International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

An Efficient Tenant LED Virtual Machine Scheduling Using Machine Learning

Mohanram M[1], Raguganapathy K C[2], Vignesh D[3], Sakthivel M[4]
[1,2,3] UG – Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Tamil Nadu
[4] Assistant Professor, Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Tamil Nadu
Emails: *mohanramm927@gmail.com[1], raguganapathy7@gmail.com[2], vv028964@gmail.com[3], sakthivelmcs@esec.ac.in[4]*

Abstract
Cloud data centers often face the dual challenge of maintaining workload balance and maximizing resource utilization due to the highly dynamic and heterogeneous nature of hosted applications. To address these limitations, this study presents a hybrid VM scheduling framework that combines Bayes-based clustering with Particle Swarm Optimization (PSO). The model first applies clustering to group tasks based on workload similarities and resource demand characteristics, while Bayesian probability reasoning is employed to refine host selection and minimize overload risk. Subsequently, PSO is utilized to search iteratively for an optimal scheduling solution by employing a fitness function that considers response time, energy efficiency, and resource utilization. A matrix-based allocation model is introduced to represent scheduling states and guide final deployment decisions in each iteration. Experimental outcomes show that the proposed approach enhances load balancing, reduces execution delays, and improves system scalability, thereby ensuring more efficient and adaptive performance in multi-tenant cloud environments.
Keywords: *Virtual Machine Scheduling, Load Balancing, Resource Allocation*

1. Introduction
Cloud computing has become a cornerstone of modern IT infrastructure, offering on-demand, scalable, and cost-effective access to computing resources. With the rapid adoption of cloud services, particularly in multi-tenant environments, cloud data centers face increasing challenges in ensuring optimal resource allocation and maintaining balanced system performance. Traditional scheduling approaches often fail to address the heterogeneity and dynamism of workloads, resulting in inefficient utilization, higher response times, and increased energy consumption. To mitigate these issues, this work proposes a hybrid scheduling framework that leverages Bayes-based clustering and Particle Swarm Optimization (PSO). Clustering groups virtual machines with similar workload patterns, while Bayesian analysis improves decision-making by evaluating the probability of overload. The PSO algorithm then refines the scheduling process through iterative optimization. Additionally, a matrix-based allocation model is employed to provide accurate state representation of resource assignments, enabling consistent and adaptive decision-making. This integrated approach offers a robust solution to dynamic VM scheduling, providing improved scalability, reliability, and energy efficiency compared to conventional methods. The cloud offers several essential services for day-to-day use, including applications, storage, processing in high performance systems, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Function as a Service (FaaS), Container as a Service (CaaS), only to mention [1] some. All of these services make it possible to increase responsiveness in a wide range of areas, with applications that are richer in functionality. However, centralization on the cloud has its drawbacks. One is latency, which is the time that elapses between the moment a request is made and the moment a response is received. Centralization can also raise some security and privacy concerns, The associate editor coordinating the review of this manuscript and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

approving it for publication was Nurul I. Sarkar. increasing vulnerability, in addition to being a single point of failure, and having lack of transparency and compliance challenges. Other drawbacks include decontextualization of data, bandwidth contracts, and reduced overall performance. The security for the cloud infrastructure has always been a persistent issue as most of the consumers and practitioners do not have clear understanding about the security factors and implementation details. [2] To some extent, the service providers have made a closed loop about the knowledge of cloud security inside the organizations and sometimes only to the selective groups. This makes the deployment of the cloud-based security protocols even harder for the researchers. Nonetheless, the recent research outcomes by various research attempts are opening the closed loops of the knowledge and exploring the possibilities of the deployment of novel and higher performing security protocols.[3] As education expands, focus shifts from teacher-centric to student-centric resource demands. Growing student numbers and broader education needs highlight the need for innovative learning environments with tailored resources [4]. However, open educational resources (OERs) face challenges in monitoring progress, with educators hesitant due to control concerns [5]. OERs may lack accuracy, completeness, and customization options. OpenStack and Caph offer open-source solutions for large-scale virtualization, supporting petabytes of data, unlimited scale, and configurable networking [6]. Ideal for education and government, they reduce costs and optimize resource utilization. Cloud providers offer software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) services Bhatia et al. [7] have provided a design of a private cloud for higher education and proof-of-concept implementation methodology for the OpenStack platform and analyzed the advantages and disadvantages of a private cloud.

Unlimited cloud storage and data outsourcing services provide data owners and enterprises with capacities for storing and processing a massive amount [8] of data. These high-quality services enable easy accessibility, high scalability, and availability [9]. Despite all the advantages, serious concerns about the data security and confidentiality in such a cloud environment have been raised. To preserve data confidentiality, many techniques support searching on the outsourced data stored in the cloud environment. However, these techniques cannot regulate access to specific stored data record or enforce access policies [10].

2. Literature Review

According to a work by XIN LU [1] et al., the information flow barrier between tenants in a shared virtual machine is hazy and challenging to determine in a cloud environment because of the extensive sharing of the top application instance and the underlying virtual machine resources. Furthermore, there is insufficient protection of the movement of tenant information between processes, which leads to the disclosure of renters' private information. As a result, a virtual border recognition-based dynamic control mechanism for the flow of sensitive tenant information is suggested. Tenant behavior and operation logs are analyses to create behavior feature vectors, and a dynamic spiking neural network-based technique for automatically recognizing the virtual boundaries of tenants is created. When the application service demand fluctuates, this technique may identify the tenant virtual security boundary dynamically. Additionally, a [11] dynamic control approach of sensitive information flow is constructed by combining the concepts of centralized and decentralized information flow control. The lattice structure is used to formally define the security label, and the rules for tenant label encryption and declassification are created, along with the control rules for the flow of information among tenants. Consequently, information flow within and outside the tenant virtual boundary can be independently, dynamically, and securely controlled. The final section provides a detailed architecture of a dynamic security control application system for the flow of sensitive data for cloud tenants. In this study, Nadya El Moussaid [2] et al. have suggested the reality that customers connect to cloud computing and storage services from various devices using specific authentication methods. Credential information, such the login and password, on the other hand, is most likely to be used intrusively without being noticed.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

Therefore, in order to ensure the security of tenants and organizations, the cloud computing security policy must handle both access control and virus analysis. This paper's primary goal is to improve security attributes by dynamically forming them through entity behavior analysis and linking them to a security class and trust level. In order to ensure the security properties—confidentiality, integrity, and availability (CIA)—we have put in place a security policy, the primary function of which is to provide a template. The outcomes of our tests demonstrate the effectiveness of our methodology in terms of categorization and the up to 95% real-time detection rate. These days, [12] one of the most popular research subjects is cloud computing security. Actually, all multi-tenant levels—IaaS, PaaS, and SaaS—must be considered in an efficient security policy and information flow control (IFC) (Caron et al., 2014; Merino et al., 2012; Vaquero et al., 2008). It is difficult for cloud computing security providers to keep their services safe, and it is also difficult for tenants to move and store sensitive data from their own secure environment to the cloud. The former mixes disparate software and services, [13] which may lead to a number of vulnerabilities that the attackers can then take advantage of. We have provided an overview of the problems and threats that the three tiers of cloud computing confront in this study. Next, we have referenced various access control models and IFC that dynamically monitor the authorization of entities. We have suggested the behavior model to formulate the security properties and IFC side by side with the CWACM to improve the separation property in order to overcome these cloud security issues. In this research, Katrina L. Kalantar [3] et al. have suggested Without the need of pathogen-specific chemicals, culturing, or prior knowledge of the microbial landscape, metagenomic next-generation sequencing (mNGS) has made it possible to quickly and objectively detect and identify microorganisms. To accurately ascertain the microbiological makeup of a sample, mNGS data analysis necessitates a number of computationally demanding processing stages. Current mNGS data processing solutions usually demand access to local server-class hardware resources and bioinformatics skills. This is a challenge for many research labs, [14] particularly those with low resources. We introduce IDseq (https://idseq.net), an open source cloud-based metagenomics pipeline and service for worldwide disease monitoring and detection. After completing host and quality filtration on raw mNGS data, the IDseq Portal runs an assembly-based alignment procedure that assigns reads and contigs to taxonomic categories. To make it easier [15] to evaluate data and generate hypotheses, the taxonomic relative abundances are presented and displayed in an intuitive web application. Additionally, IDseq offers statistics that are essential for data interpretation, including automatic internal spike-in control detection and environmental background model building. [16] The specific goal of ID seq's design was to identify new diseases. In this study, Hannes Salin [4] et al. have suggested This thesis examines bilinear maps and their application in contemporary cryptography, namely the theoretical underpinnings of pairing-based cryptography and the underlying assumptions of mathematical hardness. Elliptic curves, algebraic structures, and divisor theory serve as the foundation for the theory, which allows for the definition of explicit pairing constructs. As an example, we consider the more popular Weil pairing in more detail. Additionally, we include numerical examples of how pairing-friendly curves are created and how various cryptographic algorithms operate, as well as an explanation of pairings in practice. [17] There is a lot of overlap between computer science and mathematics in the complicated and wide field of cryptography study. Based on mathematical foundations, secure protocols are essentially safe across a range of theoretical security models and complexity levels. Pairing-based cryptography, which is structurally defined over elliptic curves and bilinear mappings, is a new subfield of such safe protocols. These kinds of pairing [18] structures have sparked a lot of study and discoveries in various cryptography subfields, including identity-based encryption and signature schemes. In addition, Boneh's seminal publication, which gave rise to numerous novel methods, further increased interest in pairing-based cryptography research. Today, [19 elliptic curves are widely employed in many real-

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

world applications and have been used in encryption for decades. However, despite the fact that there are currently very few real-world applications, pairing-based schemes which are essentially extensions of traditional elliptic curve cryptography seem to be expanding more quickly. In this study, Jinguang Han [5] et al. presented information flow control (IFC) mechanisms to govern the flow of information. Access control encryption (ACE), which supports both the no write-down and no read-up rules, was proposed as a way to improve IFC. However, there are still two problems: [20] There was no consideration of (1) how to decide whether to approve or reject a communication request; and (2) the cost of commutation increases linearly with the number of recipients. The attribute-based system (ABS) has the ability to establish fine-grained access controls and one-to-many communication. This study [21] proposes a new IFC method that combines ABS and ACE. Our plan offers the following advantages: Weak attribute privacy is achieved; fine-grained access policies on encrypted data are supported; the communication cost is linear with the number of required attributes and is independent of the number of receivers; IFC policies are defined over a universe set of attributes; and the computation cost to decide whether a communication request should be permitted or denied is constant rather than linear with the number of required attributes or receivers. [22] It is the only IFC system that uses attributes to enforce it, as far as we know. Users of cloud computing can exchange their data anywhere, at any time, across a network. Numerous pieces of evidence, [23] such as data theft and release, demonstrate the need to protect data confidentiality. [24] Symmetric encryption, identity-based encryption (IBE), attribute-based encryption (ABE), searchable encryption, functional encryption (FE), fully homomorphic encryption (FHE), and other encryption systems with unique characteristics [25] have all been proposed to safeguard the secrecy of data.

3. Existing System

Recent advancements such as 5G, Internet of Things (IoT), augmented reality, cloud gaming, and mission-critical services have expanded the range and demand for cloud-based applications. Although these technologies improve service accessibility and responsiveness, they also introduce new challenges, including congestion, bandwidth limitations, and difficulty in meeting Service Level Agreements (SLAs). To alleviate these issues, Multi-access Edge Computing (MEC) has emerged as a promising solution by bringing computational resources closer to end users, thereby reducing latency. However, the dynamic and mobile nature of MEC environments demands adaptive and automated service delivery mechanisms. Tools like Infrastructure as Code (IaC) have been introduced to automate resource deployment and management, but challenges remain in achieving optimal policy enforcement and effective workload distribution. Research in this area continues to explore more intelligent scheduling and automation techniques to ensure reliable performance under dynamic service demands.

4. Proposed System

The proposed system presents a hybrid framework for VM load scheduling in multi-tenant cloud environments, integrating Bayes-based clustering with Particle Swarm Optimization (PSO). The system uses a heuristic-driven strategy to determine the most suitable physical hosts for workload deployment, aiming to achieve efficient load balancing and long-term stability. Initially, clustering groups tasks according to workload similarities and resource needs, reducing scheduling complexity. Bayesian probability models are then applied to refine host selection, lowering the chances of overload and underutilization. PSO is employed to optimize scheduling iteratively, using a fitness function that evaluates performance indicators such as response time, energy usage, and resource utilization. To ensure accuracy, a matrix-based allocation model is used to represent scheduling states and determine final deployment vectors in each scheduling cycle. This combination delivers an adaptable, scalable, and reliable system capable of efficiently managing dynamic and heterogeneous workloads in cloud data centers.

4.1.Task and Resource Acquisition

This module is responsible for collecting workload requests from users and monitoring available computing resources in real time. Parameters such as

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

CPU demand, memory usage, bandwidth, and storage are recorded along with the current load on physical hosts. This provides accurate input for the clustering and scheduling processes.

4.2.Clustering and Bayesian Probability Analysis

Virtual machines are grouped into clusters according to workload similarity and resource requirements. Clustering reduces scheduling complexity, while Bayesian probability analysis evaluates the likelihood of resource overload or underutilization, ensuring more informed host allocation and risk minimization.

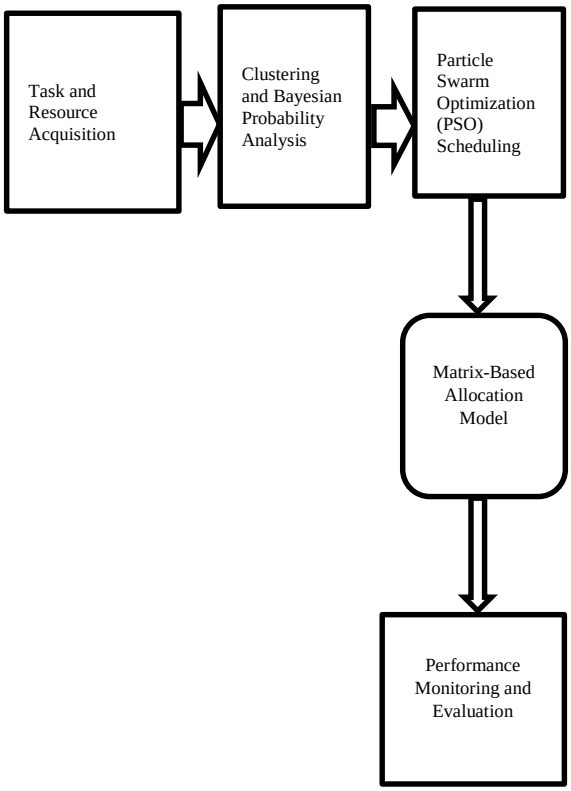

Figure 1 System Flow Diagram

4.3.Particle Swarm Optimization (PSO) Scheduling

The PSO algorithm is applied to find the most suitable VM-to-host assignments. Each candidate solution (particle) updates its position based on local and global best experiences. The fitness function considers factors such as response time, resource utilization, and energy consumption, guiding the system toward optimal scheduling outcomes.

4.4.Matrix-Based Allocation Model

This module structures and records the state of VM-to-host assignments in a matrix format. It helps track allocation history, prevents conflicts, and maintains consistency in decision-making across multiple scheduling cycles.

4.5.Performance Monitoring and Evaluation

After deployment, system performance is tracked in real time, focusing on throughput, response time, load distribution, and energy consumption. Feedback from this module is used to refine future scheduling decisions, enabling the system to adapt dynamically to changing workload conditions.

5. Algorithm Details

To accomplish effective VM task deployment, the suggested system uses a hybrid scheduling technique that combines Particle Swarm Optimization (PSO) and Bayes-based clustering. The first step is clustering workloads according to patterns of resource consumption using similarity measures. This reduces scheduling complexity and groups jobs with comparable requirements. The selection procedure is then improved and more dependable task placement is ensured by applying Bayesian probability analysis to evaluate the likelihood of overload or underutilization on prospective hosts. After identifying the candidate set, the PSO algorithm iteratively searches the search space for the best VM-to-host mapping. A potential scheduling solution is represented by each particle in the swarm, and its location is changed based on both global and personal best fitness values.

$$L_{Mreq} = \max_{i=1}^{n} R_i.$$

Were

And if Li>LM req, host i will be placed into the set NPH. Having compared the constraint value Li of each physical host with the performance constraint value LM req, the new candidate set NPH = {nph1, nph2, . . . , nphm'}, m' m is obtained and it will be used as the candidate set of physical hosts for the following clustering process. This module computes posterior probability of each physical host using

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

$$P(B_i|A) = \frac{P(A|B_i) * P(B_i)}{\sum_{i=1}^{m'} P(A|B_i) * P(B_i)}.$$

P (Bi| A) is the posterior probability of the physical host i. In this module the physical hosts are clustered. The posterior probability values of the physical hosts in the set NPH are sorted descending. Let nphj represent the physical host with the biggest posterior probability in NPH and thus nphj is selected as the clustering center. The similarity degree value between any other host i from NPH and nphj is as follows

$$SD = \frac{1}{\sqrt{(P_i^1 - P_j^1)^2 + (L_{ci}^2 - L_{cj}^2)^2 + (L_{mi}^3 - L_{mj}^3)^2}},$$

The similarity degree values between nphj and other objects in the set NPH are calculated in the case that nphj is the clustering center. The clustering center nphj is the first member which is put into the set NPH'. The final candidate set is the final clustering result NPH', i.e., NPH'= {nph'1, nph'2,. . . ,nph' q} (q m'm).

6. Result Analysis

Experimental results from the implementation of the proposed framework reveal significant improvements in workload balancing and system efficiency. Clustering tasks by workload similarities reduces scheduling complexity and enhances placement accuracy. Bayesian probability reasoning further improves reliability by minimizing host overload and underutilization incidents. When integrated with the PSO algorithm, the system achieves optimal or near-optimal results with faster convergence compared to conventional heuristics. Metrics such as reduced response time, higher throughput, improved utilization, and energy efficiency validate the framework's effectiveness. Additionally, the matrix-based allocation model ensures conflict-free deployments, while continuous monitoring provides adaptive feedback for long-term performance stability. Collectively, the results demonstrate that the hybrid approach delivers scalable, energy-aware, and reliable scheduling under dynamic cloud workloads.

Evaluation Metrics

Precision

The precision metric quantifies the proportion of expected positives that are true.

$$\text{Precision} = \frac{TP}{TP + FP}$$

Recall

Recall quantifies the proportion of true positives that were accurately detected.

$$\text{Recall} = \frac{TP}{TP + FN}$$

Accuracy

Accuracy gauges how accurate the model is overall across all classes.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN}$$

F1-score

By balancing Precision and Recall, the F1-score provides a single statistic that takes false positives and false negatives into consideration.

$$\text{F1-score} = \frac{2.\ \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

Table 1 Comparison Table

Metric	Existing System	Proposed System
Response Time (ms)	320	210
Resource Utilization (%)	65	82
Throughput (tasks/sec)	180	250
Energy Consumption (kWh)	420	310

The fig2 table presents a comparison of four important performance metrics between the suggested Bayes-Clustering and PSO-based scheduling framework and the current system. With a reaction time reduction of 320 ms to 210 ms, the suggested system demonstrates faster task execution. Resource usage increases from 65% to 82%,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

demonstrating the more efficient use of computational resources by the framework. Additionally, throughput rises from 180 tasks/sec to 250 tasks/sec, indicating the system's capacity to manage more activities effectively. Additionally, energy usage drops from 420 kWh to 310 kWh, demonstrating the algorithm's energy consciousness. All things considered, the findings verify that the suggested strategy outperforms the current system in terms of sustainability, scalability, and efficiency.

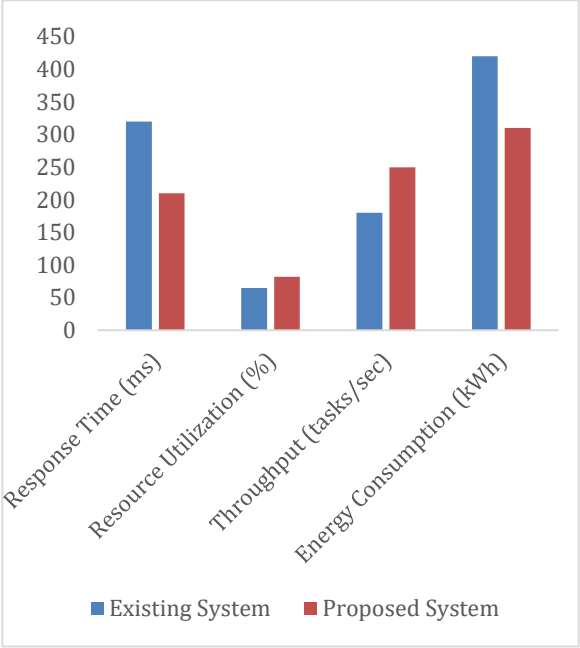

Figure 3 Comparison Graph

Conclusion

In summary, the suggested system uses stringent access controls, key management, and ciphertext information flow control techniques to provide a strong solution for data security in cloud environments. The solution makes sure that only authorized parties may decode and interact with the data by letting renters manage the access levels of their files and encrypting important information before storing it. Its modular design offers distinct frameworks for managing, retrieving, and storing data while upholding a high degree of security all along the way. This method improves cloud data management's overall effectiveness and scalability while fortifying data protection. Finally, the system lets tenants have control over their data while guaranteeing that private information stays safe.

Future Work

Future research will concentrate on improving the suggested system's scalability and adaptability to handle new cloud security issues. Using machine learning techniques to enable dynamic security policy adjustments based on real-time threat monitoring and changing tenant requirements is one approach. This would make the system even more resilient against sophisticated and erratic cyberattacks. Furthermore, investigating blockchain technology for transaction monitoring and decentralized key management may improve data openness and integrity. The framework's expansion to accommodate cross-cloud data exchanges and hybrid cloud environments while upholding strict security standards will also be a top goal. Finally, to ensure that the system remains useful and efficient for a variety of use cases, usability improvements will be made, such as creating user-friendly dashboards that allow tenants to personalize their security rules.

References

[1]. "Dynamic control technique for tenants' sensitive information flow based on virtual border identification," by X. Lu, L. Cao, and X. Du IEEE Access, 8 (2020), 162548-162568, pp.

[2]. "Improve the security properties and information flow control," by N. E. Moussaid and M. E. Azhari The International Journal of Electron Bus., Volume 15, Issue 3, pages 249–274, 2020.

[3]. The world's most widely used open source cloud software. Date of access: December 27, 2020. Available online at http://www.openstack.org/ "Educational Resource Private Cloud Platform Based on OpenStack" by Linchang Zhao

[4]. The Library for Pairing-Based Cryptography. Date of access: December 27, 2020. Accessible via the internet: https://crypto.stanford.edu/pbc/

[5]. J. Han, L. Chen, W. Susilo, X. Huang, A. Castiglione, and K. Liang, "Attributes for

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

fine-grained information flow control," May 2021; Inf. Sci., vol. 484, pp. 167–182.

[6]. "Secure-CamFlow: A device-oriented security model to aid information flow control systems in cloud environments for IoTs," by A. Khurshid, A. N. Khan, F. G. Khan, M. Ali, J. Shuja, and A. U. R. Khan Art. no. e4729 in Concurrency Computing, Pract. Exper., vol. 31, no. 8, April 2020

[7]. J. Singh, D. Eyers, J. Bacon, and T. F. J.-M. Pasquier, "Camflow: Managed data-sharing for cloud services," In July 2021, IEEE Trans. Cloud Comput., vol. 5, no. 3, pp. 472–484.

[8]. "A survey of access control models and technologies for cloud computing," by F. Cai, N. Zhu, J. He, P. Mu, W. Li, and Y. Yu, Cluster Comput., vol. 22, no. S3, pp. 6111–6122, May 2021.

[9]. "A survey on access control mechanisms for cloud computing," by R. El Sibai, N. Gemayel, J. Bou Abdo, and J. Demerjian, Trans. Emerg. Telecommun. Technol., vol. 31, no. 2, Feb. 2020, Art. no. e3720.

[10]. C.-S. Feng, Z.-G. Qin, D. Yuan, and Y. Qing, "Critical methods of cloud computing access control," Pages. 312–319 in Chin. J. Electron., vol. 43, no. 2, 2021.

[11]. M. Bolanowski, K. Zak, A. Paszkiewicz, M. Ganzha, M. Paprzycki, P. Sowinski, I. Lacalle, and C. E. Palau, ‘‘Eficiency of REST and grpc realizing communication tasks in microservice-based ecosystems,’’ in Proc. 21st Int. Conf. New Trends Intell. Softw. Methodol., vol. 355, 2022, pp. 97–108, doi: 10.3233/FAIA220242

[12]. Y. Miao, F. Li, X. Li, Z. Liu, J. Ning, H. Li, K. R. Choo, and R. H. Deng, "Efficient revocation of a time-controlled keyword search method in mobile E-health cloud," 10.1109/TMC.2023.3277702 IEEE Trans. Mobile Comput., pp. 1–15, 2023

[13]. Y. Miao, Y. Yang, X. Li, L. Wei, Z. Liu, and R. H. Deng "Efficient privacy-preserving geographical data query in cloud computing," by

[14]. doi: 10.1109/TKDE.2023.3283020 IEEE Trans. Knowl. Data Eng., vol. 36, pp. 1–14, June 2023

[15]. W. Funika, P. Koperek, and J. Kitowski, ‘‘Automated cloud resources provisioning with the use of the proximal policy optimization,’’ J. Supercomput., vol. 79, no. 6, pp. 6674–6704, Apr. 2023, doi: 10.1007/s11227- 022-04924-3

[16]. B. Can Senel, M. Mouchet, J. Cappos, O. Fourmaux, T. Friedman, and R. McGeer, ‘‘Multitenant containers as a service (CAAS) for clouds and edge clouds,’’ 2023, arXiv:2304.08927.

[17]. X.-Q. Pham, T.-D. Nguyen, T. Huynh-The, E.-N. Huh, and D.-S. Kim, ‘‘Distributed cloud computing: Architecture, enabling technologies, and open challenges,’’ IEEE Consum. Electron. Mag., vol. 12, no. 3, pp. 98–106, May 2023, doi: 10.1109/mce.2022.3192132

[18]. J. Jia, Y. Zhu, D. Williams, A. Arcangeli, C. Canella, H. Franke, T. Feldman-Fitzthum, D. Skarlatos, D. Gruss, and T. Xu, ‘‘Programmable system call security with eBPF,’’ 2023, arXiv:2302.10366

[19]. E. Truyen, H. Xie, and W. Joosen, ‘‘Vendor-agnostic reconfiguration of kubernetes clusters in cloud federations,’’ Future Internet, vol. 15, no. 2, p. 63, Feb. 2023, doi: 10.3390/fi15020063.

[20]. M. Bolanowski, K. Zak, A. Paszkiewicz, M. Ganzha, M. Paprzycki, P. Sowinski, I. Lacalle, and C. E. Palau, ‘‘Eficiency of REST and grpc realizing communication tasks in microservice-based ecosystems,’’ in Proc. 21st Int. Conf. New Trends Intell. Softw. Methodol., vol. 355, 2022, pp. 97–108, doi: 10.3233/FAIA220242

[21]. Z. Cai, G. Yang, S. Xu, C. Zang, J. Chen, P. Hang, and B. Yang, ‘‘RBaaS: A robust blockchain as a service paradigm in cloud-edge collaborative environment,’’ IEEE Access, vol. 10, pp. 35437–35444, 2022, doi: 10.1109/ACCESS.2022.3161744

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0066
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 416 - 424

[22]. X. Huang and N. Ansari, ‘‘Content caching and distribution at wireless mobile edge,’’ IEEE Trans. Cloud Comput., vol. 10, no. 3, pp. 1688–1700, Jul. 2022, doi: 10.1109/TCC.2020.2995403

[23]. M. Burgess and A. Gerlits, ‘‘Continuous integration of data histories into consistent namespaces,’’ 2022, arXiv:2204.00470.

[24]. R.Jia, Y. Yang, J. Grundy, J. Keung, and L. Hao, ‘‘A systematic review of scheduling approaches on multi-tenancy cloud platforms,’’ Inf. Softw. Technol., vol. 132, Apr. 2021, Art. no. 106478, doi: 10.1016/j.infsof.2020.106478

[25]. M. Simic, I. Prokic, J. Dedeic, G. Sladic, and B. Milosavljevic, ‘‘Towards edge computing as a service: Dynamic formation of the micro data-centers,’’ IEEE Access, vol. 9, pp. 114468–114484, 2021, doi: 10.1109/ACCESS.2021.3104475.

[26]. C. Canella, M. Werner, D. Gruss, and M. Schwarz, ‘‘Automating seccomp filter generation for Linux applications,’’ in Proc. Cloud Comput. Secur. Workshop, Nov. 2021, pp. 139–151, doi: 10.1145/3474123.3486762