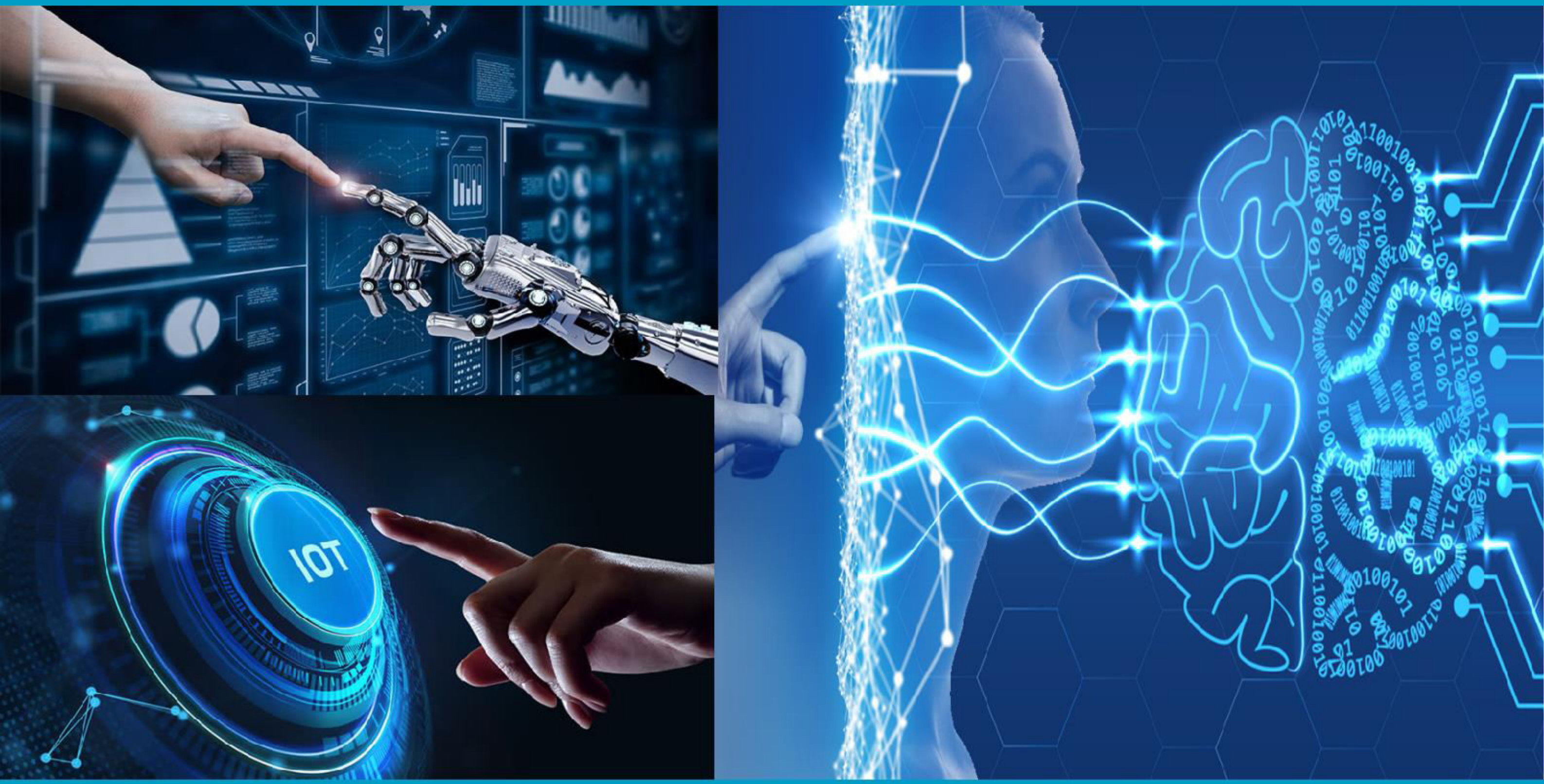
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 10, Issue 6, June 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.580

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 6, June 2023 |

Secure, Verifiable, and Fair Machine Learning on Cloud with Blockchain: Beyond Linear Regression

Dr. T.GEETHA, HEAD/MCA, R.GOWSIKA

Head, Department of MCA, Gnanamani College of Technology, Namakkal, India

Student, Department of MCA, Gnanamani College of Technology, Namakkal, India

ABSTRACT: This paper proposes an innovative approach to ML on the cloud by integrating blockchain technology, going beyond traditional linear regression models.

- The integration of blockchain with cloud-based ML offers several advantages. Firstly, it ensures the secure storage and sharing of sensitive data by leveraging the decentralized and cryptographic properties of the blockchain.
- This mitigates the risks of unauthorized access and data breaches, providing a robust framework for data privacy. Machine learning (ML) on the cloud has revolutionized various industries by enabling scalable and efficient data processing.
- However, concerns related to data privacy, security, and fairness have highlighted the need for enhanced solutions

KEYWORD: cloud services, off-chain, test, subscribe, SLA, on-chain, provider, consumer

I. INTRODUCTION

- Machine learning (ML) has emerged as a transformative technology with applications in various domains, ranging from finance and healthcare to transportation and entertainment. With the ever-increasing amount of data being generated, the cloud has become an indispensable platform for ML, offering scalable computing resources and storage capabilities. However, concerns regarding data privacy, security, and the fairness of ML models have surfaced, urging the need for innovative solutions.
- In this context, this paper proposes a novel approach to machine learning on the cloud, combining the power of blockchain with advanced ML algorithms, surpassing the limitations of traditional linear regression. Our approach aims to provide a secure, verifiable, and fair framework for ML, ensuring the integrity and privacy of data, as well as promoting fairness and transparency in the decision-making process.
- One of the key challenges in cloud-based ML is the protection of sensitive data. By leveraging blockchain, our approach enables the secure storage and sharing of data in a decentralized manner, reducing the risk of unauthorized access and data breaches. The immutability and cryptographic properties of blockchain ensure the integrity of the data throughout the ML pipeline, establishing trust among stakeholders.
- Verifiability is another critical aspect of our approach. By recording ML model training and validation processes on the blockchain, it becomes possible to provide an auditable trail of the entire ML lifecycle. This allows stakeholders to verify the legitimacy and fairness of the model's outcomes, ensuring that biases and discriminatory patterns are minimized.

II. EXISTING SYSTEM

- This paper focuses on the data analysis for CPSS when the Linear Regression is applied.
- Training process of LR is high time-consuming since it involves complex matrix operations, especially when it gets a large scale training dataset In the CPSS.

- Thus, how to enable devices to efficiently perform the training process of the Linear Regression is of significant importance.

III. PROPOSED SYSTEM

- To address this issue, in this paper, we present a secure, verifiable and fair approach to outsource LR to an untrustworthy cloud-server. In the proposed scheme, computation inputs/outputs are obscured so that the privacy of sensitive information is protected against cloud-server. Meanwhile, computation result from cloud-server is verifiable.
- Also, fairness is guaranteed by the block chain, which ensures that the cloud gets paid only if he correctly performed the outsourced workload. Based on the presented approach, we exploited the fair, secure outsourcing system on the Ethereum blockchain.
- We analyzed our presented scheme on theoretical and experimental, all of which indicate that the presented scheme is valid, secure and efficient.
- Our protocol supports decentralized proxy and key management and flexible delegation of services.
- Proposed system transferring the information security is provided by proxies, server intermediaries and client use RSA public key algorithm to ensure confidentiality and integrity and they communicate through a secure channel.

MODULES DESCRIPTION

- Data Owner
- Data Upload
- Secure Key Exchange
- Encryption
- Asymmetric key cryptographic techniques

DATA OWNER

- Data owners are either individuals or teams who make decisions such as who has the right to access and edit data and how it's used. Owners may not work with their data every day, but are responsible for overseeing and protecting a data domain.

DATA UPLOAD

- Cloud Data means any information, data, files, documents, objects, software applications, and any other information that the Cloud Customer uploads into the cloud. Cloud file sharing works when a file is stored on an online or cloud file-sharing service. The file is uploaded using the service control panel and upon successful upload the file is generated with a unique.

SECURE KEY EXCHANGE

- The key exchange protocol is considered an important part of cryptographic mechanism to protect secure end-to-end communications. An example of key exchange protocol is the Duffy and Hellman key exchange. Which is known to be vulnerable to attacks? Key exchange is a method in cryptography by which cryptographic keys are exchanged between two parties.

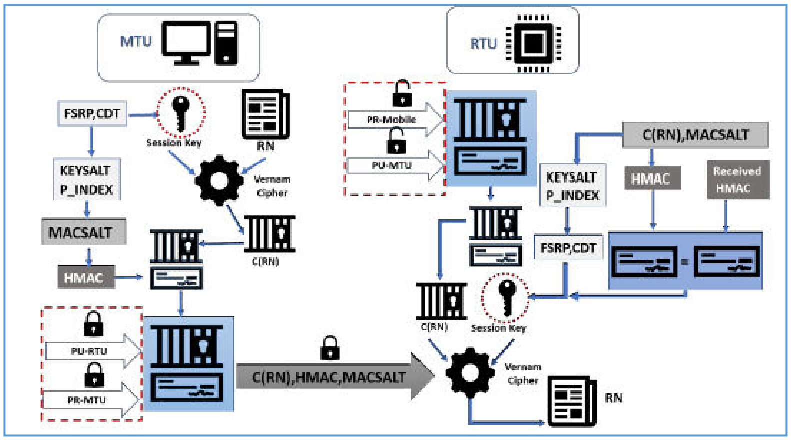
MODULES - ENCRYPTION

- Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography. In computing, unencrypted data is also known as plaintext, and encrypted data is called cipher text.

RESULT:

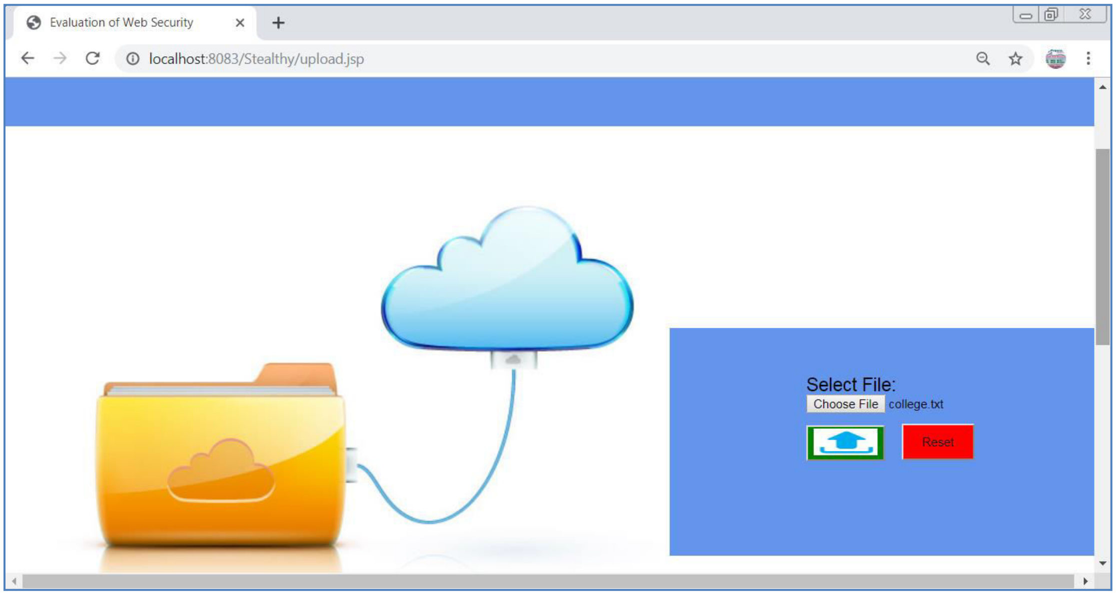
- Computation inputs/outputs of the privacy of sensitive information is protected against cloud-server.
- Also, fairness is guaranteed by the blockchain, which ensures that the cloud gets paid only if he correctly performed the outsourced workload.
- Our protocol supports decentralized proxy and key management and flexible delegation of services.

- The transferring the information security is provided by proxies, server intermediaries and client use RSA public key algorithm to ensure confidentiality and integrity and they communicate through a secure channel.
- This approach is more efficient because all the proxies will simultaneously provide content service at a time.
- Overall content service time will reduced because all the proxies will simultaneously provide content service at a time.



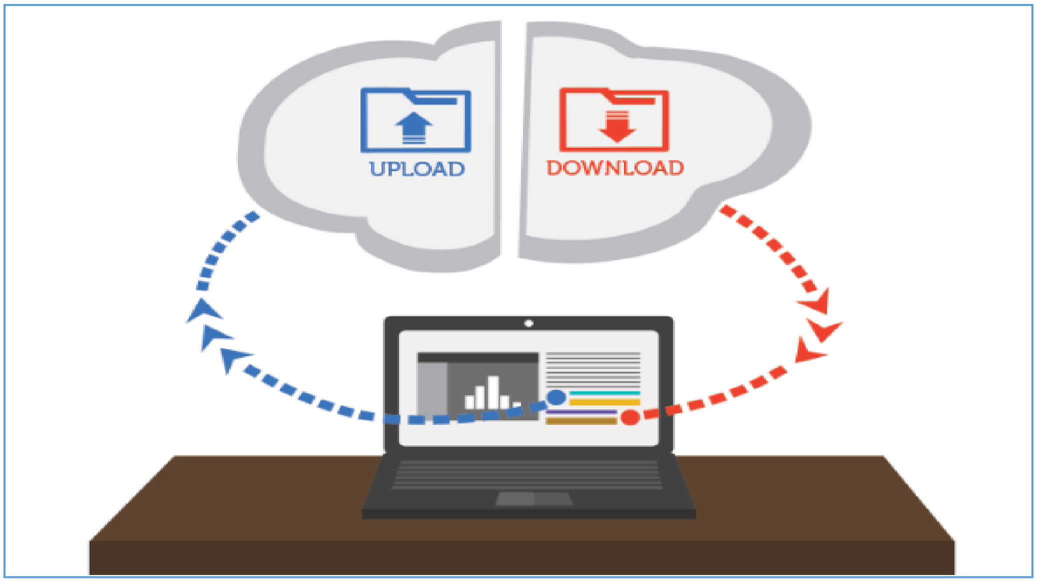
III. RESULTS

1. Upload as Encrypt file.


Evaluation of Web Security
localhost:8083/Stealthy/upload.jsp

Select File:
Choose File college.txt

2. Download as Decrypted file.



IV. CONCLUSION

- The proposed attack pattern, instead of aiming at making the service unavailable, it aims at exploiting the cloud flexibility, forcing the services to scale up and consume more resources than needed, affecting the cloud customer more on financial aspects than on the service availability.
- In the future work, we aim at extending the approach to a larger set of application level vulnerabilities, as well as defining a sophisticated method able to detect SIPDAS based attacks in the cloud computing environment.

V. FUTURE WORK

- The cloud-aided machine learning faces security challenges, including data privacy, result verifiability and payment fairness. In this work, we studied the classic linear regressions an example to show how to address these challenges.
- To the best of our knowledge, there is no generic secure outsourcing approach for all machine learning algorithms.
- Fully homomorphism encryption (FHE) is a possible solution for a generic secure outsourcing approach, but the efficiency of the FHE is too low such that the FHE-based approach is not practical. Thus, current researches focus on designing specific outsourcing approaches for particular machine learning algorithms.

REFERENCES

[1] P. Zhao, J. Yu, H. Zhang, Z. Qin, and C. Wang, “How to securely outsource finding the min-cut of undirected edge-weighted graphs,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 315–328, 2019.

[2] J. Yu, K. Ren, and C. Wang, “Enabling cloud storage auditing with verifiable outsourcing of key updates,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, 2016.

[3] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[5] N. Szabo, “Formalizing and securing relationships on public networks,” First Monday, vol. 2, no. 9, 1997.

[6] G. Rosario, G. Craig, and P. Bryan, “Non-interactive verifiable computing: outsourcing computation to untrusted workers,” in Proceedings of the 30th annual conference on Advances in cryptology CRYPTO’10, pp. 465–482, 2010.
[7] S Hohenberger and A. Lysyanskaya, “How to securely outsource cryptographic computations,” in Proceedings of Theory of Cryptography, pp. 264–282, Springer Berlin Heidelberg, 2005.
[8] “Oraclize.” http://www.oraclize.it/.
[9] “Randao: A dao working as rng of ethereum.” https:// github.com/randao/randao.
[10] V. Strassen, “Gaussian elimination is not optimal,” Numerische mathematic.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com

www.ijmrsetm.com