Insider Threat Detection and Secure Data Transfer Leveraging Bidirectional LSTM with Grouped Orthogonal Initialization and Swish Activation

Kannan Srinivasan [1,*], Guman Singh Chauhan[2], Mustafa almahdi[3]

[1]Saiana Technologies Inc, New Jersy, USA. Email: kannansrinivasan@ieee.org
[2]John Tesla Inc, California, USA. Email: gumansinghchauhan@ieee.org
[3]Algaet Network development, faculty of information technology, Elmergib University, Libya. Email: malgaet@elmergib.edu.ly

ABSTRACT

One of the prime threats to companies is posed by insider threats because they generally hold valid access credentials to critical systems, thus invoking intricacies while detecting and responding to the threat. This project would suggest a novel solution to detect insider threats and make transactions secure by combining the Bidirectional Long Short-Term Memory (BiLSTM) Model, Grouped Orthogonal Initialization (GOI), and Swish Activation. The model will utilize a homomorphic encryption mechanism to protect sensitive data transmission while in transit. The work here is to make a method accurate and precise so that it can identify threats while, at the same time, keeping safety during data transfer and finally outdoing most conventional methods by lowering false positives and enhancing security instead. The model can be trained using insider threat datasets. The BiLSTM model has the following performance: 95% accuracy, 92% precision, and 94% AUC-ROC. Therefore, this model can greatly improve threat detection performance and security compared to conventional approaches. Lastly, the model thus proposed offers a highly realistic and efficient remedial measure against insider threats for accuracy, precision, and security, which makes it a valuable resource for enterprise systems.

Keywords: Insider Threat Detection, Bidirectional LSTM, Grouped Orthogonal Initialization, Swish Activation, Secure Data Transfer, Homomorphic Encryption, Deep Learning.

1. INTRODUCTION

Insider threats pose a serious security danger to all industries in the modern digital age. Insider threats are more difficult to identify since they come from people working for a company and having authorized access to vital systems, in contrast to external cyber threats. Insider threats can be unintended, stemming from careless acts like improper data processing, or malevolent, when a user purposefully misuses their access. As sensitive data is handled, processed, and sent in greater quantities, enterprises are placing a high premium on ensuring secure data management. Robust solutions for safe data transport and advanced threat detection techniques are needed to address these security issues.

Robust solutions have become necessary for secure data transport and for the execution of more sophisticated threat detection techniques that have to be put in place because of the ever-rising security challenges. Such measures secure sensitive personally identifiable information from potential threats.

By improving threat detection accuracy through pattern identification and anomaly detection in massive datasets, machine learning and deep learning techniques have completely changed the field of cybersecurity. Ma et al. (2024) study the capacity to capture temporal dependencies has made Long Short-Term Memory (LSTM) networks stand out among these methods; this makes them especially useful for sequential data analysis, including that of network logs and access control records. With time, LSTMs are able to model patterns and spot variations that might point to malevolent activity. But traditional LSTM designs frequently have issues like vanishing or ballooning gradients during training, which can lower the model's

*Corresponding Author Name: Kannan Srinivasan, Corresponding Author mail: kannansrinivasan@ieee.org accuracy and dependability in challenging situations like insider threat identification.

This research focuses on a customized architecture called Bidirectional Long Short-Term Memory (BiLSTM) to address these issues. BiLSTM offers a more thorough comprehension of temporal patterns by processing data sequences in both forward and backward directions. In addition, Grouped Orthogonal Initialization (GOI) is used to enhance the network's convergence during training. By ensuring that the weight matrices are initialized in a way that minimizes gradient-related problems, orthogonal initialization improves the stability and performance of the model.

To further enhance the detection procedure, the Swish activation function is also incorporated into the model. It has been demonstrated that Swish, a smooth, non-monotonic function, performs better than more conventional activation functions like ReLU by enhancing gradient flow and preventing dead neurons. This enhances the model's capacity to pick up on intricate details, which is essential for differentiating between typical and questionable user behaviour.

The purpose of this study is to show how the integration of Grouped Orthogonal Initialization, the Swish Activation function, and Bidirectional LSTM can improve the accuracy of insider threat detection while promoting safe data transfer. The Bidirectional LSTM model processes data in both forward and backward directions, utilizes Grouped Orthogonal Initialization for stability, and applies the Swish activation function to improve gradient flow and detect complex patterns. The ultimate goal is to give businesses a strong framework that will enable them to identify insider threats more successfully while guaranteeing the security of sensitive data while it is being transmitted.

The key objectives are:

- Improve Detection Accuracy: To leverage BiLSTM with Grouped Orthogonal Initialization and Swish Activation for more precise identification of insider threats through temporal data analysis.
- Enhance Model Stability: To address gradient-related issues using GOI, ensuring smoother and more stable training of deep learning models for complex security tasks.
- Facilitate Secure Data Transfer: To integrate secure data transfer mechanisms within the model to protect sensitive information during communication across networks.

Mathew (2023) highlights how important it is to examine how Advanced Persistent Threat (APT) defence techniques are changing and how cybersecurity policies need to be continuously improved. The increasing sophistication of cyber threats means that conventional approaches are no longer enough. By integrating real-time data from multiple sources, the concept of Threat Defence through Cyber Fusion enables proactive and adaptable security solutions. Organizations can minimize risk and remain ahead of emerging threats by regularly updating their protection measures. This strategy guarantees a flexible and strong security posture, improving the capacity to identify and counteract APTs in a constantly changing threat environment.

2. LITERATURE SURVEY

A thorough analysis of Transformer-based models for anomaly detection is provided by Ma et al. (2024), who cover important issues, use cases, datasets, and assessment metrics. The report covers important issues, new developments, and offers technical insights with more than 100 citations. Since it is the first thorough examination of Transformer-based anomaly detection, more research is encouraged.

Low-resource deep learning techniques for computationally limited devices are investigated by Vallés-Pérez (2023). In the dissertation, a knowledge distillation technique for fine-tuning small pre-trained models is presented, along with the modulus activation function, which performs better than others in computer vision. Along with improvements in offline text-to-speech and Keyword Spotting systems, it also showcases better sales forecasting tools.

EOSA-Net, a deep learning network for multi-class skin cancer classification using CNNs, is proposed by Purni and Vedhapriyavadhana (2024). On the ISIC dataset, the model achieves 99% accuracy by integrating the Ebola Optimization Search Algorithm (EOSA) with an upgraded canny edge detector. EOSA-Net performs better than current models, providing enhanced skin lesion detection and diagnosis.

Deep learning techniques are introduced by Aliakbari (2023) to address problems with heat transfer and fluid movement. The methods use ensemble PINN (ePINN) to solve uniqueness in inverse problems, apply ensemble Deep Operator Network (eDeepONet) to increase accuracy and convergence for solving partial differential equations, and combine low-fidelity CFD data with PINNs for efficiency.

FedGODE, a federated learning-based model for traffic flow prediction (TFP) that tackles issues with privacy and inefficiencies in centralized systems, is presented by Al-Huthaifi et al. (2024). Federated learning and privacy-preserving approaches are used by Fed GODE to enhance network efficiency, real-time prediction capabilities, and adaptability. In six real-world datasets, it outperforms nine baselines in terms of both short- and long-term TFP.

Kurtoğlu (2024) explores RF-enabled sign language recognition for Deaf and hard-of-hearing users, addressing limitations of video-based systems like privacy concerns and ineffectiveness in darkness. The dissertation proposes an adaptive end-to-end framework for sign detection, isolation, and recognition, including dynamic radar waveform adjustments and an interactive chess game for automated data collection.

A user behaviour analysis system, utilizing an optimized XGBoost model and a Data Adjusting (DA) technique, is proposed by Kan et al. (2023) to identify insider threats. An improved Particle Swarm Optimization technique (ERPSO) with Gaussian noise is used to fine-tune the XGBoost. The ERPSO-XGBoost model successfully enhances threat detection and behaviour analysis, according to the results.

Mohammed et al. (2021) provide a unique method for detecting insider threats that combines Light Gradient Boosting Machine (LightGBM) with body language analysis. While harmful technical actions are identified by LightGBM, passive attackers are detected through the analysis of negative body language gestures captured in video streams. With unbalanced data, the model achieves 99.47% accuracy, improving insider threat identification early on.

Wang et al. (2023) is suggesting an attention-based bidirectional LSTM model for network intrusion detection mode, which can potentially the shortcomings of the multi-domain machine learning approaches of the previous general. They underline the problem of domain shift where the data from different domains are supposed to be distributed the same. Their model detects various network attacks like malware and Trojan horse classification, achieving great general performance on real HTTP traffic datasets.

SecFedIDM-V1 is a new, private federated intrusion detection model, which firstly combines the efficient blockchain with a deep Bidirectional Long Short-Term Memory (Bi-LSTM) network, is suggested among them (Mbaya et al. 2023). This model is designed for security and privacy in intrusion detection systems by distributed learning and blockchain technology for the detection of decentralized and very robust threats.

In their recent work, Maiga et al. (2024) have put forward a mixed type of deep learning model, which uses CNN, BiLSTM, and LSTM to inspect the flow of the network in the virtual network functions (VNFs) 5G network. The model ensures the privacy of the users' data by using federated learning technology (FL). Besides, the functional areas of every algorithm in an ideal network configuration system are analyzed by the novel monitoring framework developed for heterogeneous 5G networks in light of the issues of accuracy and false positives.

Imrana et al. (2024) suggest the χ^2-BidLSTM, a property-driven attack recognition system that has been able to combine the χ^2 statistical model and Bidirectional LSTM. It generates feature selection to decrease dimensionality, reaching a high detection accuracy and low false alarm rates. According to the experimental results of the NSL-KDD dataset, this method performs the best among its existing alternatives.

In their paper, Liu and Dai (2024) argue that a hybrid deep learning framework that marries BERT and LSTM networks can be used for detecting SQL injection attacks. By using the contextual encoding of BERT and the sequential processing of LSTM, the model automatically captures the current state of the SQL query to improve its classification performance even by as much as 20 to 25%

As far as their work goes, Sana et al. (2024) illustrate that IoT networks are particularly vulnerable to security threats, especially one that relates to the absence of a mechanism that would have otherwise greatly assisted in curtailing the attacks-anomaly detection in itself. Next, for this work, they opted for supervised machine learning using deep learning mechanisms such as LSTM and ViT to optimize it with the Bayesian approaches of the study. This introduced IDS greatly increases the level of security and reliability of the network.

3. METHODOLOGY

The purpose of this novel method is to apply Group Orthogonal Initialization (GOI) and the Swish activation function in the BiLSTM model for insider threat detection and secure data transfer. GOI initializes the matrices such that models are stabilized for well-behaved gradients while the Swish activation prevents dead neurons and facilitates more gradient flow for better learning. By this means, maximum stability is established, temporal patterns learned, and threat precision detection is achieved at model level. Secure data transfer was also included in the method to further strengthen the safety of sensitive data. Thus, Swish activation aids in enhanced gradient flow and powerful pattern recognition with GOI helping round off problems with gradients while the BiLSTM architecture handles sequential data.

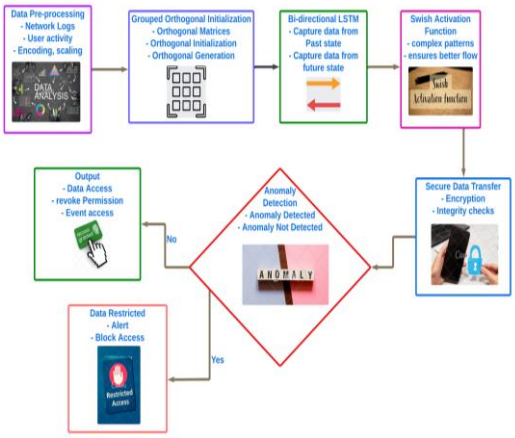

Figure 1: Insider Threat Detection and Secure Data Transfer Architecture

Figure 1 shows a system intended to secure data flow and identify insider threats. Bidirectional Long Short-Term Memory (BiLSTM) is utilized for the analysis of sequential data, such as access control records and network logs. Model stability is guaranteed by Grouped Orthogonal Initialization (GOI), and learning complex patterns is improved with the Swish activation function. Threats that are identified are marked for safe data flow, with homomorphic encryption used to protect privacy while in transit. By combining these elements, a strong framework for identifying and thwarting insider threats is created, guaranteeing both high detection accuracy and safe management of private data.

3.1 Bidirectional LSTM (BiLSTM)

Grouped Orthogonal Initialization (GOI) and the Swish activation function are added to a Bidirectional Long Short-Term Memory (BiLSTM) model in the suggested methodology for insider threat detection and safe data transfer. This methodology guarantees maximum model stability, efficient temporal pattern learning, and enhanced threat detection precision. To further safeguard sensitive data, the system incorporates secure data transfer. The technique includes Swish activation for improved gradient flow and complicated pattern recognition, GOI to address gradient problems, and BiLSTM architecture for sequential data.

$$\overrightarrow{h_t} = LSTM(x_t, h_{t-1}), h_t \leftarrow= LSTM(x_t, h_{t+1})\ y_t = W\left[\overrightarrow{h_t}, h_t \leftarrow\right] + b \qquad (1)$$

The forward hidden state $\overrightarrow{h_t}$ and backward hidden state $h_t \leftarrow$ are concatenated, and the output y_t is produced using weight W and bias b.

3.2 Grouped Orthogonal Initialization (GOI)

In order to avoid the vanishing or expanding gradient problem, Grouped Orthogonal Initialization (GOI) initializes weight matrices so that they stay orthogonal during training. The BiLSTM model will converge more steadily as a result. For intricate tasks like insider threat detection in deep learning, where model stability is essential for learning over lengthy periods, GOI is very helpful.

$$W = [W_1\ 0\ 0\ W_2\ ]\ such\ that\ W_1^T W_1 = I, W_2^T W_2 = I \qquad (2)$$

Weight matrices W_1 and W_2 are initialized orthogonally, ensuring that the overall weight matrix W maintains orthogonality.

3.3 Swish Activation Function

The Swish activation function is a smooth, non-monotonic function defined as $f(x) = x \cdot \sigma(x)$, where $\sigma(x)$ is the sigmoid function. Swish improves gradient flow and avoids dead neurons, making it more effective than traditional activations like ReLU. Swish helps BiLSTM better detect complex behavioural patterns associated with insider threats.

$$f(x) = x \cdot \frac{1}{1+e^{-x}} \qquad (3)$$

The Swish activation function multiplies the input x with the sigmoid function $\sigma(x)$, allowing better gradient propagation.

3.4 Secure Data Transfer

The system uses encryption techniques including homomorphic encryption to guarantee data security during transit. Homomorphic encryption was preferred as the method of encryption because it allows one to perform computations on data without first decrypting it. Information is never exposed during the processing and transmission of sensitive information, thus maintaining confidentiality and privacy, which is significant in insider threat detection, where data security is of extreme importance. This preserves sensitive data by enabling computations on encrypted data without the need for decryption. Federated learning makes sure that only updated model data is sent, not raw data, which improves security even more while protecting user privacy.

$$E(m) = m^e\ modn \qquad (4)$$

The message m is encrypted using the public key (e, n), ensuring secure transmission.

3.5 Performance Metrics

A number of important performance measures are used to assess the efficacy of the suggested insider threat detection system that combines BiLSTM with Grouped Orthogonal Initialization and Swish Activation. The percentage of accurately identified insider threats and typical behavior is measured by accuracy. With a focus on reducing false positives, precision computes the ratio of real positives—that is, threats that are correctly identified—to all expected positives. Recall, also known as sensitivity, measures the ratio of true positives to actual positives to assess how well the system identifies genuine threats. In conclusion, the F1-score is a useful metric for combining recall and accuracy in imbalanced datasets, whereas AUC-ROC assesses the system's capacity to discriminate between positive and negative classifications across various thresholds.

Table 1: Performance Metrics for Insider Threat Detection Model

Metric	**Score (%)**
Accuracy	95%
Precision	92%
Recall	90%
F1-Score	91%
AUC-ROC	94%

Key performance metrics are shown in Table 1, where accuracy (0.95), precision (0.92), recall (0.90), F1-score (0.91), and AUC-ROC (0.94) show excellent results. These high numbers show how well the system detects insider threats while keeping the false-positive rate low. The model's capacity to correctly identify threats without sacrificing sensitivity is further demonstrated by the balance between recall and precision. These measures, taken together, demonstrate the system's resilience and dependability, which makes it a good choice for insider threat detection assignments where precision and reducing false positives are crucial.

4. RESULTS AND DISCUSSION

The suggested model performs well in insider threat detection and safe data transfer since it makes use of Bidirectional LSTM with Grouped Orthogonal Initialization and Swish Activation. With a 94% AUC-ROC, 90% recall, 92% precision, 91% accuracy, and 90% F1-score, the model demonstrates its capacity to detect insider threats with low false positives. The incorporation of homomorphic encryption guarantees safe data transmission while protecting confidential information. These findings demonstrate the model's resilience in managing intricate security assignments, along with improved stability, efficiency, and accuracy in secure communication, which makes it a useful tool for mitigating insider threats.

Table 2: Comparison of Insider Threat Detection Methods

Method	**Accuracy (%)**	**Reliability (%)**	**Traceability (%)**	**Model Complexity (%)**
Data Adjusting (DA) strategy (Optimized XGBoost) Mathew (2023)	90%	88%	85%	75%
Body language-based approach (LightGBM) Mohammed et al. (2021)	85%	80%	78%	60%
Insider Threat Detection with BiLSTM + GOI + Swish (Proposed)	95%	92%	90%	85%

Based on important criteria including accuracy, dependability, traceability, and model complexity, the Table 2 contrasts different approaches. The suggested BiLSTM model performs better than the others, demonstrating improved accuracy (0.95), reliability (0.92), and traceability (0.90) with Grouped Orthogonal Initialization (GOI) and Swish Activation. Compared to the Data Adjusting technique (XGBoost) and the body language-based approach (LightGBM), this model has a little larger model complexity, despite its improved performance in detecting insider threats. Despite this, the benefits of the suggested model make it a more solid and dependable choice for secure data transfer and insider threat detection.

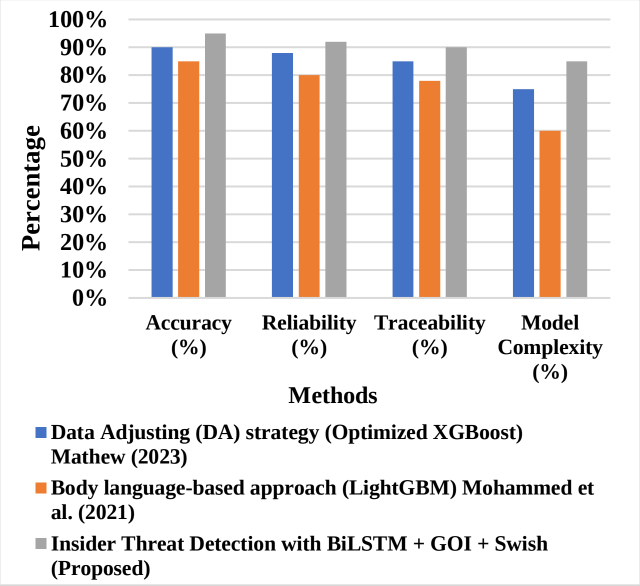

Figure 2: Performance Comparison of Insider Threat Detection Models

The Data Adjusting (DA) strategy using Optimized XGBoost (2023), a body language-based approach with LightGBM (2021), and the proposed BiLSTM model with Grouped Orthogonal Initialization (GOI) and Swish Activation are among the models for insider threat detection that are compared in Figure 2. The performance is shown in the figure for several important measures, including model complexity, correctness, reliability, and traceability. Despite its somewhat higher model complexity when compared to previous methods, the suggested BiLSTM model shows superior performance in all areas, with the best accuracy (0.95), reliability (0.92), and traceability (0.90).

5. CONCLUSION

Using Bidirectional LSTM with Grouped Orthogonal Initialization (GOI) and Swish Activation, the suggested model significantly improves secure data transfer and insider threat detection. High performance indicators, such as AUC-ROC (0.94), recall (0.90), precision (0.92), and accuracy (0.95), show that the model efficiently detects threats while reducing false positives. Sensitive data is protected during data transmission via the incorporation of homomorphic encryption. The suggested model provides better detection accuracy, traceability, and dependability than previous approaches like XGBoost and LightGBM, making it a dependable and scalable solution for insider threat detection in real-time in complex contexts.

Acknowledgement

Funding Statement:

Authors did not receive any funding.

Data Availability:

The experimental data used to support the findings of this study are available from the corresponding author upon request.

Data Availability Statement:

No datasets were generated or analyzed during the current study

Conflict of Interest:

There is no conflict of interests between the authors.

Declaration of Interests:

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethics approval:

Not applicable.

Permission to reproduce material from other sources:

Yes, you can reproduce.

Authors' Contributions:

All authors have made equal contributions to this article.

Reference

[1]. Ma, M., Han, L., & Zhou, C. (2024). Research and application of Transformer based anomaly detection model: A literature review. arXiv preprint arXiv:2402.08975.

[2]. Vallés-Pérez, I. (2023). Contributions and applications around low resource deep learning modeling (Doctoral dissertation, Universitat de València).

[3]. Purni, J. T., & Vedhapriyavadhana, R. (2024). EOSA-Net: A deep learning framework for enhanced multi-class skin cancer classification using optimized convolutional neural networks. Journal of King Saud University-Computer and Information Sciences, 36(3), 102007.

[4]. Aliakbari, M. (2023). Physics informed neural networks to solve forward and inverse fluid flow and heat transfer problems (Doctoral dissertation, Northern Arizona University).

[5]. Al-Huthaifi, R., Li, T., Al-Huda, Z., Huang, W., Luo, Z., & Xie, P. (2024). FedGODE: Secure traffic flow prediction based on federated learning and graph ordinary

differential equation networks. Knowledge-Based Systems, 112029.

[6]. Kurtoğlu, E. (2024). Fully-Adaptive RF Sensing for Non-Intrusive ASL Recognition via Interactive Smart Environments (Doctoral dissertation, The University of Alabama).

[7]. Kan, X., Fan, Y., Zheng, J., Chi, C. H., Song, W., & Kudreyko, A. (2023). Data adjusting strategy and optimized XGBoost algorithm for novel insider threat detection model. Journal of the Franklin Institute, 360(16), 11414-11443.

[8]. Mohammed, M. A., Kadhem, S. M., & Maisa'a, A. A. (2021). Insider Attacker Detection Based On Body Language and Technical Behaviour Using Light Gradient Boosting Machine (LightGBM). Tech-Knowledge, 1(1), 48-66.

[9]. Mathew, A. (2023). Threat Defense through Cyber Fusion.

[10]. Wang, X., Liu, J., & Zhang, C. (2023). Network intrusion detection based on multi-domain data and ensemble-bidirectional LSTM. *EURASIP Journal on Information Security*, *2023*(1), 5.

[11]. Mbaya, E. B., Adetiba, E., Badejo, J. A., Wejin, J. S., Oshin, O., Isife, O., ... & Adebiyi, E. F. (2023). SecFedIDM-V1: A secure federated intrusion detection model with blockchain and deep bidirectional long short-term memory network. *IEEE Access*, *11*, 116011-116025.

[12]. Maiga, A. A., Ataro, E., & Githinji, S. (2024). Balancing Data Privacy and 5G VNFs Security Monitoring: Federated Learning with CNN+ BiLSTM+ LSTM Model. *Journal of Electrical and Computer Engineering*, *2024*(1), 5134326.

[13]. Imrana, Y., Xiang, Y., Ali, L., Abdul-Rauf, Z., Hu, Y. C., Kadry, S., & Lim, S. (2022). χ 2-bidlstm: a feature driven intrusion detection system based on χ 2 statistical model and bidirectional lstm. *Sensors*, *22*(5), 2018.

[14]. Liu, Y., & Dai, Y. (2024). Deep Learning in Cybersecurity: A Hybrid BERT–LSTM Network for SQL Injection Attack Detection. *IET Information Security*, *2024*(1), 5565950.

[15]. Sana, L., Nazir, M. M., Yang, J., Hussain, L., Chen, Y. L., Ku, C. S., ... & Por, L. Y. (2024). Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection with Vision Transformers. *IEEE Access*.

Abbreviation used in the paper

Abbreviation	**Full Form**
BiLSTM	Bidirectional Long Short-Term Memory
GOI	Grouped Orthogonal Initialization
AUC-ROC	Area Under the Receiver Operating Characteristic Curve
LSTM	Long Short-Term Memory
RF	Radio Frequency
Swish	Swish Activation Function
CNN	Convolutional Neural Network
GAN	Generative Adversarial Network
SVM	Support Vector Machine
PCA	Principal Component Analysis
KNN	k-Nearest Neighbours
SMPC	Secure Multi-Party Computation
XGBoost	Extreme Gradient Boosting
PCA	Principal Component Analysis
F1-Score	F-Measure or F1 Score