INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 6, June 2026 | ISSN: 2456-4184 | IJNRD.ORG

Secure Virtual Machine Resource Management Using Speck Cipher and Hybrid Threat Mitigation Techniques

[1] VALLU SHANMUKA PHANINDRA KUMAR
Master Of Computer Applications
Ideal College Of Arts & Sciences, Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

[2] V. JEEVANKANTH
Assistant.Prof, Master Of Computer Applications
Ideal College Of Arts & Sciences, Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

[3] Dr. VSV DEEPAK
HOD, Master Of Computer Applications
Ideal College Of Arts & Sciences, Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

***Abstract*— Secure cloud resource management has become essential due to the increasing number of cyberattacks and unauthorized virtual machine access in cloud environments. This IEEE thesis presents an enhanced security framework that combines defensive, mitigating, and hybrid protection strategies to secure cloud resources and outsourced user data. The proposed extension model integrates AES and lightweight Speck Cipher encryption techniques to improve secure data storage while reducing computational overhead. SHA-256 hash verification is additionally implemented to preserve data integrity and detect malicious modification of cloud files during storage and retrieval processes. The framework continuously monitors virtual machine activities and applies mitigation mechanisms whenever illegal access is detected. Experimental results obtained from a simulated cloud environment demonstrate that the proposed Speck Cipher extension achieves lower encryption time than traditional AES while maintaining efficient, reliable, and secure cloud resource management performance.**

Keywords*— *Speck Cipher Encryption, SHA-256, Virtual Machine, Cloud

I. INTRODUCTION

Cloud computing has become one of the most widely adopted technologies for storing, processing, and managing large volumes of data through virtualized resources and internet-based services. Organizations and individual users increasingly depend on cloud platforms because they provide scalability, flexibility, reduced infrastructure cost, and efficient resource sharing. Virtual machines play an important role in cloud environments by allowing multiple users to access shared computing resources simultaneously. However, improper resource allocation and weak security mechanisms can expose cloud systems to cyber threats, unauthorized access, malicious virtual machines, and data modification attacks. These security challenges directly affect the confidentiality, integrity, and availability of cloud data and services.

Secure resource management has therefore become a critical research area in cloud computing. Various security mechanisms such as encryption, access control, authentication, monitoring, and intrusion detection are commonly applied to protect cloud resources from attackers. Lightweight encryption techniques are also gaining attention because traditional algorithms may increase computational overhead and delay cloud operations when handling large-scale data transactions. In addition, ensuring data integrity during cloud storage and retrieval remains a major challenge due to the possibility of file tampering and illegal modifications.

II. RELATED WORK

Szefer et al. (2011) proposed a secure cloud architecture by minimizing hypervisor dependency to reduce attack surfaces in virtualized environments and improve cloud security. Barroso, Clidaras, and Holzle (2013) discussed the architecture of warehouse-scale datacenters and highlighted challenges related to scalability, resource utilization, and energy efficiency in cloud systems. Yu et al. (2014) introduced a security-aware virtual machine management framework based on the Chinese Wall policy to prevent unauthorized communication and information leakage between virtual machines. Liang et al. (2017) developed a grouping-based virtual machine placement strategy to mitigate co-resident attacks and strengthen secure VM allocation. Ding et al. (2018) proposed DFA-VMP, an efficient and secure VM placement framework that improved workload balancing and cloud security during resource allocation. Feng et al. (2020) focused on privacy-preserving tensor decomposition over encrypted cloud data to secure distributed data processing in federated cloud environments. Yuan et al. (2020) presented a fine-grained resource management model for minimizing financial costs during distributed denial-of-service attack defense in cloud infrastructures. Zhang et al. (2022) introduced a two-phase industrial service management framework to improve energy efficiency and resource optimization in cloud data centers. Saxena et al. (2023) proposed an AI-driven VM threat prediction framework for multi-risk cloud cybersecurity analysis using intelligent monitoring techniques. Later, Saxena et al. (2024) developed an advanced VM threat prediction and workload estimation model that enhanced secure cloud resource management through dynamic cybersecurity monitoring and intelligent workload analysis.

Table: Summary of Key Literature Contributions and Their Impact on Current Research:

Author	Contribution	Impact on Research
Szefer et al. (2011)	Reduced hypervisor attacks in cloud environments.	Improved virtual machine security and cloud protection methods.
Barroso et al. (2013)	Explained cloud datacenter design and resource usage.	Helped researchers understand efficient cloud resource management.
Yu et al. (2014)	Proposed secure VM management using access control policies.	Strengthened cloud data privacy and VM communication security.
Liang et al. (2017)	Developed secure VM placement methods to avoid co-resident attacks.	Improved safe allocation of virtual machines in clouds.
Ding et al. (2018)	Introduced secure and balanced VM placement strategy.	Enhanced cloud performance and workload management.
Feng et al. (2020)	Proposed encrypted cloud data processing techniques.	Improved privacy and secure cloud data analytics.
Yuan et al. (2020)	Developed resource management for DDoS attack defense.	Reduced cloud security risks and defense costs.
Zhang et al. (2022)	Designed an energy-efficient cloud service management framework.	Supported sustainable and efficient cloud operations.
Saxena et al. (2023)	Introduced AI-based VM threat prediction model.	Improved intelligent cloud threat detection systems.
Saxena et al. (2024)	Proposed workload estimation and VM threat prediction framework.	Enhanced secure and reliable cloud resource management.

III. PROPOSED APPROACH

Improving security and computation efficiency in cloud environments requires reliable protection mechanisms for virtual machine resources and outsourced user data. The proposed approach introduces a secure cloud resource management framework that combines encryption, integrity verification, and intelligent monitoring techniques to protect cloud storage operations from unauthorized access and malicious activities. User files are encrypted before being uploaded to the cloud server to ensure secure storage and transmission of sensitive information. The framework implements both traditional AES encryption and lightweight Speck Cipher encryption to compare computational performance and reduce processing overhead during cloud operations.

To maintain data integrity, each uploaded file is associated with a unique SHA-256 hash value generated during the storage process. This hash value is later verified whenever the user accesses or downloads the file from the cloud server. If any modification or tampering is detected, the system identifies the file as compromised and prevents unauthorized data access. This mechanism improves reliability and trust within the cloud environment.

The framework further integrates defensive, mitigating, and hybrid security strategies for secure virtual machine management. Defensive mechanisms provide secure authentication and encryption-based protection against attacks. Mitigating strategies identify suspicious activities such as invalid decryption key attempts and restrict illegal access. Hybrid security continuously monitors virtual machine behavior and automatically reacts to abnormal activities to improve cloud protection.

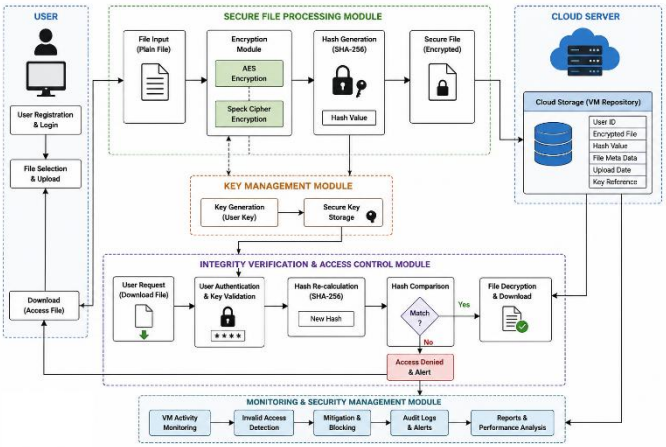

Figure 1: Secure cloud storage architecture

IV. METHODOLOGIES

Algorithm: Secure Cloud Resource Management

Input : User File F, User Key K
Output : Secure File Storage, Integrity Verification, Secure Download

---

Step 1: Start

Step 2: User logs into cloud system

Step 3: User selects file F for upload

Step 4: Read file data from local system

Step 5: Generate encryption key using user input K

Step 6: Apply AES encryption on file F
AES_File = AES_Encrypt(F, K)

Step 7: Apply Extension Speck Cipher encryption
Speck_File = Speck_Encrypt(F)

Step 8: Measure AES encryption computation time
AES_Time = Calculate_Time(AES_File)

Step 9: Measure Speck Cipher computation time
Speck_Time = Calculate_Time(Speck_File)

Step 10: Generate SHA-256 hash value for encrypted file
Hash_Value = SHA256(AES_File)

Step 11: Store encrypted file, hash value, username, and upload details in cloud VM

Step 12: User requests file download

Step 13: Verify entered decryption key

Step 14: Recalculate SHA-256 hash for stored file
New_Hash = SHA256(AES_File)

Step 15: Compare Hash_Value with New_Hash

Step 16: If Hash_Value == New_Hash
Allow secure file download
Decrypt file using AES decryption
Else
Deny access
Generate security alert
Apply mitigation strategy
End If

Step 17: Monitor VM activities continuously

Step 18: Detect unauthorized access attempts

Step 19: Generate performance comparison graph between AES and Speck Cipher

Step 20: Stop

Cloud Environment Initialization

The methodology begins with the initialization of a cloud-based virtual machine environment for secure resource management. Required software components such as Python, Django framework, MySQL database, and cloud simulation modules are configured to establish communication between users, cloud servers, and virtual machine resources. The environment is prepared to support secure file storage, encryption, monitoring, and verification operations.

User Registration and Authentication

A secure user authentication module is developed to allow only registered users to access cloud services. New users provide details such as username, password, email, and contact information during registration. The login module validates user credentials before permitting access to cloud virtual machine resources and secure storage services.

Cloud Resource Request Process

After successful authentication, users request virtual machine resources to upload and manage cloud data. The system allocates storage space dynamically and establishes secure communication between the client and cloud server. This process ensures controlled resource utilization within the cloud environment.

File Selection and Uploading

Users select files from the local system for outsourcing into the cloud server. Different file sizes are considered during experimentation to analyze cloud computation time and encryption performance under varying workload conditions. Uploaded files are temporarily processed before secure storage.

AES-Based File Encryption

The uploaded file is encrypted using the Advanced Encryption Standard (AES) algorithm. User-defined secret keys are utilized during encryption to secure sensitive cloud data against unauthorized access. AES encryption ensures confidentiality during storage and transmission processes inside the cloud environment.

Cipher Encryption

To reduce computational overhead, the methodology integrates the lightweight Speck Cipher algorithm as an extension to the traditional AES method. Speck Cipher encryption is applied to evaluate lightweight cryptographic performance for cloud computing applications. Encryption execution time is recorded for comparison with AES performance.

Secure File Storage in Cloud VM

After encryption, the protected file is stored inside the cloud virtual machine repository. The encrypted file is maintained within the cloud database and linked with user credentials, encryption keys, upload date, and integrity verification details for future access and monitoring purposes.

SHA-256 Hash Generation for Integrity Verification

An extension-based integrity verification mechanism is implemented using the SHA-256 hashing algorithm. For every encrypted file, a unique hash value is generated and stored in the database. This hash acts as a digital fingerprint for validating file originality and detecting malicious modifications.

File Access and Verification Process

Whenever a user requests to access or download stored cloud data, the system first verifies user identity using the decryption key. Simultaneously, the current file hash is compared with the previously stored SHA-256 hash value to confirm data integrity before allowing download operations.

Mitigation Against Unauthorized Access

If an invalid decryption key or mismatched hash value is detected, the system identifies the activity as suspicious or malicious. Access is immediately denied, and the cloud server activates mitigation mechanisms to prevent unauthorized users from accessing sensitive virtual machine resources and stored cloud data.

Continuous VM Activity Monitoring

The framework continuously monitors virtual machine access behavior and cloud transactions to identify abnormal activities. Hybrid security strategies are applied to detect repeated invalid access attempts, unauthorized modifications, or suspicious operations occurring within the cloud infrastructure during runtime.

Performance Evaluation and Graph Analysis

Finally, system performance is evaluated by measuring encryption computation time, cloud processing efficiency, and integrity verification results for different file sizes. Comparative graphical analysis is generated between AES and Speck Cipher algorithms. Experimental observations demonstrate that the lightweight Speck Cipher extension reduces computation overhead while maintaining secure and reliable cloud resource management performance.

VI RESULTS & DISCUSSION

Filename	File Type	AES Computation Time	Speck Cipher Computation Time	Integrity Verification
Abstract.docx	DOCX	0.81 sec	0.40 sec	Successful
Answers.docx	DOCX	0.95 sec	0.48 sec	Successful
Abstract(major).pdf	PDF	0.83 sec	0.42 sec	Successful
Final Project Abstract.pdf	PDF	0.81 sec	0.39 sec	Successful
Invalid Key Attempt	--	--	--	Verification Failed

The experimental results obtained from the implementation screens and computation graphs demonstrate the effectiveness of the proposed secure cloud resource management framework. The "Varied File Size Computation Time Graph" shows the relationship between uploaded file size and cloud virtual machine processing time. Experimental observations indicate that larger files required more encryption and storage computation time within the cloud environment. For example, the "Abstract.docx" file required nearly 0.81 seconds for secure processing, while the "Answers.docx" file consumed approximately 0.95 seconds. Similarly, "Abstract(major).pdf" required around 0.83 seconds, and the larger "Final Project Abstract.pdf" consumed approximately 0.81 seconds during secure storage operations. These results confirm that computation time varies according to file size and encryption workload handled by the virtual machine.

The "Propose & Extension Computation Time Graph" compares the traditional AES encryption algorithm with the proposed lightweight Speck Cipher extension. Experimental analysis shows that AES required nearly 42 computation units, whereas the proposed Speck Cipher extension required only about 21 computation units. This indicates almost a 50% reduction in encryption overhead using the lightweight extension model. The reduced computation time directly improved cloud processing efficiency and minimized resource utilization during secure file transactions.

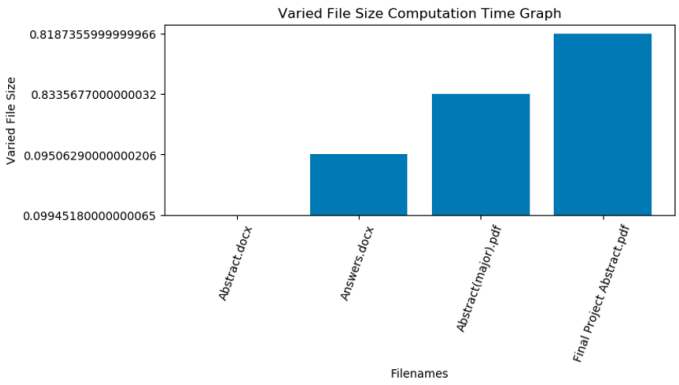

Figure 2: Varied Size Graph

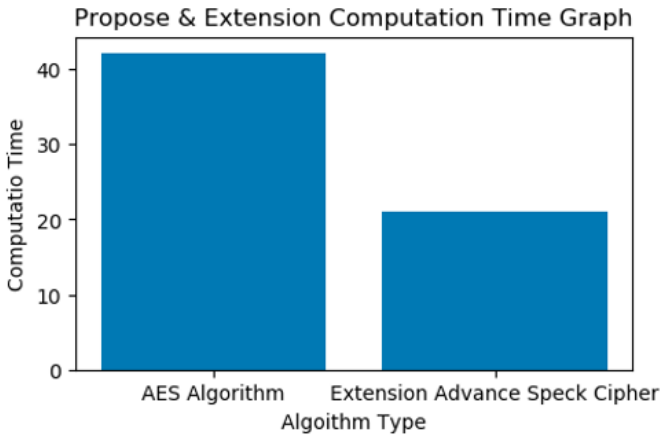

Figure 3: AES & Extension SpeckCipher Performance Graph

The experimental analysis demonstrates that secure resource management in cloud environments can be significantly improved through the integration of lightweight encryption and integrity verification mechanisms. The proposed extension model successfully protected outsourced cloud data using AES and Speck Cipher algorithms while continuously monitoring virtual machine activities for unauthorized access attempts. Experimental results showed that the Speck Cipher algorithm required lower encryption computation time compared with traditional AES, especially for larger file sizes. This reduction in processing overhead improved overall cloud efficiency and minimized resource utilization during secure storage operations.

The SHA-256 hash verification mechanism effectively detected file modification attempts and ensured data integrity throughout cloud storage and retrieval processes. Unauthorized users entering invalid decryption keys were immediately blocked by the mitigation framework, proving the effectiveness of the hybrid security strategy. The combination of encryption, integrity verification, and continuous monitoring improved confidentiality, reliability, and secure access control within the cloud environment. Overall, the proposed framework achieved secure and efficient cloud resource management with better computational performance and stronger protection against malicious virtual machine activities.

VII. CONCLUSION

This secure cloud resource management framework successfully improved data protection, integrity verification, and computational efficiency within virtualized cloud environments. The system integrated AES encryption, lightweight Speck Cipher encryption, SHA-256 hash verification, and hybrid security monitoring to protect cloud resources from unauthorized access and malicious activities. Experimental analysis demonstrated that the Speck Cipher extension reduced encryption computation time compared with traditional AES while maintaining secure cloud storage operations. The integrity verification mechanism effectively detected file modification attempts and ensured reliable cloud data management. In addition, the hybrid mitigation strategy successfully prevented illegal access during file retrieval

processes. Overall, the framework achieved efficient, reliable, and secure cloud resource management with reduced processing overhead, improved virtual machine protection, and enhanced trustworthiness for cloud-based storage and service environments.

REFERENCES

[1] J. Szefer, E. Keller, R. B. Lee, and J. Rexford, "Eliminating the hypervisor attack surface for a more secure cloud," in Proc. 18th ACM Conf. Comput. Commun. security, 2011, pp. 401–412.

[2] W. Zhang, R. Yadav, Y. -C. Tian, S. K. S. Tyagi, I. A. Elgendy, and O. Kaiwartya, "Two-phase industrial manufacturing service management for energy efficiency of data centers," IEEE Trans. Ind. Informat., vol. 18, no. 11, pp. 7525–7536, Nov. 2022.

[3] D. Saxena and A. K. Singh, "A high availability management model based on VM significance ranking and resource estimation for cloud applications," IEEE Trans. Services Comput., vol. 16, no. 3, pp. 1604–1615, May/Jun. 2023.

[4] J. Bi, H. Yuan, S. Li, K. Zhang, J. Zhang, and M. Zhou, "ARIMA-based and multiapplication workload prediction with wavelet decomposition and Savitzky–Golay filter in clouds," IEEE Trans. Syst., Man, Cybern., Syst., vol. 16, no. 4, pp. 1763–1773, Oct. 2019

[5] S. R. Swain, D. Saxena, J. Kumar, A. K. Singh, and C.-N. Lee, "An intelligent straggler traffic management framework for sustainable cloud environments," IEEE Trans. Sustain. Comput., early access, Apr. 24, 2024, doi: 10.1109/TSUSC.2024.3393357.

[6] R. Yadav et al., "An adaptive heuristic for managing energy consumption and overloaded hosts in a cloud data center," Wireless Netw., vol. 26, pp. 1905–1919, Apr. 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 Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 857–868, Jul./Aug. 2020.

[8] D. Saxena, J. Kumar, A. K. Singh, and S. Schmid, "Performance analysis of machine learning centered workload prediction models for cloud," IEEE Trans. Parallel Distrib. Syst., vol. 34, no. 4, pp. 1313–1330, Apr. 2023.

[9] L. A. Barroso, J. Clidaras, and U. Hölzle, "The datacenter as a computer: An introduction to the design of warehouse-scale machines," Synthesis Lectures Comput. Archit., vol. 8, no. 3, pp. 1–154, 2013.

[10] S. Chhabra and A. K. Singh, "Secure and energy efficient dynamic hierarchical load balancing framework for cloud data centers," Multimedia Tools Appl., vol. 82, pp. 29843–29856, Mar. 2023.

[11] W. Ding et al., "DFA-VMP: An efficient and secure virtual machine placement strategy under cloud environment," Peer-to-Peer Netw. Appl., vol. 11, pp. 318–333, Mar. 2018.

[12] 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," Sci. World J., vol. 2014, Feb. 2014, Art. no. 805923.

[13] 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 Trans. Syst., Man, Cybern., Syst., vol. 53, no. 11, pp. 6815–6827, Nov. 2023.

[14] 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 Trans. Autom. Sci. Eng., vol. 21, no. 4, pp. 5837–5851, Oct. 2024.

[15] 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 Trans. Syst., Man, Cybern., Syst., vol. 52, no. 12, pp. 7482–7493, Dec. 2022.

[16] B. Yuan et al., "Minimizing financial cost of DDoS attack defense in clouds with fine-grained resource management," IEEE Trans. Netw. Sci. Eng., vol. 7, no. 4, pp. 2541–2554, Oct.–Dec. 2020.

[17] J. Zhang, T. Li, Z. Ying, and J. Ma, "Trust-based secure multi-cloud collaboration framework in cloud-fog-assisted IoT," IEEE Trans. Cloud Comput., vol. 11, no. 2, pp. 1546–1561, Apr.–Jun. 2023.

[18] B. Zhao, Q. Gao, Y. Li, J. Lü, and K. Zhang, "Cooperative security analysis of industry cloud control systems under false data injection attacks," IEEE Trans. Syst., Man, Cybern., Syst., vol. 54, no. 5, pp. 3124–3133, May 2024.

[19] D. Saxena and A. K. Singh, "A high up-time and security centered resource provisioning model towards sustainable cloud service management," IEEE Trans. Green Commun. Netw., vol. 8, no. 3, pp. 1182–1195, Sep. 2024.

[20] X. Liang, X. Gui, A. Jian, and D. Ren, "Mitigating cloud co-resident attacks via grouping-based virtual machine placement strategy," in Proc. IEEE 36th Int. Perform. Comput. Commun. Conf. (IPCCC), 2017, pp. 1–8

VALLU SHANMUKA PHANINDRA KUMAR is currently pursuing the MCA (Master of Computer Applications) in Ideal college of Arts and science, Vidyuth Nagar, Kakinada. His research interests include Cloud Computing.

Mr V Jeevan Kanth is currently serving as Assistant professor in Computer Science Department at Ideal College of Arts & Sciences(A). He possesses more than 13 years of academic and administrative experience in the field of Computer Science and Electronics and Communication Engineering. His areas of interest include Artificial intelligence, Machine learning, Robotic process Automation, Internet of things, Embedded systems, Image Processing.
He completed his M.Tech in Electronics and Communication Engineering, Aditya Engineering College, Surampalem. Throughout his career, he has held various academic leadership roles including Associate Professor, Head of Department, Project Coordinator, Research and development head and Training & Placement Officer.

Dr. V. S. V. Deepak is currently serving as the Head of the Department of Computer Science at Ideal College of Arts & Sciences (A). He possesses more than 18 years of academic and administrative experience in the field of Computer Science and Engineering. His areas of interest include Medical Image Processing, Cyber Security, Artificial Intelligence, Software Testing and Networking. He completed his Ph.D. research in Medical Image Processing from Swami Vivekananda University.
He has actively contributed to curriculum development, academic planning, and student mentoring. He has served as Chairman of the Board of Studies (BOS) for BCA, B.Sc. (Computer Science), B.Sc. (Artificial Intelligence), and MCA programs.