Grenze International Journal of Engineering and Technology, Jan Issue

Privacy Preserving Support Vector Machines using Ring Learning with Errors

Anirudhha Subramanian[1], Harshitha Devi Gokaraju[2] and Supraja P[3]
[1-3]Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Kattankulathur - 603203, Kancheepuram (D.t), Tamil Nadu.
Email: as6214@srmist.edu.in, hg9627@srmist.edu.in, suprajap@srmist.edu.in

***Abstract*— The growing concern of protecting privacy through machine learning has led to an emphasis on data sharing and analysis. Support Vector Machines (SVMs) are frequently used for classifying and predicting tasks and are renowned for their efficiency in numerous applications and their capacity to handle both linear and non-linear data. This paper presents a privacy-preserving SVM training scheme, maintained through using Ring Learning with Errors (Ring-LWE). The Ring-LWE function, which is composed of lattice-based cryptography, offers a secure framework for realizing privacy-preserving machine learning. Encrypted data sets of various sizes are trained, and the difference in accuracy between encrypted and normal datasets is negligible.For that reason, during the training of models that use confidential information, BFV(Brakerski/Fan-Vercauteren) encryption method can be applied to maintain the confidentiality of the data.**

***Index Terms*— Support Vector Machine, Privacy preserving, Homomorphic encryption, Ring-learning with errors**

I. INTRODUCTION

Privacy-preserving support vector machines (SVMs) are a promising approach to protect private data while carrying out machine learning tasks. The need for data security and privacy has become increasingly important as the world is digitized. Homomorphic encryption has gained a lot of attention in the field of machine learning for privacy-preserving SVMs. Support vector machines are commonly used for data mining and machine learning applications, such as image recognition, credit scoring, and medical diagnosis. Nevertheless, sharing the entire dataset can sometimes be a challenge due to privacy and security considerations. To overcome this obstacle, privacy-preserving support vector machines using homomorphic encryption have been developed. These methods allow the data to be studied and classified without posing any risks of unauthorized access to the original data.
Our research employed the BFV (Brakerski-Fan-Vercauteren) scheme, a reliable post-quantum cryptography method, to secure the whole dataset. This encryption has exceptional resistance to quantum attacks, making it an ideal choice for guaranteeing durable data security. Additionally, our approach uses a special technique called homomorphic encryption, which enables us to execute math operations on the encrypted data without requiring its decryption. This is a pivotal benefit for privacy-preserving machine learning, allowing us to obtain useful findings through computation while keeping the confidential information private.
This study aimed to show the effectiveness and practicality of using encryption for machine learning tasks. A Support Vector Machine (SVM) model was trained using the entire dataset in its encrypted form, which represents

Grenze ID: 01.GIJET.10.1.73

a significant improvement compared to traditional methods that require data to be decrypted before training, thus potentially compromising privacy. To evaluate the impact of the encryption and computation strategy, experiments were conducted on several different datasets, spanning various domains and sizes. These datasets were then encrypted and SVM models were trained on them. The performance of these models was then compared to those trained on their original, unencrypted datasets.

Our research contributes to the field of privacy-preserving machine learning by providing valuable insights into the trade-offs between data privacy and model accuracy. We conducted a comparison to assess the extent to which data encryption affects the predictive capabilities of an SVM model, showing the practicality and limitations of applying privacy-preserving techniques in a real-world context. Moreover, our findings also demonstrate the feasibility of training SVM models on fully encrypted datasets using the BFV scheme. It highlights the potential benefits and challenges associated with this approach, as well as the importance of post-quantum cryptography methods in maintaining the security of sensitive data used in machine learning applications. We provide valuable guidance for machine learning practitioners in their future endeavors with secure and confidential data analysis.

II. Literature Review

Due to developments in technology related to data analysis, there have been ethical concerns relating to privacy. The usage of Computation on Encrypted Data (COED) has been seen as a way to keep people's details private while simultaneously allowing data operations to be done. Kyung Hyun Han et al. [1] gave their suggestion for a fresh approach to efficiently employing a Gaussian sampler as well as a GPU-accelerated NTT algorithm to hasten encryption. This has applications in protecting the privacy of convolutional neural network calculations and privacy-preserving SVM classification. They evaluated the RLWE-IPFE encryption algorithm and determined the best optimizations for GPU processors. They suggested ways to assist in optimization, namely performing computations in parallel, removing the need for synchronization among threads, and implementing a more efficient indexing pattern.

In 2022, Yange Chen et al.[2] evaluated past research concerning privacy-protective SVM approaches, comprising of those that apply secure two-party computations, secure multi-party computations, and homomorphic encryption, and acknowledged that while these strategies have the potential to be good, they regularly confront substantial computational demands and restricted scalability. To tackle these shortcomings, they introduced a new process which utilizes a distributed two trap doors typical key cryptosystem (DT-PKC) during the SVM classification procedure to preserve the privacy of patients, and examined the semantic security of the DT-PKC and BGN cryptosystems using the ideal-reality game and security examination technique.

Pu Duan et al. [3] proposed a novel and proficient classification model utilizing a safe calculation system for nonlinear SVMs depending on the Gaussian kernel capacity. This protocol can be developed to different kernel capacities and lessen the measure of encoded information, make the figuring procedure more straightforward, and upgrade calculation productivity. They presented a system that incorporates a disseminated two trapdoors public-key cryptosystem that guarantees the secrecy of private information and support vectors.

III. Motivation

Today, in our increasingly data-driven world, privacy worries have hit unprecedented levels. With AI and artificial intelligence continuing to develop fast, there is a strong necessity to protect delicate facts, especially when it comes to businesses such as healthcare, finance, and individual analysis. In our attempts to fight against these protection difficulties, we wanted to step in.

Moreover, The Support Vector Machine (SVM) has become a beneficial tool in the machine learning field, renowned for its proficiency in categorizing and regression jobs. Unfortunately, classic SVM initiatives normally demand direct access to unprotected facts; which can be a severe danger to the safety of private information.

R-LWE is a robust cryptographic technique known for providing secure data protection and encryption in the post-quantum era. We were thus intrigued by the prospect of using sophisticated cryptographic techniques to ensure that sensitive data are protected, as well as enabling computations on them. It was a compelling incentive to look at what could be achieved by bridging the gap in machine learning and cryptography.

IV. Problem Domain

The field of Privacy-Preserving Support Vector Machines (SVMs) with Ring Learning With Errors (Ring-LWE) is multifaceted, encompassing subjects from machine learning and data analysis utilizing SVMs, encryption and

secure computation through Ring-LWE, and knowledge of privacy hazards and their potential risks, in addition to recognizing the significance of data privacy and various categorization jobs.
Homomorphic encryption is a form of cryptography that involves transforming data into a form of encryption that can be used and studied in the same way as the original. This type of encryption allows for complex mathematical operations to be performed on encrypted data without sacrificing the integrity of the encryption. Ring Learning with Errors is a type of cryptography that relies on lattice problems. The fundamental mathematical problem in Ring Learning with Errors is to identify the coefficients of a hidden secret polynomial hidden in a set of chaotic polynomial evaluations. These evaluations are composed of a small amount of random noise that is multiplied by a random polynomial. The challenge lies in separating the hidden polynomial from the noisy evaluations, a task that is thought to be computationally difficult.

V. Problem Definition

This research is focused on finding a way to reconcile data protection and accuracy in machine learning. To do so, BFV, a scheme that defends against quantum attacks, and homomorphic encryption are utilized. A Support Vector Machine (SVM) can be trained on encrypted data, eliminating the need to decrypt it, which is the goal of this research. Experiments have been conducted to evaluate the effects of encryption on model performance and to explore the feasibility and limitations of the approach.
The challenge here is to establish a secure and confidential data analysis system for machine learning using sophisticated encrypted data techniques. Examples of such encryption systems include the BFV scheme and homomorphic encryption to train models on the data without compromising private or sensitive information[10]. This requires further investigation into how encryption impacts model accuracy and to devise effective strategies for safeguarding privacy while still obtaining meaningful results from the machine learning process.

VI. Statement

This research aims to understand the potential impact of data encryption on Support Vector Machine (SVM) models while preserving data privacy in machine learning. It tests the effectiveness of BFV scheme and holomorphic encryption on fully encrypted datasets in order to provide guidance on data security for real-world machine learning applications.

VII. Innovative Content

The paper "Privacy-Preserving Multi-Class Support Vector Machine Model on Medical Diagnosis" [2] explores a novel combination of homomorphic encryption and privacy-preserving multiclass support vector machine that will allow secure and private clinical diagnosis using cloud computing. It provides a viable option for medical professionals to obtain diagnosis support without surrendering individual data and confidentiality of the service providers.
With an improved performance on graphics processing units, the authors of the paper "cuFE: High Performance Privacy Preserving Support Vector Machine with Inner-Product Functional Encryption" [1] proposed a new implementation of IPFE. Optimization of the most laborious stage inside the IPFE plan led them to propose fresh tactics that could parallelize the Gaussian sampling. Compared to other approaches, the implemented method showed considerable speedups.

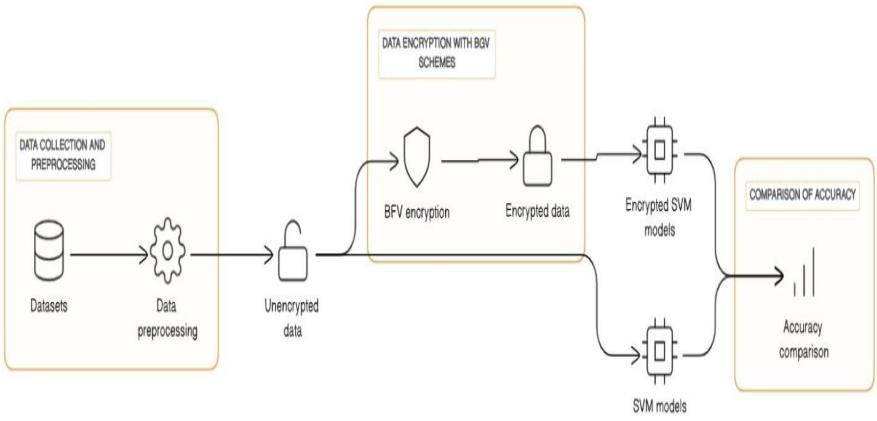
VIII. Problem Formulation

A. Data Collection and Preprocessing

Initially, we had carefully chosen datasets which covered a wide range of sizes, complexity and domains. This has enabled our analysis to be comprehensive and reflect the realities of today's world. Data sets were made up of data from a variety of areas, such as the health sector, finance and Social Sciences. Prior to model training, we conducted thorough data preprocessing to cleanse, standardize, and prepare the datasets for analysis. In order to assure the quality and coherence of data collected in our studies, this step was crucial.

B. SVM Model Training

Unencrypted Data: We took the unencrypted data and trained SVM models with it. This was used for evaluation purposes. The accuracy of these models, which represent their actual performance in the most common and standard form, has been recorded.



C. Data Encryption with BFV Schemes

Encryption of the same datasets using BFV has been a key stage in this process. It is known that this cryptographic technology can be used to secure data, while allowing for the computation of encrypted data. The use of BFV has ensured that the information is confidential and protected over an extended period of analysis [11]. In order to protect sensitive information, this encryption step introduces a new level of protection with regard to the privacy issues that arise when dealing with Personal or Confidential Information.

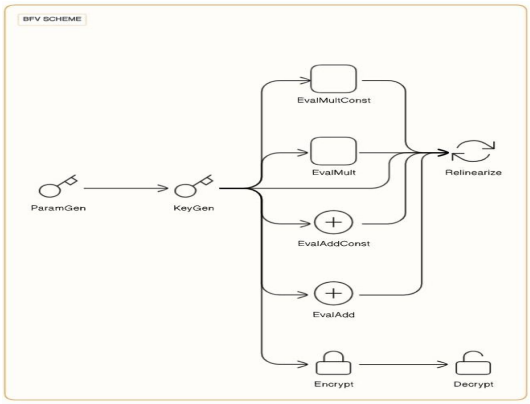
D. SVM Model Training

Encrypted Data: After encrypting our datasets, we trained SVM models with them[9]. A change from typical practices, this innovative method aimed to determine if machines could learn from encrypted data with better outcomes. Our recording of their accuracy gave us a foundation for assessing how they compared to baseline SVM models taught on uncovered information.

E. Comparison of Accuracy

The accuracy of SVM models trained on both the encrypted and unencrypted datasets was meticulously compared in the analysis's final stage. We were able to determine how data encryption affected model performance. It provided useful insights into the practicalities of using encryption algorithms like BFV in machine learning scenarios, shedding light on the trade-offs between privacy and utility.

IX. Solution Methodologies



BFV is a type of fully homomorphic encryption, which allows calculations to be carried out on encrypted data without having access to the decryption key[7]. This is achieved by forming two distinct rings: a plaintext ring and a cipher text ring. The plaintext ring is used to store unencrypted messages while the cipher text ring holds encrypted messages. As the homomorphism property of BFV establishes a link between these two rings [8], it is possible to apply functions between the two rings without having to decrypt data. This means that computations can be done on encrypted data without need for decryption.

In order to use the BFV scheme, one must first generate public and private keys. The process begins by selecting two prime numbers p and q such that q divides p-1. Subsequently, two polynomials f(x) and g(x), with coefficients in the integers modulo q, are chosen. The product of f(x) and g(x) is computed, modulo p, to produce h(x). A secret key is also chosen in the form of a polynomial of degree n-1, with coefficients in the integers modulo q. These two values as well as the parameters p, q, and n are used to create the public key (pk) and secret key (sk).
The encryption process is composed of the following steps:

1. Plaintext message m is changed into a polynomial m(x) which holds n-1 coefficients in the form of integers modulo q.
2. A random polynomial e(x) with n-1 coefficients expressed as integers modulo q is created.
3. Ciphertext c is generated by the addition of m(x) and 2e(x) modulo p, where the coefficients are each added individually.
4. The ciphertext c is encrypted using the public key pk.

The process of deciphering involves these steps:

1. Utilize the top-secret key sk to decrypt the ciphertext c, which yields the polynomial c'(x).
2. Employ the polynomial q to derive the message polynomial m'(x) by computing c'(x) modulo q.
3. Extract the plain text message m via deciphering the message polynomial m'(x).

The security of the BFV system is based upon how challenging it is to find the key s if one only has access to the public key pk and a collection of noisy ciphertexts.

TABLE I: HEART_FAILURE_CLINICAL_RECORDS DATASET

age	anaemia	creatinine_phosphokinase	diabetes	ejection_fraction	high_bp	platelets	serum_creatinine	serum_sodium	sex	smoking	time	DEATH_EVENT
75	0	582	0	20	1	265000	1.9	130	1	0	4	1
55	0	7861	0	38	0	263358	1.1	136	1	0	6	1
65	0	146	0	20	0	162000	1.3	129	1	1	7	1
50	1	111	0	20	0	210000	1.9	137	1	0	7	1
65	1	160	1	20	0	327000	2.7	116	0	0	8	1
90	1	47	0	40	1	204000	2.1	132	1	1	8	1
75	1	246	0	15	0	127000	1.2	137	1	0	10	1
60	1	315	1	60	0	454000	1.1	131	1	1	10	1
65	0	157	0	65	0	263358	1.5	138	0	0	10	1
80	1	123	0	35	1	388000	9.4	133	1	1	10	1

X. RESULTS AND SENSITIVITY ANALYSIS

In summary, the analysis of multiple datasets reveals a consistent trend: Compared to unencrypted data, model performance suffers when trained on encrypted information. Due to data encryption, this decrease is expected because it introduces additional noise and complexity that complicate pattern recognition in models.
With varying drops across datasets, accuracy degenerates; 3%, 2%, and 5% being the respective decrements felt by Datasets 1 through 3. Data characteristics and encryption approaches differ in these cases. Encryption offers significant advantages over non-encrypted data despite slight reductions in model precision.

XI. DATA MODEL

Davide Chicco and Giuseppe Jurman [4] propose the possibility of predicting the likelihood of survival in heart failure cases using just two health metrics: serum creatinine and ejection fraction. This approach of machine learning relies on a single data point for each individual, where each row stands for a person and every column additionally designates a unique health metric. Besides, the study implies that these two key factors might be incredibly useful in deducing the fate of people convalescing from heart failure.
Table II consists of more than 4,240 records and 16 attributes[5], enabling prediction of a 10-year risk of coronary heart disease (CHD). Its value to researchers and healthcare professionals is immeasurable as it assists them in assessing and understanding the risks related to CHD. With the support of this dataset, predictive models can be developed to highlight those at greater risk of this potentially deadly heart condition and allow for timely interventions and proactive healthcare strategies.
Table III, entitled "Gender Recognition by Voice and Speech Analysis," was built with the goal of distinguishing between male and female voices. It consists of 3,168 sound recordings with both male and female speakers. This dataset is a valuable asset to those exploring the development of models which can identify gender through analyzing voice and speech.

TABLE II: FRAMINGHAM DATASET

male	age	education	current smoker	CigsPerDay	BPMeds	PrevalentStroke	PrevalentHyp	diabetes	TotChol	sysBP	diaBP	BMI	heartRate	glucose	TenYearCHD
1	39	4	0	0	0	0	0	0	195	106	70	26.97	80	77	0
0	46	2	0	0	0	0	0	0	250	121	81	28.73	95	76	0
1	48	1	1	20	0	0	0	0	245	127.5	80	25.34	75	70	0
0	61	3	1	30	0	0	1	0	225	150	95	28.58	65	103	1
0	46	3	1	23	0	0	0	0	285	130	84	23.1	85	85	0
0	43	2	0	0	0	0	1	0	228	180	110	30.3	77	99	0
0	63	1	0	0	0	0	0	0	205	138	71	33.11	60	85	1
0	45	2	1	20	0	0	0	0	313	100	71	21.68	79	78	0
1	52	1	0	0	0	0	1	0	260	141.5	89	26.36	76	79	0
1	43	1	1	30	0	0	1	0	225	162	107	23.61	93	88	0

TABLE III. VOICE DATASET

meanfreq	sd	median	Q25	Q75	IQR	skew	kurt	sp.ent	sfm	mode	centroid	meanfun	minfun	maxfun	meandom	mindom	maxdom	dfrange	modindx	label
0.05978	0.06424	0.03203	0.01507	0.09019	0.07512	12.8635	274.403	0.89337	0.49192	0	0.05978	0.08428	0.0157	0.27586	0.00781	0.00781	0.00781	0	0	1
0.06601	0.06731	0.04023	0.01941	0.09267	0.07325	22.4233	634.614	0.89219	0.51372	0	0.06601	0.10794	0.01583	0.25	0.00901	0.00781	0.05469	0.04688	0.05263	1
0.07732	0.08383	0.03672	0.0087	0.13191	0.12321	30.7572	1024.93	0.84639	0.4789	0	0.07732	0.09871	0.01566	0.27119	0.00799	0.00781	0.01563	0.00781	0.04651	1
0.15123	0.07211	0.15801	0.09658	0.20796	0.11137	1.23283	4.1773	0.96332	0.72723	0.08388	0.15123	0.08896	0.0178	0.25	0.2015	0.00781	0.5625	0.55469	0.24712	1
0.13512	0.07915	0.12466	0.07872	0.20604	0.12732	1.10117	4.33371	0.97196	0.78357	0.10426	0.13512	0.1064	0.01693	0.26667	0.71281	0.00781	5.48438	5.47656	0.20827	1
0.13279	0.07956	0.11909	0.06796	0.20959	0.14163	1.93256	8.3089	0.96318	0.73831	0.11256	0.13279	0.11013	0.01711	0.25397	0.29822	0.00781	2.72656	2.71875	0.12516	1
0.15076	0.07446	0.16011	0.0929	0.20572	0.11282	1.53064	5.9875	0.96757	0.76264	0.0862	0.15076	0.10594	0.02623	0.26667	0.47962	0.00781	5.3125	5.30469	0.12399	1
0.16051	0.07677	0.14434	0.11053	0.23196	0.12143	1.39716	4.76661	0.95925	0.71986	0.12832	0.16051	0.09305	0.01776	0.14414	0.30134	0.00781	0.53906	0.53125	0.28394	1
0.14224	0.07802	0.13859	0.08821	0.20859	0.12038	1.09975	4.07028	0.97072	0.77099	0.2191	0.14224	0.09673	0.01796	0.25	0.33648	0.00781	2.16406	2.15625	0.14827	1
0.13433	0.08035	0.12145	0.07558	0.20196	0.12638	1.19037	4.78731	0.97525	0.80451	0.0117	0.13433	0.10588	0.0193	0.2623	0.34036	0.01563	4.69531	4.67969	0.08992	1

XII. COMPARISON OF RESULTS

Datasets	Accuracy of training model of unencrypted data	Accuracy of training model of encrypted data
Dataset 1	71	68
Dataset 2	63	61
Dataset 3	67	62

Across all datasets, accuracy declines when the model is trained using encrypted data as opposed to unencrypted data. This is expected since transforming the data can introduce extra noise and complexity, hindering the model's ability to recognize the patterns. The dip in accuracy is steady for all datasets, indicating that the effects of encryption on model efficiency remain relatively constant. This consistency can help in scenarios where privacy and protection are essential for decision-making and resource distribution. Yet, the degree of accuracy decrease varies from dataset to dataset. Dataset 1 experienced a decrease of 3 percentage points, in Dataset 2 it was 2 percentage points, and for Dataset 3 it was 5 percentage points. These variations could be due to the specific traits of the data as well as the encryption methods used. The difference in accuracy between the encrypted and normal datasets was negligible.

XIII. JUSTIFICATION OF THE RESULTS

The paper called "cuFE: High Performance Privacy Preserving Support Vector Machine with Inner-Product Functional Encryption" examines various techniques for implementing privacy-preserving Support Vector Machines (SVMs). The authors make use of homomorphic encryption algorithms as a way to secure the SVMs.

A different paper, "Privacy-Preserving Multi-Class Support Vector Machine Model on Medical Diagnosis," looks at the implementation of two encryption schemes based on Deterministic Trapdoor Public Key Cryptography (DT-PKC) and the BGN cryptosystem to achieve privacy preservation when using an SVM model.
Our study focuses on utilizing the BFV encryption scheme for homomorphic encryption in regards to the implementation of privacy-preserving Support Vector Machines. This method allows us to make sure that sensitive data is kept secure while allowing us to do operations on the encrypted data within the context of SVM, which proves the efficiency of advanced cryptographical techniques in preserving privacy with a maintained utility of machine learning models. This aligns with the strategies discussed in prior papers that also looked into DT-PKC, BGN cryptosystem, and homomorphic encryption.

XIV. Conclusion

Through our experiments, we trained Support Vector Machine (SVM) models using both normal and encrypted datasets of various sizes. The remarkable finding was that the difference in accuracy between the encrypted and normal datasets was negligible.. This outcome underscores the effectiveness of our approach in preserving data privacy within SVM. It serves as strong evidence that the use of Ring Learning With Error encryption allows us to secure and process data while still achieving the desired SVM results, affirming the practicality of privacy-preserving machine learning.

References

[1] K. H. Han, W. -K. Lee, A. Karmakar, J. M. B. Mera and S. O. Hwang, "cuFE: High Performance Privacy Preserving Support Vector Machine With Inner-Product Functional Encryption," in IEEE Transactions on Emerging Topics in Computing

[2] Y. Chen, Q. Mao, B. Wang, P. Duan, B. Zhang and Z. Hong, "Privacy-Preserving Multi-Class Support Vector Machine Model on Medical Diagnosis," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 7, pp. 3342-3353, July 2022.

[3] Q. Mao, Y. Chen, P. Duan, B. Zhang, Z. Hong and B. Wang, "Privacy-Preserving Classification Scheme Based on Support Vector Machine," in IEEE Systems Journal, vol. 16, no. 4, pp.5906-5916, Dec. 2022

[4] Davide Chicco, Giuseppe Jurman: Machine learning can predict survival of patients with heart failure from serum creatinine and ejection fraction alone. BMC Medical Informatics and Decision Making 20, 16 (2020)

[5] Ashish Bhardwaj. (2022). Framingham heart study dataset [Data set]. Kaggle

[6] A. C. Mert, E. Öztürk and E. Savaş, "Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 353-362, Feb. 2020

[7] Ilia Iliashenko, Vincent Zucca. Faster homomorphic comparison operations for BGV and BFV. Proceedings on Privacy Enhancing Technologies, 2021, 2021 (3), pp.246-264.⟨10.2478/popets-2021-0046⟩. ⟨hal-03506798⟩

[8] Ilia Iliashenko, Vincent Zucca. Faster homomorphic comparison operations for BGV and BFV. Proceedings on Privacy Enhancing Technologies, 2021, 2021 (3), pp.246-264. ⟨10.2478/popets-2021-0046⟩. ⟨hal-03506798⟩

[9] T. Maekawa, A. Kawamura, Y. Kinoshita and H. Kiya, "Privacy-Preserving SVM Computing in the Encrypted Domain," 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Honolulu, HI, USA, 2018, pp. 897-902,

[10] Saerom Park, Junyoung Byun, and Joohee Lee. 2022. Privacy-Preserving Fair Learning of Support Vector Machine with Homomorphic Encryption. In Proceedings of the ACM Web Conference 2022 (WWW '22). Association for Computing Machinery, New York, NY, USA, 3572–3583.

[11] Huang, H., Wang, Y. & Zong, H. Support vector machine classification over encrypted data. Appl Intell 52, 5938–5948 (2022).