INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume08 Issue08, Aug-2023, pg. 1-4

Published Date: - 01-08-2023

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

ENHANCING PRIVACY IN CLOUD ANOMALY DETECTION WITH LIGHTWEIGHT HOMOMORPHIC ENCRYPTION

Khalil Ahamed

Computer Science & Software Engineering, School of Science, Rmit University, Australia

Abstract: Anomaly detection is a critical component in ensuring the security and integrity of data in cloud computing environments. However, traditional anomaly detection methods often require data to be shared in unencrypted form, raising privacy concerns for cloud users. To address this challenge, this paper proposes a novel approach that enhances privacy in cloud anomaly detection using lightweight homomorphic encryption. The proposed method allows for the detection of anomalies in encrypted data without the need to decrypt it, thereby preserving the confidentiality of sensitive information. The study evaluates the effectiveness and efficiency of the proposed approach through experimentation and demonstrates its potential to provide privacy-preserving anomaly detection capabilities in cloud environments. By leveraging lightweight homomorphic encryption, cloud users can confidently utilize anomaly detection services while maintaining the confidentiality of their data.

Keywords: Anomaly detection, cloud computing, privacy, lightweight homomorphic encryption, data security, confidentiality, privacy-preserving computation, encrypted data analysis, data integrity, cloud security.

INTRODUCTION

Cloud computing has revolutionized the way data is stored and processed, providing scalable and cost-effective solutions for businesses and individuals. However, with the increased adoption of cloud services, data security and privacy have become major concerns. Anomaly detection is a crucial aspect of data security, enabling the identification of unusual patterns or behaviors that may indicate potential threats or data breaches. Traditional anomaly detection methods often require data to be shared in unencrypted form, exposing sensitive information to potential risks and privacy violations.

To address these privacy concerns, this paper proposes a novel approach that enhances privacy in cloud anomaly detection through the use of lightweight homomorphic encryption. Homomorphic encryption is a cryptographic technique that enables computations to be performed on encrypted data without the need for decryption. By leveraging lightweight homomorphic encryption, cloud users can confidently deploy anomaly detection services while ensuring the confidentiality of their data. This approach allows

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume08 Issue08, Aug-2023, pg. 1-4

Published Date: - 01-08-2023

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

for the detection of anomalies in encrypted data, preventing unauthorized access to sensitive information and preserving the privacy of cloud users.

METHOD

The research methodology involves the following steps to evaluate the effectiveness and efficiency of the proposed approach:

Selection of Anomaly Detection Algorithm:

A suitable anomaly detection algorithm is selected based on its compatibility with lightweight homomorphic encryption. The chosen algorithm should be capable of processing encrypted data and provide accurate anomaly detection results.

Implementation of Lightweight Homomorphic Encryption:

The selected anomaly detection algorithm is integrated with a lightweight homomorphic encryption scheme. The implementation ensures that computations on encrypted data can be performed efficiently without compromising the privacy of the cloud users.

Dataset Collection and Encryption:

A representative dataset containing both normal and anomalous data is collected. The dataset is then encrypted using the lightweight homomorphic encryption scheme to preserve data confidentiality.

Privacy-Preserving Anomaly Detection:

The encrypted dataset is used to perform anomaly detection using the integrated algorithm and lightweight homomorphic encryption. The process involves computations on encrypted data without decrypting it, thereby maintaining privacy.

Performance Evaluation:

The performance of the proposed approach is evaluated in terms of accuracy, efficiency, and computational overhead. A comparison is made with traditional anomaly detection methods that involve data decryption to highlight the privacy benefits of the proposed approach.

Security Analysis:

A thorough security analysis is conducted to assess the robustness of the lightweight homomorphic encryption scheme against potential attacks and vulnerabilities.

Experimental Validation:

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume08 Issue08, Aug-2023, pg. 1-4

Published Date: - 01-08-2023

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

The proposed approach is validated through experiments on real-world datasets to demonstrate its capability to provide privacy-preserving anomaly detection in cloud computing environments.

By following this research methodology, the paper aims to demonstrate the potential of lightweight homomorphic encryption in enhancing privacy in cloud anomaly detection. The proposed approach offers cloud users a practical and secure solution to leverage anomaly detection services while safeguarding their sensitive data from unauthorized access and privacy breaches.

RESULTS

The implementation of the proposed approach for enhancing privacy in cloud anomaly detection using lightweight homomorphic encryption yielded promising results. The experimental evaluation demonstrated that anomaly detection on encrypted data can be achieved efficiently and accurately without compromising data privacy. The use of lightweight homomorphic encryption allowed for secure computations on encrypted data, preventing unauthorized access to sensitive information.

DISCUSSION

The results highlight the effectiveness of the proposed approach in maintaining data privacy while performing anomaly detection in cloud environments. By leveraging lightweight homomorphic encryption, cloud users can confidently utilize anomaly detection services without exposing their sensitive data in unencrypted form. This enhances the overall security and confidentiality of cloud-based anomaly detection, addressing the privacy concerns associated with traditional methods.

Furthermore, the implementation of the lightweight homomorphic encryption scheme showed minimal computational overhead, making it a practical solution for real-world cloud applications. The approach efficiently handled the encryption and decryption processes, ensuring that anomaly detection can be performed in a timely manner without compromising on accuracy.

The security analysis revealed that the lightweight homomorphic encryption scheme used in the proposed approach demonstrated resilience against common cryptographic attacks. The encryption scheme effectively protected the data and the intermediate results during the anomaly detection process, providing an additional layer of security to prevent data breaches.

CONCLUSION

The research demonstrates that lightweight homomorphic encryption can be successfully utilized to enhance privacy in cloud anomaly detection. By enabling computations on encrypted data, the proposed approach ensures that cloud users' sensitive information remains confidential throughout the anomaly detection process. This approach addresses the privacy concerns associated with traditional anomaly detection methods that require data to be shared in unencrypted form.

Published Date: - 01-08-2023

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

The efficient performance of the lightweight homomorphic encryption scheme makes the proposed approach practical and feasible for real-world cloud computing applications. It provides cloud users with a secure and privacy-preserving solution for leveraging anomaly detection services without compromising the confidentiality of their data.

Overall, the study contributes to the advancement of data security and privacy in cloud computing by showcasing the potential of lightweight homomorphic encryption in anomaly detection. The proposed approach offers a valuable tool for organizations and individuals seeking to enhance the privacy of their data while utilizing cloud-based anomaly detection services. As cloud computing continues to evolve, privacy-preserving techniques like lightweight homomorphic encryption will play a crucial role in ensuring the secure and confidential processing of data in cloud environments.

REFERENCES

1. C.C. Aggarwal, Data Mining – The Textbook, Springer, 2015.
2. K. Li, H. Jiang, L.T. Yang, A. Cuzzocrea (Eds.), Big Data – Algorithms, Analytics, and Applications, Chapman and Hall/CRC, 2015, http://www.crcnetbase.com/isbn/978-1-4822-4056-6.
3. R. Agrawal, A. Kadadi, X. Dai, F. Andrès, Challenges and opportunities with big data visualization, in: Proceedings of the 7th International Conference on Management of Computational and Collective IntElligence in Digital EcoSystems, Caraguatatuba, Brazil, October 25–29, 2015, 2015, pp. 169–173.
4. I.A.T. Hashem, I. Yaqoob, N.B. Anuar, S. Mokhtar, A. Gani, S.U. Khan, The rise of "big data" on cloud computing: review and open research issues, Inf.Syst. 47 (2015) 98–115, http://dx.doi.org/10.1016/j.is.2014.07.006.
5. Gvero, Cloud computing concepts, technology and architecture by Thomas Erl, Zaigham Mahmood and Ricardo Puttini, ACM SIGSOFT Softw. Eng.Notes 39 (4) (2014) 37–38, http://dx.doi.org/10.1145/2632434.2632462.
6. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1–11, http://dx.doi.org/10.1016/j.jnca.2010.07.006.
7. D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst. 28 (3) (2012) 583–592, http://dx.doi.org/10.1016/j.future.2010.12.006.
8. K.W. Hamlen, M. Kantarcioglu, L. Khan, B.M. Thuraisingham, Security issues for cloud computing, Int. J. Inf. Secur. Priv. 4 (2) (2010) 36–48, http://dx.doi.org/10.4018/jisp.2010040103.
9. H. Kumarage, I. Khalil, Z. Tari, A.Y. Zomaya, Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling, J. Parallel Distrib. Comput. 73 (6) (2013) 790–806, http://dx.doi.org/10.1016/j.jpdc.2013.02.004.
10. J. Domingo-Ferrer, A provably secure additive and multiplicative privacy homomorphism, in: Information Security, 5th International Conference, ISC 2002 Sao Paulo, Brazil, September 30–October 2, 2002, Proceedings, 2002, pp. 471–483.