International Journal of Applied Mathematics

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

HOMOMORPHIC ENCRYPTION AND ALGEBRAIC GEOMETRY FOR PRIVACY-PRESERVING MACHINE LEARNING

[1]G. Mahalakshmi, [2]Kamala V,[3]Anju M A,[4]Dr. Vijay Franklin,[5]Dr S. Govindaraju,[6]C. Sandhiya,

[1]Assistant Professor Advanced Computer Science and Engineering Department

Vignan's Foundation for Science, Technology and Research, India

priya.nethra1@gmail.com

[2]Assistant Professor Department of Computer Science and Engineering

KGISL Institute of Technology, Coimbatore

kamalav33@gmail.com

Orc ID 0000-0001-9251-4305

[3]Assistant Professor Department of Electronics and Communication Engineering

Nehru Institute of Engineering and Technology, Coimbatore, India

anju.m.appu@gmail.com

[4]Professor Department of Computer Science and Engineering

Erode Sengunthar Engineering College, India

vijayfranklin@esec.ac.in

[5]Associate Professor Department Computer Science

St Joseph University Palanchur, Chennai, India

govindindu2010@gmail.com

[6]Assistant Professor Department of computer Science and Engineering

Nehru Institute of Engineering and Technology

sandhiyachinnasamy@gmail.com

Abstract:

The increasing acceptance of machine learning (ML) in sensitive applications such as health care, finance, and enforcement brings many serious privacy concerns requiring privacy-preserving techniques to be developed. Homomorphic encryption (HE) seems to be a good approach permitting various computations to be carried out on encrypted data without decryption thereby preserving data privacy. The disadvantages of HE are essentially the time required to do the computation and also its scalability. The results obtained have great consequences since the security obtained through this scheme seems to make it possible to apply encryption to large scale ML models. These disadvantages can be solved to a great extent

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

through the introduction of the mathematics of algebraic geometry where polynomial equations are considered. Algebraic geometry will now play an important part in rendering schemes of HE economical and practicable through research within this field. This article reveals the close inter-relation existing between homomorphic encryption and algebraic geometry and attempts to outline briefly some of the developments, problems and possibilities of this forthcoming research. However, in spite of the great advantages to be gained or the possibilities of privacy preserving schemes of HE and algebraic geometry in ML, ML is as yet under threat of moral, scalability and computational disadvantages which threaten its complete acceptance.

Keywords Homomorphic Encryption, Algebraic Geometry, Privacy-Preserving Machine Learning, Computational Overhead, Cryptography, Fully Homomorphic Encryption (FHE), Lattice-Based Cryptography, Machine Learning Models.

1. Introduction

The demand for machine learning (ML) in industries such as healthcare, investment banking, and law enforcement has increased awareness of privacy issues associated with sensitive data. Because many models require training on large-scale datasets that often involve personal and confidential data, protecting privacy is a pressing issue. Privacy protection using traditional data protection methods, such as anonymization, is no longer considered sufficient since machine-learning developments have given rise to techniques that show that individuals can be "de-identified" [1]. As a consequence, privacy-protecting techniques are currently valuable, especially for those applications requiring protection of sensitive data while allowing model generation and inference.

Homomorphic encryption (HE) is one of the most promising answers in the field of privacy-preserving machine learning. It offers a technique to process encrypted data clearly, implying that sensitive information remains privately processed. However, optimal HE is required to reach full capabilities, directing us to the area of algebraic geometry. There is a utility in algebraic geometry for the mathematical formulation leading to the efficiency and security of HE and requiring HE to be applied to more realistic machine learning applications. The purpose of this article is to explicate the junctions of both homomorphic encryption and algebraic geometry and how the two help contribute toward privacy preserving machine learning models [2]. The principles of each of the two subjects are described together with their applications, difficulties and recent innovations, to provide a clear overview of how HE and algebraic geometry will combine to promote secure machine learning in future occasions.

Ii. Understanding Homomorphic Encryption

2.1 Basic Principles of Homomorphic Encryption

Homomorphic encryption refers to a strand of encryption which allows calculations to be done on ciphertext (the encrypted data) avoiding decrypting the leader in question to undertake computations with its data. Consequently here we find a real advantage in the field of machine learning where these properties they allow models to be built up from the data. Thus data which is sensitive is not revealed, although computations are along the models concerning the data.

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Conventional encryption forms e.g. symmetric or asymmetric methods require the decrypting of the data (before any computations can take place) so as to make it possible to be processed. In the contrary case of homomorphic systems, on account of the working form applied thereon, the privacy of the data is retained in the case of computations as there is a direct way in which the operations can be performed on encrypted data.

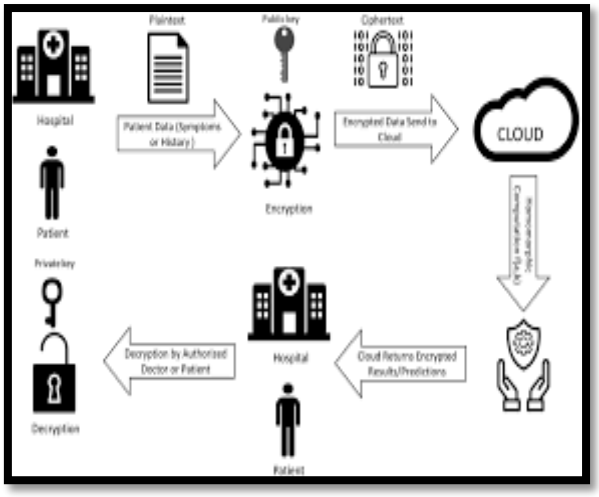

Figure 1: Basic Principles of Homomorphic Encryption

(Source: Networksimulationtools.com, 2025)

The result of the operation on them is an encryption when resolved equal to the original arithmetic process alluded to above on the original primary given values. Thus the property of homomorphic encryption is in a sense good from the standpoint of its use where data privacy or a similar derivative problem is of necessity considered. However certain function must in a few instances be included where the operations having regard to the coercive and the re-impounding negation of these various coercive expressions on the value processes which are being re-coerced from the products of these processes being done with composite outputs in keys and the values themselves.

2.2 Types of Homomorphic Encryption

Homomorphic encryption schemes are classified on the basis of the number of operations that can be performed on the encrypted data. There are 3 main classes of homomorphic encryption.

1. Partially Homomorphic Encryption (PHE): PHE is a homomorphic encryption scheme which allows only one type of operation be it a summation or a multiplication. The RSA encryption scheme is an example of PHE as it allows only multiplication operations to be carried out [4].
2. Somewhat Homomorphic Encryption (SHE): This scheme allows a limited number of addition and multiplication operations to be carried out on ciphertext. After a specific number of operations the ciphertext becomes too noisy to be processed and no more operations can be performed on the ciphertext without decryption.
3. Fully Homomorphic Encryption (FHE): FHE is a homomorphic encryption scheme which can support unlimited number of operations with any type of addition and multiplication on the

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

encrypted data. The FHE scheme was first proposed in 2009 by Craig Gentry, FHE is the most general type of homomorphic encryption which can change the spectrum of data privacy in machine learning since it allows performing complete computations on encrypted data [5].

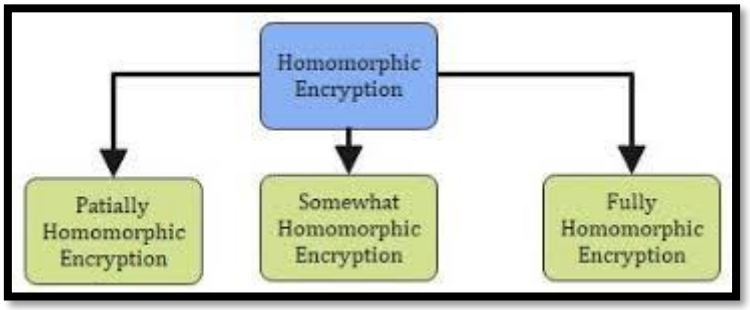

Figure 2: Types of Homomorphic Encryption

(Source: Mdpi.com, 2022)

2.3 Mathematical Foundations

The mathematical basis of homomorphic encryption lies in algebraic structures like lattices and polynomial rings. These structures give rise to encryption schemes that are provably secure to cryptographic attacks. An instance of this is lattice-based cryptography which is the basis of many of the current HE schemes e.g. fully homomorphic encryption (FHE) because of its good security properties versus quantum attacks. The security for homomorphic encryption is built on the hardness of certain mathematical problems such as the Learning with Errors (LWE) problem, which is computationally hard even for quantum computers to solve [6].

2.4 Applications of Homomorphic Encryption in Machine Learning

The main application of homomorphic encryption in machine learning is in the development of private models. Traditional machine learning often uses sensitive learning data which cannot be shared or processed by third parties because of exposure of private information. HE allows conditioned processing of encrypted data so that models can be learned and evaluated on sensitive data sets with the condition that the data remains private. HE has been applied in various applications such as secure data analysis, federated learning, and private inference, which uses the results of ML models on encrypted data (not requiring decryption).

III. Introduction to Algebraic Geometry

3.1 Basic Principles of Algebraic Geometry

Algebraic geometry is a branch of mathematics that studies the solutions to systems of polynomial equations. The subject is concerned, by mixing concepts from algebra, geometry and number theory, with the nature of some geometric objects which are defined with the help of these equations, such as curves, surfaces and other higher dimensional objects. Algebraic geometry is of fundamental importance for the theory of elliptic curves, which have become so vital in recent times in terms of modern cryptography which gives rise to homomorphic systems of enciphering messages [7]. The main features of the subject of algebraic geometry concern the investigation of the structure of polynomial rings, and the geometry of the solutions

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of polynomial equations. The theory is of special interest and importance to the subject of cryptography for the reason that 'most cryptosystems depend on the supposed difficulty of working out certain algebraic problems, some of those problems bearing a relation to one another. This difficulty may turn out to be such questions as those concerning the computation of discrete logarithms, or the solutions of equations in finite fields.

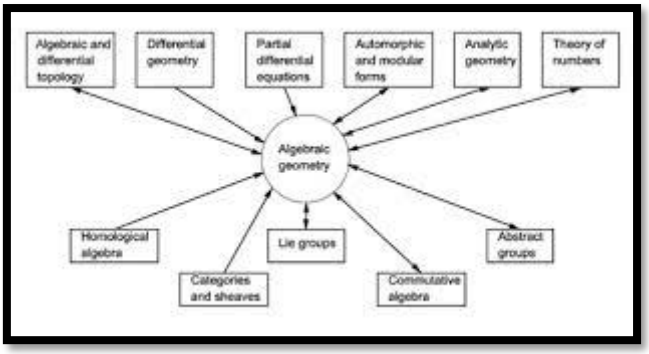

Figure 3: Basic Principles of Algebraic Geometry

(Source: Daviddarling.info, 2025)

3.2 Algebraic Curves and Surfaces in Cryptography

Cryptography utilizes algebraic curves, especially elliptic curves, to construct cryptographic systems. The algebraic features of elliptic curves are used in elliptic curve cryptography (ECC) to create secure encryption systems with fairly small key sizes. The construction of such systems is greatly aided by the essential role of algebraic geometry, which provides the theory needed to design and analyze the security operations of elliptic curve-based encryption. In the field of homomorphic encryption the role of algebraic geometry becomes even clearer, where methods from algebraic geometry are used in particular to increase performance and security in encryption systems.

3.3 Connection Between Algebraic Geometry and Homomorphic Encryption

Algebraic geometry can be applied most naturally here. The polynomial rings, which are the main objects in the homomorphic encryption schemes are related to the algebraic structures studied in the algebraic geometry. By applying algebraic geometric methods =, the researcher can construct efficient encryption schemes which supports more operations, is more secure and has lesser computations as well. The important contribution of algebraic geometry is given in the use of algebraic structure for optimizing encryption process. Say for example, the use of certain geometric objects like curves, surfaces etc. help to minimize the noise generated in encryption and decryption.

Iv. Homomorphic Encryption And Algebraic Geometry In Privacy-Preserving Machine Learning

4.1 Privacy Challenges in Machine Learning

Privacy is one of the biggest challenges involved in deploying machine learning models. As machine learning algorithms become more sophisticated, their ability to analyze large amounts

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of data, mostly containing sensitive information such as medical records, financial transactions and personal identifiers, is increased. In classical machine learning scenarios this information must be shared with third parties for model training, resulting in substantial privacy risks. Some of the most important threats to privacy in machine learning are data breach, attack by model inversion and adversarial attack. Solutions to privacy threats in the machine learning paradigm consist of privacy-preserving machine learning techniques including federated learning, secure multi-party computation (SMPC) and homomorphic encryption [10].

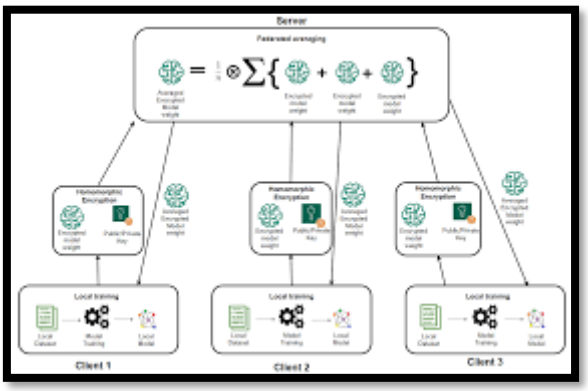

Figure 4: Homomorphic Encryption and Algebraic Geometry in Privacy-preserving Machine Learning

(Source: Mdpi.com, 2023)

4.2 Privacy-Preserving Machine Learning with Homomorphic Encryption

Homomorphic encryption offers this capability through the use of encryption of data in conjunction with the models that represent that data. In sensitive areas such as finance and health care, this may be very important. If information is compromised, serious consequences could result as a result. A situation, for example could be where there is a problem in the health area with encryption of data, such as health records or medical imagery, and the process could result in knowledge being obtained about patients, which might be of some assistance in medical predictions.

4.3 Role of Algebraic Geometry in Enhancing Homomorphic Encryption

In the development of homomorphic encryption schemes it is very important from a security and efficiency point of view to understand algebraic geometry. One of the problems of working with machine learning on encrypted data is that there are computational costs associated with the computations needed to compute on the encrypted data. There is again a considerable cost involved in performing the encryption and decryption, which limits the extent to which such systems will scale across either large size datasets or complicated models. With the use of a number of algebraic geometry techniques, researchers have been successful in optimizing homomorphic encryption schemes which allow for greater efficiency in the realm of machine learning systems [11].

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

V. Challenges And Limitations

5.1 Computational Overhead and Efficiency Issues

While homomorphic encryption has many advantages, one of the chief drawbacks is the overhead of the computations involved. The performance of computations on encrypted data is highly memory intensive as compared to working with the clear text form of data whereby the desirable application of HE to large scale machine learning models becomes impractical. The difficulty is exacerbated in the case of fully homomorphic encryption which allows all computations to be made on encrypted data but results, of course, in increased computational complexity. This has caused research on this area to continue in order to optimize homomorphic encryption schemes so that a minimum of computational overhead occurs rendering them more applicable in practical and real-world scenarios (12).

5.2 Scalability Concerns

Another disadvantage of homomorphic encryption is its scalability problem. With more and more complex machine learning models and the associated data set sizes, the cost involved with HE gives rise to an insurmountable barrier to universal acceptance. Indeed, some homomorphic ciphers are efficient for small data sets, but are inefficient for large and higher dimensional data sets associated with deep learning.

5.3 Security Considerations

Homomorphic encryption is highly secure, although it is not immune to attack. Attacks using cryptography - such as side-channel and quantum attacks - may still be threats to the security of homomorphic encryption schemes. Because they rely on hard mathematical problems (such as the Learning with Errors problem), the security of HE schemes rests on the security of the cryptographic assumptions.

Vi. Recent Advancements And Research

6.1 Current State of Research

The area of homomorphic encryption has made major strides since the 2009 inception of fully homomorphic encryption (FHE) by Craig Gentry. Gentry’s achievement in supplying arbitrary operations on encrypted data laid the groundwork for a new generation of cryptographic techniques which preserve privacy. Much of the research in the time since has been directed towards improvements in efficiency, scalability, and virtue of FHE schemes. These economic conditions concerning HE have improved largely by reducing the computational overhead associated with HE through optimizing the encryption schemes and faster algorithms. Techniques such as bootstrapping, which reduces the noise accumulated by the computations, have improved the utility for the FHE scheme. Applications in lattice-based cryptography have led to significant results because this important mathematical model has been applied directly to many of the homomorphic encryption schemes [13].

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6.2 Key Breakthroughs in Homomorphic Encryption

In recent times there has been many of great developments in homomorphic encryption, with the most notable being in our FHE schemes [10]. There has been a reduction in the costs of the computations necessary to perform operations over encrypted data. There has been great developments in noise fighting techniques and bootstrapping [7]. This allows a longer chain of computations over encrypted data to be performed without degradation of performance. In addition, also there has been a desire to decrease the sizes of ciphertexts which can often have a dramatic effect on the performance of homomorphic encryption schemes. The smaller ciphertexts not only give a decrease of the costs of the computations necessary, but also allowing the encryption of data on a more massive scale allowing HE to be applied to more massively sized data sets, and more complex ML models. An introduction of hybrid schemes which makes use of the advantages of homomorphic encryption and other cryptographic structures have shown promise [14].

6.3 Emerging Trends in Algebraic Geometry for Cryptography

The continuing advancement of algebraic geometry plays an important role in further enhancing the security and efficiency of homomorphic encryption schemes. New techniques are being explored that utilize algebraic geometric methods such as elliptic curves and lattice based cryptography that will hopefully improve the performance of HE. These new methods will lead to the possibility of finding new solutions to the complications associated with the application of homomorphic encryption in the experimental results presented in this section expressive of privacy-preserving machine learning.

Vii. Ethical And Practical Considerations

7.1 Ethical Issues in Privacy-Preserving Machine Learning

Any new technology brings its own ethical considerations. For example, privacy-preserving machine learning algorithms based on homomorphic encryption raise significant ethical issues. One of the most important of these problems involves the lack of knowledge as to how the data are processed in the encrypted format. Since the calculations are performed on the encrypted structures without knowing the values in plaintext, it is difficult to determine how the data at the final stage is affected by the calculations.

7.2 Balancing Privacy and Performance

The need to achieve a balance between privacy and performance is a key part of the development of machine learning models which respect privacy, and homomorphic encryption is very strong on privacy assurances, while being considerable in computational cost, which has an effect on the performance of the machine learning models. Since the homomorphic schemes are computationally costly, achievement of the balance between the security of data privacy and the efficient performance of machine learning models is a key need. While potential enhancement of this encryption scheme is being looked at as one means of reducing the computational costs of privacy-preserving scheme usage, the balance of privacy and performance remains a problem. This balance is of particular significance in reality, in

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

applications, when speed and accuracy of machine-learning models is so very much of an importance. Areas such as health-care, when gains in regard to timing may substitute lives saved, and finance, where time of decision is of great importance, call for privacy preserving Enhanced machine learning models which will give both secrecy and will be effectively carried out [15].

7.3 Practical Implementation in Industry

The emergence of homomorphic encryption technology into machine learning algorithms creates a number of technical and regulatory problems. Some of these are of a technological nature, that is to say there is the problem of the overhead of the calculations to be carried out in using the homomorphic encryption in order that the model itself not be slowed down in its capacity. One of these factors is of the nature of legal regulations, because some sectors of industries have problems with various and sometimes complex privacy regulations relating to the data, such as the regulations existing in Europe under the GDPR and the California regulation on personal data, known as the CCPA, which lay down very strict limitations on the handling and treatment of personal data.

Viii. Conclusion

The vastly improved privacy preserving technolgies of homomorphic encryption with that from the new algebraic geometric thought are improved possibilities for the implementation of machine learning techniques. These new techniques of encrypted data base analysis will lead to the encrypted information on sensitive items being able to be imparted. In other words, homomorphic encryption will enable to different and important item which will lead to lot of possibliities having to do with encypted data problems of the present. With this new and great ideas of new computer stored information techniques will help fasten up the thing which are presented with the grow and great bad results in commercial life which those involved with think will lead to vastly increased scandalous affairs of the policing business of the country. If they are represented and subsequentibilty analysis with the new present-day legal ideas of algebraic geometry and with the fast flow of growing knowledge will make speedily attainable the various and rapidly improved techniques of homomorphic encryption for not only work to the common people of the various businesses and advertisers but also to the intelligent patrons who take now of the thorny matter. But things in this study are happening with every day so fast that the then forces will become realized rapidly expecially with the ever new artists and users coming on the field. Allowed to go rapidly there will be very great things done with physics and creative illogic of the mathematically brilliant and esoteric theorist in each departement of the home of mind. Ultimately with this research of a fond relationship between the quickening increasing and strong solid evidence with something which will be preament of all the fruits and reply that will eventually lead to the laying down of modernity. What great things might not attainable by this element of time turning of science and abstract nonsense of are truly great science and civilization that we shall have.

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IX. References

[1] Lee JW, Kang H, Lee Y, Choi W, Eom J, Deryabin M, Lee E, Lee J, Yoo D, Kim YS, No JS. Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. iEEE Access. 2022 Mar 14; 10:30039-54.

[2] Podschwadt R, Takabi D, Hu P, Rafiei MH, Cai Z. A survey of deep learning architectures for privacy-preserving machine learning with fully homomorphic encryption. IEEE Access. 2022 Nov 3; 10:117477-500.

[3] Frimpong E, Nguyen K, Budzys M, Khan T, Michalas A. Guardml: Efficient privacy-preserving machine learning services through hybrid homomorphic encryption. InProceedings of the 39th ACM/SIGAPP Symposium on Applied Computing 2024 Apr 8 (pp. 953-962).

[4] Yuan J, Liu W, Shi J, Li Q. Approximate homomorphic encryption-based privacy-preserving machine learning: a survey. Artificial Intelligence Review. 2025 Jan 6;58(3):82.

[5] Terziyan V, Bilokon B, Gavriushenko M. Deep Homeomorphic Data Encryption for Privacy Preserving Machine Learning. Procedia Computer Science. 2024 Jan 1; 232:2201-12.

[6] Xu R, Baracaldo N, Joshi J. Privacy-preserving machine learning: Methods, challenges and directions. arXiv preprint arXiv:2108.04417. 2021 Aug 10.

[7] Meier D, Troncoso Pastoriza JR. Privacy Preserving Machine Learning. Available at SSRN 4595287. 2023 Sep 30.

[8] Salman AD, Al-Dahhan RR. Ensure Privacy-Preserving Using Deep Learning. Mesopotamian Journal of CyberSecurity. 2025 Jul 19;5(2):703-20.

[9] El Hadji Mamadou DI, ARABI W, BKAKRIA A, YAICH R. A Comprehensive Survey of Privacy-Preserving Decision Trees Based on Homomorphic Encryption. Cryptology ePrint Archive. 2025.

[10] Abdullah S. Survey: Privacy-Preserving in Deep Learning based on Homomorphic Encryption. Basrah Researches Sciences. 2022 Jun 30;48(1):10-22.

[11] Balaban B, Magara SS, Yilgor C, Yucekul A, Obeid I, Pizones J, Kleinstueck F, Perez-Grueso FJ, Pellise F, Alanay A, Savas E. Privacy-preserving machine learning (PPML) inference for clinically actionable models. IEEE Access. 2025 Feb 10.

[12] Pulido-Gaytan B, Tchernykh A, Leprévost F, Bouvry P, Goldman A. Toward understanding efficient privacy-preserving homomorphic comparison. IEEE Access. 2023 Sep 14; 11:102189-206.

[13] Tan S, Knott B, Tian Y, Wu DJ. CryptGPU: Fast privacy-preserving machine learning on the GPU. In2021 IEEE Symposium on Security and Privacy (SP) 2021 May 24 (pp. 1021-1038). IEEE.

Received: August 07, 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[14] Carpov S, Gama N, Georgieva M, Jetchev D. GenoPPML–a framework for genomic privacy-preserving machine learning. In2022 IEEE 15th International Conference on Cloud Computing (CLOUD) 2022 Jul 10 (pp. 532-542). IEEE.

[15] Adamsetty R, Cherukuri AK, Jonnalagadda A. Securing machine learning models: Homomorphic encryption and its impact on classifiers. Annals of Mathematics and Computer Science. 2025 Jan 10;26:141-58.

Received: August 07, 2025