Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Employing Brakerski/Fan-Vercauteren's for secure data classification in GRU networks for sentiment analysis

Nibras Hadi Jawad

Department of Mathematics, College of Education, University of Al-Qadisiyah, Iraq. Email: nibras.hadi@qu.edu.iq

ARTICLE INFO

Article history:
Received: 25 /09/2025
Rrevised form: 09/11/2025
Accepted : 16 /11/2025
Available online: 30/12/2025

Keywords:

Homomorphic encryption,

BFV, GRU.

ABSTRACT

Due to the widespread use of technology and the resulting vast amounts of big data, which are beneficial for product and application development, sentiment analysis is one such benefit. It allows users to understand their opinions and guide development and growth in the right direction. However, the use of sensitive textual data remains a matter of privacy and requires careful handling. Therefore, users must be provided with the necessary guarantees regarding the security of their privacy. This work introduces a privacy-preserving binary sentiment analysis system that categorizes text as positive or negative through comprehensive contextual understanding while safeguarding user data using homomorphic encryption. The Gated Recurrent Unit (GRU) model is trained on unencrypted data of type IMDB and performs inference on encrypted inputs with the BFV graded homomorphic encryption technique. To facilitate efficient encrypted inference, it was replaced non-polynomial activations with low-degree polynomial approximations, reduce the depth of multiplication. The accuracy attained by the proposed technique is 90.1%.

PHD.

https://doi.org/ 10.29304/jqcsm.2025.17.42581.

1. Introduction

One of the fundamental requirements that users seek is maintaining their privacy, especially when commenting and giving opinions about the products and services offered by companies. This procedure ensures comfort and credibility in expressing opinions, as the other party is unaware of the content of the comment. Simultaneously, it allows the product owner to obtain the information from users more accurately for analysis, product improvement, and development. Therefore, one of the best guarantees for maintaining user privacy is the use of homomorphic encryption, which allows data processing without the need for decryption. Exactly using BFV (Brakerski/Fan-Vercauteren's) [1], which maintains data privacy and confidentiality, along with deep neural networks GRU (Gated Recurrent Unit) for data analysis [2], is very beneficial. However, problems and challenges arise regarding compatibility and the ability of the two systems to work together to obtain accurate and efficient analytical results. Since each system (BFV and GRU) follows a different behavior, the difficulty and challenge lie in how to integrate the two systems to achieve the desired results [3].

∗Corresponding author Nibras Hadi Jawad

Email addresses: nibras.hadi@qu.edu.iq

Communicated by ‘sub etitor’

Among the research and studies presented by researchers in this field are: Podschwadt, R., & Takabi, in 2020 [4]. Researchers employed RNNs and homomorphic CKKS encryption. Instead of querying the cipher dictionary, the client's embedding layer converted text into vectors and encrypted it before transferring it to the server. To reduce noise amplification, the client decrypts and re-encrypts every 27-time steps. The system's encrypted data accuracy was 86.47%, matching its text performance. Pulido-Gaytan, and et al., in 2021[5]. The paper addresses problems of earlier privacy-preserving machine learning (PPML) models by implementing a typical ResNet-20 model utilizing RNS-CKKS FHE with bootstrapping. shows that the suggested model ResNet-20's testing on CIFAR-10 dataset 91.89%. Lee, J. W., and et al., in 2022 [6]. The study implements a standard ResNet-20 model using the RNS-CKKS scheme with bootstrapping to address limitations of previous privacy-preserving machine learning (PPML) models and tested on the CIFAR-10 dataset, . It uses advanced approximation methods to accurately evaluate functions like ReLU and Softmax, and achieves 98.43% s. Song, C., and et al., in 2024 [7]. REsidue ACTivation HE (ReActHE), a unique HE-friendly deep neural network, is used to develop a precise and privacy-preserving algorithm employing a non-approximating HE method on the activation function. For HE-friendly nonlinear activation in deep neural networks, the adopted residue activation with a scaled power activation function. The thoroughly evaluate ReActHE using biomedical and imaging datasets. Njungle, N. B., and et al., in8] 2025]. PRIVSPIKE, a privacy-preserving SNN inference framework using CKKS homomorphic encryption, is presented in this study. Two leaky integrate-and-fire techniques for evaluating activation functions are shown. Using LeNet-5 and ResNet-19 models, PRIVSPIKE achieves encrypted inference accuracies of 98.10%, 79.3%, 98.1%, and 66.0% on MNIST, CIFAR-10, Neuromorphic MNIST, and CIFAR-10 DVS.

In this scholarly article, in the second section, there is background about the BFV Homomorphic Encryption Scheme and GRU Models. Followed the methodology of the proposed system in the third section. In the fourth section, it explains the experiments and results, as well as the conclusion.

2. Background

Understanding some basic concepts is crucial for comprehending the processes and procedures that are followed. They are as follows:

2.1. BFV Homomorphic Encryption Scheme

FHE is homomorphic encryption that allows multiplication and addition without decryption. Random math on encrypted text is possible with FHE [9]. One of the most secure and useful kinds of homomorphic encryption, this variant supports addition and multiplication, produces accurate encryption results, and recovers the original text despite its complexity and expensive computations [10], as shown in Fig1. The BFV scheme is depending on the second generation of FHE that based on Ring-Learning with Errors (RLWE) hardness problem [11]. BFV's behavior differs from normal encryption behavior in its operational steps: it starts with key generation, which includes creating a secret key sk (a symmetric key used for both encryption and decryption) is generated from random distribution the subspace of R2= {0, 1}. A public key pk is generated based on sk (used solely for encryption); the second step is encryption of plaintext pt with the public key to produces c= (c0, c1); the third step involves (evaluation of) the encrypted data by performing addition and multiplication homomorphic operations on them c~=(c1,c2), this is where the difference from regular encryption lies; and the final step is decryption using the private key [1] [12].

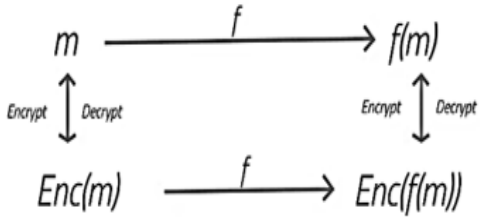


Fig. 1– Fully Homomorphic Encryption

2.2. Gated Recurrent Unit (GRU) neural networks

GRU is a type of recurrent neural network (RNN) with two gates—an update gate and a reset gate—to manage sequential data and solve the vanishing gradient problem. GRUs simplify LSTM design while maintaining

performance, making them useful for natural language processing, speech recognition, and time-series analysis [13]. GRUs govern information flow with two main gates. These gates choose which secret data to keep, change, or reject. The second gate is for update controls on how much of the previous concealed state is preserved for the current time step. The reset gate controls how much of the prior concealed state is deleted, filtering out unnecessary information. See in Fig 2. GRU gates let the network selectively save important information from earlier steps, which helps understand long sequences. GRUs have fewer parameters and no output gate or context vector. This speeds up training and reduces computing needs [14].

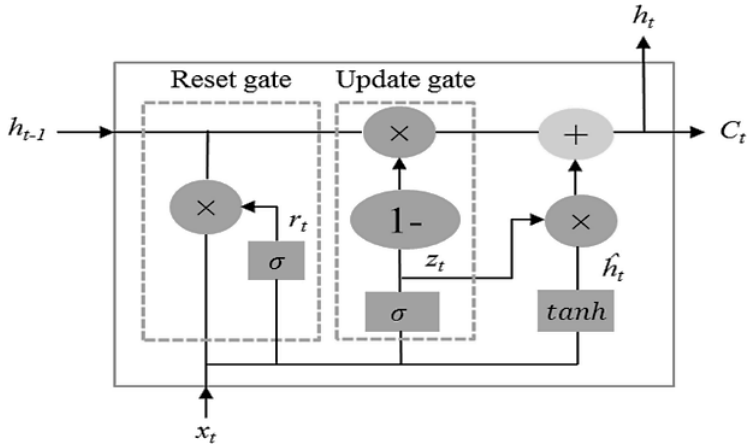


Fig. 2– Gated Recurrent Unit (GRU) [14]

3. The Proposed System (PPECS-GRU)

The primary challenge of this research is maintaining user privacy when analyzing emotions using classification to achieve greater credibility and user comfort when commenting (Analyzing user responses without revealing their identity). This is accomplished by building an integrated system that uses GRU to classify emotions (positive/negative) based on user data, which will be encrypted using BFV to protect user privacy during the classification process. The proposed system Privacy-Preserving Emotion Classification System- GRU (PPECS-GRU) involves devising a method to adjust the GRU's work to the BFV homomorphic algorithm. BFV operates as a linear algorithm, relying on basic operations like addition and multiplication. As for the GRU's internal structure, it is non-linear due to the activation functions it uses (sigmoid, tanh), which are fundamental to the GRU neural network for learning and modeling various real-world patterns. Therefore, it is essential to make the GRU BFV-friendly in operation, by making the GRU behave like a BFV.

3.1. Activation function of PPECS-GRU

The activation function is non-linear and is not suitable for working with BFV, because the evaluation processes are linear. So, the proposal is about how to modify the activation function to be friendly with FHE so that it is compatible with working with it and can be evaluated homomorphically. One of the advantages of the activation function is the speed of convergence with the weights, which leads to more accurate calculation efficiency and is distinguishable to improve the inputs to the other layer. The proposed an activation function whose work is polynomial and what is approximate of the work of these functions with varying ranges and degrees to make GRU compatible with FHE and to make the function handle addition and multiplication only without affecting the accuracy of the results. To work with the appropriate function, using the approximation function based on the Hard Sigmoid function instead of using the Sigmoid activation function. The Hard Sigmoid function provides the approximation equation for the Sigmoid approximation is (f(x) = {0 if x ≤ -1, (x/6) + 0.5 if -1 < x < 1, 1 if x ≥ 1}). And use Tylor series (1 + x + 0.5 * x2) /∑ (1 + x + 0.5 * x2) instead of tanh, see Fig 3.

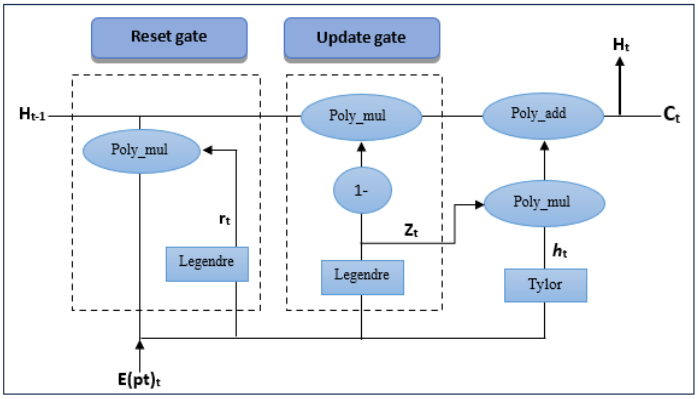


Fig. 3– Privacy-Preserving Emotion Classification System- GRU (PPECS-GRU)

3.2. Building the Proposed Model of PPECS-GRU

The process works as follows: Data is encrypted on the client device using BFV. In the BFV algorithm, a simple secret key sk is used, which is the selection of a random value from the values (0, 1) sk ∈ R2={0, 1}. The traditional secret key generator has been replaced by another generator DUff-skg that was previously designed in [15] with specifications and powers much higher than the traditional secret key generator. Simultaneously, the server generates a PPECS-GRU model and trains it on plain data of the same type as the client's IMDB database with total 50,000 movie reviews, equally distributed between 25,000 favorable and 25,000 negative ratings. The ciphertext c= ($c0$, $c1$) is then sent by client to the server, which then classifies the text by performing operations directly on the encrypted data (addition/multiplication) to return the expected result, which is either positive or negative. The addition and multiplication operations used by the GRU classification network will be changed to homomorphic operations used by BFV to ensure compatibility, see Algorithm 1 and 2. One of the characteristics of homomorphic encryption is its ability to multiply plaintext with ciphertext, which eliminates the need to encrypt the weights before multiplying them by the values of the encrypted text. To reduce the computational cost of multiplying two ciphertexts, the Relinearization operation is used as Algorithm 2. This greatly reduces the number of homomorphic multiplication operations required, thus avoiding the increased noise generated by each homomorphic multiplication operation. This result is then sent to the website or film owner to be added to the results of the sentiment analysis (positive/negative) that the owner uses to improve or modify their work. There is no need to decrypt the data, as the model will return a specific percentage reflecting the sentiment, whether positive or negative. See Fig 4.

Algorithm (1): Addition and Multiplication Homomorphic Operations of PPECS-GRU

Input: N, c1, c2
Output: C~

Begin
Def Poly_Add (c1, c2)

Initialize Sums Array
1 Sums= [ ] (with length N)
2 For i=0 to len(c1)−1:
2.1 Sums[i]= c1 [i] Add Second Polynomial
3 For j= 0 to len(c2)−1:
3.1 Sums[j]+ = c2[j]% N
4 Return Sums(**C~**)
End

Algorithm (2): Relinearization operation of two ciphertext

Input: N, q, c1, c2
Output: Result that is list of integers with length N elements

Begin
1 Compute T = $\lfloor \sqrt{q} \rfloor$
2 Compute $L=\lfloor log_T q \rfloor$
3 rlk=[]
4 Generate a_i from (generate_random_chaotic_keys1(L,q)) and
5 Generate e_i from (gen_normal_poly(L))
6 c0 =Δ^{-1} .($c^1{}_0 * c^2{}_{0R}$)
7 c1 =Δ^{-1} .[($c^1{}_0 * c^2{}_1$)+ ($c^1{}_1 * c^2$)]
8 c2 =Δ^{-1} .($c^1{}_1 * c^2{}_1$)
9 for i in range(0, L):
9.1 rlk = ([-(a_i . sk+ e_i)+ T^i. $sk^2]_q$, a_i)
10 for z in range(0, L):
10.1 new_c0 $= \left[\sum_{i=1}^{L} \text{rlk}\ (i)(0).c2^i\right]_q$
10.2 new_c1 $= \left[\sum_{i=1}^{L} \text{rlk}\ (i)(1).c2^i\right]_q$
11 Return (new_c0 , new_c1)
End

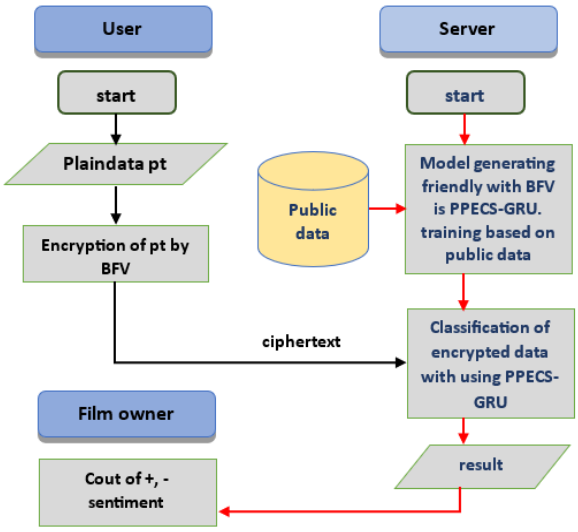


Fig. 4 – Architecture of PPECS-GRU

4. Experiments and Results

4.1. A. Approximation Function (AF)

In the proposal, a Sigmoid function was replacedwith the linear polynomial equation Hard Sigmoid function, yielding a result that closely resembled the sigmoid function. The function applied the experiment to 1000 values, focusing on the intervals [-1,1] as it is the best period to achieve the best results. The Root Mean Square Error (RMSE) function yielded (0.02231 error), see Fig **5**. Instead of using the tanh function, that applied the Taylor series to 1000 values, also within the period (-0.5, 0.5), and for the 2nd degree, there is the RMSE (0. 0000089852 error). The results were very similar to the tanh function results, see Fig 6.

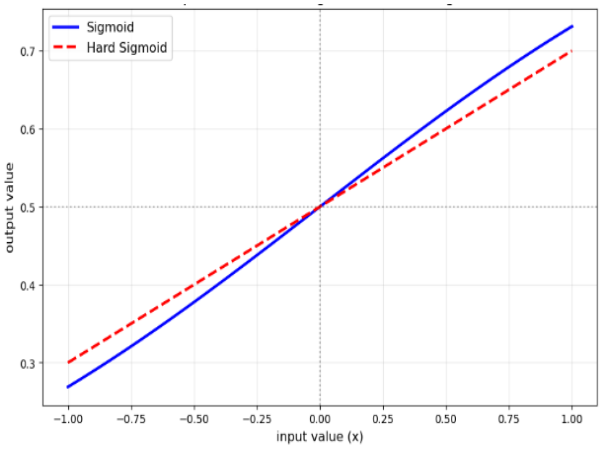


Fig. 5 – Comparison Between Sigmoid and Hard Sigmoid

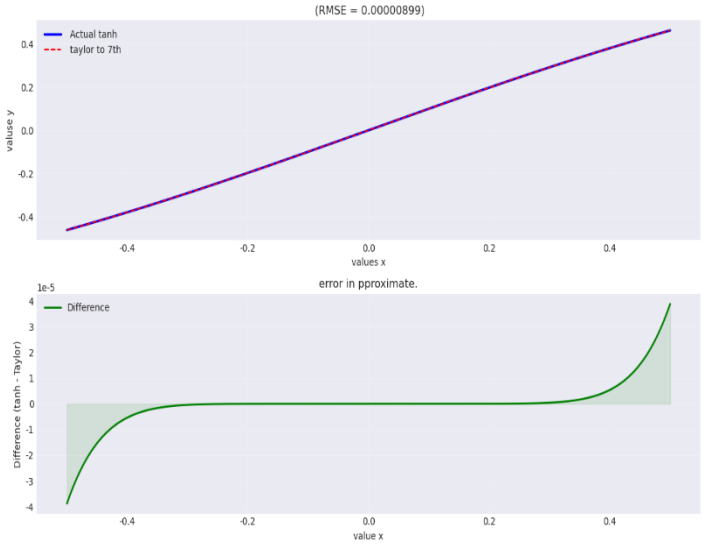


Fig. 6 – Comparison Between tanh and Tylor

The proposed approximation functions followed a non-linear behavior as shown in the Fig 5and Fig 6The proposed functions' outputs were comparable to those of the Sigmoid and tanh functions. In the Fig 6 for the range [-1, 1], let a1 = -1 and a2 = 1, reveals that the proposed function provides an uninterrupted path for drawing between a1 and a2, demonstrating that the proposed function is a continuous function, where the function f(x) is performed on the values of x in the range [-1, 1], for 100 values. The approximation functions are monotonic and differentiable, where function's values change continuously upwards. The graph in Fig 7 reveals an upward trend in the function, and shows that the monotonicity of the ReLU function and the proposed function are centered around zero. It also explains that all input values of the ReLU function and its derivatives result in outputs that are limited to between 0 and 1 values.

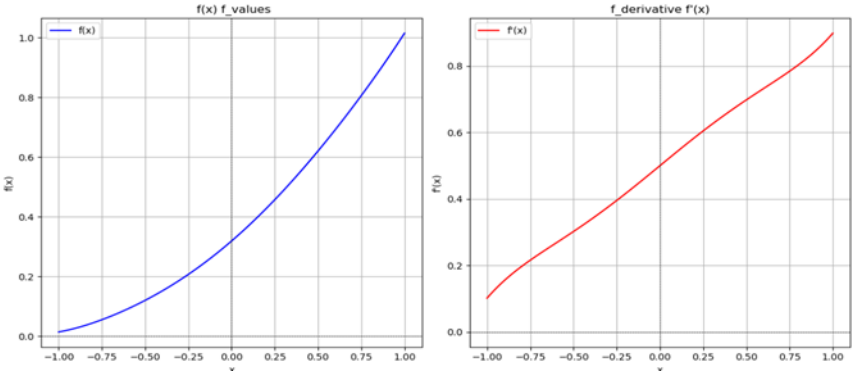


Fig. 7 – Monotonic and Differential

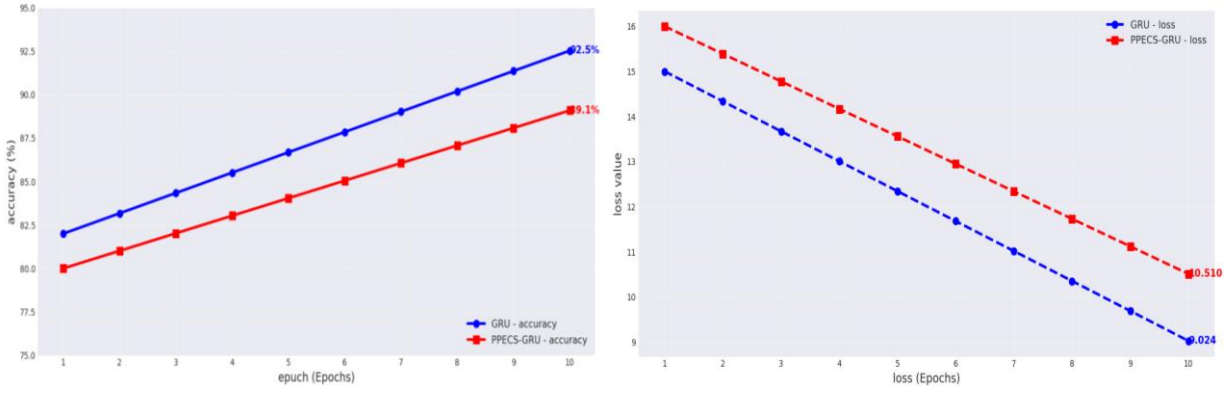
4.2. Classification Performance of Proposed PPECS-GRU Models

The performance evaluation utilized the PPECS-GRU model to analyze a IMDB database containing 50,000 movie reviews, categorized into two sentiment groups: 25,000 positive, and 25,000 negatives. The proposed work presented a valuable approach to protecting the privacy of reviews, analyzing users' feelings about being viewed, and dealing with different types of responses. The trained model layers were adapted to behave like BFV by making modifications to the model so that it could handle encoded data by modifying the addition and multiplication operations with homomorphic BFV operations. The results indicated, as in Table 1, that the model exhibited strong performance in running GRU using BFV encryption on the encrypted data, and compared them to the results of GRU without encryption that uses the usual activation functions, with the classification outcomes for explicit data marginally surpassing those for encrypted data. This minor variation in performance suggests that our approach successfully preserved user data privacy while minimally impacting prediction accuracy and maintaining performance quality. The result is a significant accomplishment, hence augmenting data security and privacy throughout the analysis and prediction phases.

Table 1 - Comparison Between Performance of Standard GRU and PPECS-GRU.

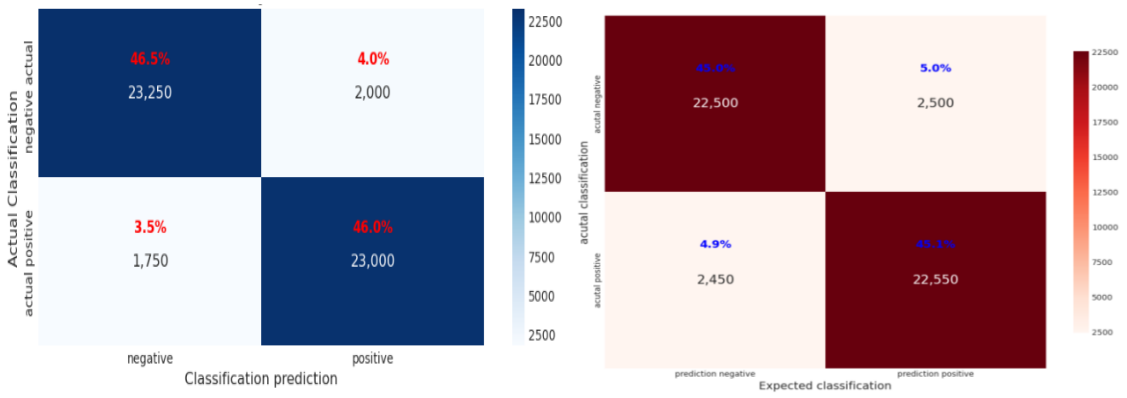
Neural network	Accuracy	loss	Precision	Recall	F1-scores	security	time	Epochs	Layers
Advantage	92.5	8.362	92	92	92	No	0.02	10	2
disadvantage	90.1	9.901	90	90.2	90	Yes	0.08	10	2

The results, as shown in Table 1, indicate that PPECS-GRU achieved an accuracy of 90.1%, while GRU achieved slightly higher accuracy at 92.5% (see Fig 8a). The loss ratio was minimal for both models (see Fig 8b). The Precision, Recall, and F1 scores obtained were good. PPECS-GRU maintains the privacy of revisions and classifies data in its encrypted format, whereas GRU lacks this feature, relying on explicit data for classification. Fig 9 shows the confusion matrix, which indicates that the number of correct predictions is significantly higher than the number of incorrect predictions for both models. The noise from homomorphic operations is negligible due to the network's two layers, so it doesn't affect the results. Overall, both approaches (PPECS-GRU Model, and GRU) yielded high and close prediction results with minimal loss.



(a) Accuracy **(b) loss**

Fig. 8 - (a) accuracy; (b) loss.



(a) GRU **(b) PPECS-GRU**

Fig. 9 – confusion matrix (a) GRU; (b) PPECS-GRU.

5. Conclusion

The purpose of this work is to classify an IMDB-type dataset encoded using GRU networks. The analysis of the results and the challenges encountered led to the conclusion: The work of neural networks and homomorphic encryption algorithms is incompatible, so classifying homomorphic encrypted data using GRUs is one of the challenges that needs to be solved to make the work of the GRU network compatible with the work of the FHE algorithm. Several layers, some nonlinear, make up the GRU network's designed model. BFV, a linear polynomial algorithm, uses alternative approximation functions instead of activation functions, and it gives results very close to the original activation functions. The non-linear neural network layers must be converted to linear layers, and the network must be trained based on this change, as it is trained on explicit data to obtain the required weights. Then return to the other challenge, which is predicting positive or negative sentiment based on homomorphic encoded reviews (since the data are double values) by network encoding, which relies on changing the multiplication mechanism using the same multiplication function that the BFV algorithm deals with and depends on basic operations such as addition and multiplication, in contrast to GRU networks that handle intricate operations. This resulted in addressing and altering each layer separately. The number of layers that can be put in the model's neural network is limited by the depth of the BFV multiplication operations. Exceeding this limit will introduce excessive noise, leading to incorrect results. The accuracy results of the proposed PPECS-GRU model, which uses the approximate activation function for classifying encrypted feelings, were good but slightly lower than those of the model when used for unencrypted data.

References

[1] Inferati Inc. , “Introduction to the BFV FHE Scheme”, Washington, USA. https://inferati.com/blog/fhe-schemes-bfv, 2021.
[2] Dey, R., & Salem, F. M. , “ Gate-variants of gated recurrent unit (GRU) neural networks”. In 2017 IEEE 60th international midwest symposium on circuits and systems (MWSCAS) (pp. 1597-1600). IEEE.2017 .
[3] William Stallings, “Cryptography and Network Security Principles and Practice”, Fifth edition. Prentice-Hall, Inc, 1995.
[4] Podschwadt, R., & Takabi, D. Classification of Encrypted Word Embeddings using Recurrent Neural Networks. In PrivateNLP@ WSDM (pp. 27-31).2020 .
[5] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities. Peer-to-Peer Networking and Applications, 14(3), 1666-1691. 2021.
[6] Lee, J. W., Kang, H., Lee, Y., Choi, W., Eom, J., Deryabin, M., ... & No, J. S. Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. iEEE Access, 10, 30039-30054. 2022.
[7] Song, C., & Shi, X. ReActHE: A homomorphic encryption friendly deep neural network for privacy-preserving biomedical prediction. Smart Health, 32, 100469.2024 .
[8] Njungle, N. B., Jahns, E., Stojkov, M., & Kinsy, M. A. PrivSpike: Employing Homomorphic Encryption for Private Inference of Deep Spiking Neural Networks. arXiv preprint arXiv:2510.03995.2025 .
[9] J. Fan and F. Vercauteren, “Somewhat Practical Fully Homomorphic Encryption,” Proc. 15th Int. Conf. Pract. Theory Public Key Cryptogr., pp. 1–16, 2012.
[10] C. Gentry, “A Fully Homomorphic Encryption Scheme,” Dissertation, no. September, p. 169, 2009.
[11] E. M. Alsaedi and A. Farhan, “RCAE_BFV: Retrieve Encrypted Images using Convolution AutoEncoder and BFV,” Iraqi J. Comput. Commun. Control Syst. Eng., vol. 22, no. 3, pp. 48–61, 2022.
[12] M. Babenko and E. Golimblevskaia, “About One Property of Number Rank in RNS,” Proc. 2021 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2021, pp. 212–216, 2021, doi: 10.1109/ElConRus51938.2021.9396072.
[13] Mohsen, S., “ Recognition of human activity using GRU deep learning algorithm”. Multimedia Tools and Applications, 82(30), 47733-47749. 2023.
[14] Salem, F. M., “Gated RNN: the gated recurrent unit (GRU) RNN”. In Recurrent neural networks: from simple to gated architectures (pp. 85-100). Cham: Springer International Publishing.2021 .
[15] NH Jawad, “ FHE Cryptographic Systems with Using Chaotic Secret Key Generation”, Boletim da Sociedade Paranaense de Matemática.vol. 43, ISSN-0037-8712, 2025.