Evaluating the Effectiveness of Homomorphic Encryption in Big Data: A Descriptive and Diagnostic Analysis

W.C.K. Jayaweera[1] and A.R. Fathima Shafana[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]charunikosala9723@seu.ac.lk, [2]arfshafana@seu.ac.lk

Abstract

The ever-increasing volume of data generated from various sources, including the Internet of Things (IoT) and digital channels, presents a significant challenge for organizations. This rapid growth often necessitates offloading data analysis to the cloud due to limitations on local server capacity. However, security concerns arise when analyzing sensitive data in the cloud environment. Traditional encryption methods, while effective in protecting data at rest, require decryption prior to analysis, potentially exposing sensitive information. On the other hand, Homomorphic Encryption (HE) is gaining popularity as it – offers a solution by enabling computations to be performed directly on encrypted data. This paper investigates the effectiveness of homomorphic encryption on big data through descriptive and diagnostic analyses. Result suggest that this approach is better in terms of execution time and is particularly well-suited for big data analytics due to its inherent scalability.

Keywords: FHE, OpenFHE, BFV, BGV, CKKS

VI. INTRODUCTION

Big data refers to massive datasets that traditional computing methods struggle to handle (Shekhawat,*et al.,* 2019). Fueled by the constant influx of information, big data is characterized by a variety of attributes: volume (immense size), variety (diverse sources and formats), velocity (rapid generation and processing), veracity (accuracy and reliability), variability (continuously changing nature), complexity (intricate relationships), value (potential for insights), vulnerability (susceptibility to breaches), volatility (frequent fluctuations), validity (ensuring data quality), and visualization (effective representation). These characteristics necessitate a multifaceted approach for data governance, management, and analysis (Al-Mekhlal, M. and Khwaja, A.A., 2019). Data from various sources, including Internet of Things (IoT) devices (Kuri, *et al.,* 2017), cyber-physical systems (Gao, *et al.,* 2018), social media, and scientific research, increases the big data growth. To extract valuable insights from this data, advanced analytics techniques like artificial intelligence (AI), machine learning, and deep learning are crucial. As big data has invaded various sectors like business, healthcare, and education, a comprehensive understanding of its characteristics has become an essential. This understanding empowers governments, industries, and academic institutions to leverage big data's potential for a competitive advantage and significant value creation (Al-Mekhlal, M. and Khwaja, A.A., 2019).

The constant integration of new technologies is generating enormous amount of data on both individuals and organizations. This data is paramount for big data analytics, a powerful process that involves meticulous processing and analyzing massive datasets to extract valuable insights (Zaraket, *et al.,* 2022). These insights can be used for a variety of applications, such as precisely targeted advertising campaigns, and personalized healthcare decisions (Hong, *et al.,* 2016). Big data analytics is an essential tool for unlocking the hidden potential within these vast datasets. However, the lack of sophisticated analytical techniques, would leave this data unused. Thus, big data analytics empowers businesses and governments to transform this raw data into actionable intelligence, driving informed decisions across various sectors (Kumarage, *et al.,* 2016).

The ever-growing volume and complexity of big data necessitates a robust infrastructure to handle its storage and processing, resulting in the rise of cloud-based solutions (Al-Mekhlal, M. and Khwaja, A.A., 2019), which offer scalable and cost-effective platforms for big data analytics. Cloud computing provides the flexibility and power needed to process massive datasets,

enabling businesses and organizations to unlock the transformative potential of big data (Biksham, V. and Vasumathi, D., 2017). Despite the many advantages that big data provides, there are also concerns related to the personal data leakages that could collapse many individuals and organizations (Iezzi, M., 2020; Kuri, *et al.*, 2017). Data breaches exposing sensitive details like financial records, medical histories, or social security numbers can lead to identity theft, financial losses, and reputational damage for users. Especially, companies and organizations face serious consequences from data leaks, such as losing customer trust, facing large fines for non-compliance, and disrupting business operations.

The risks associated with data leakages in the domain of big data could be mitigated using encryption. Encryption refers to the method of converting the data into an unreadable format, often known as ciphertext. This ciphertext can only be converted back to its original form with a decryption key. Without this key, unauthorized users cannot understand the data, making it useless to them. By using encryption, organizations can greatly reduce the risk of data breaches and the resulting harm. (Kumarage, *et al.*, 2016).

With vast amounts of confidential data being generated, ensuring its privacy becomes a significant challenge, especially in public cloud environments where data security is inherently more complex (El Makkaoui, K., Ezzati, A. and Hssane, A.B., 2015). Despite the fact that traditional data encryption offers a layer of protection, its limitations should not be overlooked since the data needs to be decrypted before processing, leaving it vulnerable during this window (Alharbi, A., Zamzami, H. and Samkri, E., 2020).

This paper investigates the potential of Homomorphic Encryption (HE) to address this vulnerability (Chauhan, *et al.*, 2015). HE emerges as a revolutionary approach for secure data analytics in the big data era which allows users to perform operations directly on encrypted data, without ever decrypting it (Chauhan, *et al.*, 2015; Waziri, V.O., *et al.*, 2015). This means that the data remains secure and scrambled throughout its entire lifecycle, from storage and transmission to processing and analysis.

HE offers several advantages. It enables secure collaboration between data owners and untrusted data analysts, which is crucial for many industrial applications (Hamza et al., 2022). Data owners can share their encrypted data with analysts, knowing the information remains confidential. HE also reduces the performance overhead of traditional decryption-processing cycles, making data analysis more efficient while preserving privacy (Alabdulatif, Khalil, and Yi, 2020). However, HE is still under development, and different schemes have varying capabilities. Fully Homomorphic Encryption (FHE) allows both addition and multiplication on encrypted data but is computationally expensive (Zaraket et al., 2022; Chauhan et al., 2015). Partially Homomorphic Encryption (PHE) offers a compromise, supporting either addition or multiplication but not both (Chauhan et al., 2015). As research continues, HE libraries like HElib, SEAL, PALISADE, and TFHE are being improved for better efficiency and functionality (Iezzi, 2020).

II. RELATED WORKS

Due to the many advantages that HE offers for big data, different variants of HE has been employed from time to time for secure data transmission and storage. For instance, Kuri, *et al.*, introduce a novel privacy-preserving machine learning model, PP-ELM, designed for secure outsourced machine learning (Kuri, *et al.*, 2017). PP-ELM leverages additively homomorphic encryption, enabling an outsourced server to perform computations on encrypted data without decryption, ensuring data privacy. In addition, Verifiable Fully Homomorphic Encryption (VFHE) emerges as a promising solution for handling noise in encrypted data. VFHE combines homomorphic encryption with verifiability, allowing computations on encrypted data while guaranteeing their correctness (Ahmed, E.Y. and El Kettani, M.D.E.C., 2017). Whereas, Alabdulatif, A., Khalil, I., Reynolds, M., Kumarage, H. and Yi, X. (2017) used a distributed Fully Homomorphic Encryption (FHE) algorithm using MapReduce to address the potential data misuse by Cloud Service Providers (CSPs) or unauthorized access by malicious attackers. This approach facilitates data analysis tasks entirely on the cloud platform, eliminating the need for a Trusted Third Party (TTP). In another work, Alabdulatif, A., Kumarage, H., Khalil, I. and Yi, X. (2017) proposed a novel privacy-preserving anomaly detection model for the cloud

ISBN 978-955-627-028-0

environment using a lightweight homomorphic encryption approach for distributed data clustering on encrypted data, effectively utilizing cloud resources. To overcome limitations inherent to homomorphic encryption, this model integrated with a trusted private server within the cloud for computations requiring decryption. This collaboration ensured a secure and scalable anomaly detection on encrypted data.

The other variants included a novel homomorphic cryptosystem introduced by Pang and Wang (2020) supporting multiple cloud users with distinct public keys. This innovation caters to customers with limited computing resources who might leverage the cloud for association rule mining tasks (Pang, H. and Wang, B., 2020). Building upon the Paillier cryptosystem Zaraket et al (2022) proposed Vector-based Homomorphic Operations (SAVHO) for secure analytics that demands both security and efficiency.

In addition, research efforts like the distributed privacy-preserving Expectation-Maximization (EM) algorithm for Gaussian mixture modeling underscored the focus on scalability within the cloud context. This approach showed advantages such as scalable distribution settings and accelerated performance of FHE computations while maintaining high analysis accuracy (Alabdulatif, *et al.,* 2020). Moreover, a generic Privacy-Preserving Auction Scheme (PPAS) was proposed, encompassing an untrusted third-party trading platform comprised of two independent entities: the Auctioneer and the Intermediate Platform (Gao, *et al.,* 2018).

III. METHODOLOGY

A. Open-source Software Libraries Implementation FHE Schemes

Several open-source software libraries implementing FHE schemes are available to date. Among them, HElib, PALISADE, SEAL, HEAAN, FullRNS-HEAAN, Concrete, and FHEW are included (See Table 01).

HElib was developed by Shai Halevi and Victor Shoup. It is a sophisticated software library dedicated to the implementation of homomorphic encryption (HE), with a particular emphasis on the Brakerski-Gentry-Vaikuntanathan (BGV) scheme. The Smart-Vercauteren ciphertext packing techniques are leveraged, and the Gentry-Halevi-Smart optimizations are incorporated to enhance efficiency (Halevi, S. and Shoup, V., 2014).

The PALISADE Lattice Cryptography Library offers a comprehensive, layered framework that is designed for homomorphic encryption (HE) and a range of advanced lattice-based protocols. These include identity-based encryption, attribute-based encryption, and program obfuscation, making it a versatile tool for implementing cutting-edge cryptographic solutions (Polyakov, *et al.,* 2017).

Microsoft SEAL provides two distinct homomorphic encryption schemes, each with unique properties. The BFV and BGV schemes enable modular arithmetic on encrypted integers, resulting in precise results. Conversely, the CKKS scheme supports addition and multiplication on encrypted real or complex numbers, though only approximate results are yielded (https://github.com/microsoft/SEAL).

HEAAN (Homomorphic Encryption for Arithmetic of Approximate Numbers) is an open-source, cross-platform software library dedicated to the implementation of the approximate homomorphic encryption scheme introduced by Cheon, Kim, Kim, and Song (CKKS). The CKKS schemes are exclusively executed, with all their inherent properties fully supported (https://github.com/snucrypto/HEAAN).

The FHEW library, licensed under the GNU General Public License, implements a fully homomorphic encryption scheme that enables the homomorphic evaluation of arbitrary Boolean circuits on encrypted data. Efficient performance is achieved by utilizing the FFTW library, and the research ”FHE bootstrapping in less than a second” by Ducas and Micciancio forms the basis (https://github.com/lducas/FHE).

Table 01: Font format for this publication

HE Library	**HE Scheme**					
	BFV	**BGV**	**CKKS**	**FHEW**	**TFHE**	**GSW**
HElib		YES	YES			
PALISADE	YES	YES	YES	YES	YES	
SEAL	YES	YES	YES			
HEAAN			YES			
FHEW					YES	YES

ISBN 978-955-627-028-0

A new openFHE library (Al Badawi, *et al.,* 2022), designed by some of the authors of the PALISADE, HElib, HEAAN, and FHEW libraries, has been introduced. The design of this new library started with PALISADE and supports all common FHE schemes. Eventually, all supported FHE schemes in this library will include bootstrapping and scheme switching. Additionally, this library can support multiple hardware abstraction layers (HAL).

As shown in Table 02, OpenFHE is an open-source FHE library that includes efficient implementations of all common FHE schemes. In this study, the OpenFHE library will be utilized for the implementation of Big Data analytics using the BFV, BGV, and CKKS schemes, as the scope of this study is limited to arithmetic operations.

Table 02: OpenFHE Schemes (AL Badawi, *et al*., 2022)

Scheme	**Purpose**
BFV (Brakerski/Fan-Vercauteren)	Integer Arithmetic
BGV (Brakerski-Gentry-Vaikuntanathan)	Integer Arithmetic
DM/FHEW (Ducas-Micciancio)	Evaluating Boolean circuits and arbitrary functions over larger plaintext spaces using lookup tables
CGGI/TFHE (Chillotti-Gama-Georgieva-Izabachene)	Evaluating Boolean circuits and arbitrary functions over larger plaintext spaces using lookup tables
LMKCDEY	Evaluating Boolean circuits and arbitrary functions over larger plaintext spaces using lookup tables

B. Implementation of Homomorphic Encryption for Big Data Analytics

The first step involved the identification of suitable homomorphic encryption (HE) Library that can be effectively utilized for big data analytics. Once the appropriate HE Library was identified, the next phase was to implement these libraries within the context of big data analytics arithmetic functions. The implementation of Big Data analytics was carried out in Linux environment. Specifically in the latest version of Ubuntu 24.04. The installation of the OpenFHE library on the Linux environment was guided by the process outlined on the OpenFHE official website. Prerequisites such as g++ and clang were installed as stipulated in the provided documentation.

Subsequent to setting up the environment, the functionalities for descriptive and diagnostic analytics were developed. The implementation was divided into distinct modules corresponding to the CKKS, BFV, and BGV schemes. Each scheme was separately integrated to ensure comprehensive support for the various encryption methodologies. Initially, the dataset was stored in a CSV file. Distinct datasets were employed for testing both types of analytics. Upon uploading the data, it was subjected to a cleaning process to ensure accuracy and consistency.

Separate implementations were developed for each of the three encryption schemes—BFV, BGV, and CKKS. This separation was crucial to measure the time taken for each scheme to complete the analysis accurately. For descriptive analytics, statistical measures such as mean, median, and mode were computed. These metrics provided insights into the central tendencies and distribution of the data. In the case of diagnostic analytics, the focus was on determining the correlation between pairs of variables. This involved assessing the relationships and dependencies between different data points to uncover underlying patterns and trends.

Comparative analysis was conducted based on the time taken for the analytics. Each scheme was executed ten times to obtain an average and more accurate results. This approach ensures a comprehensive evaluation of performance and allows for the identification of any potential variations or inconsistencies in the execution times across the different encryption schemes. By averaging the results from multiple runs, a more reliable measure of each scheme's efficiency could be derived.

IV. RESULT AND DISCUSSION

This study investigated the efficiency of three homomorphic encryption (FHE) schemes (BFV, BGV, CKKS) implemented through the OpenFHE library for secure big data analytics. We focused on three key performance metrics: encryption time, descriptive analytics time, and diagnostic analytics time. Each FHE scheme was

ISBN 978-955-627-028-0

evaluated on its ability to perform these tasks on encrypted data while maintaining efficiency.

Our analysis revealed a significant difference in execution times between various data analysis tasks. All three FHE schemes exhibited considerably faster processing times for descriptive analytics, which involves basic statistical computations, compared to both encryption and diagnostic analytics. This finding suggests that FHE holds promise for applications requiring encrypted data exploration and basic statistical analysis. Encryption time remained relatively consistent across all three schemes, indicating that the base overhead of encrypting data is comparable for each approach.

Among the FHE schemes evaluated, BFV demonstrated the most efficient performance for descriptive analytics, achieving an average execution time of only 1.6 milliseconds. BGV and CKKS followed closely behind with average times of approximately 3.4 milliseconds. This suggests that BFV might be the preferred choice for use cases prioritizing rapid encrypted data exploration.

Table 03: OpenFHE Schemes

	Avg. time or read and clean(ms)	**Avg. time for encryption (ms)**	**Avg. time for analytics (ms)**
Descriptive Analysis			
BFV	11.3	64047.4	1.6
BGV	13.5	68455.6	3.4
CKKS	16.5	6623.9	3.4
Diagnostic Analytics			
BFV	50.2	327921.1	83.7
BGV	182.4	350033.0	65.1
CKKS	52.2	357448.4	70.4

For diagnostic analytics, which involve more complex computations, all FHE schemes displayed noticeably higher execution times compared to descriptive analytics. However, even with this increase, BFV maintained its lead as the fastest scheme, averaging 83.7 milliseconds. BGV and CKKS showcased comparable performance for diagnostic analytics, with average times hovering around 65-70 milliseconds.

One limitation encountered during the study was a linking error that arose when working with very large numbers. This error suggests a potential constraint within the virtual machine environment used for the analysis. Further investigation is needed to determine if this limitation is inherent to the virtual machine or specific to the configuration employed. Overcoming this limitation would be crucial for enabling the analysis of even larger datasets using FHE.

In conclusion, the OpenFHE library demonstrates significant promise as a platform for implementing data analytics functionalities on encrypted data. While encryption itself remains computationally expensive, the substantial speed advantage observed for descriptive analytics highlights the potential of this approach for secure data exploration and basic statistical analysis. Future research should focus on exploring the application of OpenFHE for predictive modeling, which would broaden its utility in advanced data analysis scenarios. Additionally, investigating methods to address the limitations encountered when working with very large numbers would be highly beneficial for expanding the practical applications of FHE in big data analytics.

REFERENCES

Ahmed, E.Y. and El Kettani, M.D.E.C., 2017. A verifiable fully homomorphic encryption scheme to secure big data in cloud computing. In International Conference on Wireless Networks and Mobile Communications, Rabat (pp. 1-5).

Al Badawi, A., Bates, J., Bergamaschi, F., Cousins, D.B., Erabelli, S., Genise, N., Halevi, S., Hunt, H., Kim, A., Lee, Y. and Liu, Z., 2022, November. Openfhe: Open-source fully homomorphic encryption library. In proceedings of the 10th workshop on encrypted computing & applied homomorphic cryptography (pp. 53-63).

Alabdulatif, A., Khalil, I., Reynolds, M., Kumarage, H. and Yi, X., 2017. Privacy-preserving data clustering in cloud computing based on fully homomorphic encryption.

Alabdulatif, A., Khalil, I. and Yi, X., 2020. Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption. Journal of Parallel and Distributed Computing, 137, pp.192-204.

Alabdulatif, A., Khalil, I., Zomaya, A.Y., Tari, Z. and Yi, X., 2020. Fully homomorphic based privacy-preserving distributed expectation maximization on cloud. IEEE Transactions on Parallel and Distributed Systems, 31(11), pp.2668-2681.

Alabdulatif, A., Kumarage, H., Khalil, I. and Yi, X., 2017. Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption. Journal of Computer and System Sciences, 90, pp.28-45.

Alharbi, A., Zamzami, H. and Samkri, E., 2020. Survey on homomorphic encryption and address of new trend. International Journal of Advanced Computer Science and Applications, 11(7).

Al-Mekhlal, M. and Khwaja, A.A., 2019, August. A synthesis of big data definition and characteristics. In 2019 IEEE international conference on Computational Science and Engineering (CSE) and IEEE international conference on Embedded and Ubiquitous Computing (EUC) (pp. 314-322). IEEE.

Al-Rummana, G.A. and Shende, G.N., 2018. Homomorphic encryption for big data security: A survey. International Journal of Computer Sciences and Engineering, 6(10), pp.503-511.

Alloghani, M., Alani, M.M., Al-Jumeily, D., Baker, T., Mustafina, J., Hussain, A. and Aljaaf, A.J., 2019. A systematic review on the status and progress of homomorphic encryption technologies. Journal of Information Security and Applications, 48, p.102362.

Biksham, V. and Vasumathi, D., 2017. Homomorphic encryption techniques for securing data in cloud computing: A survey. International Journal of Computer Applications, 975(8887).

Chauhan, K.K., Sanger, A.K. and Verma, A., 2015, December. Homomorphic encryption for data security in cloud computing. In 2015 International conference on information technology (ICIT) (pp. 206-209). IEEE.

Das, D., 2018, January. Secure cloud computing algorithm using homomorphic encryption and multi-party computation. In 2018 International Conference on Information Networking (ICOIN) (pp. 391-396). IEEE.

El Makkaoui, K., Ezzati, A. and Hssane, A.B., 2015, June. Challenges of using homomorphic encryption to secure cloud computing. In 2015 International Conference on Cloud Technologies and Applications (CloudTech) (pp. 1-7). IEEE.

Gao, W., Yu, W., Liang, F., Hatcher, W.G. and Lu, C., 2018. Privacy-preserving auction for big data trading using homomorphic encryption. IEEE Transactions on Network Science and Engineering, 7(2), pp.776-791.

Guan, S., Zhang, C., Wang, Y. and Liu, W., 2024. Hadoop-based secure storage solution for big data in cloud computing environment. Digital Communications and Networks, 10(1), pp.227-236.

Halevi, S. and Shoup, V., 2014. Algorithms in helib. In Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I 34 (pp. 554-571). Springer Berlin Heidelberg.

Hallman, R.A., Diallo, M.H., August, M.A. and Graves, C.T., 2018, March. Homomorphic Encryption for Secure Computation on Big Data. In IoTBDS (pp. 340-347).

Hamza, R., Hassan, A., Ali, A., Bashir, M.B., Alqhtani, S.M., Tawfeeg, T.M. and Yousif, A., 2022. Towards secure big data analysis via fully homomorphic encryption algorithms. Entropy, 24(4), p.519.

Hong, M.Q., Wang, P.Y. and Zhao, W.B., 2016, April. Homomorphic encryption scheme based on elliptic curve cryptography for privacy protection of cloud computing. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 152-157). IEEE.

Iezzi, M., 2020, December. Practical privacy-preserving data science with homomorphic encryption: an overview. In 2020 IEEE International Conference on Big Data (Big Data) (pp. 3979-3988). IEEE.

Karuturi, S.R.V. and Satish, N.M., 2020. Big Data Security and Data Encryption in Cloud Computing. International Journal of Engineering Trends and Applications (IJETA), 7(4), pp.35-40.

Kocabas, O. and Soyata, T., 2015, June. Utilizing homomorphic encryption to implement secure and private medical cloud computing. In 2015 IEEE 8th International Conference on Cloud Computing (pp. 540-547). IEEE.

Kumarage, H., Khalil, I., Alabdulatif, A., Tari, Z. and Yi, X., 2016. Secure data analytics for cloud-integrated internet of things applications. IEEE Cloud Computing, 3(2), pp.46-56.

Kuri, S., Hayashi, T., Omori, T., Ozawa, S., Aono, Y., Wang, L. and Moriai, S., 2017, November. Privacy preserving extreme learning machine using additively homomorphic encryption. In 2017 IEEE symposium series on computational intelligence (SSCI) (pp. 1-8). IEEE.

Lducas (2017) GitHub - lducas/FHEW. https://github.com/lducas/FHEW.

Marwan, M., Kartit, A. and Ouahmane, H., 2016, October. Applying homomorphic encryption for securing cloud database. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt) (pp. 658-664). IEEE.

Microsoft (2024) GitHub - microsoft/SEAL: Microsoft SEAL is an easy-to-use and powerful homomorphic encryption library. https://github.com/microsoft/SEAL.

Mr, M.M.P., Dhote, C.A. and Mr, D.H.S., 2016. Homomorphic encryption for security of cloud data. Procedia Computer Science, 79, pp.175-181.

Pang, H. and Wang, B., 2020. Privacy-preserving association rule mining using homomorphic encryption in a multikey environment. IEEE Systems Journal, 15(2), pp.3131-3141.

Patil, T.B., Patnaik, G.K. and Bhole, A.T., 2017, January. Big data privacy using fully homomorphic non-deterministic encryption. In 2017 IEEE 7th International Advance Computing Conference (IACC) (pp. 138-143). IEEE.

Polyakov, Y., Rohloff, K., Ryan, G.W. and Cousins, D., 2017. Palisade lattice cryptography library user manual. Cybersecurity Research Center, New Jersey Institute of Technology (NJIT), Tech. Rep, 15.

Shekhawat, H., Sharma, S. and Koli, R., 2019, February. Privacy-preserving techniques for big data analysis in cloud. In 2019 second international conference on advanced computational and communication paradigms (ICACCP) (pp. 1-6). IEEE.

Snucrypto (2023) GitHub - snucrypto/HEAAN. https://github.com/snucrypto/HEAAN.

Waziri, V.O., Alhassan, J.K., Ismaila, I. and Noel, M.D., 2015. Big data analytics and data security in the cloud via fully homomorphic encryption.

Zaraket, C., Hariss, K., Chamoun, M. and Nicolas, T., 2022. Cloud based private data analytic using secure computation over encrypted data. Journal of King Saud University-Computer and Information Sciences, 34(8), pp.4931-4942.

ISBN 978-955-627-028-0