IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

COLOSSAL ENCIPHER ISOLATION CONSERVE CLASSIFIER

[1]Supriya S, [2]Pooja D

[1]Student, [2]Student
[1] B.Tech Information Security and Digital Forensics,
[1]Dr.MGR Educational and Research Institute, Chennai, India

Abstract: One of the basic functions of this application is fully related to the agriculture farming and the yield fields. The main purpose of the project is how to rise classifying to the customers, such as fully holomorphic encryption. It supports a number of useful computations on cipher text in a broad range of applications, such as e-voting, private information retrieval, cloud security, and privacy protection. While FHE schemes do not require any interaction during computation. The key limitations are large cipher text expansion and inefficiency. Thus, to overcome these limitations, we develop a novel cryptographic tool, MAS-Encryption, to support real-value input and secure computation on the multiply-add structure. This application has related to the rise, yields and farming related empowerment to improve the crop cultivation yields by giving some ideas to the farmers. It will also give additional knowledge about the fertilizer and yields for the farmer needs. These data will be collected from the respective fields and it may acquire from the right data set. The data will be stored in a chain like method for data security. The previous data set values will be added in the database in respective manner. They are not required for the additional value of the fertilizers as well as the yields data. Then all of rice's data's encryption format classify to the customers. We prove that the constructed classifiers are secure and evaluate their performance using real-world datasets. Experiments show that our proposed MASE scheme and MASE based classifiers are efficient, in the sense that we achieve an optimal trade-off between computation efficiency and communication interactions. Thus, we avoid the inefficiency of FHE based paradigm.

I. INTRODUCTION

1.1 SCOPE OF THE PROJECT

Secure is a forward looking, highly sophisticated and secure distributed record keeping system which will help in the storage and analysis of large amount of agriculture database which can be traced down to all past transactions. This system mainly works on all the data's converted to the encoded format, after that they send it to the customers. This data is delivered to the vehicle machinery system. Farmers are uploading all details, including location, land details, that farmers' current varieties, all yield details. This application includes the fertilizers and crop details with full conformation, and it may have improved for the stability and conformability to the users. The farmer can take a conversation with this support as well as admin for each improvement. But it will be maintained by the higher authority with full security. Only authorized person can access with the user's data. To secure the data we have implemented the Security method and the data will be linked with other data with most security and effective data. For the huge data admin can easily add the data set and the farmer can easily search the needs for the specific fertilizers. It has to maintain the data transaction in an effective and secure manner. This information will also be maintained by the higher authority. This application gives user-friendly experience, and it gives comfort to the users.

1.2 EXISTING SYSTEM

In the existing system, we have seen many real-time problems that are faced by the farmers. For the first time in the literature, in this method all are converted to encryption method. We present an efficient, secure outsourcing scheme for convex separable programming problems such as e-voting, private information retrieval, cloud security, and privacy protection. While FHE schemes do not require any interaction during computation, the key limitations are large cipher text expansion and inefficiency. Thus, to overcome these limitations, we develop a novel cryptographic tool, MAS-Encryption (MASE), to support real-value input and secure computation on the multiply-add structure.

Disadvantages

- One person has to maintain all the details for all the team.
- Storing a massive amount of data in the cloud may pose severe challenges of information theft.
- Data manipulation since all the data is always online, and this leads to a significant problem as its data could be altered for he harmful causes.
- A bunch of works studying privacy issues in cloud computing.

- It is indeed challenging and different since clients only allow very few local computing and storage resources, which significantly limits the number of computations that can be operated by themselves to preserve the privacy of the data.

1.3 PROPOSED SYSTEM

In the proposed system, we have to implemented techniques by which all the uploaded and updating details are from the client (Farmers). All these details are converted to encryption method, and the main purpose is all details are securely delivered to the customers. We propose a novel cryptographic tool MAS-Encryption, which is designed to support both real-value input and secure computations on a multiply-add structure. Compared to FHE and PHE approaches, it achieves an optimal trade-off between computation efficiency and communication interactions. Rice production in Punjab has increased most of times in the past seven decades, mainly due to increased grain yield rather than increased planting area. This increase has come from the development of high-yielding varieties and improved crop management practices, such as optimum transplanting time, nitrogen fertilization, improved weed and irrigation management. These include the development of new varieties with high yield potential, resilience to climate change and tolerance to major abiotic stresses such as drought and heat, and the establishment of integrated crop management and new crop establishment method, namely direct seeded rice.

Advantages

- Efficient transformation-based scheme to solve the secure outsourcing computation of large-scale.
- Our secure outsourcing scheme is based on efficient arithmetic operations instead of heavy computations like holomorphic encryptions.
- Secure transformation of vector and matrices is computationally indistinguishable both in value and in a structure under a chosen-plaintext attack (CPA).
- This algorithm achieves noticeable time savings which increases production, reduces yield gap, and ensures the household food security for the vulnerable section of small and marginal farmers.

1.4 BOTTOM LINE AND FUTURE ENHANCEMENT

In this application, we have presented by a traditionally followed basic framework for rice supply chain management generally follows the multi stage supply chain system including: Farmers as the basic supplier of paddy, middlemen or agents, rice processing industries, distribution agents, and retailers; as the interlinked upstream and downstream stages. We have mainly implemented data encryption method and all the data are secured and efficiently delivered by the customer's side. Privacy will be increasingly important, as our society become more networked and data about individuals are increasingly digitalized such as a tool has several potential applications, for example to protect the privacy of classifiers with multiply add structures. To demonstrate the utility of MASE, we use two examples, namely: to construct a privacy-preserving NB classifier with minimal Bayes risk (i.e., MBR-PPNB classifier) and to construct a privacy-preserving SVM classifier (i.e., PPSVM classifier). In order to be practical for real-world applications, our constructions do not rely on the FHE. We also proved the security of the two private classifiers, as well as demonstrating that both classifiers are very efficient.

In future we can developed new feature and techniques by using neural networks it is high accuracy compared to machine learning.

II – LITERATURE SURVEY

Literature survey gives the overall description of the reference papers that have been referred to design the application using which the problem of the existing applications and technologies are identified. This is also used to overcome limitations and to enhance the existing application.

2.1 Privacy-Preserving Machine Learning with Fully Homomorphic Encryption for Deep Neural Network – 2021

Fully homomorphic encryption (FHE) is one of the prospective tools for privacy preserving machine learning (PPML), and several PPML models have been proposed based on various FHE schemes and approaches. Although the FHE schemes are known as suitable tools to implement PPML models, previous PPML models on FHE encrypted data are limited to only simple and non-standard types of machine learning models. These non-standard machine learning models are not proven efficient and accurate with more practical and advanced datasets. Previous PPML schemes replace non-arithmetic activation functions with simple arithmetic functions instead of adopting approximation methods and do not use bootstrapping, which enables continuous homomorphic evaluations. Thus, they could not use standard activation functions and could not employ a large number of layers. The maximum classification accuracy of the existing PPML model with the FHE for the CIFAR-10 dataset was only 77% until now. In this work, we firstly implement the standard ResNet-20 model with the RNS-CKKS FHE with bootstrapping and verify the implemented model with the CIFAR-10 dataset and the plaintext model parameters. Instead of replacing the non-arithmetic functions with the simple arithmetic function, we use state-of-the-art approximation methods to evaluate these non-arithmetic functions, such as the ReLU, with sufficient precision. Further, for the first time, we use the bootstrapping technique of the RNS-CKKS scheme in the proposed model, which enables us to evaluate a deep learning model on the encrypted data. We numerically verify that the proposed model with the CIFAR-10 dataset shows 98.67% identical results to the original ResNet-20 model with non-encrypted data. The classification accuracy of the proposed model is 90.67%, which is pretty close to that of the original ResNet-20 CNN model.

2.2 GIM: Gaussian Isolation Machines – 2020

In many cases, neural network classifiers are likely to be exposed to input data that is outside of their training distribution data. Samples from outside the distribution may be classified as an existing class with high probability by softmax-based classifiers; such incorrect classifications affect the performance of the classifiers and the applications/systems that depend on them. Previous research aimed at distinguishing training distribution data from out-of-distribution data (OOD) has proposed detectors that are external to the classification method. We present Gaussian isolation machine (GIM), a novel hybrid (generative-discriminative) classifier aimed at solving the problem arising when OOD data is encountered. The GIM is based on a neural network and utilizes a new loss function that imposes a distribution on each of the trained classes in the neural network's output space, which can be approximated by a Gaussian. The proposed GIM's novelty lies in its discriminative performance and generative capabilities, a combination of characteristics not usually seen in a single classifier. The GIM achieves state-of-the-art classification results on image recognition and sentiment analysis benchmarking datasets and can also deal with OOD inputs.

2.3 Machine Learning Classification over Encrypted Data - 2020

Machine learning classification is used in numerous settings nowadays, such as medical or genomics predictions, spam detection, face recognition, and financial predictions. Due to privacy concerns, in some of these applications, it is important that the data and the classifier remain confidential. In this work, we construct three major classification protocols that satisfy this privacy constraint: hyperplane decision, Naïve Bayes, and decision trees. We also enable these protocols to be combined with AdaBoost. At the basis of these constructions is a new library of building blocks for constructing classifiers securely; we demonstrate that this library can be used to construct other classifiers as well, such as a multiplexer and a face detection classifier. We implemented and evaluated our library and classifiers. Our protocols are efficient, taking milliseconds to a few seconds to perform a classification when running on real medical datasets.

III - DESIGN

3.1 DESIGN

3.1.1 System Architecture

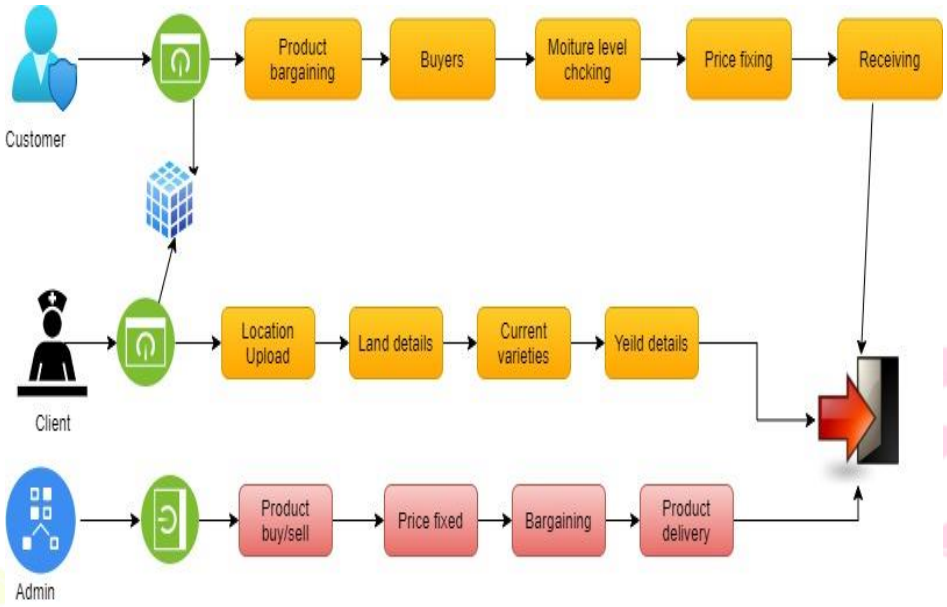

Fig. 1 – System architecture

IV – IMPLEMENTATION

4.1 MODULE DESCRIPTION

4.1.1 Modules

- Admin
- Client
- Customers
- Bargaining
- Land Verification
- Cultivation Details

Admin

This module describe about the role of admin. Admin can view all the user and user details they only have access to have seen the details. They will maintain the overall data in most secure manner and immediate response will be given to the end-users. The admin will act as a buyer and seller. When each crop yielding is finished, the admin can fix the price for all the crops. They have made the bargaining price for the buyer, and it will depend upon the crops. The product delivery will be made at a time and the status will be updated to the buyer as well as seller. The crop will be transferred to the buyer with the registered transportation with proper packaging and immediate response for the delivery.

Client

This module gives the information about the employee data which will be secured and maintained by the managers. If the client user is new to the application, they want to register to this application after that they can access the application easily. They have access to update and upload the farmer location, land details, current varieties with the yield details. So, seller have the responsibilities to maintain the details securely and can't accessed by the unauthorized persons.

Customers

This module gives the information about the employee data which will be secured and maintained by the managers. If the client user new to the application, they want to register to this application after that they can access the application easily. The customers have to bargain the price for the respective crop, and it will be sale by the seller. The customer can check the moisture level of the purchasing crop and it will be reduced the cost of the crop. Once the customer had seen the crop, they can fix the price for that individual crop for the receiving of the crop.

Bargaining

Bargaining or haggling is a type of negotiation in which the buyer and seller of a good or service debate the price and exact nature of a transaction. Retailers can choose to sell at posted prices or allow bargaining: selling at a public posted price commits the retailer not to exploit buyers once they enter the retail store, making the store more attractive to potential customers, while a bargaining strategy has the advantage that it allows the retailer to price discriminate between different types of customers. Haggling has largely disappeared in parts of the world where the cost to haggle exceeds the gain to retailers for most common retail items. If the bargaining produces agreement on terms, the transaction takes place. Bargaining is an alternative pricing strategy to fixed prices.

Land verification

Patta, also known as Record of Right, is a legal document issued by the government of Tamil Nadu in the name of the actual owner of the property. The document specifies details such as Patta number, District, taluk and village details, Property ownership (Name of the Owner), Survey number and subdivision, Type of land (Wet/Dry), Total area of land, and Property tax details. Chitta is a land revenue record specifying land area, property owner name, type of land, etc. The Village Administrative Officer (VAO) and the Office in the Taluk are responsible for the maintenance of the document. Electricity Bill or Previous Property Tax receipt for proof of ownership, Sale Deed photocopy should be submitted to the Tehsildar office for authentication, these are all the documents which is verified in this application.

Cultivation details

Cultivation is the act of caring for raising plants. Your desire to grow your own fruits and vegetables in the backyard mans you'll be engaged in some heavy cultivation. The word cultivation is most often used to talk about the ways that farmers take care of crops. Household level information like land owned, possessed, net sown area and area cropped more than once, whether soil was tested and whether recommendations followed, irrigation facilities and machinery and whether some of them remained unused that are all we saved as a land cultivation details.

V – CONCLUSION

In this application, we have presented by a traditionally followed basic framework for rice supply chain management generally follows the multistage supply chain system including farmers as the basic supplier of paddy, middlemen or agents, rice processing industries, distribution agents, and retailers; as the interlinked upstream and downstream stages. We have mainly converted all data by the encryption method. All this data is secured and efficiently delivered by the customer's side. Privacy will be increasingly important, as our society become more networked and data about individuals are increasingly digitalized. A tool has several potential applications, for example to protect the privacy of classifiers with multiply add structures. To demonstrate the utility of MASE, we use two examples, namely: to construct a privacy-preserving NB classifier with minimal Bayes risk (i.e., MBR-PPNB classifier) and to construct a privacy-preserving SVM classifier (i.e., PPSVM classifier). In order to be practical for real-world applications, our constructions do not rely on the FHE. We also proved the security of the two private classifiers, as well as demonstrating that both classifiers are very efficient.

ACKNOWLEDGMENT

We are very thankful for our Head of the Department Dr. S. Geetha and our Project guide Arun Raj for their guidance and support in making this Research paper. Its their motivation from initial stage to till the end helped us to complete this research paper. We would also like to extend our sincere thanks to other faculties who helped us to complete the project.

REFERENCES

[1] MAS encryption and its application in privacy classifiers – by *Chong-zhi Gao* School of Computer Science, Guangzhou University, Guangzhou, China, *Jin Li* School of Computer Science and the Institute of Artificial Intelligence and Blockchain, Guangzhou University, Guangzhou, China, *Shibing Xia* of School of Computer Science, Guangzhou University, Guangzhou, China, *Kim-Kwang Raymond Choo*of Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX, USA, *Wenjing Lou*of Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, *Changyu Dong* of School of Computing Science, Newcastle University, Newcastle Upon Tyne, U.K

[2] M. Ball, T. Malkin, and M. Rosulek. Garbling gadgets for boolean and arithmetic circuits. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pages 565–577, New York, NY, USA, 2016. ACM.

[3] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In Proceedings of the 19th Annual Symposium on Theory of Computing (STOC), pages 218–229, New York, NY USA, May 1987. ACM Press

[4] S. Bauer, L.-P. Nolte, and M. Reyes. Fully automatic segmentation of brain tumor images using support vector machine classification in combination with hierarchical conditional random field regularization. In G. Fichtinger, A. Martel, and T. Peters, editors, Medical Image Computing and Computer-Assisted Intervention – MICCAI 2011, pages 354–361, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg

[5] H. Zhu, X. Liu, R. Lu, and H. Li. Efficient and privacy-preserving online medical prediagnosis framework using nonlinear svm. IEEE Journal of Biomedical and Health Informatics, 21(3):838–850, May 2017

[6] M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz. A bayesian approach to filtering junk E-mail. In Learning for Text Categorization: Papers from the 1998 Workshop, Madison, Wisconsin, 1998. AAAI Technical Report WS-98-05

[7] X. Liu, K. R. Choo, R. H. Deng, R. Lu, and J. Weng. Efficient and privacy-preserving outsourced calculation of rational numbers. IEEE Transactions on Dependable and Secure Computing, 15(1):27–39, Jan 2018

[8] P. Pullonen and S. Siim. Combining secret sharing and garbled circuits for efficient private ieee 754 floating-point computations. In M. Brenner, N. Christin, B. Johnson, and K. Rohloff, editors, Financial Cryptography and Data Security, pages 172–183, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg

[9] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences, 379:42–61, 2017

[10] M. Kantarcıoglu, J. Vaidya, and C. Clifton. Privacy preserving naive bayes classifier for horizontally partitioned data. In IEEE ICDM workshop on privacy preserving data mining, pages 3–9