**Literature Review (Long Version)**

1. This paper proposes a novel middlebox technique – SlimBox which uses searchable encryption technique. It is based on OXT scheme where inverted searching is performed on k-gram strings to match the rules against the network traffic. The SlimBox takes encrypted rule set and encrypted traffic as input and outputs encrypted action that has to be taken. The main advantage of this work is that it consumes less bandwidth and it is efficient is detecting malicious traffic.
2. This work proposes a novel homomorphic encryption framework based on Conjugacy Search Problem over non-abelian rings for addition, subtraction, multiplication, division and comparison operation. Developed Logistic Regression, SVM, Decision Tree and Random Forest Algorithm for classification using ciphertexts. The analysis shows that the proposed work is efficient for performing operations and using them in Machine Learning models.
3. This survey paper gives a brief introduction about homomorphic encryption and its latest advances. The author also gives the state of art in the field of Machine Learning applied on homomorphically encrypted data, application of Homomorphic encryption and libraries developed which implements homomorphic encryption such as SEAL, HELib etc. The author suggests that bootstrapping techniques should be improves and concludes that there is a lot of potential in FHE and MLaaS.
4. Used Pallier crypto system to encrypt and decrypt data homomorphically. Took sales data, trained Single variable Linear Regression using encrypted data, predicted the sales and the results were validated. This paper acts as a proof of concept that Machine Learning algorithms can be applied on homomorphically encrypted data.
5. Comparison paper
6. CryptoNet
7. Homomorphic Encryption for Machine Learning in Medicine and Bioinformatics
8. Private Machine Learning Classification Based on Fully Homomorphic Encryption
9. A method which incorporates federated learning and homorphic encryption where each organization trains the data locally using Isolation Forest Algorithm to detect outlier (i.e. anomalies) and shares partial information which is encrypted homomorphically based on which a collective decision is taken to detect anomalies by the central server.

**References:**

1. Liu, Q., Peng, Y., Jiang, H., Wu, J., Wang, T., Peng, T., & Wang, G. (2022). SlimBox: Lightweight Packet Inspection Over Encrypted Traffic. IEEE Transactions on Dependable and Secure Computing.
2. Li, J., Kuang, X., Lin, S., Ma, X., & Tang, Y. (2020). Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. Information Sciences, 526, 166-179.
3. Pulido-Gaytan, L. B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., & Radchenko, G. (2021). A survey on privacy-preserving machine learning with fully homomorphic encryption. In High Performance Computing: 7th Latin American Conference, CARLA 2020, Cuenca, Ecuador, September 2–4, 2020, Revised Selected Papers 7 (pp. 115-129). Springer International Publishing.
4. Behera, S., & Prathuri, J. R. (2020, November). Application of homomorphic encryption in machine learning. In *2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS)* (pp. 1-2). IEEE.
5. Bost, R., Popa, R. A., Tu, S., & Goldwasser, S. (2014). Machine learning classification over encrypted data. Cryptology ePrint Archive.
6. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., & Wernsing, J. (2016, June). Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In International conference on machine learning (pp. 201-210). PMLR.
7. Wood, A., Najarian, K., & Kahrobaei, D. (2020). Homomorphic encryption for machine learning in medicine and bioinformatics. ACM Computing Surveys (CSUR), 53(4), 1-35.
8. Sun, X., Zhang, P., Liu, J. K., Yu, J., & Xie, W. (2018). Private machine learning classification based on fully homomorphic encryption. IEEE Transactions on Emerging Topics in Computing, 8(2), 352-364.
9. Itokazu, K., Wang, L., & Ozawa, S. (2021, July). Outlier Detection by Privacy-Preserving Ensemble Decision Tree U sing Homomorphic Encryption. In 2021 International Joint Conference on Neural Networks (IJCNN) (pp. 1-7). IEEE.