RESEARCHERID
THOMSON REUTERS
[Verma et al., 10(2), Feb 2025]

ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"A COMPREHENSIVE REVIEW OF SECURITY STRATEGIES IN CLOUD COMPUTING: VIRTUAL MACHINES, MIGRATION, AND COMMUNICATION PROTOCOLS"

Purnima Verma [1], Prof. Sanmati Kumar Jain [2]

[1] M. Tech Scholar, Department of Computer Science and Engineering, Vikrant Institute of Technology and Management, Indore, Madhya Pradesh, India

[2]Associate Professor & HOD, Department of Computer Science and Engineering, Vikrant Institute of Technology and Management, Indore, M.P. India

ABSTRACT

The exponential growth of cloud computing has revolutionized how data is managed, accessed, and secured. This review paper critically examines the current landscape of cloud security, with a focused analysis on the security of virtual machines (VMs), optimized virtual machine migration strategies to minimize SLA violations, and cloud communication security protocols. The literature discussed spans from cryptographic data auditing methods and blockchain-based integrity verification to adaptive firewall architectures and identity-based encryption mechanisms. Additionally, it highlights the importance of reducing vulnerabilities during live VM migration and fortifying cloud communications against evolving cyber threats. The study identifies key challenges, advantages, and limitations of existing security techniques, while also suggesting areas for future research, particularly in the adoption of intelligent, scalable, and decentralized security frameworks. This paper serves as a comprehensive resource for understanding and enhancing security mechanisms in modern cloud environments.

Key Words: *Cloud Computing, Virtual Machine Security, Data Integrity, VM Migration, SLA, Violation, Cloud Communication.*

I. INTRODUCTION

The rapid evolution of cloud computing has ushered in a new era of technological advancement, significantly transforming how data is stored, processed, and managed across the virtual landscape. As organizations increasingly migrate their operations to cloud-based environments, the security of virtual machines (VMs) and the integrity of cloud communications have emerged as paramount concerns. The burgeoning reliance on cloud infrastructures necessitates a critical evaluation of current security measures, their efficacy, and the potential areas for enhancement. This literature review aims to dissect the existing methodologies and technologies deployed to safeguard cloud environments, focusing on the security of virtual machines, the dynamism of firewall strategies, and the robustness of cloud communication protocols.

The examination begins with a review of secure cloud auditability for virtual machines, highlighting the importance of adaptive characterization in monitoring and securing cloud-based assets. This segment delves into the challenges of ensuring comprehensive visibility over VM activities within the cloud, emphasizing the need for dynamic and flexible auditing mechanisms that can cater to the evolving landscape of cloud security. Following this, the discussion transitions to an exploration of VM migrations and the strategies employed to minimize Service Level Agreement (SLA) violations. This review underscores the critical balance between operational efficiency and the maintenance of high security and performance standards during VM migrations.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Furthermore, this chapter encompasses a critical analysis of the development and implementation of dynamic firewall rule-building engines tailored for hybrid cloud environments. The focus on hybrid clouds underscores the complexity of securing diverse and interconnected cloud infrastructures, necessitating innovative approaches to firewall management and rule optimization. Lastly, the chapter discusses the pivotal role of cloud communication security, evaluating the existing protective measures and the potential for leveraging machine learning to enhance security protocols. Throughout this literature review, significant research gaps are identified, signaling areas where further investigation and innovation are crucial for advancing cloud security measures and ensuring the protection of virtualized cloud resources.

II. REVIEW ON SECURE CLOUD AUDITABILITY FOR VIRTUAL MACHINES

Dean et al. [1] presented a seminal paper on scaling deep learning across distributed systems, proposing an architecture that allows for efficient training of large-scale neural networks over thousands of machines. The methodology hinges on a distributed approach that divides the neural network's parameters across the system, significantly speeding up the training process. This method allowed for unprecedented scaling of deep learning tasks, demonstrating remarkable improvements in training time for large datasets. However, the approach requires substantial computational resources and network bandwidth, which could be limiting factors for smaller organizations.

Li et al. [2] explored the scaling of distributed machine learning through the use of a parameter server, a framework designed to handle the distribution and collection of parameters when training models across many machines. The paper introduces an architecture that efficiently synchronizes the model's parameters across a distributed network, thereby facilitating faster and more scalable machine learning tasks. While this method significantly improves scalability and processing speed, it also introduces challenges related to network latency and the complexity of managing synchronization across many nodes.

Li et al. [3] present a comprehensive exploration of the parameter server framework designed for distributed machine learning, aiming to address the challenges associated with handling large-scale data across distributed environments. This framework facilitates efficient and scalable machine learning computation, allowing for the management of large volumes of parameters and their distribution among multiple machines for parallel processing. The method employed by Li et al. focuses on a client-server architecture where the server stores the global model parameters, and the clients (or workers) perform computations on subsets of data, periodically updating the global model with their local changes. This approach enables the leveraging of distributed computing resources to speed up machine learning tasks significantly. One of the key advantages of this system is its ability to scale linearly with the number of machines, thereby reducing the computational time as the network size increases. However, a potential disadvantage is the complexity involved in ensuring consistency and reducing communication overhead between the servers and clients, which can become significant challenges as the scale of the system grows.

Wang et al. [4] focused on the critical area of privacy-preserving public auditing for secure cloud storage. They developed a novel scheme that enables third-party auditors to verify the integrity of data stored in the cloud without compromising the privacy of the data contents. This approach cleverly uses cryptographic techniques to ensure data integrity and privacy simultaneously, providing a robust solution for secure cloud storage services. However, the cryptographic operations involved can impose computational overheads on the system, potentially affecting performance.

Yan et al. [5] proposed an efficient remote data possession checking protocol that allows cloud storage clients to verify the integrity of their data without retrieving it. The protocol is designed to be lightweight and secure, minimizing the computational and bandwidth requirements for both the client and the cloud service provider. This innovation is particularly advantageous for ensuring data integrity in cloud storage, but the protocol's reliance on specific cryptographic assumptions could limit its applicability in scenarios where these assumptions do not hold.

Sookhak et al. [6] present a novel approach for auditing big data storage in cloud computing environments utilizing divide and conquer tables. This method aims to improve the efficiency and scalability of auditing processes without compromising security. By dividing data into manageable blocks and employing conquer tables for auditing, the

ISSN : 2455-9679
SJIF Impact Factor : 6.008

scheme allows for parallel processing, significantly reducing the time required for audits. The advantage of this approach is its scalability and efficiency, making it suitable for large-scale cloud storage systems. However, the complexity of managing divide and conquer tables could be seen as a drawback, potentially increasing the overhead for cloud service providers.

Zhao et al. [7] introduce a user stateless privacy-preserving TPA (Third Party Auditor) auditing scheme for cloud storage, focusing on enhancing user privacy without compromising the efficiency of the audit process. Their method leverages cryptographic techniques to ensure that the TPA can verify data integrity without needing to access the actual data or requiring users to maintain state information. This scheme offers significant privacy advantages and reduces the burden on users. However, the reliance on cryptographic operations may introduce computational overhead, affecting performance in resource-constrained environments.

Wang [8] proposes an identity-based distributed provable data possession (ID-DPDP) framework for multi cloud storage environments. This framework allows users to verify the integrity of their data across different clouds in a secure and efficient manner, using identity-based cryptography to simplify key management and reduce overhead. The advantage of this approach is its elimination of the complex certificate management typically required in traditional public key infrastructure (PKI) systems, making it more user-friendly. The downside might be the potential for scalability issues as the system grows, given the inherent challenges in managing identity- based keys at a large scale.

Hussain A A et al. [9] focus on identity-based proxy-oriented data uploading and remote data integrity checking in public cloud environments. Their work addresses the security and efficiency challenges of data integrity verification by introducing a proxy component that acts on behalf of the users. This model not only enhances data security but also supports efficient data uploading and integrity checking processes. One major advantage is the reduced load on users for managing their data integrity. However, introducing a proxy entity may raise concerns regarding the trustworthiness and potential bottleneck issues, particularly in scenarios with high data throughput.

Zhang et al. [10] develop an efficient ID-based public auditing mechanism for outsourced data in cloud storage. Their approach utilizes identity-based cryptography to facilitate the auditing process, allowing for secure and efficient verification of data integrity without revealing sensitive information. The method stands out for its simplicity and the reduced need for complex key management procedures. However, the dependence on the ID-based scheme might limit flexibility and adaptability in dynamically changing cloud environments.

Yu et al. [11] propose an identity-based remote data integrity checking mechanism that ensures perfect data privacy preservation for cloud storage. This method leverages identity-based cryptography to verify the integrity of the data stored in the cloud without revealing any data content, effectively addressing the privacy concerns associated with conventional integrity checking approaches. The advantage of this scheme is its ability to provide strong data privacy while still ensuring data integrity. However, the reliance on identity-based cryptography might introduce challenges in key management and scalability in a large-scale cloud environment.

Shen et al. [12] focus on enabling identity-based integrity auditing along with data sharing, incorporating sensitive information hiding to enhance security in cloud storage. They utilize identity-based encryption and signature schemes to facilitate auditing and sharing processes, ensuring that sensitive data remains hidden even during the integrity verification. This approach significantly improves privacy and data sharing capabilities but may incur additional computational overhead, making it less efficient for time-sensitive applications.

Zhu et al. [13] introduce a secure and efficient data integrity verification scheme for cloud-IoT environments, based on short signatures. This scheme is designed to be lightweight to accommodate the limited resources of IoT devices while providing robust security features for cloud storage. The main advantage is the low computational requirement, making it suitable for IoT devices. However, the use of short signatures might raise concerns over long- term security due to potential vulnerabilities to quantum computing attacks.

He et al. [14] develop a public integrity auditing framework for dynamic regenerating code-based cloud storage, which ensures data integrity and supports data recovery. By integrating regenerating codes with auditing mechanisms, this

ISSN : 2455-9679
SJIF Impact Factor : 6.008

method not only verifies the integrity of cloud-stored data but also enhances data availability through efficient regeneration. While it offers improved data resilience and integrity verification, the complexity of implementing regenerating codes could be a barrier for widespread adoption.

Yu et al. [15] propose a blockchain-based service composition architecture for cloud manufacturing, aiming to enhance the trust and security of service transactions. By leveraging blockchain technology, this architecture ensures transparent and tamper-proof record- keeping. The advantage lies in its ability to foster trust among participants in cloud manufacturing ecosystems. However, the performance and scalability issues associated with blockchain technology could limit its applicability in large-scale manufacturing settings.

Yang et al. [16] present a blockchain-based scheme for publicly verifiable data deletion in cloud storage, addressing the challenge of ensuring that data is irrevocably deleted upon request. This method capitalizes on the immutability and transparency of blockchain to provide verifiable proof of data deletion. Its major strength is in enhancing user trust regarding data deletion, but the potential for increased blockchain storage requirements poses a notable disadvantage.

Zhang et al. [17] explore a blockchain-based approach for public integrity verification in cloud storage, specifically targeting the issue of procrastinating auditors. This solution aims to incentivize auditors to perform timely and honest verification tasks through blockchain smart contracts. It enhances the reliability of audit processes, but the dependence on smart contract security and performance could be seen as a drawback.

Zhang et al. [18] introduce a two-stage plant species recognition method that combines local mean clustering with weighted sparse representation classification. While not directly related to cloud computing or cryptographic algorithms, this research highlights the potential of advanced data analysis techniques. The method offers high accuracy in plant species recognition but may face challenges in handling very large datasets or in adapting to different domains.

Zhang et al. [19] propose a blockchain-assisted public-key encryption with keyword search mechanism to protect against keyword guessing attacks in cloud storage. This approach enhances data security by

allowing encrypted search functionalities without compromising keyword privacy. The advantage is the improved security against search-related attacks, though the added complexity and computational costs for encryption and search operations are potential disadvantages.

Kim et al. [20] develop a secure authentication-management human- centric scheme for mobile cloud computing using blockchain, focusing on building trust for personal resource information. This scheme enhances security and trust through decentralized authentication and management, offering significant advantages in privacy and user control. However, the reliance on blockchain may introduce challenges related to scalability and mobile device resource consumption.

Li et al. [21] focus on a blockchain-based searchable symmetric encryption scheme that aims to enhance security and privacy for cloud storage services. This method allows for efficient and secure search operations over encrypted data, addressing concerns over data privacy and searchability. While it significantly improves data security and search functionality, the complexity of the encryption and search process might impact system performance.

III. REVIEW ON VM MIGRATIONS WITH REDUCED SLA VIOLATION

Barham et al. [22] explore the Xen virtualization platform, focusing on its architecture and the benefits it provides for secure and efficient virtualization in cloud computing environments. The method used involves a detailed examination of Xen's design principles, particularly its paravirtualization approach, which allows for high performance with minimal overhead. The paper highlights advantages such as significant efficiency improvements over full virtualization techniques and improved security isolation between virtual machines. However, it also notes disadvantages, including the need for modifications to the guest operating system and potential compatibility issues with certain hardware and software configurations.

Clark et al. [23] discuss the process and challenges of live migration of virtual machines, emphasizing its significance for load balancing, fault tolerance, and maintenance in cloud data centers. They present a comprehensive method for achieving efficient live migration with minimal service downtime and network overhead. The advantages outlined include enhanced system reliability and flexibility in resource management. However, the paper also identifies disadvantages, such as the complexity of migration management and potential security vulnerabilities during the migration process.

Padala et al. [24] present a performance evaluation of virtualization technologies, with a focus on server consolidation using VMware ESX Server. Their method involves empirical testing and analysis of various performance metrics, including CPU, memory, and I/O throughput. The study reveals advantages such as significant improvements in resource utilization and cost savings on hardware. On the downside, the research points out that virtualization can introduce performance overheads and may require complex management strategies for optimal performance.

Murugesan [25] introduces the concept of green IT and its application in cloud computing, advocating for environmentally sustainable practices in the IT sector. The paper methodologically reviews principles and practices of green IT, including energy-efficient computing and data center operations. Advantages include reduced energy consumption and operational costs, as well as a lower carbon footprint for IT operations. The primary disadvantage is the initial investment and effort required to implement green IT practices effectively.

Djenna et al. [26] analyze security problems in cloud infrastructure, particularly focusing on vulnerabilities and attacks that can compromise the integrity, confidentiality, and availability of cloud resources. Their method involves a survey of common security threats and the evaluation of existing security measures. They point out the advantage of raising awareness and understanding of security challenges in cloud environments. However, the paper also highlights the disadvantage of the constant evolution of security threats, which requires ongoing research and updates to security practices.

Riste part et al. [27] examine information leakage in third-party compute clouds, presenting a methodological analysis of side-channel attacks and their implications for multi-tenant cloud environments. The paper's advantages include a detailed understanding of cloud- specific attack vectors and practical recommendations for mitigating such risks. The disadvantages include the difficulty of completely eliminating side-channel vulnerabilities without significant changes to cloud architecture and operations.

Fan et al. [28] explores a security protection model specifically designed for live migration in KVM (Kernel-based Virtual Machine) virtualization. The study introduces a novel approach that focuses on minimizing the security risks associated with the live migration process. The method involves enhancing the authentication and encryption mechanisms during migration. The advantage of this model is its ability to significantly reduce the risk of data leakage and unauthorized access during the migration process. However, one disadvantage is the potential increase in migration time due to the added security layers.

Oberheide et al. [29] investigate the empirical exploitation of live migration of virtual machines, highlighting vulnerabilities in the migration process that could be exploited by attackers. Through practical experiments and attack simulations, this study showcases how live migrations can be intercepted and manipulated. The main advantage of this research is its real-world applicability in demonstrating security flaws, while a disadvantage is the lack of a proposed solution to mitigate these vulnerabilities.

Yamunadevi et al. [30] focus on enhancing security in virtual machine live migration specifically for KVM environments. The paper proposes a framework that integrates secure authentication and encryption techniques to safeguard the migration process. The advantage is the practical approach to securing live migrations, though the framework may introduce performance overheads, posing a disadvantage.

Fan et al. [31] delve into the issue of memory leakage during live migration in virtualized environments. This research presents an analysis of the security risks associated with memory leakage and proposes a method to detect and mitigate such risks. The main advantage is the in-depth focus on a specific vulnerability, memory leakage, while a disadvantage

ISSN : 2455-9679
SJIF Impact Factor : 6.008

is the narrow scope of the solution, limiting its application to other migration security issues.

Dawoud et al. [32] examine security challenges in Infrastructure as a Service (IaaS) environments, proposing solutions to enhance the security of live virtual machine migrations. The paper offers a comprehensive overview of IaaS security vulnerabilities and suggests a multi-layered security framework. This framework's advantage is its comprehensive approach, but it may be complex to implement, serving as a disadvantage.

Anala et al. [33] present a framework designed to ensure the secure live migration of virtual machines. The framework emphasizes robust authentication and secure data transmission channels. The advantage of this framework is its emphasis on a holistic security approach, while the complexity of deployment might be seen as a disadvantage.

Biedermann et al. [34] aim to improve the security of virtual machines during live migrations by introducing an enhanced monitoring and control system for migration processes. This approach's advantage is its ability to dynamically respond to security threats, but it may require significant resources to implement, which is a disadvantage.

Back et al. [35] discuss traffic analysis attacks and the trade-offs in anonymity-providing systems, offering insights into how these attacks can be mitigated. While the paper primarily focuses on anonymity, its methods and findings can indirectly benefit the security of live VM migrations by improving data privacy. The advantage lies in the detailed analysis of anonymity threats, but the indirect application to live VM migration security could be considered a disadvantage.

Oberheide et al. [36] reiterate their earlier work on the exploitation of live VM migrations, further emphasizing the practical aspects and potential countermeasures. This follow-up provides a deeper understanding of the vulnerabilities, serving as both an advantage in its depth and a disadvantage in potentially limited solutions offered.

Aiash et al. [37] tackle the secure live migration of virtual machines, identifying key issues and proposing a set of solutions to ensure the integrity and confidentiality of data during migration. The paper's strength lies in its detailed solution-oriented approach, though the specific focus on certain technologies could limit its applicability across different virtualization platforms.

IV. Review on Cloud Communication Security

An et al. [38] explored the development of automated security analysis and enforcement mechanisms for cloud computing by employing graphical models. Their method integrates various security domains within the cloud environment to offer a holistic view of potential vulnerabilities and enforcement strategies. The advantage of this approach lies in its ability to visualize and automate the detection of security issues, thus enhancing the robustness of cloud security. However, the complexity of implementing these graphical models across diverse cloud services and the potential for overlooking context- specific threats can be seen as disadvantages.

Luna et al. [39] focused on quantitatively assessing cloud security using service level agreements (SLAs) to establish a framework for understanding and negotiating security expectations between cloud service providers and their clients. This quantitative approach aids in creating a more transparent and measurable understanding of security provisions, potentially leading to higher trust in cloud services. The downside could be the difficulty in quantifying certain security aspects and the reliance on accurate and honest reporting from providers.

Gonzales et al. [40] proposed "Cloud-Trust," a security assessment model tailored for Infrastructure as a Service (IaaS) clouds. This model aims to evaluate the security posture of IaaS offerings, providing users with a metric-based evaluation of potential risks. Its advantage lies in offering a standardized method to assess security, facilitating informed decisions by users. However, its effectiveness is heavily dependent on the accuracy of the underlying metrics and the model's ability to adapt to new threats.

Li et al. [41] enhanced IoT security in cloud-based environments through an integrated approach combining security

ISSN : 2455-9679
SJIF Impact Factor : 6.008

mechanisms with a reputation system for cloud services. This dual approach not only secures data but also incentivizes cloud services to maintain high- security standards. The primary advantage is the reinforcement of trust in cloud services; however, the reliance on the reputation system's accuracy and potential manipulation are notable disadvantages.

Halabi et al. [42] investigated the use of game theoretical models to form secure cloud federations, offering a novel perspective on enhancing cloud security through collaborative efforts among cloud providers. This strategy promotes a cooperative approach to security, potentially leading to more robust defense mechanisms. The main advantage is the innovative use of game theory in security, while a disadvantage is the complexity of coordinating among multiple entities with potentially conflicting interests.

V. Conclusion

In conclusion, this review underscores the critical importance of evolving and adapting security strategies in cloud computing environments. With the proliferation of virtualized infrastructures and hybrid cloud models, ensuring secure virtual machine operation, seamless migration, and trustworthy communication has become more pressing than ever. The review reveals a significant progression in methodologies—from conventional cryptographic techniques to cutting-edge blockchain-based and identity-based frameworks—each offering unique benefits and trade-offs. However, many solutions introduce complexity, computational overhead, or scalability challenges. As cloud services continue to expand, future research must prioritize lightweight, automated, and intelligent security solutions that balance performance, scalability, and privacy. Embracing innovations such as AI-driven security monitoring, decentralized audit mechanisms, and context-aware adaptive protocols will be crucial in fortifying the next generation of cloud systems.

REFERENCES

[1] J. Dean, G. S. Corrado, R. Monga, "Large scale distributed deep networks", Proc. Int. Conf. Neural Inf. Process. Syst, pp. 1223- 1231, 2013.
[2] M. Li, "Scaling distributed machine learning with the parameter server", Proc. Int. Conf. Big Data Sci. Comput. (BigDataSci), pp. 583-598, 2014.
[3] Z. Li, A. Smola, "Parameter server for distributed machine learning", Proc. Big Learn. NIPS Workshop, pp. 1-10, 2013.
[4] C. Wang, S. S. M. Chow, Q. Wang, "Privacy-preserving public auditing for secure cloud storage", IEEE Trans. Comput., vol. 62, no. 2, pp. 362-375, Dec. 2013.
[5] H. Yan, J. Li, J. Han, Y. Zhang, "A novel efficient remote data possession checking protocol in cloud storage", IEEE Trans. Inf. Forensics Security, vol. 12, no. 1, pp. 78-88, Jan. 2017.
[6] M. Sookhak, F. R. Yu, A. Y. Zomaya, "Auditing big data storage in cloud computing using divide and conquer tables", IEEE Trans. Parallel Distrib. Syst., vol. 29, no. 5, pp. 999-1012, May 2018.
[7] H. Zhao, X. Yao, X. Zheng, T. Qiu, H. Ning, "User stateless privacy-preserving TPA auditing scheme for cloud storage", J. Netw. Comput. Appl., vol. 129, pp. 62-70, Mar. 2019.
[8] H. Wang, "Identity-based distributed provable data possession in multicloud storage", IEEE Trans. Services Comput., vol. 8, no. 2, pp. 328-340, Mar. 2015.
[9] Hussain A A, R. Subashini, "Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud", IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1165- 1176, Jan. 2019.
[10] J. Zhang, Q. Dong, "Efficient ID-based public auditing for the outsourced data in cloud storage", Inf. Sci., vol. 343, pp. 1-14, May 2016.
[11] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage", IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767-778, Apr. 2017.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

[12] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage", IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331-346, Feb. 2019.

[13] H. Zhu, Y. Yuan, Y. Chen, Y. Zha, W. Xi, B. Jia, Y. Xin, "A secure and efficient data integrity verification scheme for cloud- IoT based on short signature", IEEE Access, vol. 7, pp. 90036- 90044, 2019.

[14] K. He, C. Huang, J. Shi, J. Wang, "Public integrity auditing for dynamic regenerating code-based cloud storage", Proc. IEEE Symp. Comput. Commun. (ISCC), pp. 581-588, Jun. 2016.

[15] C. Yu, L. Zhang, W. Zhao and S. Zhang, "A blockchain-based service composition architecture in cloud manufacturing", International Journal of Computer Integrated Manufacturing, pp. 1-15, 2019.

[16] C. Yang, X. Chen and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage", Journal of Network and Computer Applications, vol. 103, pp. 185-193, 2018.

[17] Y. Zhang, C. Xu, X. Lin and X.S. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors", IEEE Transactions on Cloud Computing, 2019.

[18] S. Zhang, H. Wang and W. Huang, "Two-stage plant species recognition by local mean clustering and Weighted sparse representation classification", Cluster computing, vol. 20, no. 2, pp. 1517-1525, 2017.

[19] Y. Zhang, C. Xu, J. Ni, H. Li and X.S. Shen, "Blockchain- assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage", IEEE Transactions on Cloud Computing, 2019.

[20] H.W. Kim and Y.S. Jeong, "Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain", Human-centric Computing and Information Sciences, vol. 8, no. 1, pp. 11, 2018.

[21] H. Li, H. Tian, F. Zhang and J. He, "Blockchain-based searchable symmetric encryption scheme", Computers & Electrical Engineering, vol. 73, pp. 32-45, 2019.

[22] Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., Warfield, A.: Xen and the art of virtualization. In: Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles (SOSP19), pp. 164–177. ACM Press (2003)

[23] Clark, C., Fraser, K., Hand, S., Hansen, J.G., Jul, E., Limpach, C., Pratt, I., Warfield, A.: Live migration of virtual machines. In: Proceedings of NSDI, pp. 273–286. USENIX Association, Berkely (2005)

[24] Padala, P., Zhu, X., Wang, Z., et al.: Performance evaluation of virtualization technologies for server consolidation. Virtualiz. VMware ESX Serv. 9, 161–196 (2007).

[25] Murugesan, S.: Harnessing green IT: principles and practices. In: Proceeding of IT Professional, vol. 10, pp. 24–33. IEEE Computer Society (2008)

[26] Djenna, A., Batouche, M.: Security problems in cloud infrastructure. In: The 2014 International Symposium on Networks, Computers and Communications, pp. 1–6. IEEE (2014)

[27] Ristenpart, T., Tromer, E., Shacham, H., et al.: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: CCS Conference, pp. 199–212 (2009)

[28] Fan, W., Kong, B., Zhang, Z.J., Wang, T.T., Zhang, J., Huang, W.Q.: Security protection model on live migration for KVM virtualization. J. Softw. 27(6), 1402–1416 (2016). (in Chinese)

[29] Oberheide, J., Cooke, E., Jahanian, F.: Empirical exploitation of live migration of virtual machines. In: Black Hat DC Briefings, Westin Washington DC City Center (2008)

[30] Yamunadevi, L., Aruna, P., Sudha, D.D., et al.: Security in virtual machine live migration for KVM. In: 2011 International Conference on Process Automation, Control and Computing (PACC), pp. 1–6. IEEE (2011)

[31] Fan, W., Huang, W.Q., Jiang, F., Liu, C., Lv, B., Wang, R.R.: Research on security of memory leakage in live migration based virtualization. In: Twenty-Fourth National Conference on Information Security (IS 2014), vol. 09, pp. 12–17 (2014)

[32] Dawoud, W., Takouna, I., Meinel, C.: Infrastructure as a service security: challenges and solutions. In: The 7th International Conference on Informatics and Systems (INFOS), pp. 1–8 (2010)

[33] Anala, M.R., Shetty, J., Shobha, G.: A framework for secure live migration of virtual machines. In: 2013 International Conference on IEEE Advances in Computing, Communications and Informatics (ICACCI), pp. 243–248 (2013)

[34] S. Biedermann, M. Zittel and S. Katzenbeisser. Improving Security of Virtual Machines during Live Migrations. Eleventh Annual Conference on Privacy, Security and Trust (PST). 2013.

 ISSN : 2455-9679
SJIF Impact Factor : 6.008

[35] A. Back, U. Mller, and A. Stiglic. Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems. Information Hiding, volume 2137 of Lecture Notes in Computer Science, page 245-257. Springer, 2001.
[36] J. Oberheide, E. Cooke, F. Jahanian.Empirical Exploitation of live migration of virtual machines. Proc of Black Hat DC, March 24, 2008.
[37] M. Aiash, G. Mapp and O. Gemikonakli, "Secure Live Virtual Machines Migration: Issues and Solutions," 2014 28th International Conference on Advanced Information Networking and Applications Workshops, Victoria, BC, Canada, 2014.
[38] S. An, A. Leung, J. B. Hong, T. Eom and J. S. Park, "Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security," in IEEE Access, vol. 10, pp. 75117-75134, 2022.
[39] J. Luna, A. Taha, R. Trapero and N. Suri, "Quantitative Reasoning about Cloud Security Using Service Level Agreements," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 457-471, 1 July-Sept. 2017.
[40] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 523-536, 1 July-Sept. 2017.
[41] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang and D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," in IEEE Access, vol. 7, pp. 9368-9383, 2019.
[42] T. Halabi and M. Bellaiche, "Towards Security-Based Formation of Cloud Federations: A Game Theoretical Approach," in IEEE.