Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023

Industrial Security Framework for ML in IIOT Systems

MOHAMMAD SUMAYA BANU PG Scholar, Dept of CSE, Quba College of Engineering & Technology, Venkatachalam, AP, India.

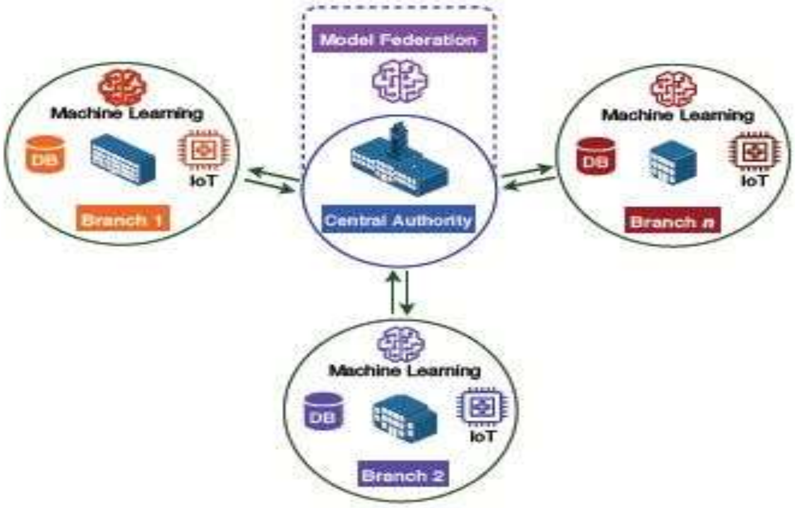
M.HYMAVATHI Assistant Professor, Dept of CSE, Quba College of Engineering & Technology, Venkatachalam, AP, India.

ABSTRACT

Energy, agriculture, mining, transportation, and healthcare are just a few of the top industries being transformed by the industrial internet of things (IIoT). The Industrial Internet of Things (IIoT) revolutionises data collection, exchange, analysis, and decision-making by utilising sensors and actuators with computation and communication capabilities. Industry 4.0, which mainly relies on machine learning (ML) to take use of the vast interconnectedness and large volumes of IIoT data, is primarily driven by IIoT. Yet, ML models that are trained on private information are more vulnerable to hostile attacks.This study proposes the PriMod Chain framework, which combines differential privacy, federated machine learning, the Ethereum block chain, and smart contracts to guarantee privacy and trustworthiness on IIoT data. Using simulations created in Python with socket programming on a general-purpose computer, the viability of PriMod Chain in terms of privacy, security, dependability, safety, and resilience was assessed.

1. INTRODUCTION

A large-scale IIOT-based industry setup is made up of a number of businesses that are widely dispersed geographically..



Human-specific sensitive private data is significantly entangled in sectors like open finance and smart healthcare. Because of this complexity, dispersed data collecting techniques in an IIoT-based Industry 4.0 environment are rather difficult to implement. Sensitive data can be used to train ML models that potentially reveal private or sensitive information to highly skilled attackers. An adversary may undertake a "man in the middle" assault in order to alter the original ML knowledge that the source transferred. It is possible to create malicious algorithms and make them available as a part of the training procedures used to memorise sensitive data. Thus, trustworthiness and privacy are crucial elements of ML in IIoT systems.

2. LITERATURE SURVEY

Block chain for the IoT and industrial IoT: A review Qin Wang, Xinqi Zhu, Yiyang Ni, Li Gu, Hongbo Zhu . Computer Science Internet Things . 2020

Prior to summarizing the security requirements for the development of IoT and Industrial 4.0, we first describe the fundamental structure and key characteristics of block chains. Then, we investigate how blockchain's security tools and technology can be used with the Internet of Things for Industry 4.0..

Blockchain Applications for Industry 4.0 and Industrial IoT: A Review TejasviAlladi, Vinay Chamola, +1 author Kim-Kwang Raymond Choo . Published 2019 . Business, Computer Science . IEEE Access

Block chain's potential has received a lot of attention in literature and the media, particularly in the banking and payment sectors. At the company level, one relatively new trend is the use of blockchain as the foundation for immutability and internet security. Industrial Internet of Things and Industry 4.0 are examples of emerging application domains (IIoT)..

Blockchain-Enabled Secure Energy Trading With Verifiable Fairness in Industrial Internet of Things : Meng Li, DonghuiHu, +2 authors Zijian Zhang . Published 2020 . Computer Science . IEEE Transactions on Industrial Informatics

In this article, it was suggested to develop a secure energy trading system and enhance energy quality for Industry 4.0 by using a block chain-based energy trading scheme to monitor and control the energy trading process. To preserve user privacy, we specifically use anonymous authentication, and to provide verifiable fairness during energy trading, we create a timed-commitments-based approach.

3. PROBLEM STATEMENT

The adoption of Internet of Things (IoT) devices in so many applications has raised serious questions about user security and privacy. Two recent examples of IIoT-based Industry 4.0 systems are real-time quality monitoring in additive manufacturing and fault detection and isolation in industrial processes. The increasing growth of cyber dangers renders the current security and privacy measures ineffective.

As a result, hackers can use anyone on the Internet as a target. Since the resulting outputs can be used to predict and detect vulnerabilities in IoT-based systems, Machine Learning (ML) methods are utilised to generate precise outputs from huge, complicated databases..In addition, BC approaches are gaining use in contemporary IoT applications to address security and privacy concerns. There have been numerous studies on either ML algorithms or BC methods. The need for a comprehensive overview of current work addressing security and privacy concerns using ML algorithms and BC approaches arises from the fact that these research focus on either security or privacy issues using ML algorithms or BC techniques..

LIMITATIONS OF SYSTEM

Due to a lack of block lever data verification, the system now in use leaks a lot of information. Due to a lack of ABE approaches, the current uses very little security and doesn't use digital signs..

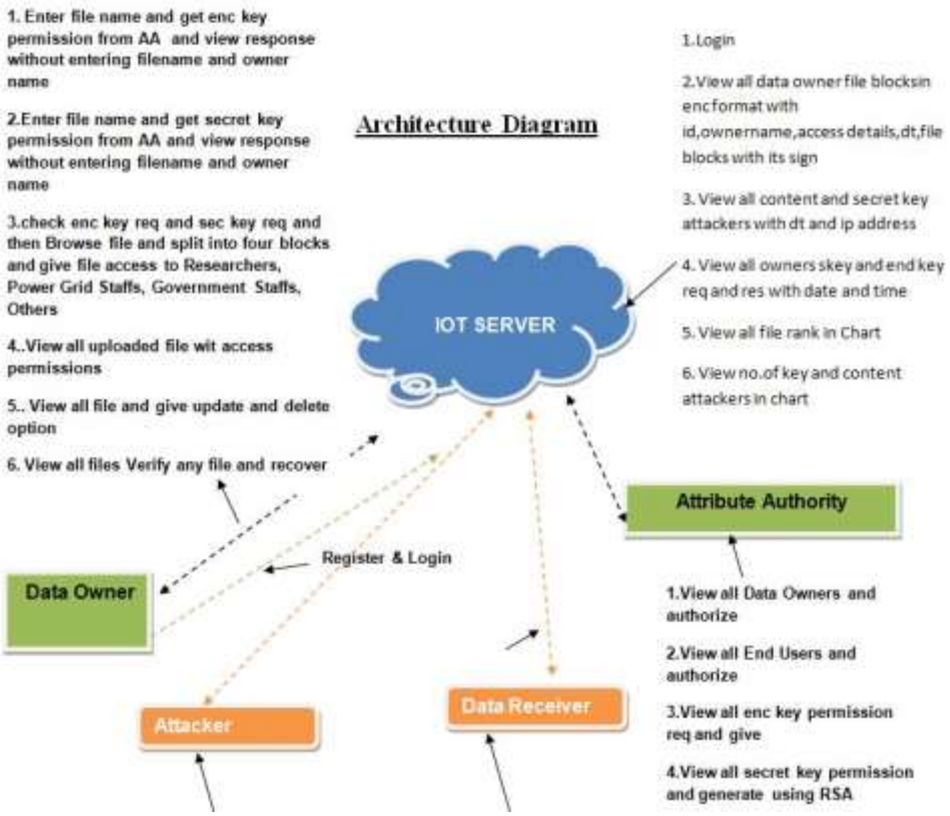
4. PROPOSED SYSTEM

In order to address the privacy and trust challenges of machine learning in IIoT systems, the system suggests a framework called PriModChain (Privacy-preserving trustworthy machine learning model training and sharing framework based on block chain). Differential privacy, federated learning (FedML), smart contracts, and the Ethereum block chain are all combined in PriModChain (EthBC). For off-chain data management, PriModChain makes use of the interplanetary file system (IPFS). A privacy paradigm known as differential privacy (DP) maximises privacy by reducing the possibility of individual record identification. [10]. The amount of data about a data item that can, in theory, be made available to a third party for analysis is limited by DP. Federated learning is a method for creating machine learning models from datasets that are dispersed across various sites. A distributed ledger of data records kept by network nodes not controlled by a single entity is known as a block chain. The blockchain's data blocks are linked to one another using cryptographic concepts. A block chain-based application will by default become transparent and attack-resistant..Ethereum is a free and open-source platform for decentralised applications that manage value in the digital realm. "Smart contracts" are the name for the programmes that execute on the Ethereum Virtual Machine (EVM). Two of the most widely used programming languages for creating smart contracts on Ethereum are Solidity and Vyper. A peer-to-peer distributed file system called IPFS offers a content-addressed block storage format with content-addressed hyperlinks and fast throughput. Once an agreement is reached between the distributed entities (DISTEN) and the central authority (CENTAUTH), the smart contract gives PriModChain transparency while creating the global ML model. To enforce security, EthBC ensures that this agreement is backed by the greatest level of data encryption..

FEATURES

The multi-key encryption protocol's security verification has been implemented, giving the system more power. The device PriModChain's multi-key encryption security procedures were put into use to make sure there were no unforeseen security flaws.

5. ARCHITECTURE


Architecture Diagram
1. Enter file name and get enc key permission from AA and view response without entering filename and owner name
2.Enter file name and get secret key permission from AA and view response without entering filename and owner name
3.check enc key req and sec key req and then Browse file and split into four blocks and give file access to Researchers, Power Grid Staffs, Government Staffs, Others
4..View all uploaded file wit access permissions
5.. View all file and give update and delete option
6. View all files Verify any file and recover
1.Login
2.View all data owner file blocksin encformat with id,ownername,access details,dt,file blocks with its sign
3. View all content and secret key attackers with dt and ip address
4. View all owners skey and end key req and res with date and time
5. View all file rank in Chart
6. View no.of key and content attackers in chart
IOT SERVER
Attribute Authority
Register & Login
Data Owner
Attacker
Data Receiver
1.View all Data Owners and authorize
2.View all End Users and authorize
3.View all enc key permission req and give
4.View all secret key permission and generate using RSA

6. IMPLEMENATION

6.1 Data Owners (*DO*) :

DO choose the access policy and use CP-ABE to encrypt the data. The servers will receive the encrypted data. In the system, DO are taken for honest people..

6.2 Data Receivers (*DR*) :

The decryption request is sent by DR to the server, and the cypher texts are obtained online. They can only access the plaintexts if their attributes meet the requirements of the cypher text's access regulations. Data requesters and recipients may band together to gain access to data that would not otherwise be available separately..

6.3 IOT Server :

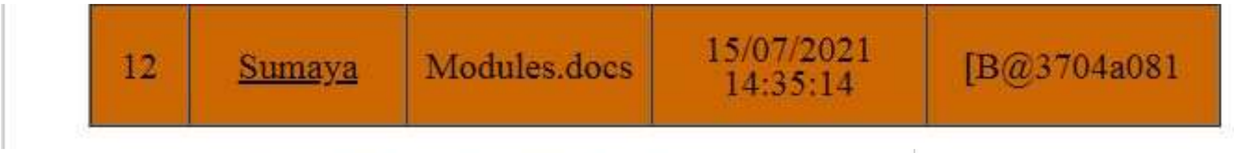
The server is in charge of managing a sizable amount of data. DO cannot put their trust in them. Hence, in order to guarantee data confidentiality, DO must set the access policy. It is expected that CS will not work with DR..

6.4 Attribute Authority (AA) :

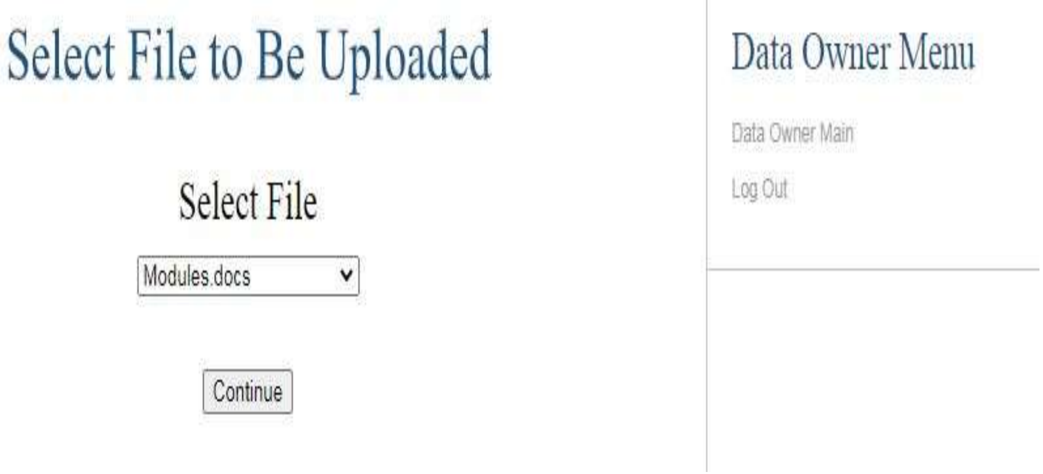
Users must register with AA, who then evaluates their qualities and generates their secret key SK when necessary. It executes the Setup process and provides each DO with a master key MK and public key PK. It is regarded as completely reliable.

7. RESULTS

The above permission is given by Authority.



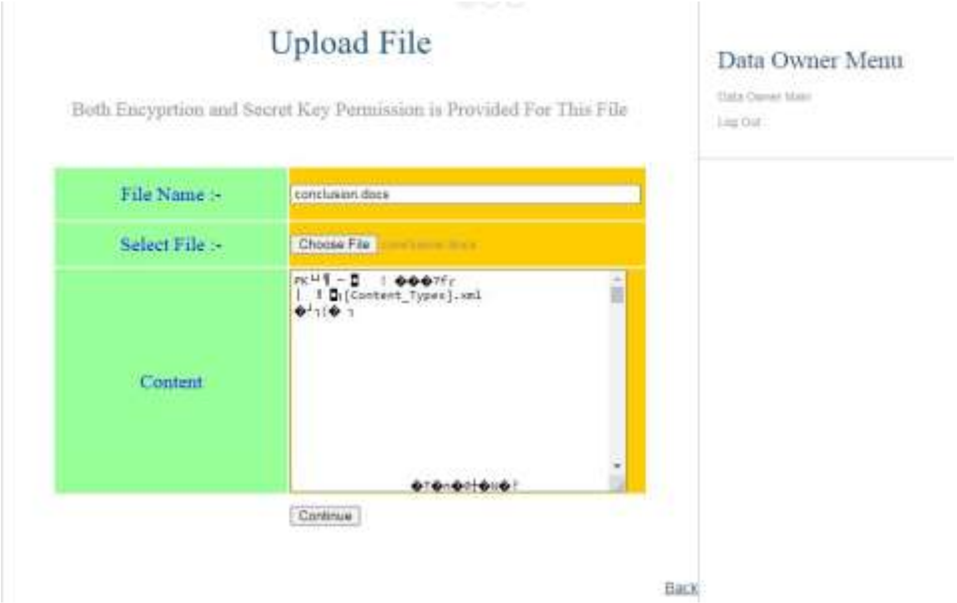
12	Sumaya	Modules.docs	15/07/2021 14:35:14	[B@3704a081



Select File to Be Uploaded

Select File

Modules.docs

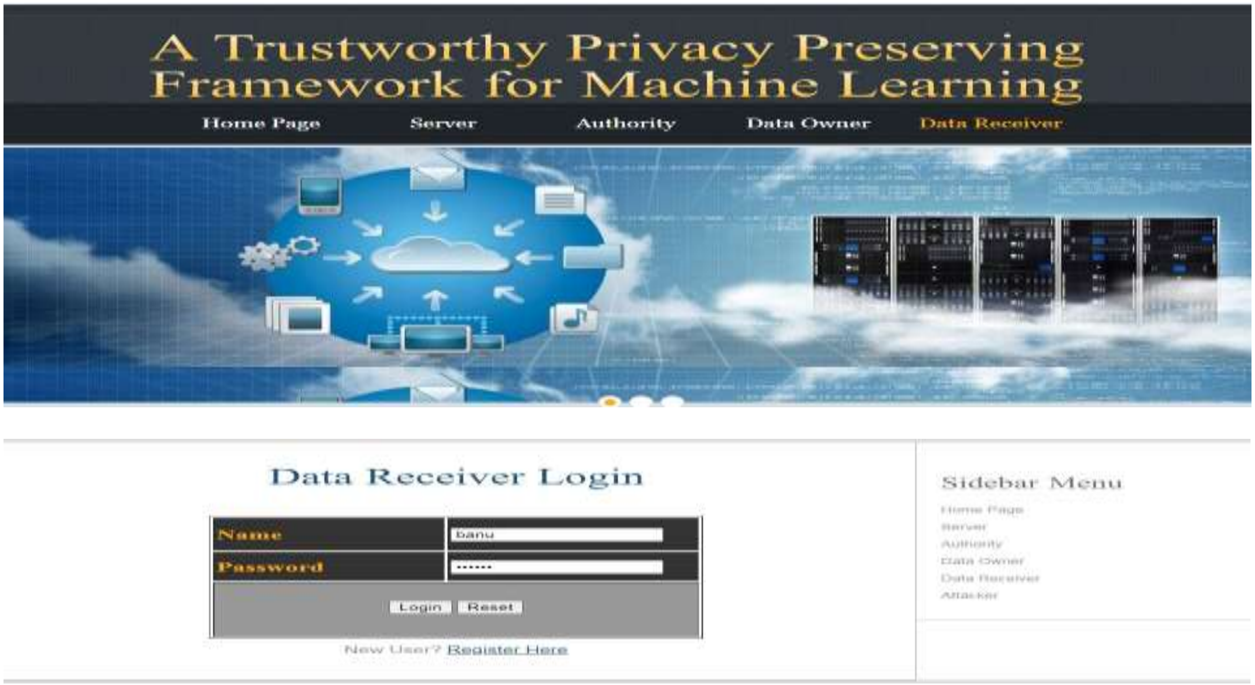


Upload File

Both Encyprtion and Secret Key Permission is Provided For This File

File Name :-	conclusion.docx
Select File :-	Choose File conclusion.docx
Content	PK└¶ – ▯ ! ���7fr │ ‼ ▯ [Content_Types].xml �┘┐(� ┐ �г�ŋ�ºϯ�ŧ�ǀ

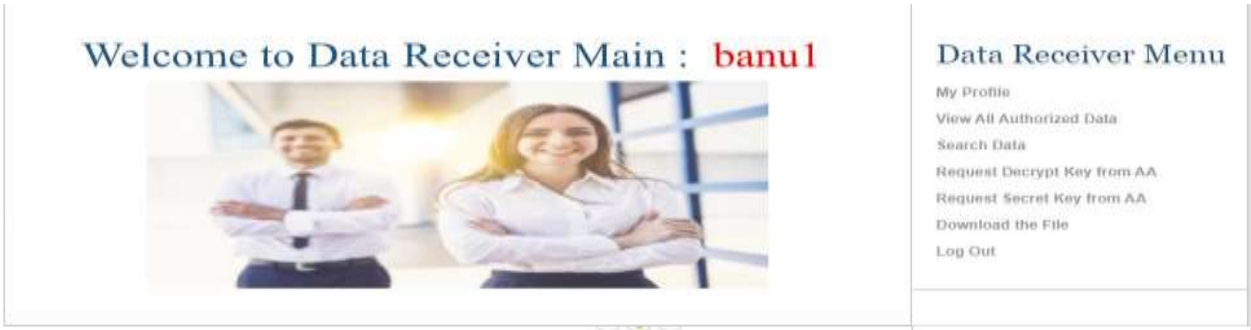
Next the Data Receiver, The operations that are performed by the Data Receiver are listed below and the Data Receivers should also get registered themselves before the login as same as the Data Owner.



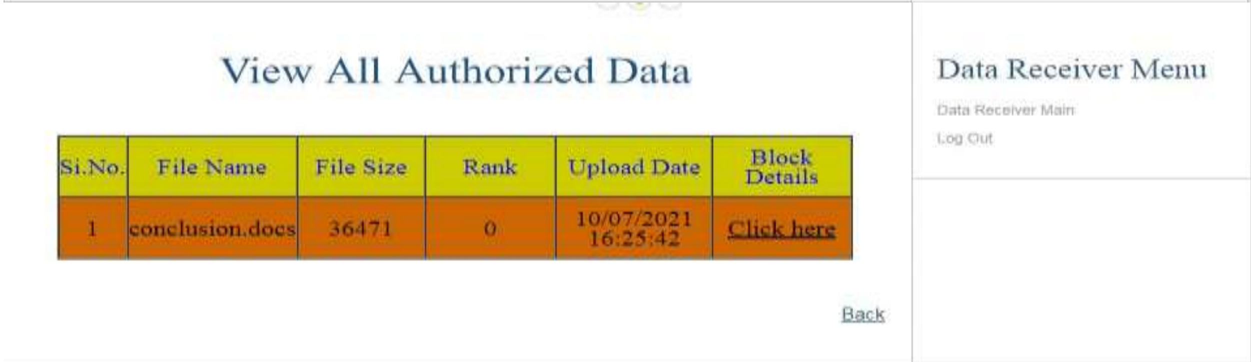
A Trustworthy Privacy Preserving
Framework for Machine Learning
Home Page
Server
Authority
Data Owner
Data Receiver

Data Receiver Login

Name	banu
Password	••••••

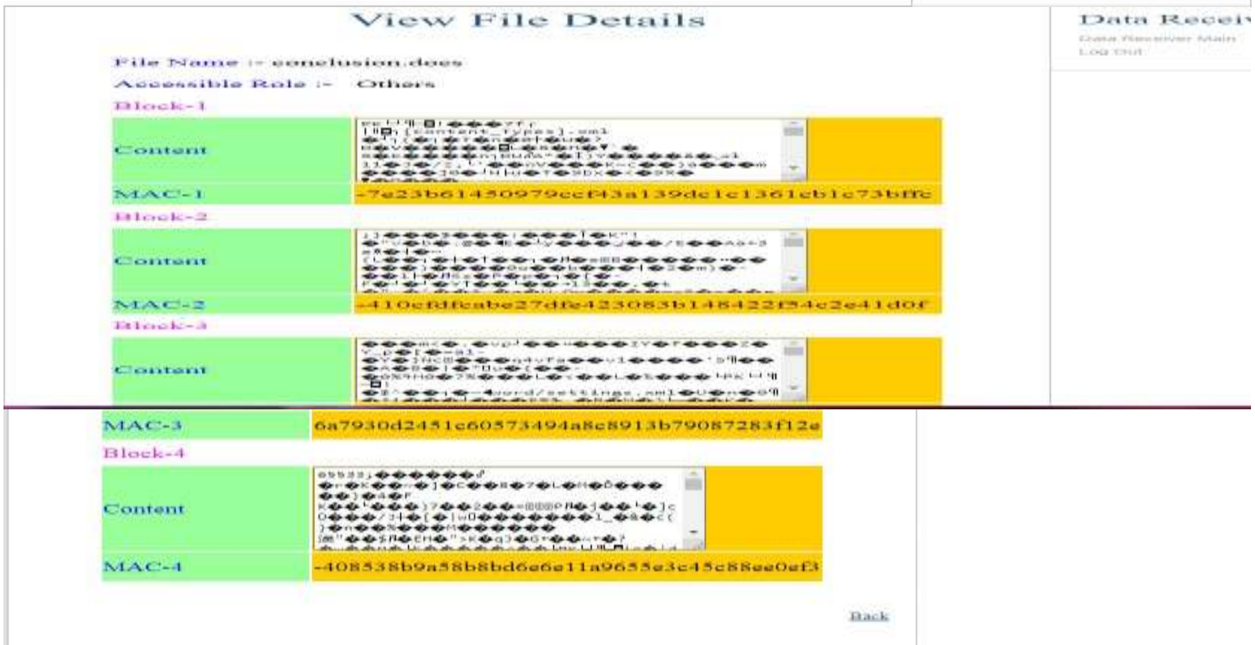


Welcome to Data Receiver Main : banu1



View All Authorized Data

Si.No.	File Name	File Size	Rank	Upload Date	Block Details
1	conclusion.docs	36471	0	10/07/2021 16:25:42	Click here



View File Details

File Name :- conclusion.docs
Accessible Role :- Others

Block-1

Content	[illegible]
MAC-1	-7e23b61450979ccf43a139dc1c1361cb1c73bffc

Block-2

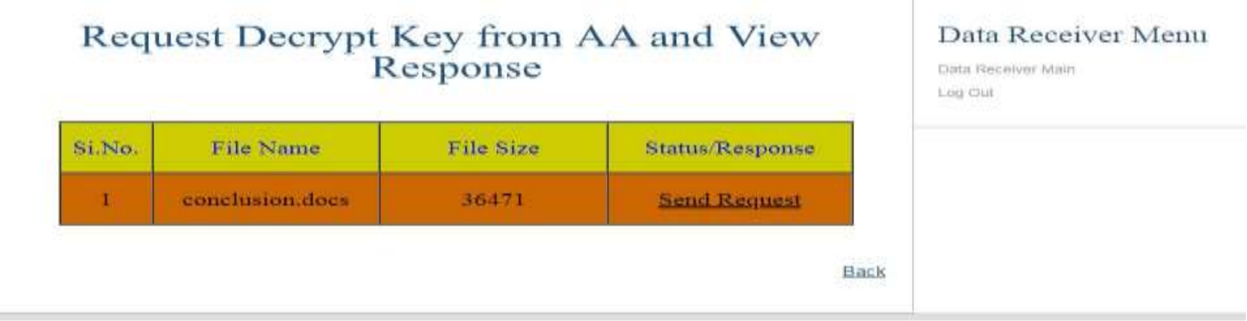
Content	[illegible]
MAC-2	-410cfdfcabe27dfe423083b148422f54c2e41d0f

Block-3

Content	[illegible]
MAC-3	6a7930d2451c60573494a8c8913b79087283f12e

Block-4

Content	[illegible]
MAC-4	-408538b9a58b8bd6e6e11a9655e3c45c88ee0ef3



Request Decrypt Key from AA and View Response

Si.No.	File Name	File Size	Status/Response
1	conclusion.docs	36471	Send Request

8. CONCLUSION

In an IIoT environment, we proposed a brand-new framework called PriModChain that may be utilised for reliable machine learning and sharing. To impose privacy and trustworthiness on ML in the IIoT, PriModChain combines the principles of smart contracts, blockchain, federated learning, differential privacy, and interplanetary file system (IPFS). While differential privacy imposes privacy on the ML models, federated learning serves as the overall framework for federating and sharing ML models. When smart contracts and the Ethereum blockchain are combined, the framework gains traceability, transparency, and immutability..With safe P2P content distribution, IPFS delivers immutability, low latency, and quick decentralised archiving. The viability of the suggested framework was examined in terms of privacy, security, dependability, safety, and resilience. In terms of the five pillars of trustworthiness, PriModChian produces good results, demonstrating that it is a workable solution for trustworthy privacy-preserving machine learning in IIoT systems. One of the suggested work's potential future directions is to research various methods for reducing latency in order to increase efficiency.

REFERENCES

[1] R. Iqbal, T. Maniak, F. Doctor, and C. Karyotis, “Fault detection andisolation in industrial processes using deep learning approaches,” IEEETransactions on Industrial Informatics, vol. 15, no. 5, pp. 3077–3084,2019.
[2] S. A. Shevchik, G. G. Masinelli, C. Kenel, C. Leinenbach, and K. Wasmer,“Deep learning for in situ and real-time quality monitoring inadditive manufacturing using acoustic emission,” IEEE Transactions onIndustrial Informatics, 2019.
[3] M. S. Hossain, M. Al-Hammadi, and G. Muhammad, “Automatic fruitclassification using deep learning for industrial applications,” IEEETransactions on Industrial Informatics, vol. 15, no. 2, pp. 1027–1034,2018.
[4] R. S. Peres, A. D. Rocha, P. Leitao, and J. Barata, “Idarts–towardsintelligent data analysis and real-time supervision for industry 4.0,”Computers in Industry, vol. 101, pp. 138–146, 2018.
[5] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov,K. Talwar, and L. Zhang, “Deep learning with differential privacy,” inProceedings of the 2016 ACM SIGSAC Conference on Computer andCommunications Security. ACM, 2016, pp. 308–318.
[6] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, “Membershipinference attacks against machine learning models,” in Security andPrivacy (SP), 2017 IEEE Symposium on. IEEE, 2017, pp. 3–18.
[7] C. Song, T. Ristenpart, and V. Shmatikov, “Machine learning modelsthat remember too much,” in Proceedings of the 2017 ACM SIGSACConference on Computer and Communications Security. ACM, 2017,pp. 587–601.
[8] M. Fredrikson, S. Jha, and T. Ristenpart, “Model inversion attacksthat exploit confidence information and basic countermeasures,” inProceedings of the 22nd ACM SIGSAC Conference on Computer andCommunications Security. ACM, 2015, pp. 1322–1333.

[9] F. Fraile, T. Tagawa, R. Poler, and A. Ortiz, "Trustworthy industrial iotgateways for interoperability platforms and ecosystems," IEEE Internetof Things Journal, vol. 5, no. 6, pp. 4506–4514, 2018.

[10] P. Kairouz, S. Oh, and P. Viswanath, "Extremal mechanisms for localdifferential privacy," in Advances in neural information processingsystems, 2014, pp. 2879–2887.

[11] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, andM. Atiquzzaman, "Local differential privacy for deep learning," IEEEInternet of Things Journal, 2019.

[12] Y. Wang, X. Wu, and D. Hu, "Using randomized response for differentialprivacy preserving data collection." in EDBT/ICDT Workshops, vol.1558, 2016.

[13] M. Bun and T. Steinke, "Concentrated differential privacy: Simplifications,extensions, and lower bounds," in Theory of CryptographyConference. Springer, 2016, pp. 635–658.

[14] H. B. McMahan, E. Moore, D. Ramage, and B. A. y Arcas, "Federatedlearning of deep networks using model averaging," 2016.

[15] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning:Concept and applications," ACM Transactions on Intelligent Systems andTechnology (TIST), vol. 10, no. 2, p. 12, 2019.

[16] J. Benet, "Ipfs-content addressed, versioned, p2p file system," arXivpreprint arXiv:1407.3561, 2014.

[17] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamar´ıa,"Blockchain and smart contracts for insurance: Is the technology matureenough?" Future Internet, vol. 10, no. 2, p. 20, 2018.

[18] H. B. McMahan, E. Moore, D. Ramage, S. Hampson et al.,"Communication-efficient learning of deep networks from decentralizeddata," arXiv preprint arXiv:1602.05629, 2016.

[19] C. J. Cremers, "The scyther tool: Verification, falsification, and analysisof security protocols," in International Conference on Computer AidedVerification. Springer, 2008, pp. 414–418.

[20] G. Lowe, "A hierarchy of authentication specifications," in Proceedings10th Computer Security Foundations Workshop. IEEE, 1997, pp. 31–43.

[21] C. Cremers and S. Mauw, "Security properties," in Operational Semanticsand Verification of Security Protocols. Springer, 2012, pp. 37–65.

[22] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrialinternet of things (iiot): An analysis framework," Computers in Industry,vol. 101, pp. 1–12, 2018.

[23] A. Sedgewick, "Framework for improving critical infrastructure cybersecurity,version 1.0," Tech. Rep., 2014.

[24] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Usingblockchain for medical data access and permission management," in2016 2nd International Conference on Open and Big Data (OBD).IEEE, 2016, pp. 25–30.