IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305315 |

Data Protection from APT Using Homomorphic Linear Authenticator (HLA) in Cloud Computing

Dharani G, Thirumurugan T, Bharathkumar S, Balaji S

Department of Information Technology, K. S. R College of Engineering, Tiruchengode, India

ABSTRACT: The paper presents a novel approach for data protection against Advanced Persistent Threats (APTs) in cloud computing environments, leveraging Homomorphic Linear Authenticator (HLA) technology. HLA enables secure authentication and verification of data integrity while preserving confidentiality through homomorphic encryption schemes. By employing HLA, cloud service providers and users can ensure the confidentiality, integrity, and authenticity of data even in the presence of APTs. The paper outlines the architecture and functionality of the proposed HLA-based system for data protection in the cloud, discussing key components such as homomorphic encryption algorithms, authentication mechanisms integrated via HLA, and protocols for verifying data integrity in a cloud environment. It also presents a comprehensive analysis of the proposed approach's efficacy in mitigating APTs' threats compared to traditional security measures and evaluates the performance overhead incurred by HLA in terms of computational complexity and communication overhead. The research contributes to the advancement of cloud security by introducing a robust solution for safeguarding sensitive data from APTs, enhancing trust and confidence in cloud computing infrastructures.

KEYWORDS: Data protection, Cloud computing, HLA, Protection, Homomorphic.

I. INTRODUCTION

The paper discusses the importance of data protection in the digital age, particularly in the context of cloud computing. The rise of APTs has raised concerns about security vulnerabilities, particularly in the face of sophisticated threats. The integration of Homomorphic Linear Authenticator (HLA) as a defense mechanism offers a solution, allowing data to be authenticated without revealing its content. This paper explores the benefits of HLA, including preserving data privacy and integrity, and thwarting unauthorized access attempts. It provides a comprehensive analysis of the synergy between HLA and cloud computing, aiming to provide a holistic understanding of how organizations can strengthen their data protection strategies against APTs. By leveraging HLA's cryptographic capabilities, businesses can maintain the confidentiality, integrity, and availability of their critical data assets, fostering trust and resilience in the digital ecosystem. The paper concludes that HLA deployment is a pivotal advancement in data protection, offering a potent defense against APTs within cloud computing. It not only strengthens organizations' security posture but also boosts confidence in the reliability and integrity of cloud-based operations in a hostile cyber landscape.

.

A. Linear Authenticator

Linear authenticators are cryptographic techniques used to verify the integrity of data. They generate a short authentication tag or signature based on the content of the data. This tag can then be used to verify whether the data has been tampered with or altered in any way. Linear authenticators are particularly useful in cloud computing environments where datamay be stored across multiple servers or transmitted over networks, as they provide a means of ensuring data integrity throughout its lifecycle.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305315 |

B. Homomorphic Encryption

Homomorphic encryption is a technique that allows computations to be performed on encrypted data without decrypting it first. This means that data can remain encrypted while still undergoing various computations, preserving its confidentiality. In the context of data protection from APTs, homomorphic encryption ensures that even if attackers gain accessto the encrypted data, they cannot decipher its contents without the appropriate decryption keys.

C. Combining HLA in cloud computing

Combining Homomorphic Linear Authenticator (HLA) in cloud computing for data protection against Advanced Persistent Threats (APTs) represents a sophisticated approach to safeguarding sensitive data in the digital realm. This amalgamation leverages the strengths of both homomorphic encryption and linear authentication to create a robust security framework. Homomorphic encryption allows computations to be performed on encrypted data without the need for decryption, ensuring data confidentiality even during processing. Meanwhile, linear authenticators generate authentication tags based on data content, facilitating integrity verification without compromising confidentiality. By integrating HLA techniques, organizations can ensure that their data remains secure from APTs throughout its lifecycle in the cloud.

II. LITERATURE REVIEW

[1] The "A Review of APT Attack Detection Methods and Defense Strategies" provides an in-depth analysis of techniques used to identify and mitigate Advanced Persistent Threats (APTs), including methods like anomaly detection and signature-based detection, and their effectiveness varies depending on implementation environment and resources.

[2 The study examines the impact of feature selection and normalization on network intrusion detection performance. Featureselection reduces dimensionality and improves model performance, while normalization ensures uniformity and better model convergence. However, inappropriate normalization can distort data distribution and affect model accuracy, making understanding these interplays crucial for optimizing intrusion detection systems.

[3] The study explores the impact of feature selection and normalization techniques on network intrusion detection systems. Feature selection reduces the dimensionality of the dataset by identifying relevant features, improving model efficiency and predictive capabilities. Normalization ensures uniformity in data by scaling values to a standard range, facilitating better convergence during machine learning model training. It prevents certain features from dominating the model training process due to larger scales. However, the study also highlights the potential drawbacks of inappropriate normalization techniques, which can distort data distribution and lead to inaccuracies in model predictions. Therefore, understanding the interplay between feature selection and normalization is crucial for optimizing intrusion detection systems. By carefully selecting relevant features and applying appropriate normalization techniques, researchers and practitioners can develop more robust and accurate models for identifying and mitigating cybersecurity threats effectively.

[4] The text discusses the use of graph databases and machine learning techniques for anomaly detection in log data to combatadvanced persistent threats (APTs). It highlights the benefits of graph databases for comprehensive analysis and machine learning algorithms for identifying APT patterns. However, challenges like scalability and continuous updates may arise. Despite these, the integration offers a promising strategy for cybersecurity defenses.

[5] The text discusses the use of Support Vector Machine (SVM) in detecting and classifying Advanced Persistent Threats (APTs) and attacks. SVM's robustness and accuracy in distinguishing malicious and benign activities enable proactive defensemeasures against cyber threats. However, drawbacks include the need for large datasets and potential misclassification errors in complex threat landscapes. Despite these, SVM offers a promising approach to enhance cybersecurity defenses..

[6] The Cyber Kill Chain approach is a cybersecurity method that breaks down the stages of a cyberattack into sequential steps, enabling security teams to identify and mitigate threats more effectively. It provides a structured framework for understandingand responding to attacks, enabling organizations to proactively defend against Advanced Persistent Threats (APTs). However,it may not be suitable for all types of attacks and may require significant resources and expertise. Overall, it should be complemented by other strategies for comprehensive protection against evolving threats.

[7] A network intrusion detection system (NIDS) based on machine learning for software-defined networks can

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305315 |

detect and respond to security threats in real-time using advanced algorithms. This system can adapt to new network behavior patterns, enhancing its effectiveness in identifying and mitigating cyber threats. However, it faces challenges such as potential false positives, the complexity of machine learning algorithms, and the need to ensure data privacy and security to prevent potentialvulnerabilities and attacks on the system.

[8] The study "Efficient Detection of Hacker Communities Based on Twitter Data Using Complex Networks and Machine Learning Algorithm" uses complex network analysis and machine learning algorithms to identify hacker communities on Twitter. This approach leverages the interconnected structure of Twitter data to detect hidden relationships among users involved in hacking activities. However, potential drawbacks include data privacy issues, algorithmic biases, and the dynamicnature of hacker behavior.

[9] Advanced Persistent Threats (APTs) are sophisticated cyber attacks launched by skilled adversaries to infiltrate and remainundetected within targeted systems. Their stealthy nature makes them difficult to detect and mitigate using traditional security measures. APT campaigns involve meticulous planning, reconnaissance, and tailored attacks to exploit specific vulnerabilities. However, prolonged presence can result in severe data breaches, financial losses, and reputational damage. APTs also pose a challenge of attribution, as attackers often use techniques to obfuscate their identities. Despite these challenges, attribution is crucial for understanding the motives behind APT campaigns and implementing effective cybersecurity measures to defend against future attacks.

[10] The text discusses the use of machine learning algorithms in identifying cybersecurity attacks by analyzing network features. It suggests that this method can efficiently detect potential threats, enhancing organizations' security measures. However, it also highlights the challenges and limitations of this method. The complexity of analyzing diverse network features requires sophisticated algorithms and techniques, while building robust models can be resource-intensive and technically demanding. False positives, where the system incorrectly identifies benign activities as threats, can lead to unnecessary alerts and operational disruptions. Cyber attackers constantly evolve their techniques to evade detection, posing a constant challengefor cybersecurity professionals. Adapting to these evolving tactics requires ongoing research, innovation, and updates to detection systems. The text concludes that while machine learning has immense potential, addressing the complexities, limitations, and challenges associated with its implementation is crucial for its effectiveness in real-world scenarios. This requires developing advanced algorithms, refining detection methodologies, and staying vigilant against emerging threats in the ever-evolving cybersecurity landscape.

III. EXISTING SYSTEM

The project focuses on detecting advanced persistent threats (APTs) using machine learning algorithms and behavioral analytics. It uses data from network traffic, system logs, and user behavior to establish baselines for normal network behavior.
Machine learning models are trained on large datasets to recognize subtle patterns and adapt to new threats, ensuring ongoing effectiveness in cybersecurity.

The existing work titled " A novel approach for detecting advanced persistent threats " The system uses behavioral analytics to understand user intent and distinguish between legitimate and malicious activities, enhancing threat detectionaccuracy and reducing false positives. Real-time monitoring and response are crucial, flagging detected threats for further investigation and triggering automated response mechanisms. Human analysts validate alerts and provide context to detected anomalies. This approach represents a significant advancement in APT detection, combining machine learning, behavioral analytics, and real-time monitoring. By continuously evolving to adapt to the changing threat landscape, this project offers a proactive defense againstsophisticated cyber attacks.

This innovative approach to APT detection enhances cybersecurity by utilizing machine learning, anomaly detection, and contextual analysis, thereby enhancing resilience against sophisticated and persistent threats, thus enhancing defenses and mitigating risks in a complex threat landscape.

IV. PROPOSED SYSTEM

The proposed work aims to improve data protection against advanced persistent threats (APTs) in cloud computing by integrating homomorphic linear authentication (HLA) techniques. HLA offers a secure and efficient alternative to traditional cryptographic techniques, ensuring data privacy and integrity. By integrating HLA into cloud-based

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305315 |

authentication protocols, authentication operations can be performed directly on encrypted data, preserving confidentiality and verifying user identities.This eliminates the need to decrypt sensitive information, reducing the risk of data exposure. HLA also facilitates linear operations on encrypted data, enabling efficient processing and scalability in cloud environments, especially for complex

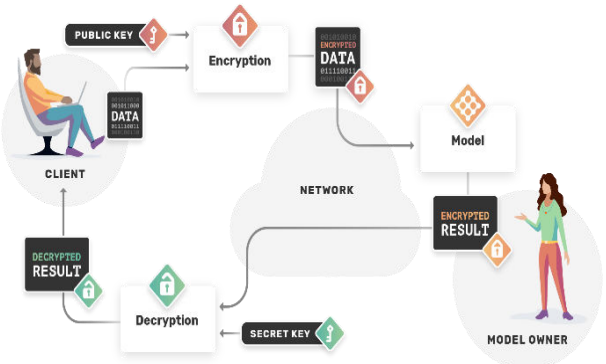

Figure 1 Flow chat of the proposed Design

computations or large datasets. This approach can handle authentication tasks at scale while maintaining stringent security requirements.

The use of HLA enhances data privacy by minimizing the exposure of sensitive information to unauthorized parties. Encrypted data prevents adversaries from gaining insights or exploiting vulnerabilities in transit, reducing attack surface and enhancing authentication resilience against APTs and malicious actors. The proposed approach emphasizes interoperability with existing cloud computing frameworks and authentication protocols, allowing organizations to leverage existing infrastructure without significant modifications or disruptions. This facilitates adoption and deployment across diverse cloud platforms and service providers, making it practical and accessible for organizations of all sizes.

The proposed work enhances data protection against APTs in cloud computing environments by utilizing HLA techniques. This enhances authentication mechanisms with robust security, efficiency, and privacy-preserving capabilities, mitigating APT risks while leveraging cloud computing's scalability and flexibility for enhanced security and resilience.

V. SYSTEM DESIGN SYSTEM

Homomorphic linear authentication (HLA) is a cryptographic technique that protects sensitive data from advanced persistent threats (APTs) in cloud computing environments. It ensures encryption, preventing unauthorized access and allowing computations to be performed directly on encrypted data. HLA enhances cybersecurity by reducing the risk of APTs accessing and exploiting sensitive information. However, implementing HLA requires careful consideration of performance overhead, encryption protocols, and regular security audits.

A. System Architecture

Homomorphic Linear Authentication (HLA) is a method used to protect sensitive data against Advanced Persistent Threats (APTs) in cloud computing systems architecture. HLA combines the principles of homomorphic encryption and linear authentication to ensure data confidentiality and integrity. It enables computations on encrypted data without decryption, ensuring data confidentiality even in the event of a security breach. Linear authentication, on the other hand, provides a scalable and efficient mechanism for verifying data integrity, ensuring data protection against unauthorized modifications or tampering attempts. HLA represents a significant advancement in data protection against APTs in cloud computing systems architecture, enhancing security and safeguarding sensitive information from persistent threats.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305315 |

Homomorphic encryption is the core of HLA, allowing computations to be performed on encrypted data without decryption. This ensures that sensitive data remains confidential even if the cloud infrastructure is compromised. Linear authentication, on the other hand, provides a scalable and efficient mechanism for verifying data integrity. Linear authentication techniques represent authentication processes as linear equations, allowing for rapid and parallelized verification of data integrity.

By combining homomorphic encryption with linear authentication, HLA offers a robust solution for protecting data against APTs in cloud computing systems architecture. Sensitive data can be encrypted before transmission to the cloud, ensuring its confidentiality even in the event of a security breach. Linear authentication mechanisms provide a scalable and efficient means of verifying data integrity, protecting against unauthorized modifications or tampering attempts. Overall, HLA represents a significant advancement in data protection against APTs in cloud computing systems architecture.

B. Linear Authentication

Linear Authentication is a crucial tool in protecting data from Advanced Persistent Threats (APTs) in cloud computing environments. It is based on representing authentication operations as linear equations, enabling efficient and scalable processing across vast datasets. This approach aligns with the scalable nature of cloud computing infrastructures, allowing computations to be performed on encrypted data without decryption. Linear Authentication also offers robust safeguards against unauthorized modifications or tampering attempts, bolstering data integrity. It acts as a sentinel, continuously monitoring data integrity and alerting system administrators to potential security breaches. Combining Linear Authentication with other security measures like intrusion detection systems, access controls, and threat intelligence feeds can create formidable barriers against APTs.

C. Privacy Preservation

Privacy preservation is a crucial aspect of data protection, especially in the face of advanced persistent threats (APTs) targeting cloud computing environments. Homomorphic Linear Authentication (HLA) is a robust solution that prioritizes the confidentiality of sensitive information while ensuring its integrity through authentication processes. HLA's core principle lies in homomorphic encryption, a cryptographic technique that enables computations to be performed on encrypted data without the need for decryption. This ensures that sensitive information remains hidden from unauthorized parties, including cloud service providers and potential attackers.

Normalization techniques are applied to standardize pixel values across images, ensuring consistent brightness and contrast levels. This enhances the model's ability to extract meaningful features from input images

The linear nature of HLA's authentication operations minimizes the exposure of sensitive information during the verification process. It operates on encrypted representations of the data, reducing the risk of privacy breaches or data exposure. HLA's emphasis on privacy extends beyond the authentication phase to the entire data lifecycle within the cloud environment, encrypting data at rest, in transit, and during processing. This comprehensive approach aligns with regulatory requirement

D. Integrity Verification

Integrity verification is a crucial aspect of the Homomorphic Linear Authentication (HLA) data protection approach in cloud computing environments. It ensures data integrity by applying linear authentication techniques, which are efficient and scalable. The process relies on data consistency, establishing a baseline for data integrity to identify deviations and flag unauthorized modifications. HLA's proactive nature allows for continuous monitoring and verification of data integrity in real- time, minimizing security incidents and enhancing resilience against APTs. Integrity verification is essential for maintaining trust in cloud-based systems, particularly in industries like healthcare, finance, and government. It also addresses internal risks, such as inadvertent errors and insider threats. HLA complements other security measures, offering robust protection against various security threats in cloud computing environments. Overall, integrity verification is a vital aspect of HLA's data protection strategy.

HLA's proactive nature allows for continuous monitoring and verification of data integrity in real-time, minimizing the impact of potential security incidents and enhancing resilience against APTs. It is essential for maintaining trust and confidence in cloud-based systems, particularly in industries where data integrity is paramount.

One advantage of integrity verification within the HLA framework is its proactive nature, enabling continuous monitoring and verification of data integrity in real-time. This proactive approach minimizes the impact of potential

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305315 |

security incidents and enhances overall resilience against APTs.

In addition to protecting against external threats like APTs, integrity verification addresses internal risks, including inadvertenterrors and insider threats. By enforcing strict integrity checks and controls, HLA helps mitigate the risk of data corruption or unauthorized alterations caused by internal actors or system malfunctions.

In conclusion, integrity verification is a fundamental aspect of the HLA data protection approach, enhancing the security, reliability, and trustworthiness of cloud-based systems in the face of APTs and other security threats.

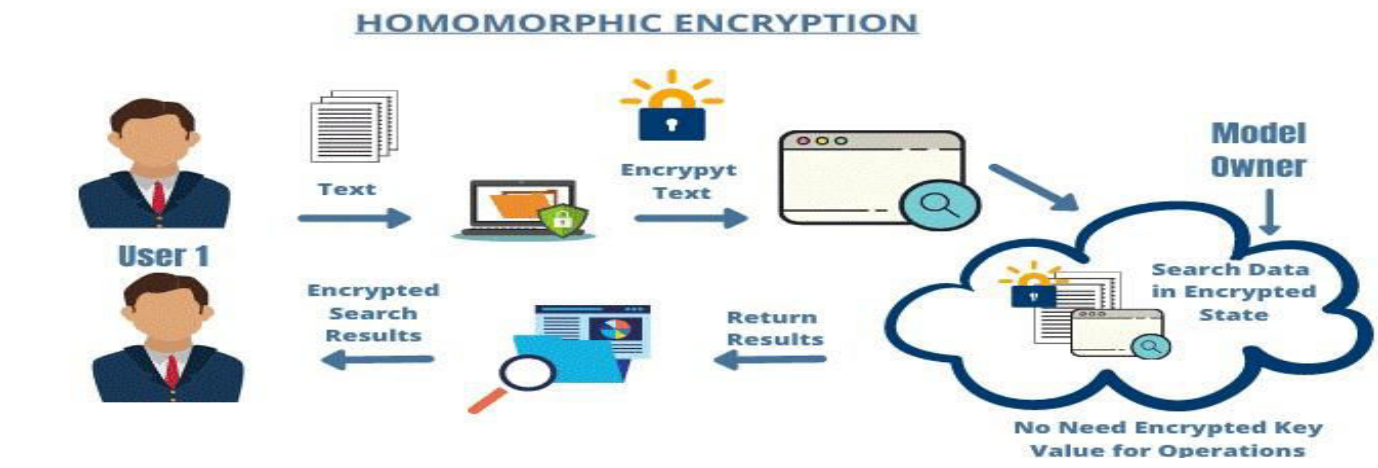

Figure 2 Data processing

1) Encryption Phase

The encryption phase involves encrypting sensitive data before storage or processing in the cloud environment. This ensures unauthorized access without decryption keys. Homomorphic encryption techniques allow computations to be performed directly on encrypted data without decryption. Encryption algorithms like RSA, paillier, or BFV preserve confidentiality. The encrypted data is securely transferred to the cloud for further processing.

2) Processing/Authencation phase

The Processing/Authentication Phase in cloud computing uses homomorphic linear authentication to protect encrypted data from Advanced Persistent Threats (APTs). This phase ensures confidentiality, enables data analytics, machine learning, and integrity verification, and maintains the data's confidentiality. Authentication mechanisms verify the data's integrity without compromising its confidentiality. The resulting data or authentication outcomes are securely transmitted back to authorized users or applications, ensuring end-to-end security in the cloud computing environment.

C. Key Features

There are a couple of key features in the proposed design, and Secure Processing and integrity verification are the primary elements.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305315 |

1) Secure processing

Secure processing is crucial for protecting sensitive information in cloud computing environments, especially against Advanced Persistent Threats (APTs). It involves performing operations on data without compromising its confidentiality, integrity, or authenticity. Homomorphic linear authentication allows computations and authentication checks to be performed directly on encrypted data, reducing the risk of exposure to APT attacks.

This allows organizations to perform data analytics, machine learning, and integrity verification on encrypted data, leveraging cloud computing's computational power while maintaining data confidentiality. Encrypted data remains confidential throughout the processing phase, preventing unauthorized access or tampering, thus mitigating the risk of APTs gaining access and preventing data breaches.

2) Integrity verification

Integrity verification is a crucial aspect of data protection against Advanced Persistent Threats (APTs) in cloud computing. It ensures that encrypted data remains unaltered and authentic throughout its lifecycle, guarding against unauthorized modifications or tampering. Authentication mechanisms, such as cryptographic hashes or digital signatures, verify the integrity of encrypted data without decryption. This layer of defense helps organizations detect and respond to unauthorized alterations, mitigating the risks posed by persistent threats. Integrity verification also enhances trust and reliability in cloud computing environments, fostering confidence in system security.

VI. CONCLUSION

In summary, Homomorphic linear authentication is a sophisticated and effective approach to data protection from Advanced Persistent Threats (APTs) in cloud computing. This method uses encryption techniques for secure processing and authentication without decryption, ensuring data confidentiality even against skilled adversaries. Integrity verification is crucial in maintaining the trustworthiness of encrypted data, guarding against unauthorized modifications or tampering. Authentication mechanisms enable organizations to verify data integrity without compromising confidentiality, enhancing security and reliability in cloud computing environments.

Key features of this approach include encryption without decryption, secure processing, confidentiality, integrity verification, and end-to-end security. Implementing homomorphic linear authentication helps organizations mitigate risks posed by persistent threats and protect sensitive information effectively, fostering trust and confidence in their cloud computing infrastructure. As cyber threats evolve, adopting innovative strategies and technologies is essential for organizations to stay ahead of the ever-changing threat landscape and safeguard their valuable assets.

VII. FUTURE WORK

The development of data protection from Advanced Persistent Threats (APTs) using homomorphic linear authentication in cloud computing could be enhanced through research into efficient algorithms and optimizations. Integrating homomorphic authentication with other security technologies, such as machine learning-based anomaly detection or decentralized identity management systems, could provide a comprehensive defense against APTs. Standardization and interoperability of homomorphic encryption protocols across different cloud platforms could facilitate seamless deployment. Research into cryptography and cybersecurity could lead to more robust and resilient homomorphic authentication techniques.

REFERENCES

1. R. D. Chen, X. S. Zhang, W. N. Niu, and H. Y. Lan, “A Research on Architecture of APT Attack Detection and Countering Technology,” Dianzi Keji Daxue Xuebao/Journal Univ. Electron. Sci. Technol. China, vol. 48, no. 6, pp. 870–879, 2019, doi: 10.3969/j.issn.1001- 0548.2019.06.011.
2. S. Moothedath et al., “A Game Theoretic Approach for Dynamic Information Flow Tracking to Detect Multi-Stage Advanced Persistent Threats,” vol. 9286, no. c, 2018, doi: 10.1109/tac.2020.2976040.
3. Alsaffar, A. Alfahhad, B. Alqhtani, L. Alamri, S. Alansari, N. Alqahtani and D.A. Alboaneen, Machine and deep learning algorithms for Twitter spam detection. In International Conference on Advanced Intelligent Systems and Informatics. Springer, Cham, (pp. 483–491). (2019)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305315 |

4. Fowler, K.: Data Breach Preparation and Response: Breaches are Certain, Impact is Not. Elsevier Science, 2016.
5. Lewinson, Python for finance cookbook. Birmingham: Packt Publishing, Limited, 2020.
6. VERIS, "The vocabulary for event recording and incident sharing," VERIS Community, 2020.
7. Botacin, M.; de Geus, P.L.; Gregio, A. Who Watches the Watchmen: A Security-focused Review on Current State-of-the-art Techniques, Tools, and Methods for Systems and Binary Analysis on Modern Platforms. ACM Comput. Surv.Rev. 2018, 51, 69
8. Manning, C.; Raghavan, P.; Schütze, H. Introduction to Information Retrieval; Cambridge University Press: Cambridge, UK, 2010; Volume 16, pp. 100–103
9. Yen, T.-F.; Oprea, A.; Onarlioglu, K.; Leetham, T.; Robertson, W.; Juels, A.; Kirda, E.: Beehive: Large-scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks. In: Proceedings of the 29th Annual Computer Security Applications Conference. ACSAC '13, ACM, New Orleans, Louisiana, USA, S. 199–208, 2013, isbn: 978- 1-4503-2015-3, url: http://doi.acm.org/10.1145/ 2523649.2523670.
10. Sahabandu, B. Xiao, A. Clark, S. Lee, W. Lee, and R. Poovendran, "DIFT Games: Dynamic Information Flow Tracking Games for Advanced Persistent Threats," Proc. IEEE Conf. Decis. Control, vol. 2018-Decem, no. Cdc, pp. 1136–1143, 2019, doi: 10.1109/CDC.2018.8619416.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details