CroPAiD: Protection of Information in Agriculture Cyber-Physical Systems using Distributed Storage and Ledger

S. L. T. Vangipuram[1] , S. P. Mohanty[2] , and E. Kougianos[3]
University of North Texas, Denton, TX 76203, USA.[1,2,3]

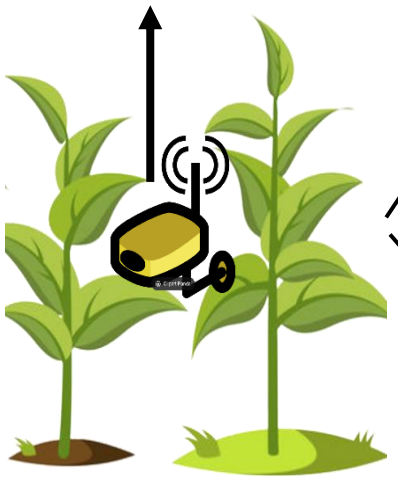
Email: lt0264@unt.edu[1] , saraju.mohanty@unt.edu[2], and elias.kougianos@unt.edu[3].

Talk Outline

1. Smart Agriculture
2. Introduction/Existing Systems
3. Motivation for CroPAiD
4. Related Works
5. Challenges in IoAT
6. Why CroPAiD?
7. Novelty in CroPAiD?
8. A-CPS
9. Distributed Storage - IPFS
10. STREAMS & MAM
11. Architecture and Algorithms
12. Technologies/ Datasets
13. Implementation and Results
14. Conclusion & Future work

Smart Agriculture

Modern Equipment



Agricultural Data

Robots

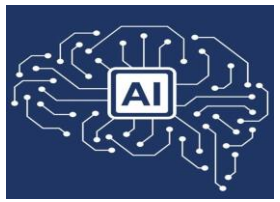
IoAT

Satellites

Visualization

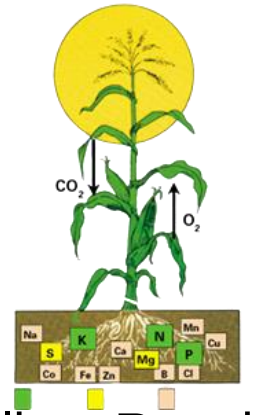
Drones

AI



- Smart agriculture is an advanced procedure of conducting agricultural activities using technologies such as internet of things (IoT), sensors, artificial intelligence, and robots to increase farm productivity.
- It is an innovative way to reduce human effort and make the best use of available resources.

Introduction/Existing Designs



Fertilizer Requirements

Nitrate Contamination

Crop Disease

Agriculture Data

Collecting & Storing Agricultural Data

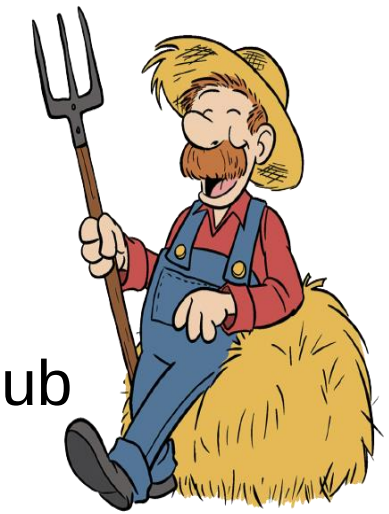
Traditional/ Conventional Storage Systems

Cloud

Research Institutes

Desktop Manager

Network Hub



Farmers

Motivation for CroPAiD

Motivations

Central Limitations

- Single point failure.
- Security Breaches.
- Data Confidentiality Issues.
- Unresponsive for massive real-time data.
- Increase in costs
- Bottlenecks in data access.

Cloud Drawbacks

- Data loss or theft.
- Insecure Interfaces.
- Denial of service attack.
- Data Leakage.
- Vulnerabilities through different technologies.

Cybersecurity Issues

- Malware attacks.
- Phishing Attacks.
- Ransomware Attacks.
- Internet anonymity.
- Attack on middleware, network & application layers.

Sensor Problems

- Communication problems.
- Security Breaches.
- Use of Different Technologies.
- Challenges in Storage.

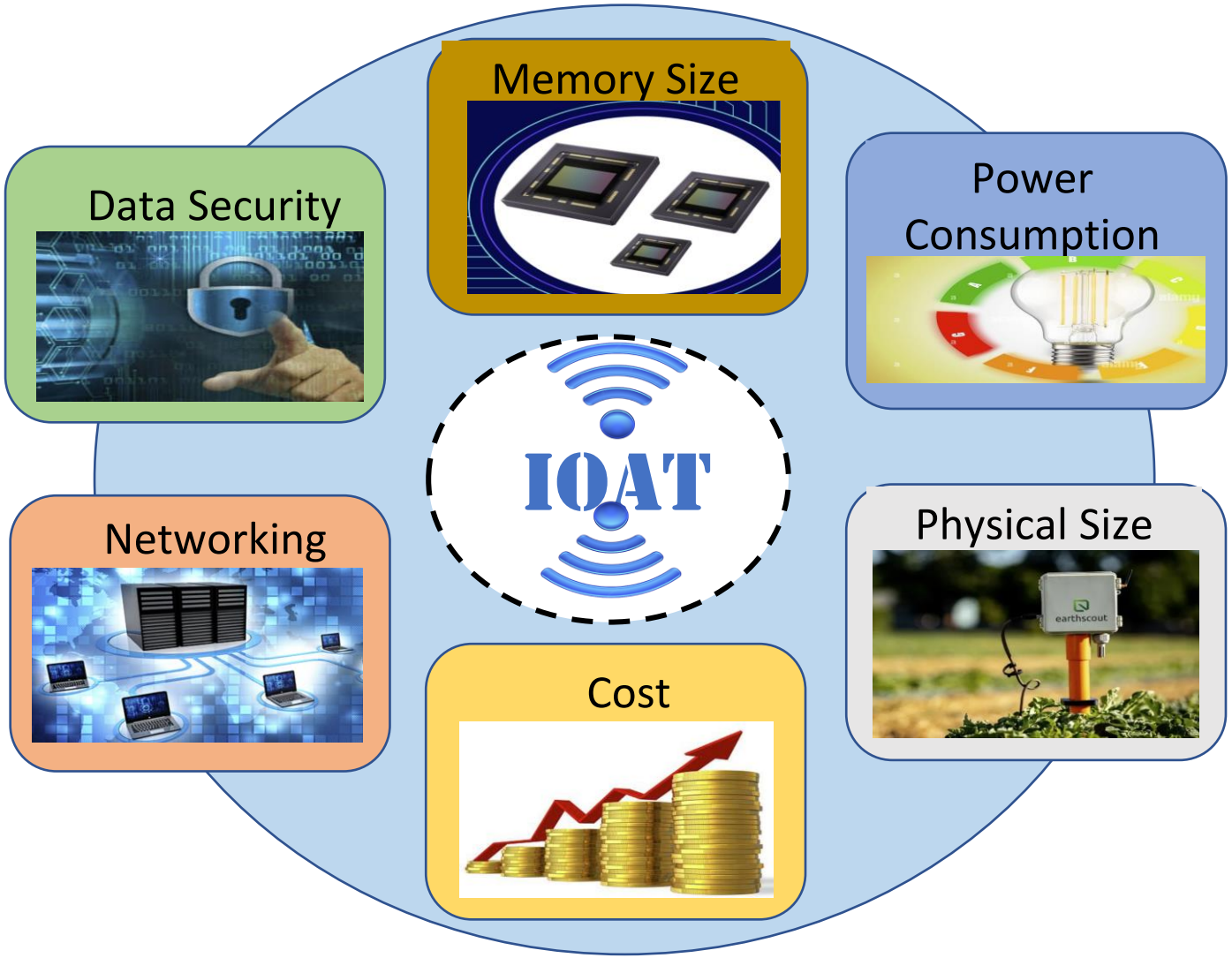
Blockchain Disadvantages

- Scalability
- Storage Issues.
- Security.
- Privacy.
- Cost.
- Energy consumed.
- Private-key visibility during wallet creations.

Related Works

Application	Storage & Sharing Technology	Cost	Platform	Energy Consumption
G-DaM [5]	IPFS + DS+ Public BC	Low	Distributed + Decentralized	High
agroString [6]	corda Private BC	Zero	Decentralized	High
Traceability[7]	+ Database+ BC	Low	Decentralized	High
Traceability [8]	BC	High	Decentralized	High
Crop Monitoring [9]	IOTA Tangle	Zero	Distributed Ledger	Low
Access Control [10]	IOTA Tangle	Zero	Distributed Ledger	Low
CroPAiD [Current Paper]	IPFS + DS+ IOTA Tangle	Zero	Distributed + Ledger	Low

Challenges in IoAT-Internet-of-Agro-Things

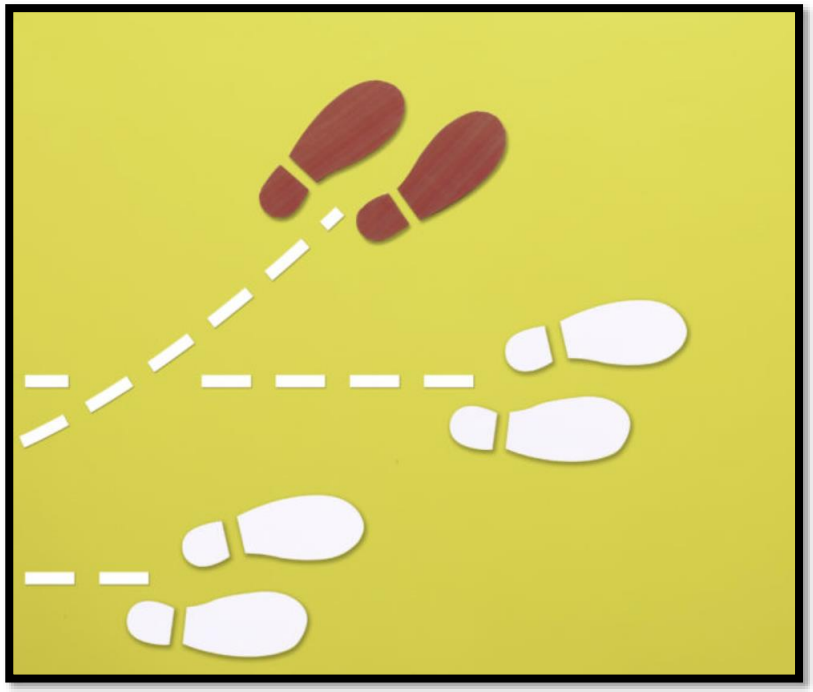


- Memory Size
- Power Consumption
- Physical Size
- Cost
- Networking
- Data Security

Why CroPAiD?

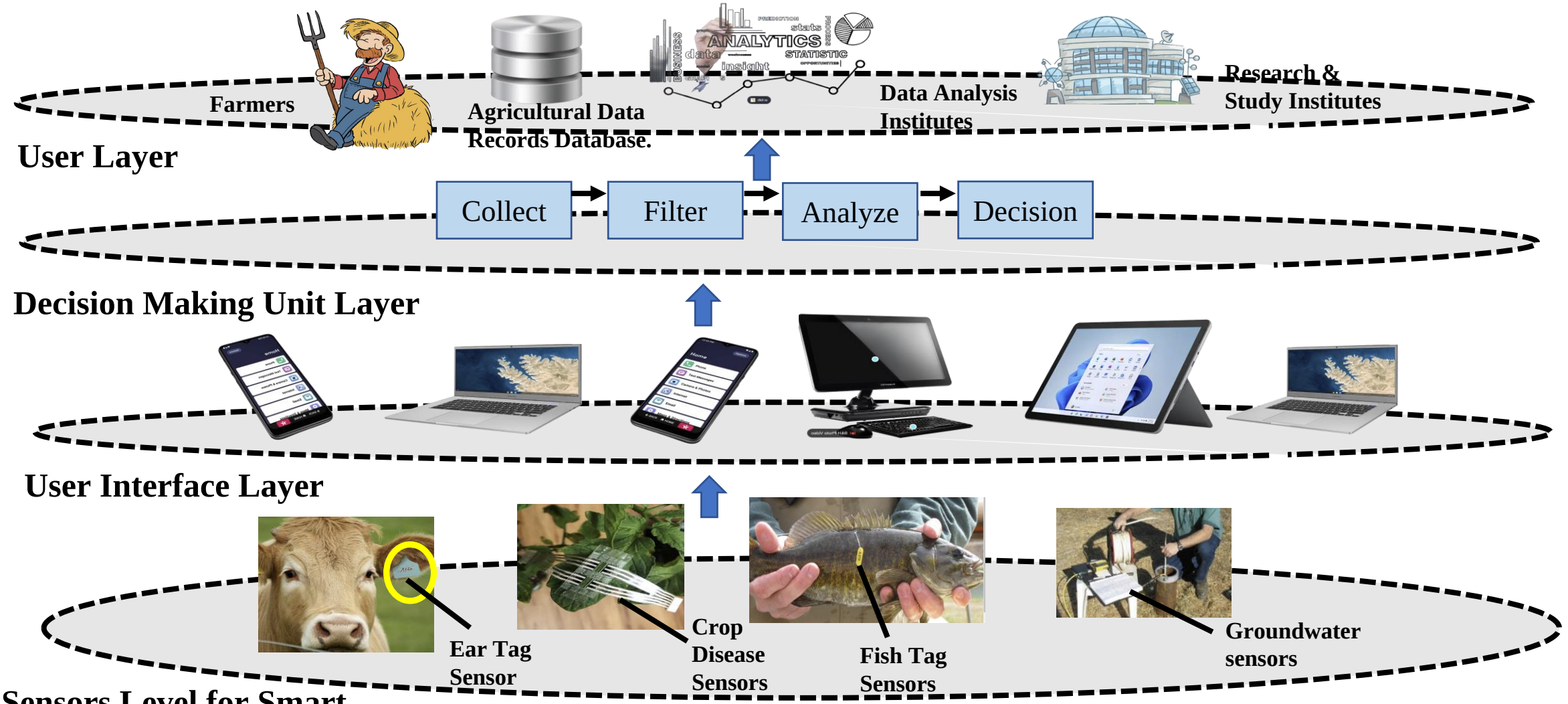
- A unique system with Tangle to increase the quality of data and avoid drawbacks of sensor things.
- To move bulk data to IOTA and avoid double spending issues of Tangle, the current system uses distributed storage systems near the edges.
- The imitations of conventional storage databases, cloud, and central systems are circumvented using the IOTA distributed ledger platform.
- Increasing security, data integrity, and evading data tampering by the IOTA system.

Novelty in CroPAiD

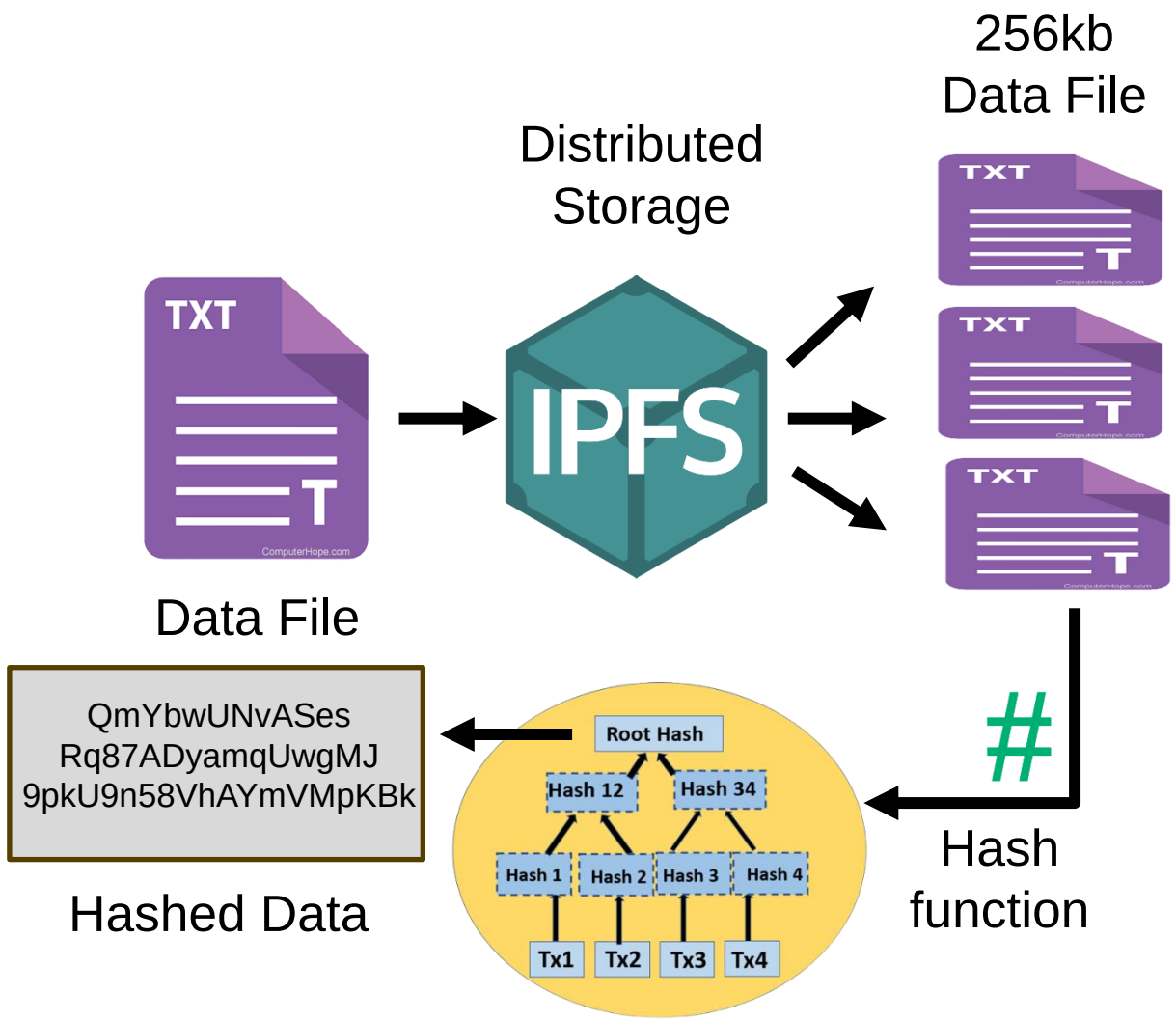


- Overcoming blockchain high transaction fees and energy usage through distributed ledger system of Tangle.
- Using Double hashing procedure for the agricultural data through IPFS and Tangle to increase security and privacy of data.
- A state-of-the-art architecture.
- Designing a Cost-efficient infrastructure and showing results with zero transaction fees and secured hashes.

A-CPS: Agriculture Cyber Physical Systems

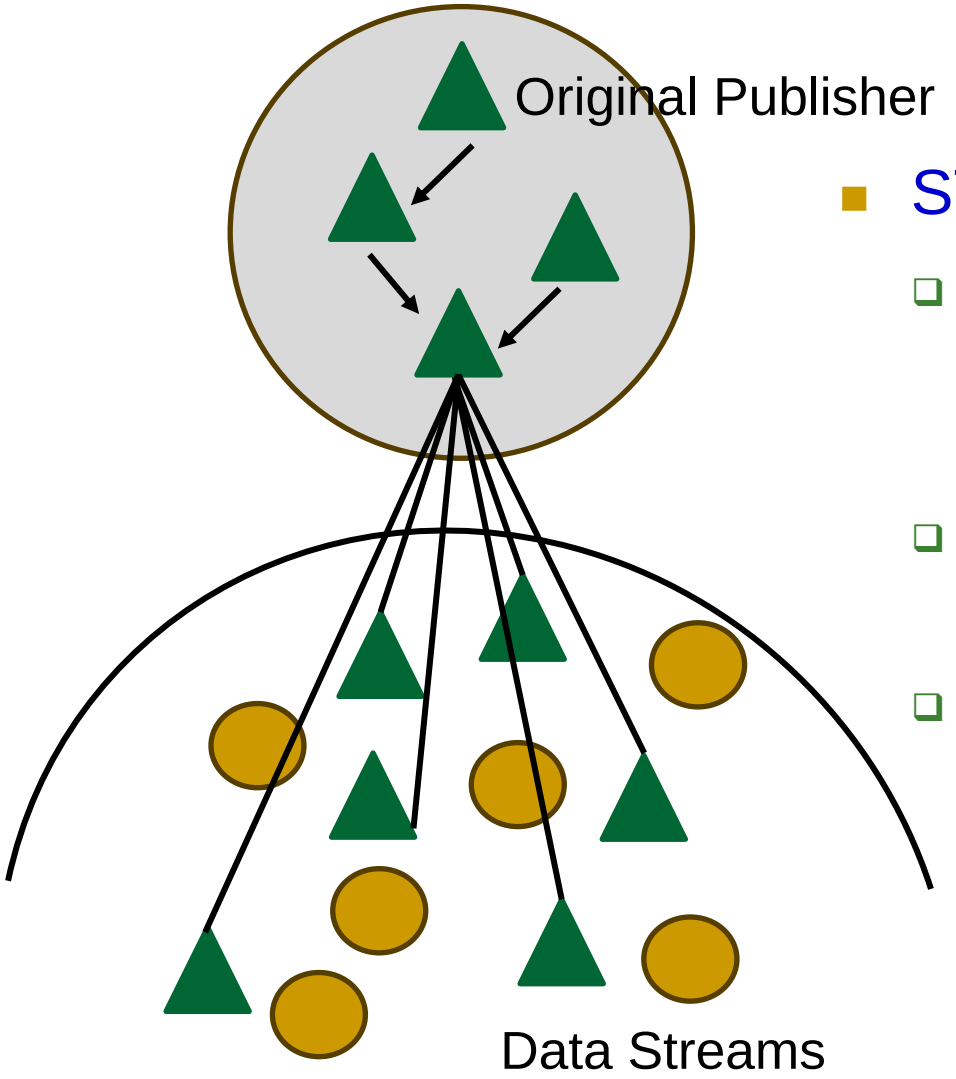


Distributed Storage-IPFS



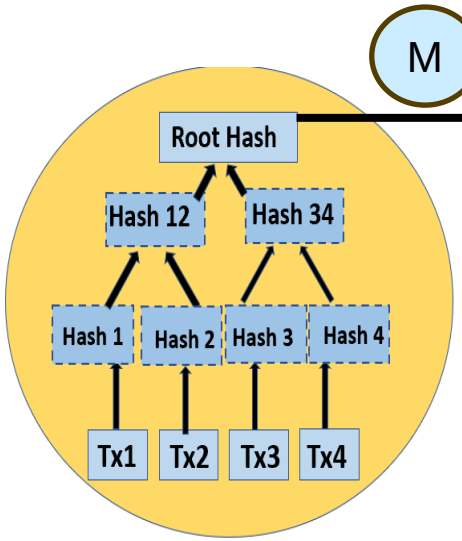
- A distributed storage-IPFS or Interplanetary File System is an internet protocol used to store data.
- It avoids data or asset duplicates across the network to evade double spending problems.
- IPFS collects the addresses of the data in the network. IPFS is used as an off-chain storage.
- Each data is divided into 256 kb data size blocks.

How Security in IOTA Tangle-STREAMS



- STREAMS
  - All branches of data streams reference a common root and state of data belonging to publisher for authenticity.
  - The Tangle data uses streams to always guarantee data integrity.
  - Streams enable users to control the ownership of data and receive payments.

How Security in IOTA Tangle-MaM



Markle Tree

Tree's root as the address of the transaction

Public Mode

Hash of the Tree's root as the address of the transaction

Private Mode

H M

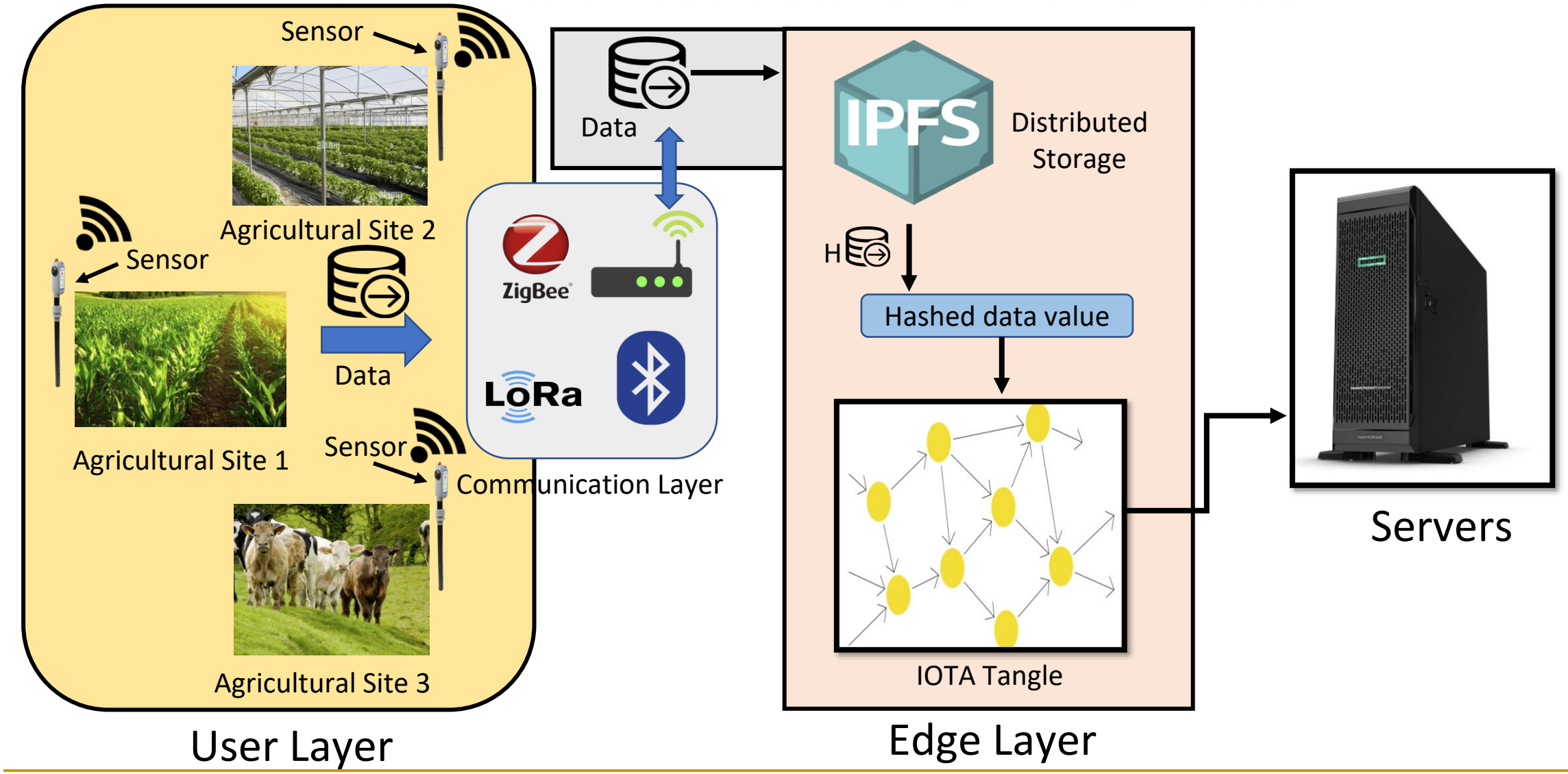
Authorization Key with Hash of the Tree's root as the address of the transaction

Restricted Mode

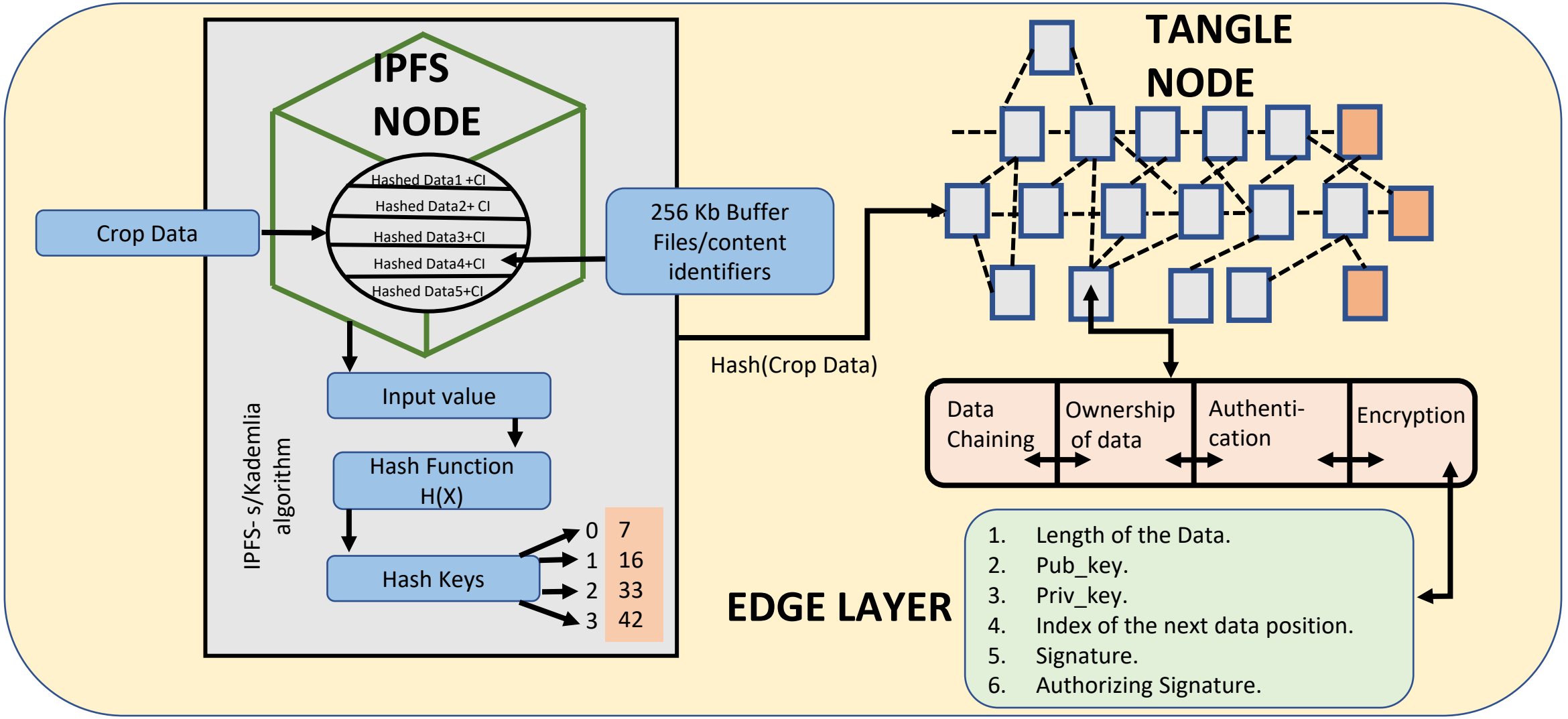
+ H M

- Three Modes: Public, Private and Restricted.
- MAM fulfills an important need for integrity and privacy.
- MaM uses Merkle tree to hash the messages and give the root Message.
- A MAM publisher can decide to split the channel at any point in time, which means future messages use a new Merkle tree whose root has not been revealed before

Novel Architecture of CroPAiD



Detailed Data Flow



Proposed Algorithms – (I)
Crop Data File to IPFS

1: Inside the Edge layer the Distributed storage (DS_E) generate both Public and Private Keys (DS_{pu}, DS_{pr}) for the Crop Data.

2: $DS_E(C_d) \longrightarrow DS_E(C_{dbf265\ KB})$.

3: The file gets hashed through cryptography method using SHA 256/SHA 3 to give unique id represented as C_{Id}(Content Identifiers).

4: $Encr(DS_{pu})S = H(DS_{pr} * A)$, where A is a constant ,* is a mathematical operation that is calculated in single direction and H is the secured hash function.

5: **if** C_d is equal $H(DS_{pr}* A)$ is equal $H(DS_E(C_{dbf265\ KB}))$ **then**

6: Publishing $H(C_{dbf265\ KB}) \longrightarrow$ IPFS.

7: **else**

8: Process End.

9: **end if**

10: Repeat the steps from 1 through 10 whenever a file is uploaded in the edge layer

Proposed Algorithms – II

Crop Data File in IOTA Tangle

1:We represent $H(C_d)_{ipfs}$ coming from ipfs as input data to IOTA as Tangle(In_{iota}).

2:$In_{iota} \longrightarrow In_{iota}$, $In_{iota}len$, $In_{tangle}Prkey$, $In_{tangle}Pukey$, ind,

3:nex-ind,sign $auth_{sign}$.

4:Random Source $\longrightarrow S_d$.

5:$S_d \longrightarrow In_{tangle}Prkey$, $In_{tangle}Pukey$.

6:$H(In_{tangle}Pukey) \longrightarrow I$.

7:A different key pair is generated for the next input data (Next-In $_{iota}$) from another random source.

8:The key pair from the next input data is (Next-In $_{tangle}Prkey$) and (Next-$In_{tangle}Pukey$).

9:$H(Next\text{-}In_{tangle}Pukey) \longrightarrow n\text{-}I$.

10:A digest d is calculated for signature.

11:$d= H((In_{iota}) + (In_{iota}len) + (In_{tangle}Pukey) + (n\text{-}I)$.

12:sign= signature(d + $In_{tangle}Prkey$)

13: **if** $H(In_{iota})$==sign+$In_{tangle}Pukey$ **then**

14:Verification Success.

15: **else**

16:Process End.

17:For authorization, we need the public(IoT_{Pukey}) and private keys (IoT_{Prkey})of the IoT device.

18:$auth_{sign}$ = signature(IoT_{Prkey})

19: **if** $auth_{sign}$== signature(IoT_{Pukey}) **then**

20:Authentication Success.

21: **else**

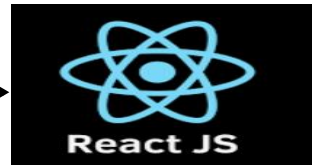
22:Process End.

23: **end if**

24: **end if**

25:Repeat the steps from 1 through 25 whenever a file is moved from IPFS in the edge layer.

Technologies used for Implementation

- React JS for Front end → 

- NodeJS → 

- JSON file configuration → 

→ 

- IPFS Node → 

- AWS DynamoDB → 

Edge

Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz, 32.0 GB RAM

Datasets

- When a crop gets infected, it damages and changes all the primary functions of the food that can harm humans when consumed.
- Crop infected data is beneficial in predicting future crop damage and helps improve crop yield.
- Such data is crucial for farmers and scientists to take precautions and perform research and study.
- This data need to be transmitted in a secure manner without any tampering for correct analysis.

(a) Apple-healthy and Apple-Cedarapplerust.

(b) Potato-healthy and Potato-Lateblight

(c) Cherry-healthy and Cherry-Powderymildew.

(d) Corn-healthy and Corn-Commonrust.

(e) Grape-healthy and Grape-Esca (Black-Measles).

(f) Tomato-healthy and Tomato-Bacterialspot.

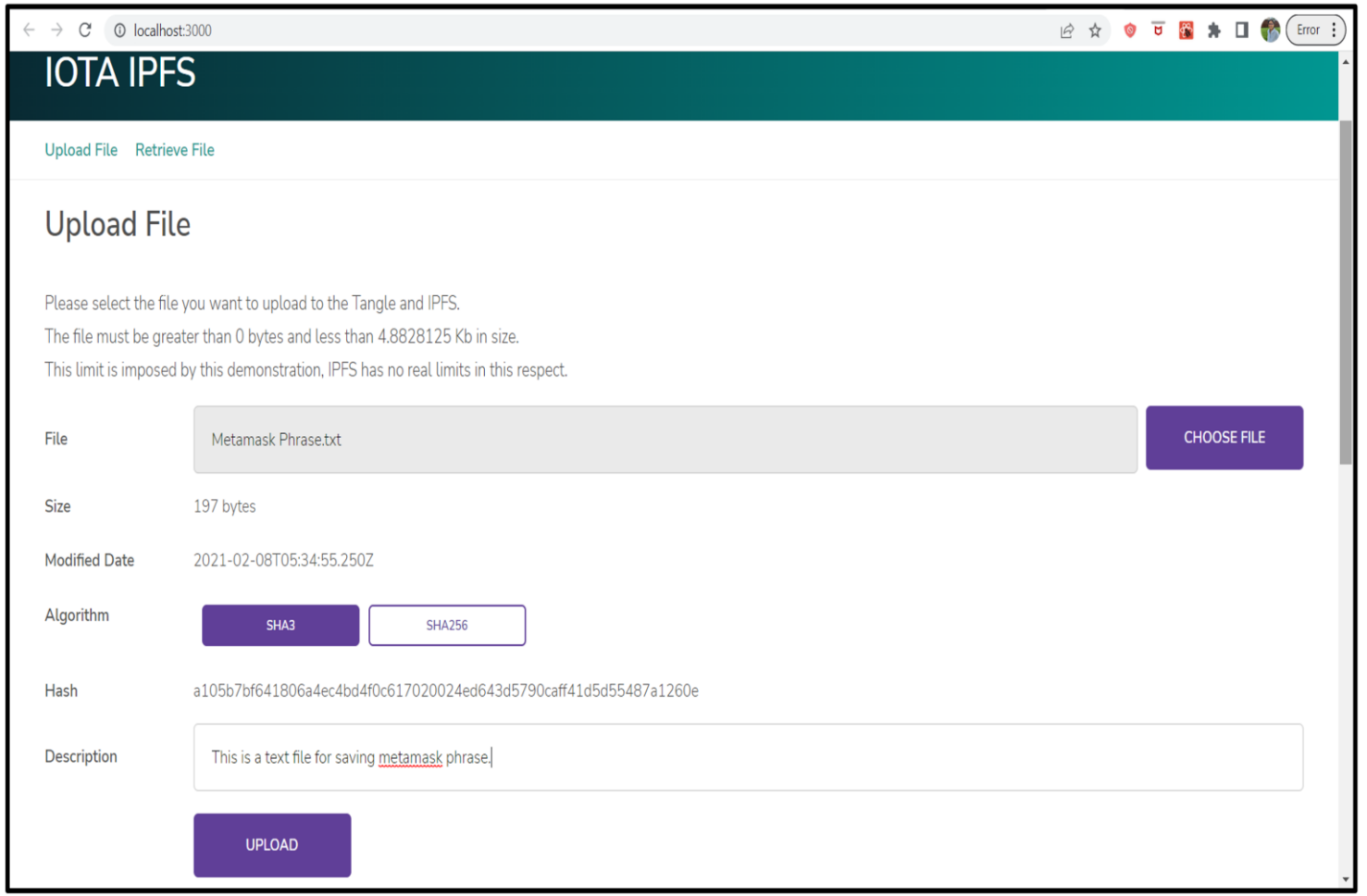
Datasets

File Name	Size	.ZIP Size	Source of Dataset Link.
Apple-Healthy	25.7 MB	23.8 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Apple-Cedarapplerust	3.25 MB	2.9 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Cherry-healthy	15.1 MB	14.06 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Cherry-Powderymildew	12.8 MB	11.41MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Corn-healthy	14.9 MB	13.39 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Corn-Commonrust	18.4 MB	16.72 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Grape-healthy	6.87 MB	6.29 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Grape-Esca(BlackMeasles)	28.6 MB	27.30 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Peach-healthy	6.16 MB	5.54 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Peach-Bacterial spot	32.8 MB	29.89 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Potato-healthy	3.17 MB	3.05 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Potato-Lateblight	17.5 MB	16.5 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Tomato-healthy	37.0 MB	35.29 MB	https://www.kaggle.com/datasets/divumarcus/plant-health
Tomato-Bacterial spot	30.5 MB	27.5 MB	https://www.kaggle.com/datasets/divumarcus/plant-health

CroPAiD Functional Verification

- The User-Interface of the current application is shown here. It is built using React JS to communicate with the Backend IOTA Tangle.

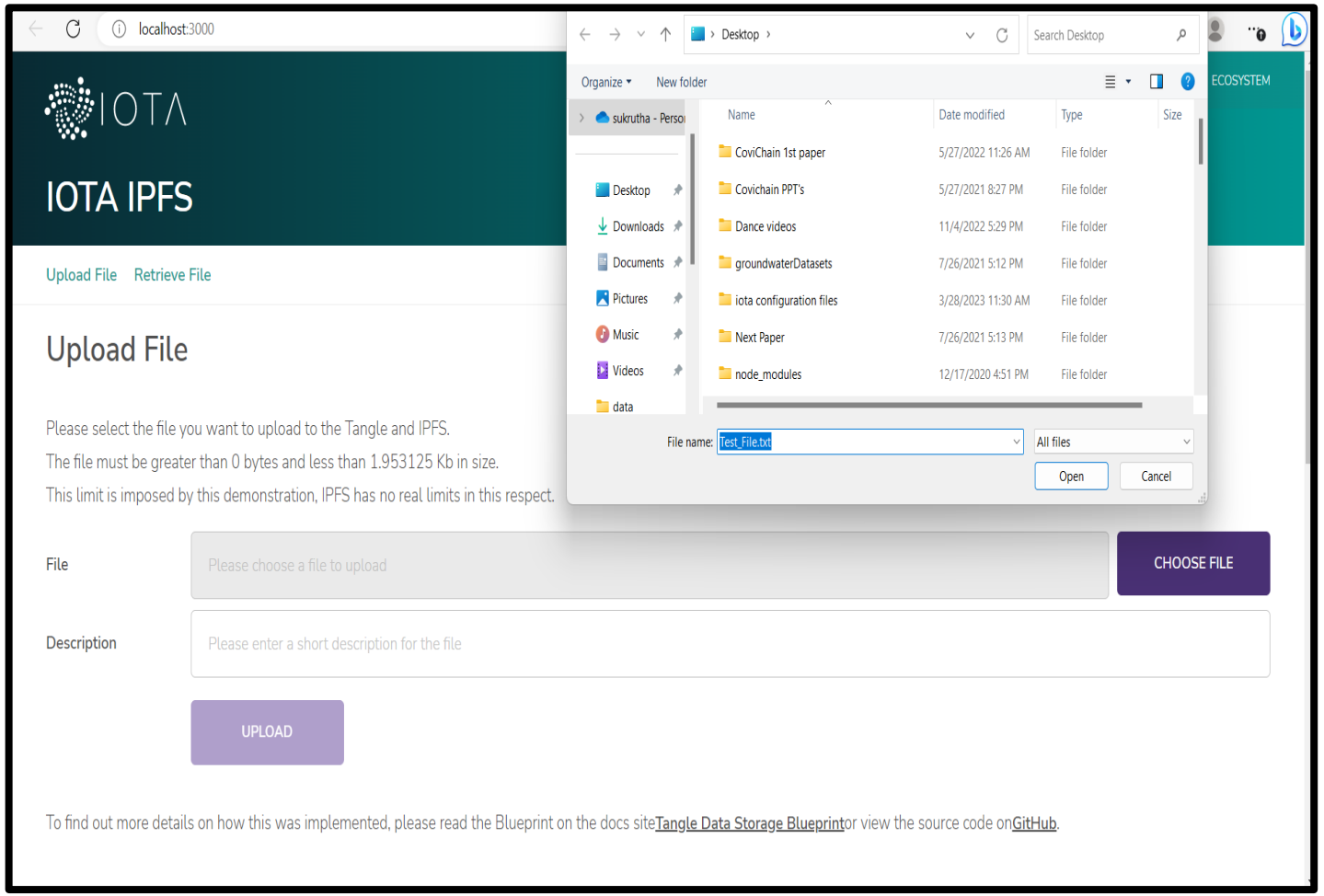
- The size of the input file can be modified in the JSON configuration.



User Interface for CroPAiD

Uploading

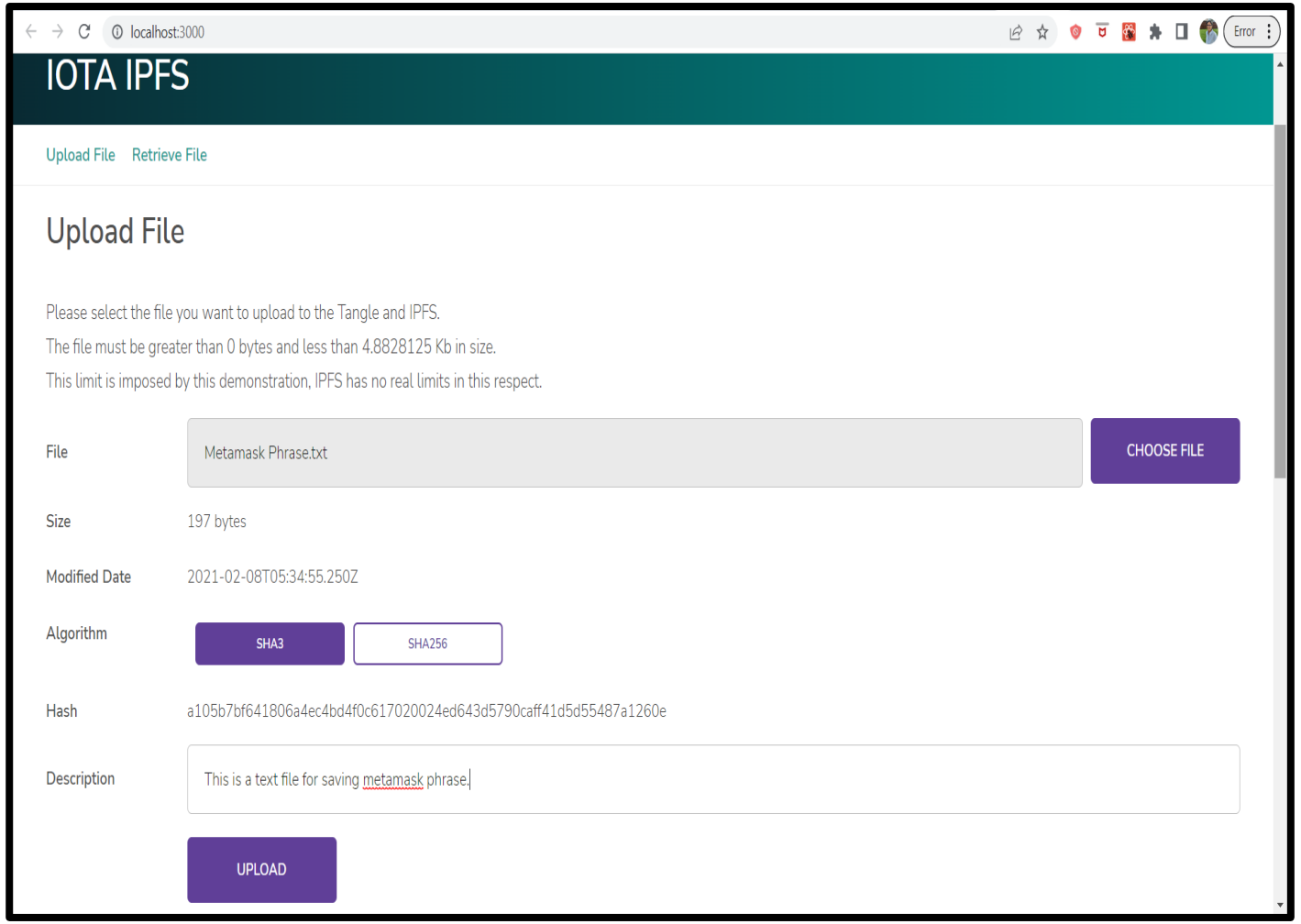
- We upload the crop data file to the IPFS node to get the hash of the file.
- The IPFS hash file generated does not have the time stamp but avoids duplicates and double-spending attacks on the data transferred.



Uploading File

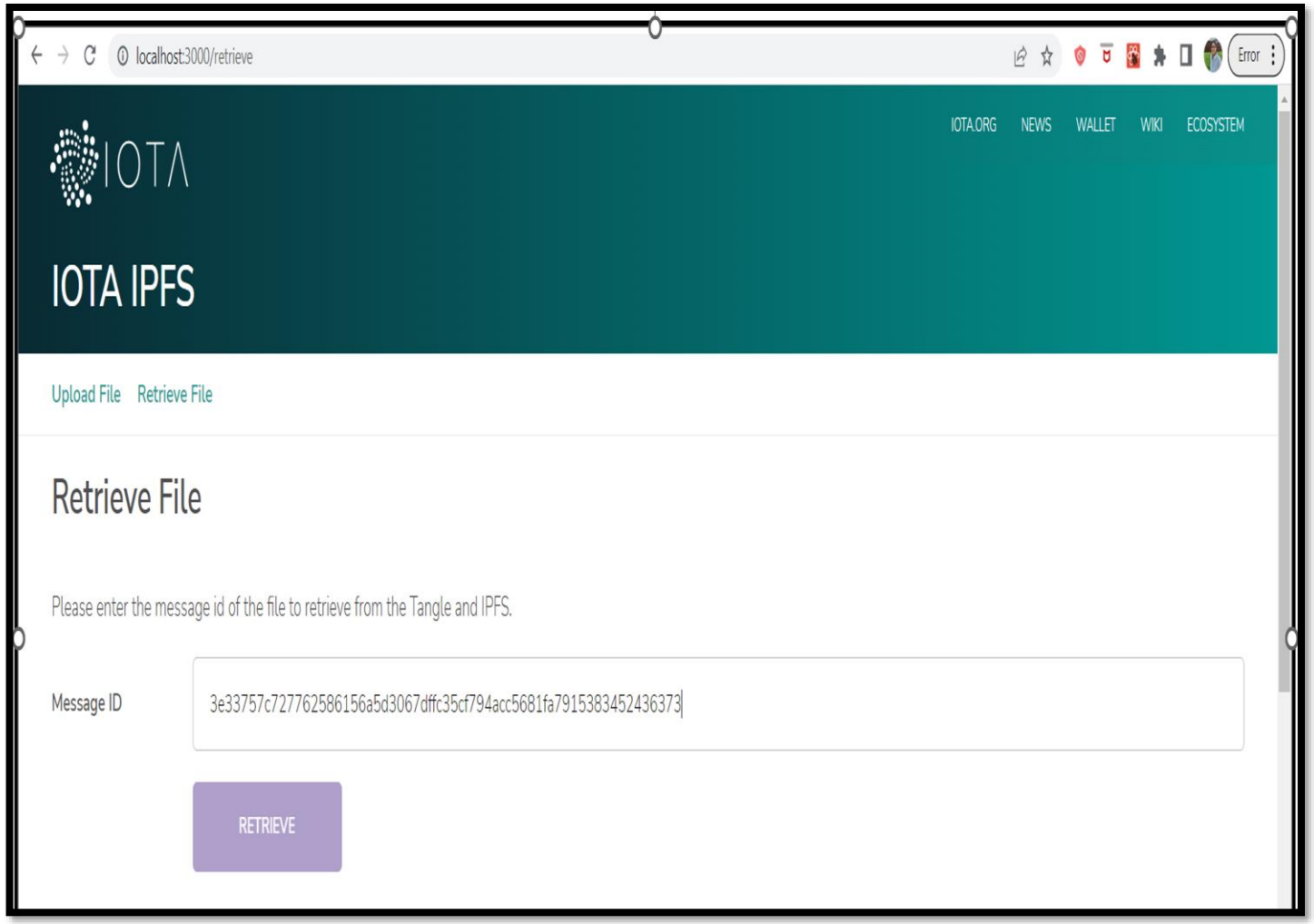
Hash

- The application further takes the IPFS hash as an input to the IOTA node to give another hash from the tangle platform.



Retrieve File

- The file can be retrieved from the IOTA Tangle.
- Once both the hashes were received from the application,we used the message unique ID to retrieve the original file



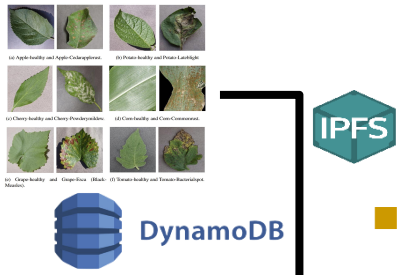
Experiment Results of CroPAiD

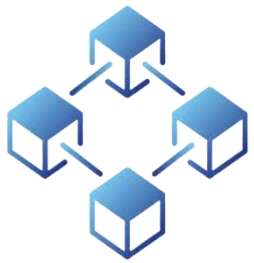
File Name	Size	.ZIP Size	IPFSHash	Tangle Hash
Apple-Healthy	25.7 MB	23.8 MB	QmXWpe6Q5v9qH7Wwgr 5HH5BmB78Q2u4wP WFd7NkvooFZrP	SKJYF76R3947IRYREIU598475FHKEUR834759IFR30WP WEKDSVLDKFROIRFHDKJ
Apple-Cedarapplerust	3.25 MB	2.9 MB	QmYuERUhBu8fuXRa b7RkWwDqDZKHcn8Dp kUwpopaNMjAB3	GZSDUAYR87R675RWRYGJDHFU9586ERUFJBLDIR43950 35RTHGKVJS579048EOIHK
Cherry-healthy	15.1 MB	14.06 MB	QmPRkovGVUgYx2ue hy1g5QHwqECXpd1No CXAsUehznjU5t	JHSGFUY5R635RWGFJSHVET875985WIGDSHVLUSP5T9 8 FHDVJDOYW8R76487RITHK
Cherry-Powderymildew	12.8 MB	11.41 MB	QmTy9g2ENwSP66D V2qkUP7XchCd9AQ maznM8saZbvz1xcY	CMVNGGF653RFHHKJLLOUUERWEQSCCBBJH87966453 FDJ GHKJUYRTEESXZVFMHKJO
Corn-healthy	14.9 MB	13.39 MB	QmZkM4ymQCXKThL hY6igBMPxcjwaNa uGj6Khvnr1rfuHNh	LQREWRR5473FCVVNGH67892DHGNCSK53FHSFFKJOI W RW9345FDGERSBHYUKIOUQW
Corn-Commonrust	18.4 MB	16.72 MB	QmVCm8uXgyvnQEfvC bDpPxZ95XNuTyS ir7thRMMLfoNzFi	FR5476HYHKHNCVZSA338687UYKJNGGFTR544333DEH GJUIIPKNMNBBFVDFSEW4YU
Grape-healthy	6.87 MB	6.29 MB	QmX1ohMDQqRqtvDG PYVGZjyfVx3zuVEK TXxKRmj6VJxc75	MNXBFYO5I73RGKLD7879HSJRY764934UTWJHEUFQJO 7GDAPOLKLKOIUSDWKNMND4
Grape-Esca(BlackMeasle)	28.6 MB	27.30 MB	QmZw4X69QyptuNWj bA3o6NWAK6x9ve eb3CcXZdPWQV6qcY	MNXBFYO5I73RGKLD7879HSJRY764934UTWJHEUFQJO 7GDAPOLKLKOIUSDWKNMND4

Experiment Results of CroPAiD

File Name	Size	.ZIP Size	IPFSHash	Tangle Hash
Peach-healthy	6.16 MB	5.54 MB	QmUCANWk22uX6JC Bew8SCRXXDbMfru XyfCj7YJmSJesmYz	MNZCJHARU8473EIDHKSJ FLJG9485029QPWADJSLKFWOR IAJFKZJFKSDJLLKPLSKJ
Peach-Bacterial spot	32.8 MB	29.89 MB	QmdWXdTy8LaTHaL wFAPe49FCBd5eii jaM43kMd16yj13S7	BVKJSDYFIWUR23OUOQFH SKDLSEORIQPOWASJCDKFLKI KDFIY98T4OIP4O549TIDH
Potato-healthy	3.17 MB	3.05 MB	QmenHxheRqXnXE57D mL6Ncgvr3pTJ9Ed g9KFXW58ei5R6z	XJSTF346TIUWFH7W6457VI SU6WILQURW87RIFI8479WR IUFLSJKAS511OQALSJWP
Potato-Lateblight	17.5 MB	16.5 MB	QmbY6uwyER8WYXbz C8ES9xS6iXumS yK2oy757EgUp2gcxR	U6785GHFVDBXDSEWR5687I JKGNBMCVXDSWQUTIOUPIK BMNVVDGTR6E4R7T8987JJ
Tomato-healthy	37.0 MB	35.29 MB	QmTozqarvDLCzaqX rt2895H9jBVPsiFx 12JedBc9Jy4NFA	VDFER4557YHGDDSXZMNK JOU865GGJJLDVXVGSAWUWO IWNVHZFQ5E7TIUGVJHIFJH
Tomato-Bacterial spot	30.5 MB	27.5 MB	Qmbzvc2Pk4qN9vR 13vvvuFhWiDNhWjh TtMEB12PUcDZwGP	MBSJAOEUGD7847KI387HOW SKDHGVXMSLEDUR6E6R9TUWSBXKBO FIF8EE6RWFSBVK

Conclusion





- Novel idea for Agricultural Quality Data, Trust, privacy & security.
- Proposes a state-of-the-art architecture.
- Application is built with distributed architecture for storage and transmissions evading central and cloud limitations.
- The paper resolves various issues raised that include data security, privacy, integrity, and overcoming bottlenecks and latencies of conventional platforms, traditional database, cloud, central, and blockchain storage systems.
- The Tangle uses tools such as MAM and STREAMS for communication and to secure the data received from the distributed storage system.

Future Work

- Automation to the system.
- Can be enhanced and connected to the real time systems to see the actual performance in the true world.
- Application in different domains especially in Healthcare to provide security and privacy to the sensitive data using IPFS and IOTA Tangle.


THANK
YOU