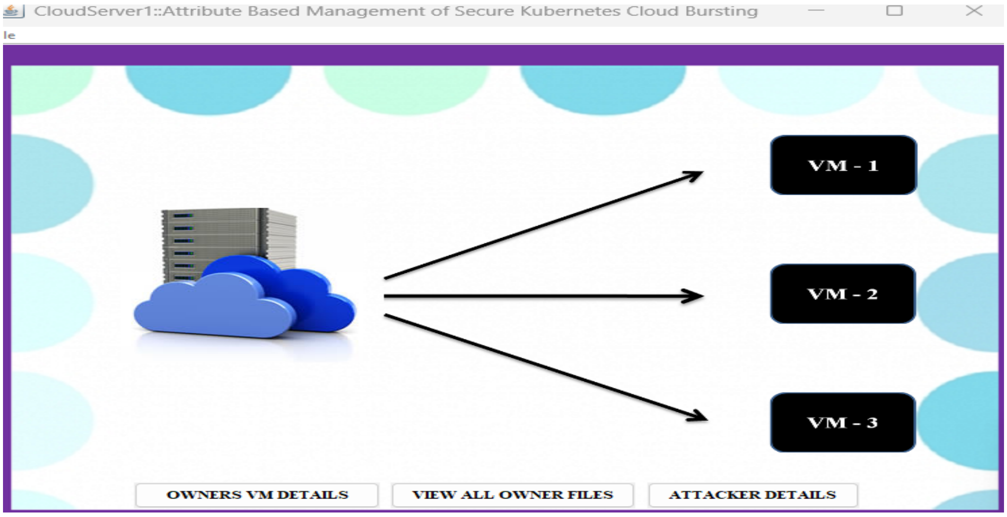

CloudServer1::Attribute Based Management of Secure Kubernetes Cloud Bursting
le
VM - 1
VM - 2
VM - 3
OWNERS VM DETAILS
VIEW ALL OWNER FILES
ATTACKER DETAILS

Fig 4: Cloud Server

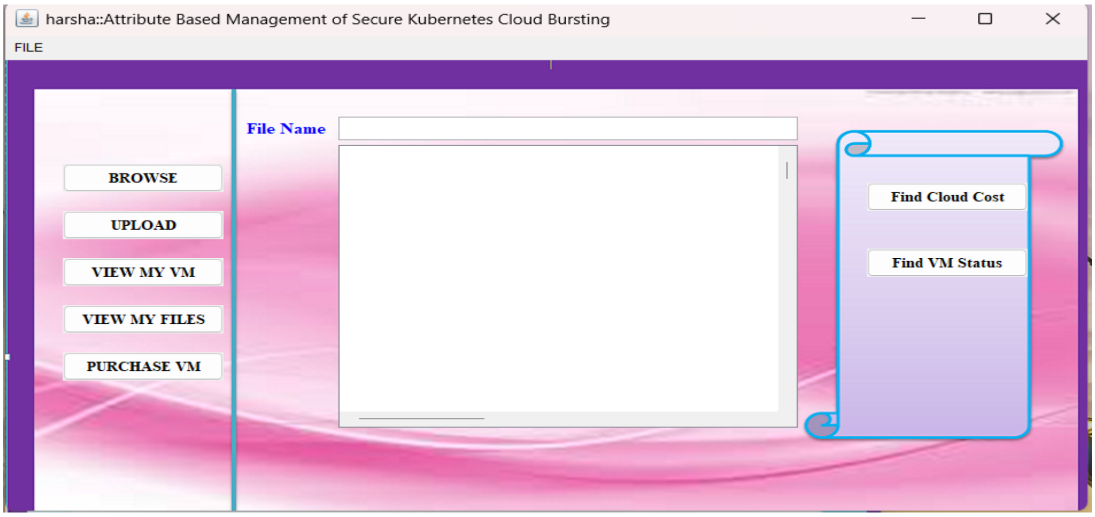
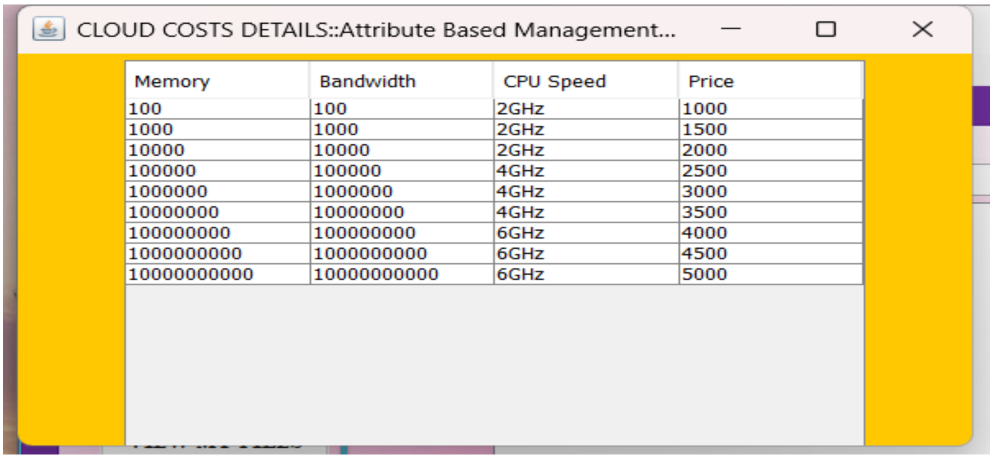
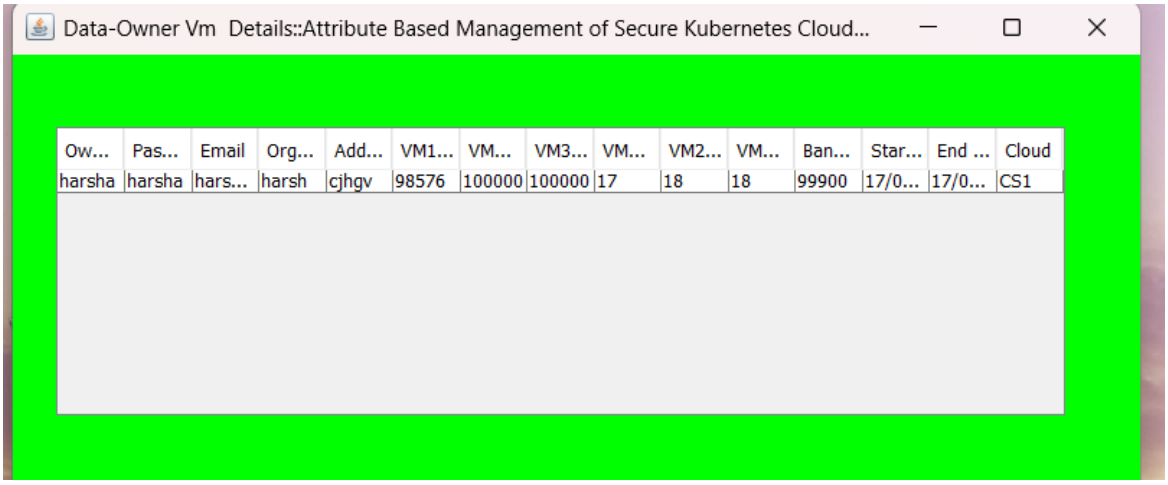


Fig 5: Operational unit


CLOUD COSTS DETAILS::Attribute Based Management...

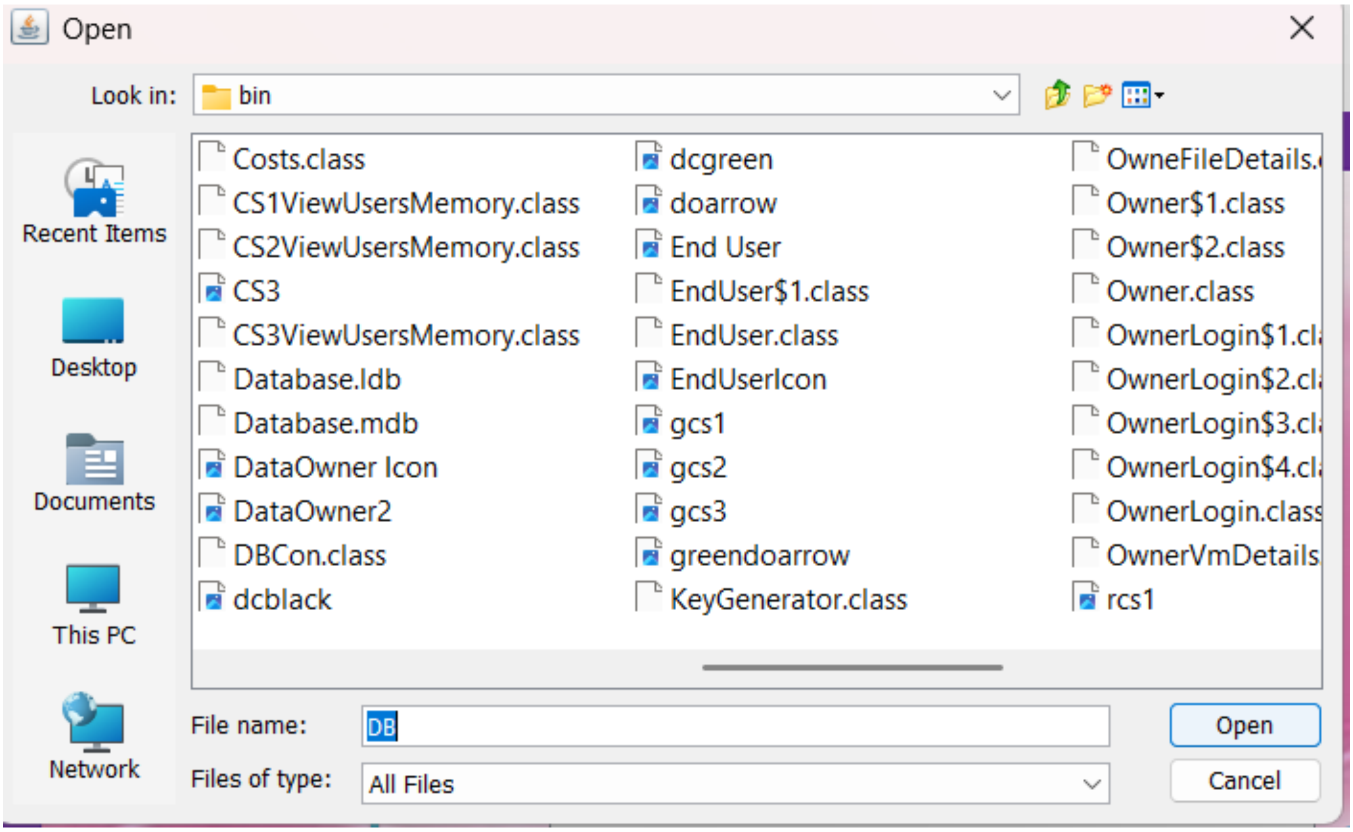
Memory	Bandwidth	CPU Speed	Price
100	100	2GHz	1000
1000	1000	2GHz	1500
10000	10000	2GHz	2000
100000	100000	4GHz	2500
1000000	1000000	4GHz	3000
10000000	10000000	4GHz	3500
100000000	100000000	6GHz	4000
1000000000	1000000000	6GHz	4500
10000000000	10000000000	6GHz	5000

Fig 6: Purchase of VM Based on Price, Bandwidth, CPU Speed and Memory Size


Data-Owner Vm Details::Attribute Based Management of Secure Kubernetes Cloud...

Ow...	Pas...	Email	Org...	Add...	VM1...	VM...	VM3...	VM...	VM2...	VM...	Ban...	Star...	End ...	Cloud
harsha	harsha	hars...	harsh	cjhgv	98576	100000	100000	17	18	18	99900	17/0...	17/0...	CS1

Fig 7:data owner Details



Open

Look in: bin

Recent Items
Desktop
Documents
This PC
Network

Costs.class
CS1ViewUsersMemory.class
CS2ViewUsersMemory.class
CS3
CS3ViewUsersMemory.class
Database.ldb
Database.mdb
DataOwner Icon
DataOwner2
DBCon.class
dcblack
dcgreen
doarrow
End User
EndUser$1.class
EndUser.class
EndUserIcon
gcs1
gcs2
gcs3
greendoarrow
KeyGenerator.class
OwneFileDetails.
Owner$1.class
Owner$2.class
Owner.class
OwnerLogin$1.cl
OwnerLogin$2.cl
OwnerLogin$3.cl
OwnerLogin$4.cl
OwnerLogin.class
OwnerVmDetails
rcs1

File name: DB

Files of type: All Files

Open
Cancel

Fig 8: File Storing Process

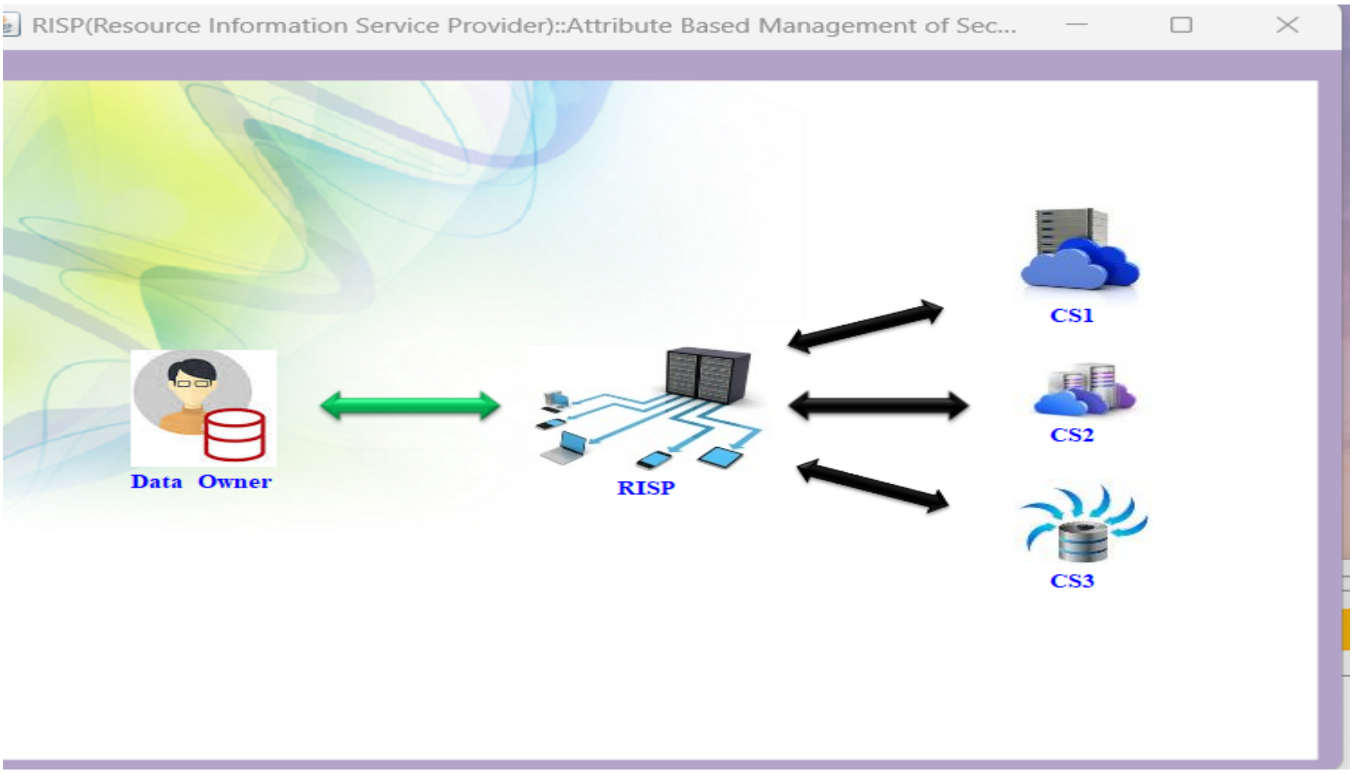

RISP(Resource Information Service Provider)::Attribute Based Management of Sec...
Data Owner
RISP
CS1
CS2
CS3

Fig 9: Storing of File in Cloud-Server

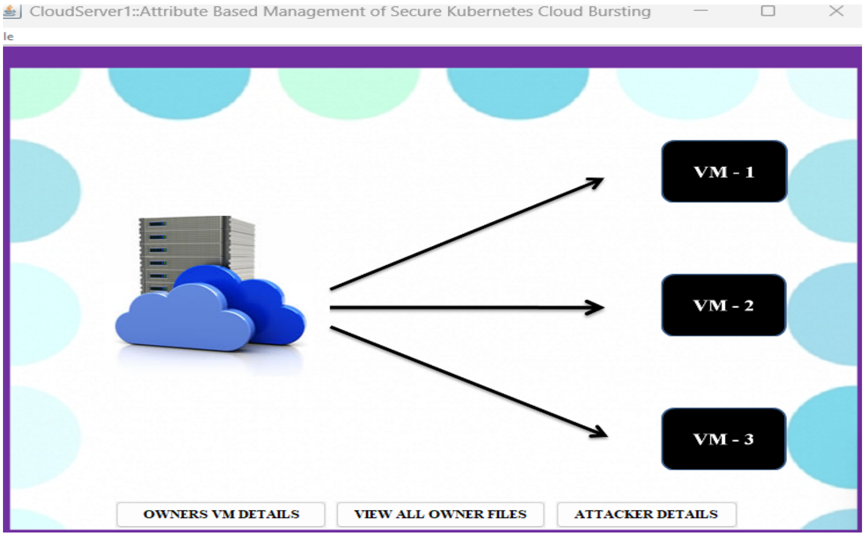
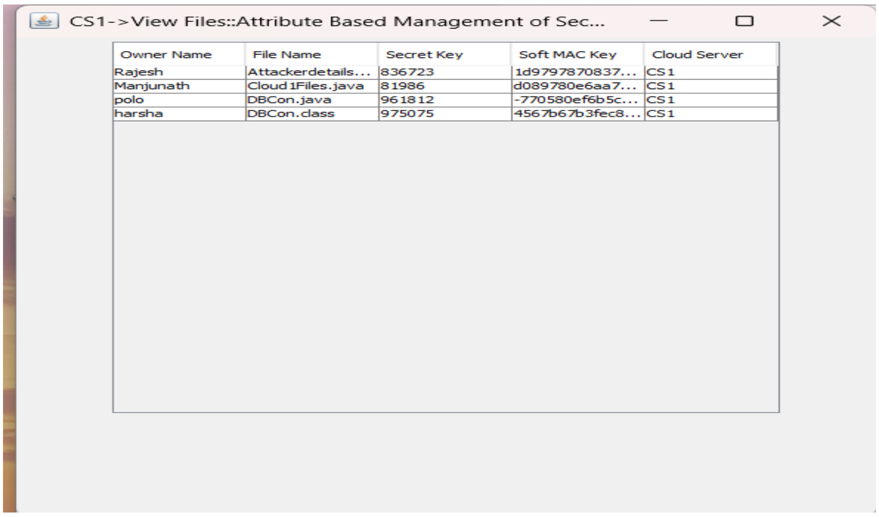

CloudServer1::Attribute Based Management of Secure Kubernetes Cloud Bursting
VM - 1
VM - 2
VM - 3
OWNERS VM DETAILS
VIEW ALL OWNER FILES
ATTACKER DETAILS

Fig 10: Cloud-Server Storing Process after checking the Security From RISP



Owner Name	File Name	Secret Key	Soft MAC Key	Cloud Server
Rajesh	Attackerdetails...	836723	1d9797870837...	CS1
Manjunath	Cloud1Files.java	81986	d089780e6aa7...	CS1
polo	DBCon.java	961812	-770580ef6b5c...	CS1
harsha	DBCon.class	975075	4567b67b3fec8...	CS1

Fig 11: Stored Details or Owner Details

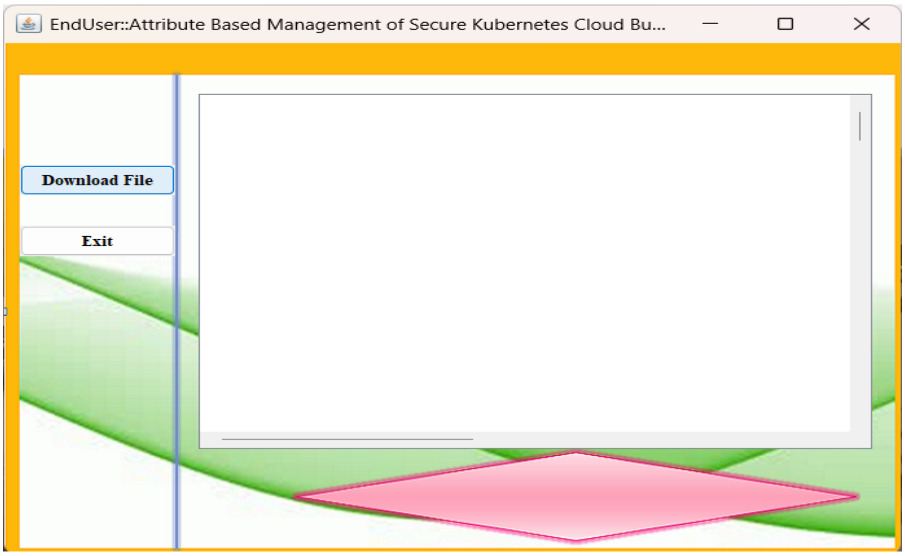
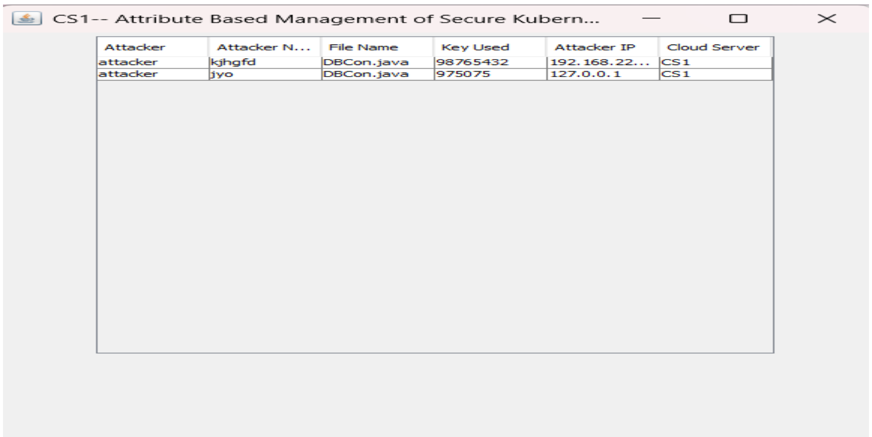

EndUser::Attribute Based Management of Secure Kubernetes Cloud Bu...
Download File
Exit

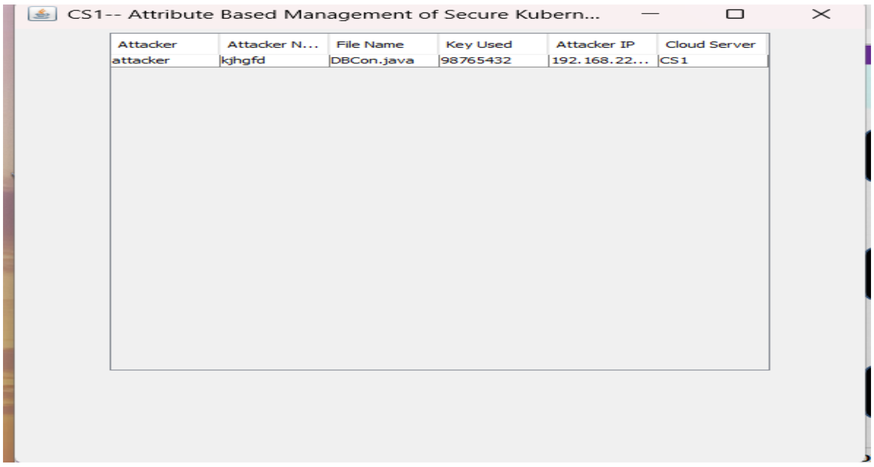
Fig 12: End-User Process



CS1-- Attribute Based Management of Secure Kubern...

Attacker	Attacker N...	File Name	Key Used	Attacker IP	Cloud Server
attacker	kjhgfd	DBCon.java	98765432	192.168.22...	CS1
attacker	jyo	DBCon.java	975075	127.0.0.1	CS1

Fig 13:Authorized Secutre Kubernets



CS1-- Attribute Based Management of Secure Kubern...

Attacker	Attacker N...	File Name	Key Used	Attacker IP	Cloud Server
attacker	kjhgfd	DBCon.java	98765432	192.168.22...	CS1

Fig:14 After Unblocking the Authorized User

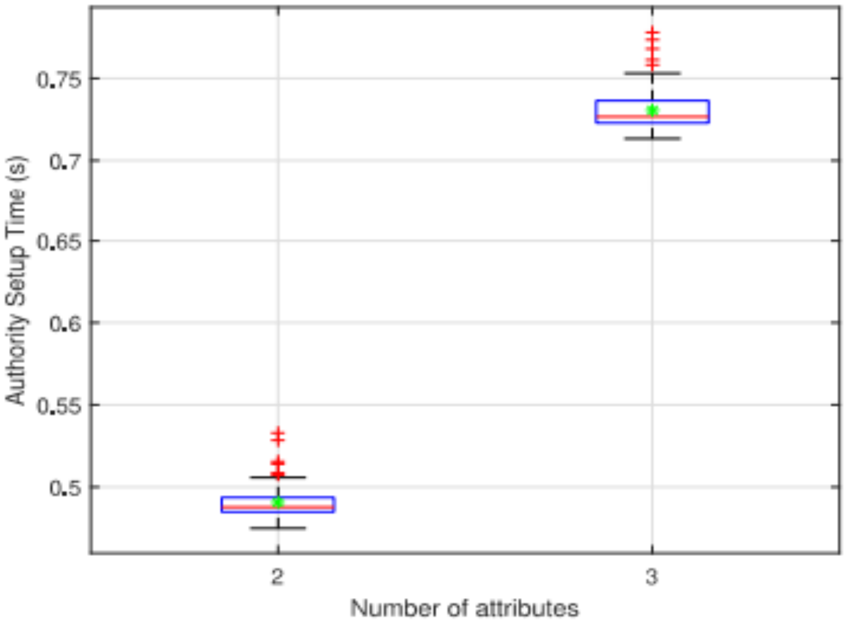


Fig 15:Blocks Plot Of Setup Authority

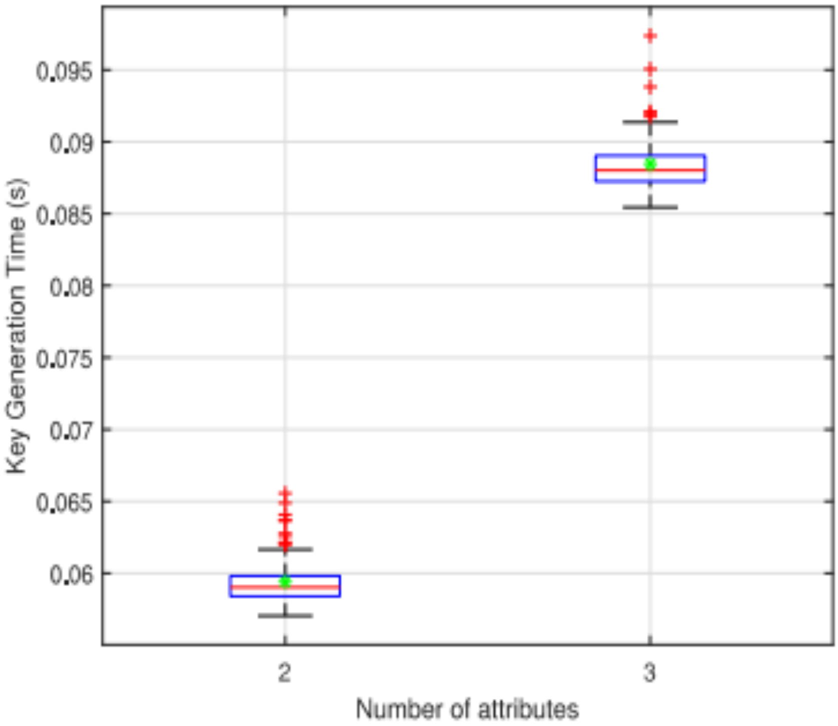


Fig: 16 Blocks Plot Of Setup Authority

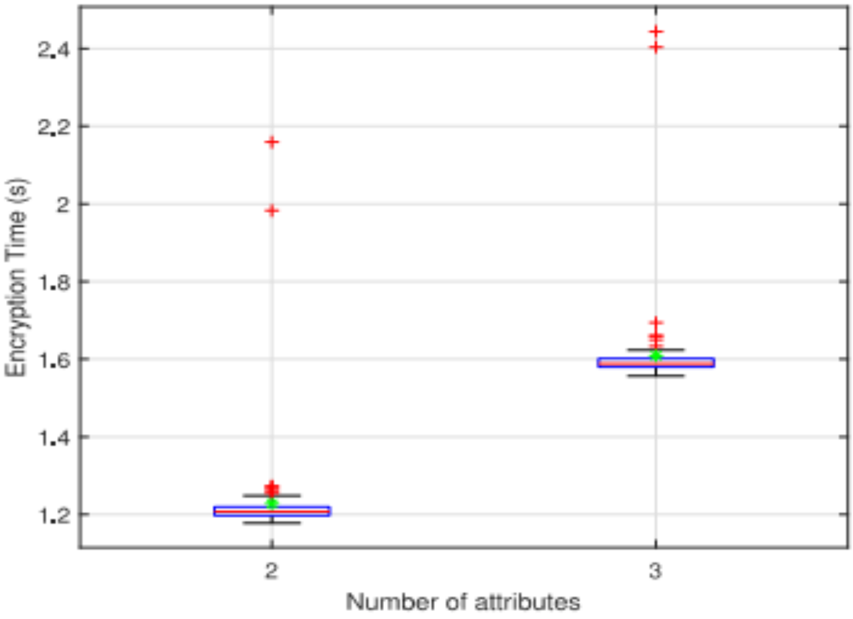


Fig: 17 Box plot of the encryption time

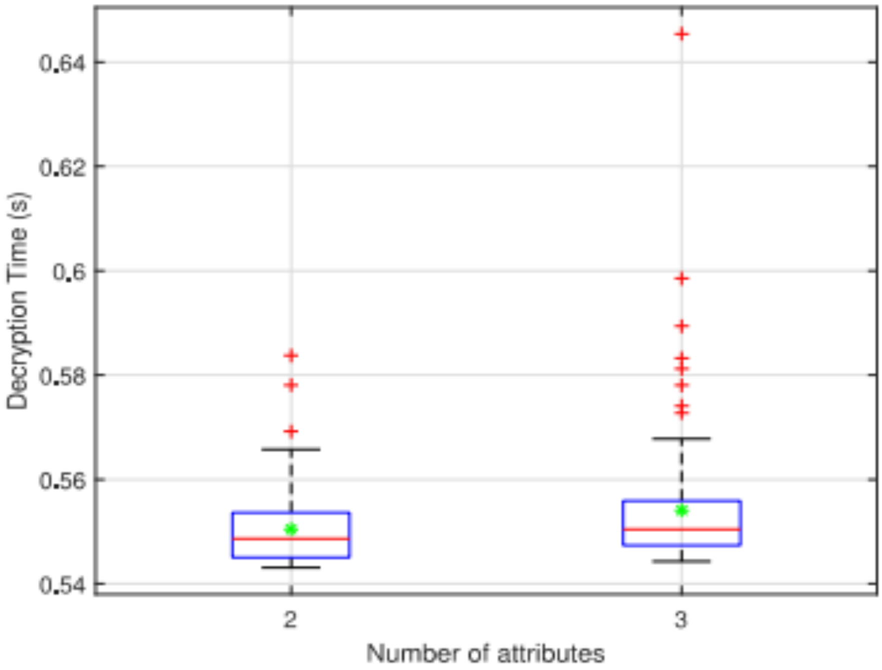


Fig 18: Box plot of the decryption time

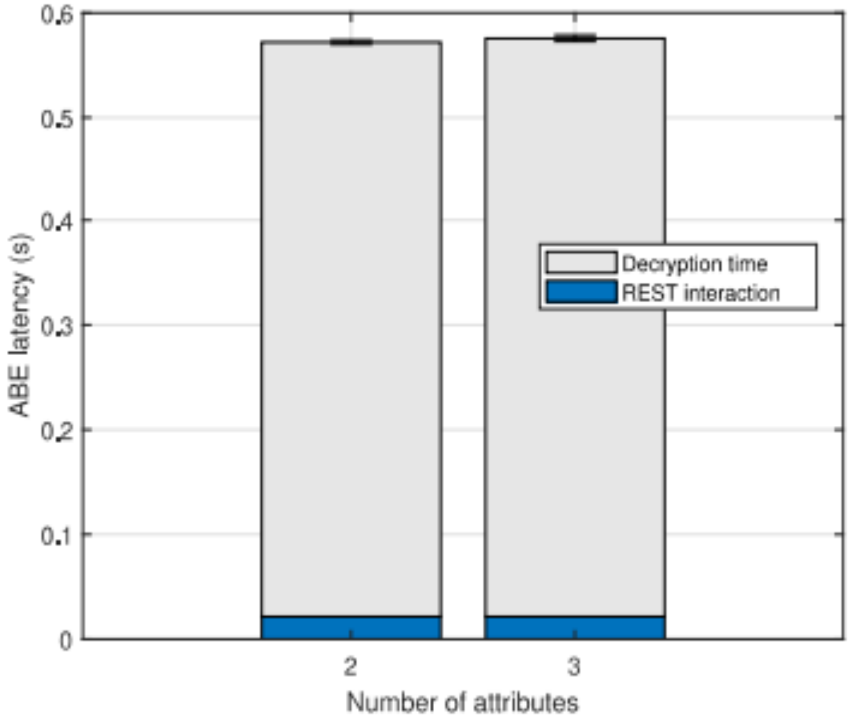


Fig 19: Latency associated with ABE function

V. CONCLUSION AND FUTURE WORK

This study's contributions and outline areas where additional research could be beneficial. The conclusion provides a succinct summary of the research, reiterating the main objectives and methodologies employed, highlighting key findings and their implications, and emphasizing the significance of the study. Importantly, the conclusion should not introduce new information but rather synthesize existing content to reinforce the study's contributions. The future scope, often integrated within the conclusion, outlines potential directions for subsequent research by identifying unanswered questions, limitations of the current study, and areas that warrant deeper exploration. By proposing future research avenues, authors can guide the academic community toward addressing gaps and building upon the existing work. Effectively combining the conclusion and future scope provides a comprehensive closure to the research paper, reinforcing the study's value and inspiring continued scholarly inquiry.

REFERENCES

1. Amazon Web Services, Inc. (n.d.). *Amazon Elastic Kubernetes Service (Amazon EKS)*. Retrieved June 8, 2023, from https://aws.amazon.com/eks/?nc1=h_ls
2. Google. (n.d.). *Google Kubernetes Engine*. Retrieved June 8, 2023, from https://cloud.google.com/kubernetes-engine
3. International Business Machines Corporation. (n.d.). *IBM Kubernetes Service*. Retrieved June 8, 2023, from https://www.ibm.com/cloud/kubernetes-service
4. Docs.rs. (n.d.). *Module aw11 rabe*. Retrieved January 5, 2024, from https://docs.rs/rabe/latest/rabe/schemes/aw11/index.html
5. Oracle Computing Software Company. (n.d.). *Oracle Cloud Native Services—Container Engine for Kubernetes*. Retrieved June 8, 2023, from https://www.oracle.com/cloud/cloud-native/container-engine-kubernetes/
6. Kubernetes.io. (2019, March). *Security best practices for Kubernetes deployment*. Retrieved from https://kubernetes.io/blog/2016/08/security-best-practices-kubernetes-deployment/
7. Google. (2023, December). *Anthos*. Retrieved from https://cloud.google.com/anthos
8. Palo Alto Networks, Inc. (2023, December). *Cloud Native Application Protection Platform*. Retrieved from https://www.paloaltonetworks.com/prisma/cloud/cloud-native-application-protection-platform
9. Kubernetes.io. (2023, July). *Configuration best practices: Using labels*. Retrieved from https://kubernetes.io/docs/concepts/configuration/overview/#using-labels
10. CloudBees Software Company. (2023, December). *Configuring CloudBees Build Acceleration for Agent Cloud Bursting*. Retrieved from https://docs.cloudbees.com/docs/cloudbees-build-acceleration/latest/configuration-guide/config-accelerator-agents-for-cloud-burst
11. Periasamy, K., Periasamy, S., Velayutham, S., Zhang, Z., Ahmed, S. T., & Jayapalan, A. (2022). A proactive model to predict osteoporosis: An artificial immune system approach. *Expert Systems*, *39*(4), e12708.
12. Ahmed, S. T., Basha, S. M., Ramachandran, M., Daneshmand, M., & Gandomi, A. H. (2023). An edge-AI-enabled autonomous connected ambulance-route resource recommendation protocol (ACA-R3) for eHealth in smart cities. *IEEE Internet of Things Journal*, *10*(13), 11497-11506.
13. Kumar, S. S., Ahmed, S. T., Sandeep, S., Madheswaran, M., & Basha, S. M. (2022). Unstructured Oncological Image Cluster Identification Using Improved Unsupervised Clustering Techniques. *Computers, Materials & Continua*, *72*(1).
14. Pasha, A., Ahmed, S. T., Painam, R. K., Mathivanan, S. K., Mallik, S., & Qin, H. (2024). Leveraging ANFIS with Adam and PSO optimizers for Parkinson's disease. *Heliyon*, *10*(9).
15. Sreedhar, K. S., Ahmed, S. T., & Sreejesh, G. (2022, June). An Improved Technique to Identify Fake News on Social Media Network using Supervised Machine Learning Concepts. In *2022 IEEE World Conference on Applied Intelligence and Computing (AIC)* (pp. 652-658). IEEE.
16. Ahmed, S. T., Fathima, A. S., Nishabai, M., & Sophia, S. (2024). Medical ChatBot assistance for primary clinical guidance using machine learning techniques. *Procedia Computer Science*, *233*, 279-287.

17. GitHub. (2023, December). *Kubernetes autoscaler*. Retrieved from https://github.com/kubernetes/autoscaler
18. Pecoraro, F., Clemente, F., & Luzi, D. (2020). The efficiency in the ordinary hospital bed management in Italy: An in-depth analysis of intensive care unit in the areas affected by COVID-19 before the outbreak. *PLOS ONE, 15*(9), e0239249.
19. Hassan, M., Tuckman, H. P., Patrick, R. H., Kountz, D. S., & Kohn, J. L. (2010). Hospital length of stay and probability of acquiring infection. *International Journal of Pharmaceutical and Healthcare Marketing, 4*(4), 324–338.
20. Microsoft Corporation. (2018, August 31). *Securing Kubernetes workloads in hybrid settings with Aporeto*. Retrieved from https://cloudblogs.microsoft.com/opensource/2018/08/31/securing-kubernetes-workloads-hybrid-cloud-aporeto/
21. Virtual Kubelet. (2023, December). *Virtual kubelet*. Retrieved from https://virtualkubelet.io/
22. Ahuja, R., & Mohanty, S. K. (2020). A scalable attribute-based access control scheme with flexible delegation cum sharing of access privileges for cloud storage. *IEEE Transactions on Cloud Computing, 8*(1), 32–44.
23. Ameer, S., Benson, J., & Sandhu, R. (2022). An attribute-based approach toward a secured smart-home IoT access control and a comparison with a role-based approach. *Information, 13*(2), 60.
24. Balouek-Thomert, D., Renart, E. G., Zamani, A. R., Simonet, A., & Parashar, M. (2019). Towards a computing continuum: Enabling edge-to-cloud integration for data-driven workflows. *International Journal of High Performance Computing Applications, 33*(6), 1159–1174.
25. Baresi, L., Mendonça, D. F., Garriga, M., Guinea, S., & Quattrocchi, G. (2019). A unified model for the mobile-edge-cloud continuum. *ACM Transactions on Internet Technology, 19*(2), 1–21.
26. Bellare, M., Waters, B., & Yilek, S. (2010). Identity-based encryption secure against selective opening attack. *Cryptology ePrint Archive*, Report 2010/159. https://eprint.iacr.org/2010/159
27. Benedetti, P., Femminella, M., Reali, G., & Steenhaut, K. (2022). Reinforcement learning applicability for resource-based auto scaling in serverless edge applications. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)* (pp. 674–679).
28. Benitez, S. (2024, January 5). *Meet Rocket*. Retrieved from https://rocket.rs/
29. Bera, S., Prasad, S., Sreenivasa Rao, Y., Das, A. K., & Park, Y. (2023). Designing attribute-based verifiable data storage and retrieval scheme in cloud computing environment. *Journal of Information Security and Applications, 75*, 103482.
30. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *Proceedings of the IEEE Symposium on Security and Privacy (SP'07)* (pp. 321–334).
31. Böhm, S., & Wirtz, G. (2022). Cloud-edge orchestration for smart cities: A review of Kubernetes-based orchestration architectures. *EAI Endorsed Transactions on Smart Cities, 6*(18), e2.
32. Boneh, D. (2007). Bilinear groups of composite order. In *Proceedings of the 1st International Conference on Pairing-Based Cryptography* (p. 1).
33. Boneh, D., Goh, E., & Nissim, K. (2005). Evaluating 2-DNF formulas on ciphertexts. In *Proceedings of the Theory of Cryptography Conference* (pp. 325–341).
34. Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2016). Borg, Omega, and Kubernetes. *Communications of the ACM, 59*(5), 50–57.