

Dynamic VM Surveillance and Encrypted Access Control For Cloud Workload Protection

Sai Pranay Teja¹, Pacha Supriya²

¹Department of CSE, Koneru Lakshmaiah Foundation, Vaddeswaram, Andhra Pradesh, India. Email: 2401050049@kluniversity.in,

² Assistant Professor Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green fields, Vaddeswaram, Guntur, A.P., psupriya@kluniversity.in, supriya.miname@gmail.com

Abstract

Secure Resource Management (SRM) is crucial in cloud computing environments that share resources across virtual machines (VMs) and have potential attack surfaces for malicious actions. A lack of use of resources may compromise system integrity and lead to undesirable access. To address this problem, threat countermeasures are categorised into 3 strategies, namely defense, mitigation and hybrid, through a meta-analytical approach. To stop incursions, defensive tactics implement strong access control, AES-based encryption, and vulnerability management. The primary concerns of mitigating techniques are monitoring, incident handling and controlled use of files with significant validation procedures. AI-driven adaptive monitoring is included into hybrid techniques to instantly identify and stop unauthorized virtual machine activity. The lightweight Speck cipher technique, which is more computationally efficient than AES, is also used to lower encryption delay and check data integrity using file-hash associations. Comparative study is presented using different graph representations of file size and timing of encryption, in which efficient SRM can be achieved only within a limited context. The methodology is validated with simulated cloud and virtual machine environments to showcase the feasibility and success of the proposed strategies for using resources securely in real-time cloud infrastructure protection.

Keywords— Cyber threats, hypervisor vulnerability, resource utilization (RU), secure resource management (SRM), virtual machine (VM) vulnerability.

I. INTRODUCTION

Cloud computing is a basic paradigm in various industries such as business, academia, industry and in digital service platforms. It transforms traditional IT environments into agile, flexible and elastic service-oriented architectures that provide access to computing resources such as processing power, storage space and network infrastructure on demand, as needed, and on a scalable basis [1]. Organizations may effectively manage varying workloads, lower capital costs, and enhance overall service delivery by implementing cloud computing. Much of this revolution is due to virtualization, a basic technology that hides the physical machine and allows multiple virtual machines (VMs) to run on a single machine [2].

Cloud data centers (CDCs) are crucial to support these virtualized environments and to accommodate large-scale online transactions and service provisioning among geographically distributed customers [3]. In addition to being cost-effective, these environments offer better scalability, resource pooling and elasticity. Virtualization does, however, provide a number of security risks in addition to its many advantages. Cloud environments are shared, thus, vulnerabilities may be introduced at multiple levels, such as the hypervisor and virtual machine configurations, and could be targeted by malicious users [4].

Some of the cyberthreats that exist in virtualized cloud infrastructure include VM escape, side-channel attacks, data leakage, illegal access, and VM hijacking [5]. The attackers can exploit vulnerabilities in the virtual machine (VM) environment or in the hypervisor to move laterally between VMs and compromise the isolation of these machines and potentially the data they host, compromising data availability, integrity, or confidentiality. By allowing adversaries to deduce private information from nearby virtual instances using cache timing or other side-channel techniques, co-residency attacks increase these dangers [6].

Moreover, poor or poor-performing resource allocation mechanisms can lead to isolation problems and performance limitations, which can further limit the reliability and accuracy of cloud-based systems [7]. These issues have made Secure Resource Management (SRM) an important issue in cloud computing. SRM application combines the preventive defensive and reactive mitigation, to ensure the confidentiality, integrity and availability of resources. Access control, encryption, intrusion detection, trust management, and lightweight cryptographic techniques designed for cloud constraints are all included.

With constantly evolving cyber threats, intelligent and adaptive security frameworks are vital to deployment. Apart from protecting cloud environments from internal and external attacks, good SRM ensures seamless and continuous service provisioning [8].

II. RELATED WORK

Shen et al. [9] proposed a key agreement method based on block design specifically designed for group data sharing in the cloud computing environment. In addition to guaranteeing data confidentiality, integrity, and resistance against numerous security dangers including collusion and impersonation, their technique enables secure key distribution across numerous users. Additionally, users can join or leave the group without jeopardizing the security of group communications because to the proposed scheme's support for dynamic group membership. This solution is suitable for a large scale platform in the cloud as it leverages the block design theory which provides more efficiency in computing.

Liu et al. [10] suggested a two-factor security protection technique to handle user authentication and data privacy in cloud storage. The method enhances access control and data security in cloud systems by fusing the advantages of two-factor authentication (2FA) and attribute-based encryption (ABE). The authors concentrate on making sure that, even in the event that the cloud server is attacked, only authorized users can access encrypted data. Their method achieves safe key delegation, user revocation and fine-grained access control, which are all necessary for maintaining security of distributed, multi-tenant, cloud settings.

Saxena et al. [11] carried out a thorough performance analysis of machine learning-based workload prediction models for cloud computing in the areas of resource allocation and task handling. To forecast future workloads and maximize resource provisioning, they assessed a number of supervised learning methods, such as support vector machines (SVM), random forests (RF), and neural networks. They found that machine learning models that are driven by workload can significantly increase the efficiency of resources, lower energy consumption, and maintain service-level agreements (SLAs). This research is crucial for implementing intelligent decision-making in cloud operations and enabling dynamic and real-time resource management.

The fundamental architecture of cloud data centers was discussed by Barroso, Clidaras and Holze [12] and a detailed overview of warehouse-scale machines (WSMs) for supporting the modern cloud services was presented. Designing scalable, economical, and energy-efficient data centers that house massive numbers of virtual machines (VMs) and applications is the main emphasis of their work. The authors emphasize the importance of designing cloud architecture to be fault-tolerant, energy-efficient, and efficient in terms of computation. They made way for other progress in the architecture and abilities of cloud infrastructure.

Chhabra and Singh presented a safe and energy efficient dynamic hierarchical load balancing (DH-LB) for cloud data center [13]. This platform can address dual challenges of performance and energy management by dynamically assigning workloads to virtual machines (VMs) based on energy awareness and threat detection. A security engine that looks for any irregularities during load transfer is incorporated with the hierarchical load balancing approach. This approach helps their strategy reduce energy use and the risk of performance degradation, while maintaining a balance between energy savings and security compliance.

To solve the problem of VM placement, Ding et al. [14] proposed a virtual machine placement approach (DFA-VMP), which is effective and safe in a cloud environment. This approach considers the cost of communication and security risks and optimizes placement of virtual machines across physical machines. The authors successfully solve the problem of placement to minimize energy consumption, maximize tenant isolation and protect against the VM-based attacks by creating the problem of placement as a multi-objective optimization process. They use a dynamic fuzzy algorithm (DFA) to consider various goals such as load distribution, power saving, and security improvement.

To prevent the data leakage and inter-tenant attacks in cloud computing, Yu et al. [15] proposed a security-aware cloud virtual machine management system based on Chinese Wall policy. They propose a paradigm that ensures separation of data in virtual machines (VMs) spanning different security domains, thus setting access limits. The Chinese Wall strategy lessens the possibility of insider threats and lateral movement assaults by prohibiting access to competing data sets once a person has accessed a specific dataset. To guarantee the compliance with the confidentiality rules for cloud services, the authors use this paradigm to manage access control dynamically.

Finally, an Artificial Intelligence-based Virtual Machine Threat Prediction Model for Multi-risk Analysis in Cloud Cyber Security (MRACC) was presented by Saxena et al. [16]. Their approach takes a proactive step to predict future threats by analysing the historic behaviour of virtual machines. It takes into account a number of risk factors to generate early alerts, such as attack surface, vulnerabilities within the system, and previous events. The idea enhances the cloud service provider's ability to detect, prioritize, and respond to cybersecurity threats through the use of real-time information and automated decision-making. In the era of new and advanced threat vectors and zero-day attacks on cloud-based platforms, this contribution is particularly significant.

Saxena et al. [17] proposed a safe method of resource management which takes into account dynamic workload estimation and VM threat prediction in Industrial cloud environments. Their technology uses intelligent forecasting algorithms to proactively manage security concerns, hence improving cloud reliability.

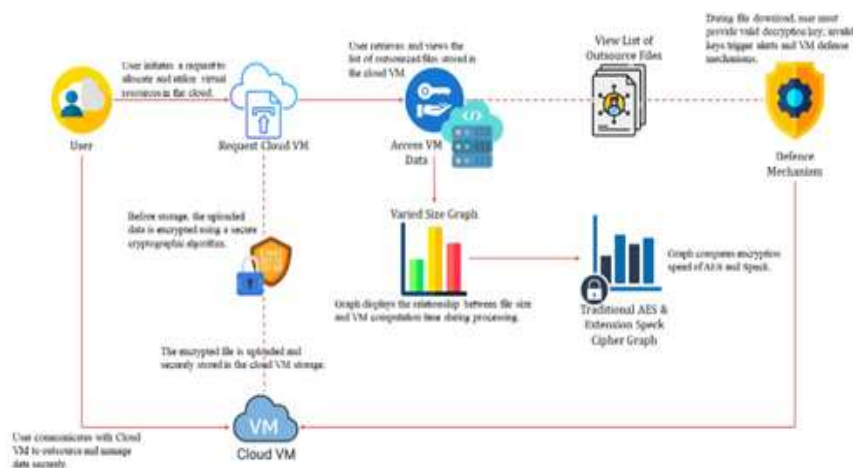
In heterogeneous networked multi-agent systems (nMAS), Yin et al. [18] developed a cloud-based event-triggered predictive control model which was able to effectively mitigate the impact of transmission delays and denial-of-service (DoS) attacks. They contribute to the resilience of systems in critical applications.

In Yuan's et al. [19] work, they proposed an inexpensive security method to prevent Distributed Denial-of-Service (DDoS) attacks in cloud platform services using fine-grained resource management to reduce financial damages without compromising service availability.

Finally, a trust-based secure multi-cloud collaboration framework designed for cloud-fog-IoT contexts was proposed by Zhang et al. [20], enabling safe data sharing and collaboration between various cloud service providers. Their method deals with data integrity and trust management in distributed cloud systems.

III. MATERIALS AND METHODS

The proposed solution integrates defensive, mitigating, and hybrid security approaches, providing a secure framework for managing resources in cloud environments. AES encryption is used in defensive measures to safeguard data both during transit and at rest, guaranteeing that only authorized users may access it [9]. To mitigate techniques, unwanted access attempts are mitigated by checking the decryption keys before they are allowed to be downloaded [10]. The hybrid method has been introduced to monitor VM activities in real time, so as to detect and block abnormal or hazardous VM behaviors [16]. The data is verified at retrieval for integrity, and a lightweight Speck cipher is employed for encryption to reduce computational complexity. This comprehensive approach enhances the security and reliability of data within cloud-based systems, ensuring it remains available, confidential, and secure.



"Fig. 1. System Architecture"

The system architecture (Fig. 1) shows that the system can secure cloud resources: Users upload data by submitting a request to the cloud virtual machine. Confidentiality is ensured by encryption of the data before storing it using the Speck or AES cipher. Later, users check keys to access files; unsuccessful attempts set off defense systems. Hash-based integrity verification is also supported by the system. There are two graphs for performance measurement: AES and Speck encryption speed; VM calculation time for various file sizes. It is run securely, effectively and monitored with cloud data management.

A) Modules

Signup Here: By inputting the necessary information, this module enables new users to create an account. User information is securely saved behind the scenes to be used in future for authentication. The registration process ensures that only authorised users have access to the cloud system, allowing them to upload, encrypt and access sensitive data safely.

Cloud User Login: Using their login information, registered users can access this module. It authenticates the user based on existing user information to ensure safe access to other system capabilities such as file upload, encryption, and data access. It's the gateway to secure cloud communications.

Request Cloud VM: This module can be used by selecting files to upload to cloud outsourcing. Files are encrypted with a user-defined key and each file has a unique hash. By taking these precautions, the data is protected and future integrity checks prior to file access are made possible.

Access VM Data: Users can browse and retrieve their uploaded files from the cloud virtual machine (VM) using this module. Users have to input the proper decryption key to ensure security. Access is granted when the request is approved and access is denied when it is not approved with a warning to the user of potential illegal activity.

Varied Size Graph: This module shows how long it takes the cloud virtual machine to process and store files of various sizes. The graph displays the relationship between file size and processing time / server response, which helps with analyzing the system performance and efficiency with different storage requirements.

Traditional AES & Extension Speck Cipher Graph: In this section the Speck Cipher and the conventional AES algorithm are compared regarding the encryption time. It emphasizes the benefits of Speck Cipher in improving the encryption rate and reducing the computational costs in general by visualizing how Speck Cipher reduces the computation time.

B) Methods/Technologies

1. **AES (Advanced Encryption Standard):** Before saving file data on the cloud, it is safely encrypted using the symmetric encryption technique AES. It uses a user-defined key to encrypt plain text into ciphertext to ensure that only the intended users, who possess the correct key, can decrypt the information and access it, thus preventing unauthorized users or changes.

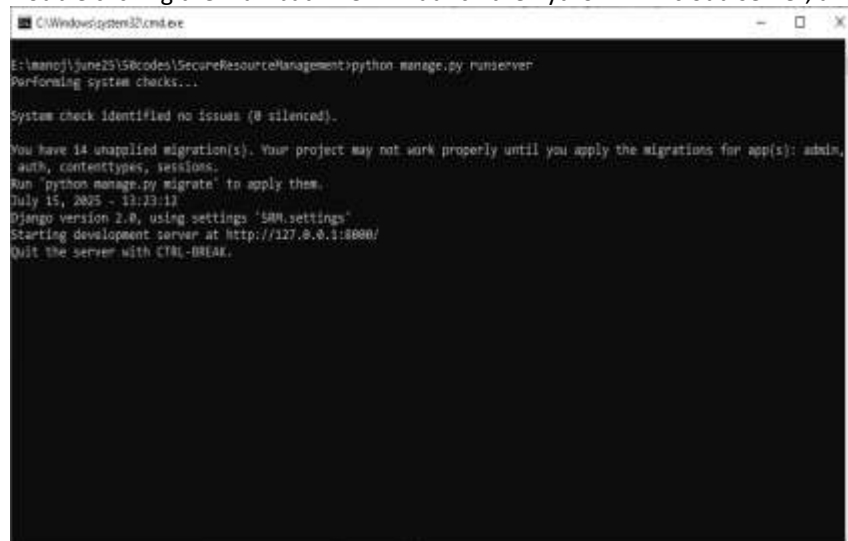
2. **Speck Cipher:** Speck A lightweight and effective block cipher, the Speck Cipher is intended for settings with constrained processing power. For quicker encryption with less processing overhead, it is used as an alternative to AES. Speck aids in optimizing encryption speed and resource usage in this system, which makes it appropriate for cloud platforms handling large amounts of data and user requests.

3. **Hashing (for data integrity verification):** Each file submitted will produce one fixed-size hash value. These hash values are used to verify the integrity of the data when accessing a file. The file is intact if the hash doesn't change. Changes to the file will result in a different hash, which indicates that the file has been corrupted or modified.

4. **Key-Based Access Control:** This method guaranties that files from the cloud can only be accessed or downloaded by authorized users. Users have to provide a decryption key to recover encrypted data. If an invalid key is typed, it is denied access, which further secures the system and prevents access to unwanted files.

IV. EXPERIMENTAL RESULTS

Double clicking the "run.bat" file will launch the Python WEB cloud server, and show the following page.



```
C:\Windows\system32\cmd.exe
E:\manoj\June25\58codes\SecureResourceManagement>python manage.py runserver
Performing system checks...

System check identified no issues (0 silenced).

You have 14 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin,
auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
July 15, 2025 - 11:23:12
Django version 2.0, using settings 'SRM.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

Created a python server in the above screen. Open a browser, enter the URL <http://127.0.0.1:8000/index.html> and press Enter to display the following page.



To go to the screen below, click the “User Sign up” option on the screen above.



The user fills out the sign up information in the screen above and clicks on the button to go to the below screen.



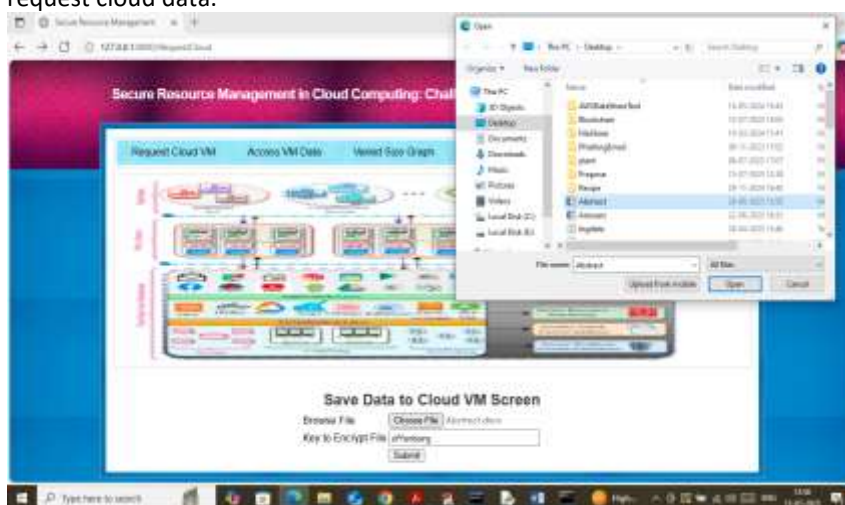
Once the user sign-up process is done in the above screen, click the "Cloud User Login" link and you will be directed to the following screen.



Once logged in, the person above will see the following page.



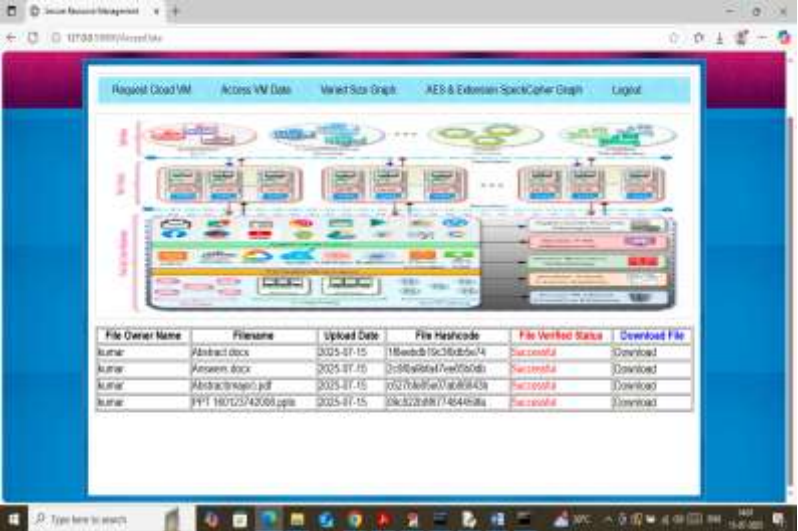
Clicking on "Request Cloud VM" in the above screen will take the user to the page below, from which they can request cloud data.



Click the button below to select the file to be cloud outsourced, upload it, type the encryption key and click the button.



The file data above has been successfully encrypted and a hash code for verification of the file has been created. This hashcode will be checked for correctness of the file. Similarly, you can upload as many files as you want. Select the "Access VM Data" to display the list of uploaded files below.



The user will be able to see in the screen above a list of outsourced files, all of which have been validated against hashes and are found to be valid. By clicking on the blue link that is provided to download the file, they will then be taken to the site below.



The user is asked to input the decryption key in the screen above: The file will only download and display on the site below after the key is validated. By using the key cloud, it will protect itself from all threats.



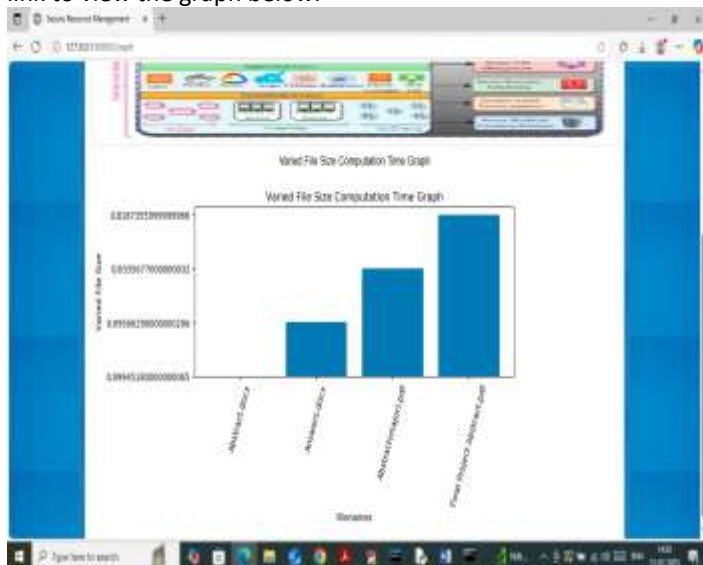
The file will be downloaded in the browser status bar on the screen above - if we input the wrong key, the site below will appear.



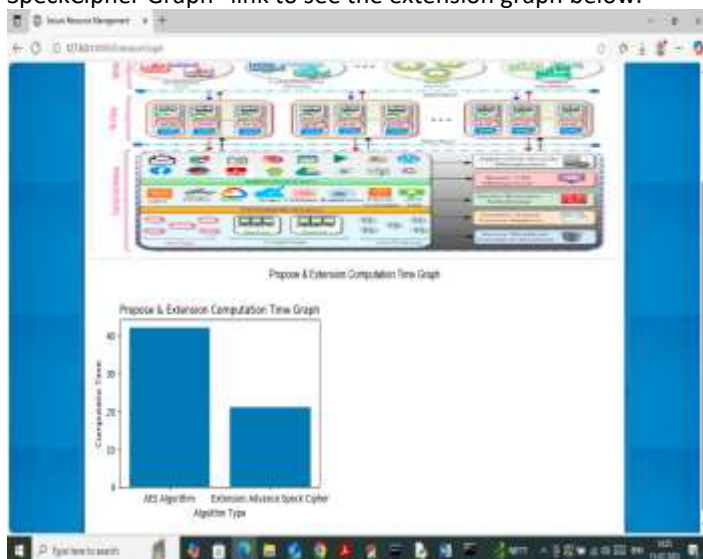
The result is as follows: The result is shown below and the above screen shows an invalid key.



Once VM has alerted the user to the existence of invalid access, it will become defensive and engage in mitigation to protect itself from such users, as illustrated in the screen above. Click on the "Varied Size Graph" link to view the graph below.



In the above graph the x-axis represents the "file name" and the y-axis the VM computation time for variable file size storage. VMs are slower to store and process requests with large files. Click on the "AES & Extension SpeckCipher Graph" link to see the extension graph below.



The extension graph above is plotted on the x-axis with the names of the algorithms and on the y-axis with length of the algorithms. The extensions in both cases were shorter in time.

V. CONCLUSION

This is achieved by a hybrid of defensive, mitigating and hybrid tactics, which enables an effective safe and effective resource management system in cloud computing environments. The system uses key-based authentication and AES encryption to guaranty data confidentiality and restricted access. The Speck cipher technique is introduced as a light-weight alternative with reduced encryption computation time but still maintaining almost adequate security to further improve the speed. File-hash verification adds an important layer of data integrity checking to provide customers with assurance that their outsourced data is consistent and authentic, even when stored on a shared virtual machine or other shared storage medium.

Real-time monitoring of VM activities enhances system resilience and responsiveness by detecting and blocking any access attempts that are not authorized. The system not only prevents attacks, but it also protects against damage should an attack occur, combining preventative techniques with damage-reduction techniques in one system. The tiered strategy guaranties the safe and effective use of cloud resources. Deploying this architecture

in real-world applications is feasible, particularly when operational efficiency and strong data security are crucial. The result shows that cloud infrastructure can be considerably strengthened against changing cyber threats by combining lightweight cryptography techniques with sophisticated monitoring.

The system can be enhanced by using blockchain technology to ensure transparent auditing by making all file transactions and virtual machine access immutable and traceable. Future studies could explore using AI-powered anomaly detection algorithms to further enhance real-time danger prediction. It is also possible to provide cross-platform support and compatibility with the multi-cloud environment. Even better, it could be possible to process data without decrypting it, with the help of homomorphic encryption. One possible extension of the framework for wider applicability is to add several users and organizations to the collaboration in a safe manner.

REFERENCES

- [1] Ebadinezhad, S., & Alsaroah, A. H. A. (2025, January). Comparative Analysis of Edge-based and Cloud-based Intrusion Detection Systems: A Systematic Literature Review. In 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI) (pp. 707-714). IEEE.
- [2] Saxena, D., & Singh, A. K. (2024). Workload pattern learning-based cloud resource management models: Concepts and meta-analysis. *IEEE Transactions on Sustainable Computing*.
- [3] Santos, A., Martins, J., Pestana, P. D., Gonçalves, R., São Mamede, H., & Branco, F. (2024). Factors Affecting Cloud Computing Adoption in the Education Context—Systematic Literature Review. *Ieee Access*, 12, 71641-71674.
- [4] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *Ieee Access*, 9, 57792-57807.
- [5] Deepa, M., & Dhiipan, J. (2022, December). A Meta-Analysis of Efficient Countermeasures for Data Security. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 1303-1308). IEEE.
- [6] Yadav, Rahul and Zhang, Weizhe and Li, Keqin and Liu, Chuanyi and Shafiq, Muhammad and Karn, Nabin Kumar, "An adaptive heuristic for managing energy consumption and overloaded hosts in a cloud data center," *Wireless Networks*, vol. 26, pp. 1905–1919, 2020.
- [7] J. Feng, L. T. Yang, Q. Zhu, and K.-K. R. Choo, "Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 4, pp. 857–868, 2018.
- [8] Yadav, Rahul and Zhang, Weizhe and Li, Keqin and Liu, Chuanyi and Laghari, Asif Ali, "Managing overloaded hosts for energy-efficiency in cloud data centers," *Cluster Computing*, pp. 1–15, 2021.
- [9] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block designbased key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 996–1010, 2017.
- [10] J. K. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-factor data security protection mechanism for cloud storage system," *IEEE Transactions on Computers*, vol. 65, no. 6, pp. 1992–2004, 2015.
- [11] D. Saxena, J. Kumar, A. K. Singh, and S. Schmid, "Performance analysis of machine learning centered workload prediction models for cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 34, no. 4, pp. 1313–1330, 2023.
- [12] L. A. Barroso, J. Clidaras, and U. Holzle, "The datacenter as a computer: " An introduction to the design of warehouse-scale machines," *Synthesis lectures on computer architecture*, vol. 8, no. 3, pp. 1–154, 2013.
- [13] S. Chhabra and A. K. Singh, "Secure and energy efficient dynamic hierarchical load balancing framework for cloud data centers," *Multimedia Tools and Applications*, pp. 1–14, 2023.
- [14] W. Ding, C. Gu, F. Luo, Y. Chang, U. Rugwiro, X. Li, and G. Wen, "Dfa-vmp: An efficient and secure virtual machine placement strategy under cloud environment," *Peer-to-Peer Networking and Applications*, vol. 11, pp. 318–333, 2018.
- [15] S. Yu, X. Gui, J. Lin, F. Tian, J. Zhao, and M. Dai, "A security-awareness virtual machine management scheme based on chinese wall policy in cloud computing," *The Scientific World Journal*, vol. 2014, 2014.
- [16] D. Saxena, I. Gupta, R. Gupta, A. K. Singh, and X. Wen, "An aidriven vm threat prediction model for multi-risks analysis-based cloud cybersecurity," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2023.
- [17] D. Saxena, R. Gupta, A. K. Singh, and A. V. Vasilakos, "Emerging vm threat prediction and dynamic workload estimation for secure resource management in industrial clouds," *IEEE Transactions on Automation Science and Engineering*, 2023.

- [18] X. Yin, Z. Gao, D. Yue, and S. Hu, "Cloud-based event-triggered predictive control for heterogeneous nmass under both dos attacks and transmission delays," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 12, pp. 7482–7493, 2022.
- [19] B. Yuan, H. Zhao, C. Lin, D. Zou, L. T. Yang, H. Jin, L. He, and S. Yu, "Minimizing financial cost of ddos attack defense in clouds with finegrained resource management," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2541–2554, 2020.
- [20] J. Zhang, T. Li, Z. Ying, and J. Ma, "Trust-based secure multi-cloud collaboration framework in cloud-fog-assisted iot," *IEEE Transactions on Cloud Computing*, 2022.