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

Sukrutha L. T. Vangipuram[1 [0000−0002−1964−5381]],
Saraju P. Mohanty[1 [0000−0003−2959−6541]], and Elias Kougianos[2 [0000−0002−1616−7628]]

[1] Department of Computer Science and Engineering, University of North Texas, USA.
lt0264@unt.edu, saraju.mohanty@unt.edu
[2] Department of Electrical Engineering, University of North Texas, USA.
elias.kougianos@unt.edu

Abstract. The agricultural domain has had a significant role throughout history in human societies across the globe. With the fast growth of communication and information systems, the structure of farming procedures has evolved to new modern standards. Although multiple features helped gain from these advancements, there are many current and rising threats to security in the agricultural domain. The present paper gives novel methods and architectural designs and implements distributed ledger through the Tangle platform. Initially, the article discusses the threats and vulnerabilities faced in the farming sector and presents an extensive literature survey, and later conducts an experiment for distributing data through a tangle distributed ledger system. The authors highlight the limitations of central, cloud, and blockchain and suggest mitigation measures through distributed IOTA systems and distributed storage facilities for data and the possible influence these solutions can bring in the aspects of data security in the agricultural sector.

Keywords: Smart Agriculture · Precision Agriculture · Precision Farming · Agriculture Cyber-Physical Systems (A-CPS) · Internet-of-Agro-Things (IoAT) · Cybersecurity · Blockchain · Distributed Ledger Technology (DLT) · IOTA Tangle · Distributed Storage · InterPlanetary File System (IPFS)

1 Introduction

Smart agriculture is designed as Agriculture Cyber-Physical Systems (A-CPS) using Internet-of-Agro-Things (IoAT). IoAT collect data from multiple sensors installed on farming fields for data analysis and decision-making. The sensors and communication devices record the statistics and understand the machine-to-machine and machine-to-human interactions. With the Internet of Things, the model of agriculture has shifted to precision agriculture on farming fields, including in areas of planting, feeding, lessening water and fertilizer use, and supporting intelligent systems with reduced energy consumption [1]. The Fig. 1 illustrates how modern equipment and IoAT are helping to collect critical data from the fields for agricultural research and science institutes and farmers. These IoAT things require additional features such as real-time data streaming and end-to-end data security. From the agricultural point of view in data security, there are two main concerns, including the collection and storage of farming data. As there is a variety of data residing in fields, conventional monitoring methods cannot be applied, and also the data can be exposed to human errors. With the increase in information

and communications systems, the number of cyber crimes have also increased worldwide, stealing and harming a variety of assets. Existing cloud systems have multiple limitations of central storage, continuous connectivity, security risks through different providers, bandwidth constraints, and faint backup procedures. The cyber security procedures combine different techniques to give high protection against attacks on data [2]. Blockchain (BC) is a Distributed Ledger Technology (DLT), a new way to share data securely through cryptographic hashes in a distributed platform that is being applied in various domains nowadays. The agricultural field is also taking advantage of the decentralized features of blockchain, but these systems are going through complex steps to generate blocks and consume energy with on-chain storage [3]. To face issues in blockchain, the applications are designed with off-chain storage solutions and exercise other methods to avoid cost, latency, and energy consumption.

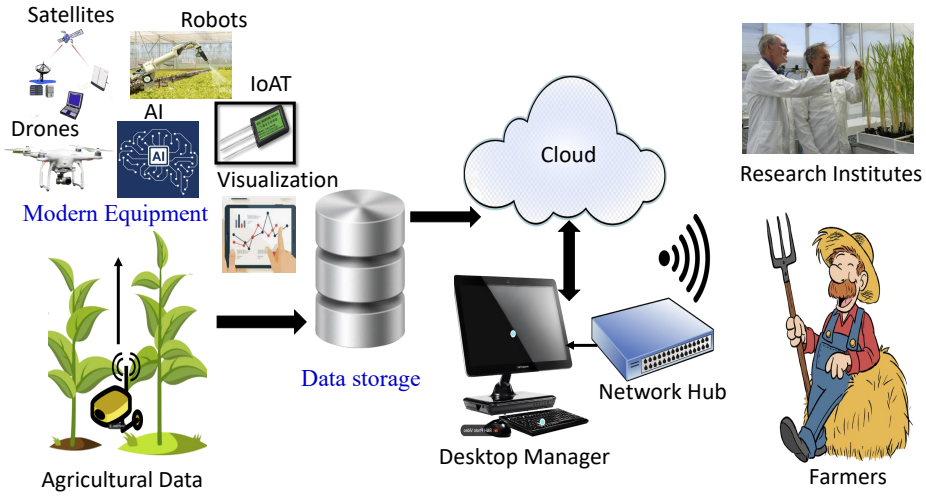


Fig. 1. Data collected from modern equipment's in agriculture.

Tangle is another Distributed Ledger Technology (DLT) that does not require fees and validates the transaction nodes at full speed. The transactions are said to be valid if the previous two transaction's history does not conflict with the current transaction. The consensus mechanism, proof of Work (PoW), is not used for validating the transaction but for keeping the network secure from spam. The overall throughput of the tangle is infinite, and the consensus mechanism is used for defining the limits of the throughput. A distributed storage (IPFS) system is a platform for storing data, websites, applications, and accessing files [4] and does everything a central system does but without a central storage system. Some of the motivations for implementing current paper CroPAiD are listed in the Fig. 2. Combining both tangle and IPFS can bring more security and privacy to sensitive agricultural data. The information stored on the IPFS network generates a cryptographic hash through a content identifier to retrieve the data later securely.

The paper follows the given order: We discuss various prior works using conventional and modern methods for transmitting and storing sensitive agricultural data in Section 2. The

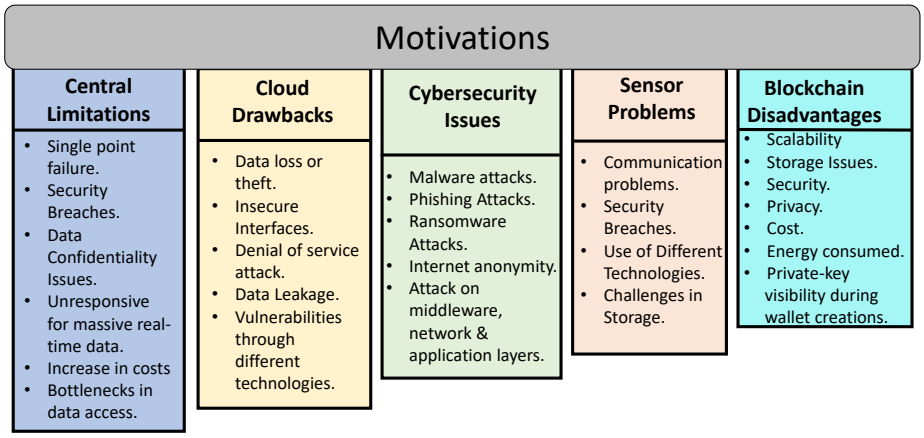


Fig. 2. Motivations for the CroPAiD.

Section 3 elaborates on problems raising through modern and traditional methods and list the novel solutions provided through current system. In Section 4 and Section 5, we define various components, provide a state of the architecture for CroPAiD and give algorithm steps for navigating the data over IPFS and Tangle, respectively. The implementation of the system and the results obtained are shown in Section 6 followed by the conclusions and further research aspects in Section 7.

2 Related Works

For agricultural data storage, usually, the data is collected in conventional local databases or cloud systems. In the current agricultural 4.0 era, many researchers and scholars are conducting profound studies on how modern data storage methods can be introduced. Launching ledger technology into IoT for data security can be done in two scenarios; the first is making use of off-chain data storage with the help of distributed storage-IPFS or traditional local databases. The second is the direct storage of data on distributed ledger systems.

The paper [5] G-DaM sends the data collected from the Internet of Things to the near edges for storing the data in distributed platforms and public blockchain technology. The application overcomes the traditional data sharing and limitations of central and cloud systems and increases the quality and integrity of the data. The agroString [6] proposed an intelligent IoT-based edge system for the management of data through a private corDapp application. The system sends the information collected from the IoT edge sensors through the private blockchain to avoid traditional public blockchain systems' costs and energy consumption and evade bottlenecks of central and cloud systems. The application implements an IoAT-edge for collecting temperature and humidity datasets and sends those readings to the corDapp to bring integrity, trust, visibility, and data quality to each supply chain stakeholder.

The paper [7] uses blockchain for fruit and vegetable traceability to overcome traditional centralized systems. With the help of a dual storage structure- "database + blockchain" the system designs the application using an on-chain and off-chain storage technique to reduce the load pressures and increase the data integrity throughout the supply chain. The results

of the system exhibit improved security of secluded information and further enhance the authenticity and reliability of data. Information modifications and tampering with the sensitive data collected in a supply chain may lead to serious issues regarding the quality and safety of the end product. The article [8] makes use of blockchain for time stamping, traceability, and tamper-proofing of data with the help of smart contracts. The solidity language contract manages the agricultural product transactions with access control and improves the upload and response times.

Crop monitoring is essential to keep a check for pests, weeds, and diseases in the crops. Monitoring is done using different sensors to see the current state of the product to project and predict what will be the next state and issues arising in the crops. The farmer takes preventive measures accordingly based on the information collected in the crop monitoring. Field monitoring plays a vital role in increasing crop yield, and modern IoT technology and communication systems are beneficial in fulfilling this requirement. An efficient crop monitoring system is proposed in sFarm [9] through a sensor to collect the data and share the real-time data securely using IOTA Tangle distributed ledger platform. With the help of IOTA, the central, cloud, public, and private blockchain limitations are overcome, saving energy and time for uploading and validation. Many distributed access control technologies through blockchain are already in practice for dealing with centralized and cloud network limitations, but they, too, inherit some drawbacks, such as high fee transactions and low throughput. The paper [10] proposes a novel access control framework based on IOTA that enables free transactions with higher throughput.

Using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) technology, access rights are encrypted to provide access control and store the data on the distributed ledger Tangle. IOTA Tangle has some disadvantages and security threats, such as a parasite chain attack that is a common double-spending attack. To decrease these types of attacks, the paper [11] gives an efficient method for detecting a parasite chain. The authors measure a score function at each IOTA transaction to see the importance level. Any change in this importance is reflected in the 1st and 2nd order of the derivates, thus giving accurate results in detecting the parasite chain attack. All the above-discussed prior works try to improve the security in transmitting and storing agricultural data, but the current system adds additional features of distributed storage of IPFS to the IOTA distributed ledger platform to overcome conventional and modern limitations as given in the Table 1.

Table 1. Comparing Prior works with Current application CroPAiD.

Application	**Storage and Sharing**	**Cost**	**Platform**	**Energy Consumption**
G-DaM [5]	IPFS+Public BC	Low	Distributed+Decentralized	High
agroString [6]	Private BC-corDapp	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 + IOTA Tangle	Zero	Distributed Storage + ledger	Low

3 Novel Contributions of the Current Paper

3.1 Modern communication technologies in Agriculture

With the increase in demand for food in the global market, the need for reduced costs and increased agricultural production has given way to using new technologies, which is an attractive choice for farmers and companies [12]. Some of the advantages of IoT applications in the agricultural sector include crop health monitoring, pest infestation, water management, frost protection, and decision support. This new method of using novel communication technologies in agriculture is denoted as precision agriculture or precision farming (PF) [13]. The use of satellites and GPS in farming helps in digitizing agricultural measurements to see the accuracy and efficiency of the crop. Based on the measurements collected from these precision agriculture tools, the farmers and the experts in the field, study and analyze the variations of crops and livestock data. To collect different types of information from the fields, the farmer would use IoT nodes that come with specific features that make them useful in limited domains [14].

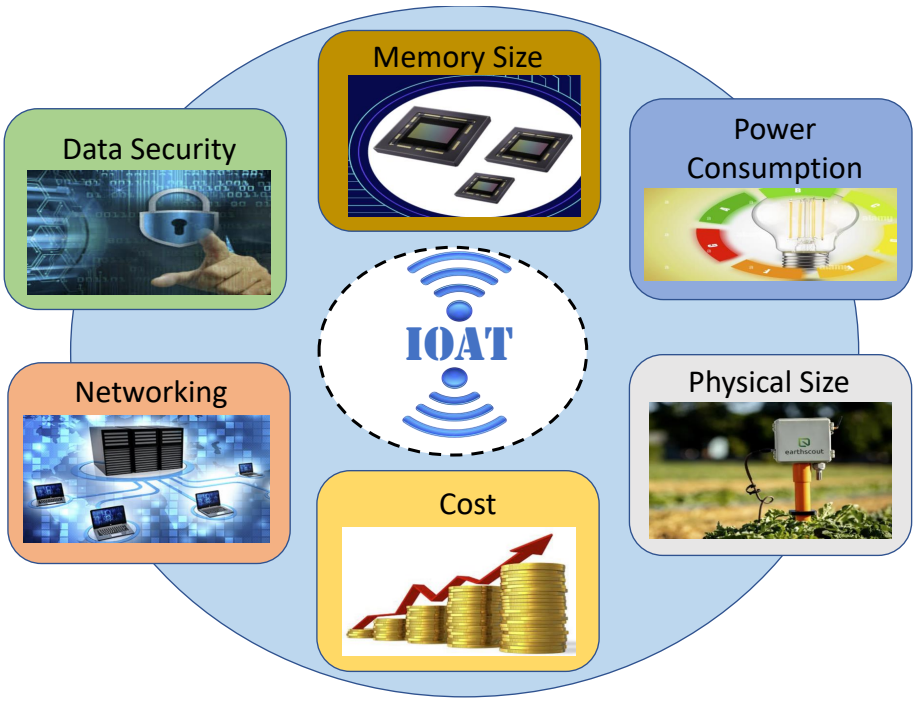


Fig. 3. Challenges in IoAT.

3.2 Data Threats through contemporary systems in farming

With the emergence of new communication systems and the addition of the Internet of Things (IoT) in farming, unknown security risks and data threats arise in the cyber-physical

environment. These data risks are mainly related to cyber security, data integrity, and data loss disturbing the stakeholder businesses [15]. The constraints of the IoAT are given in Fig. 3. Precision Farming uses vast modern machinery in the fields, leading to higher consequences and threats. Farming is possible in open grounds where weather and environmental conditions are inconsistent, leading to malfunctioning of the machinery and technical equipment in the fields, resulting in wrong measurements and hence wrong analysis [16]. Additionally, the temperature and humidity conditions can affect sensor things for communication, which can lead to data loss [17]. The cybersecurity issue is a worldwide severe threat activity that uses a smart device to access sensitive personal and government information. Although strict restrictions have been implanted through law enforcement, the hackers take advantage of internet anonymity and attack middleware, network, and application layers [2].

3.3 Novel Solutions Proposed

The novel contributions of the current paper CroPAiD include:

- A unique system is designed 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.
- 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 is presented for the current system CroPAiD.
- Designing a Cost-efficient infrastructure and presenting results with zero transaction fees and secured hashes.

4 Overview of the proposed Framework - The CroPAiD

4.1 Agriculture Cyber-Physical Systems (A-CPS)

The cyber-physical systems (CPS) combines the software and hardware components to execute a well-defined task. A system that connects and manages the physical attributes towards its computing capabilities and a design that connects and controls the physical organizations with virtual structures through networks. The combination of wireless sensor networks that supervise the physical entities can enhance itself in real-time scenarios. The CPS are applied in multiple domains to help in substituting conventional methods and integrating various platforms and technologies together [18]. Smart Agriculture is one of the domains that can benefit from CPS due to its modern and smarter applicability in monitoring and controlling farming activities and gathering the information associated with crops, soil, livestock hygiene, and weather in real-time, along with maintaining the environment and preserving energy. Fig. 4 gives different layers of cps and their connectivity in physical systems through smart devices to control and manage the data in an intelligent way.

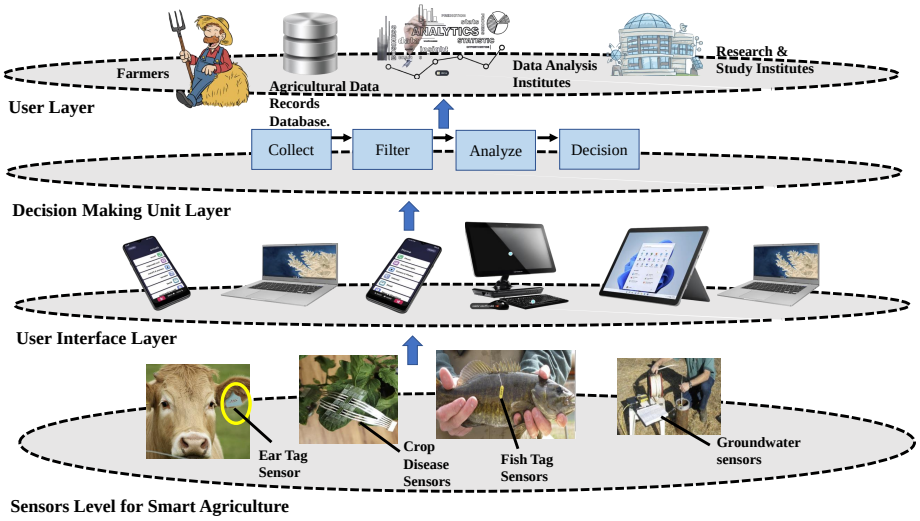


Fig. 4. Agriculture Cyber-Physical Systems (A-CPS).

4.2 Distributed Storage - IPFS

One of the limitations of Tangle is that the attackers can implant several duplicates of the data that can lead to double-spending transactions [19]. A user can create and spend the same digital asset multiple times, which must be checked and prevented. A distributed storage-IPFS or Interplanetary File System is an internet protocol mainly to store data, avoid data or asset duplicates across the network, and collect the addresses of the data in the network. By stopping asset duplication, the IPFS can help in avoiding double spending issues. By using IPFS as off-chain storage for IOTA tangle, the information is stored in a distributed platform, reducing local database, central, and cloud constraints. The data is recognized through content, and every piece of information is divided into 256 kb maximum length blocks. Every block is labeled with a unique identifier for the content through the cryptographic hash. The distributed hash table of IPFS is based on the principle of distributed key-value store. Both node identifiers and distance metrics strategies in IPFS help in storing and retrieving the data quickly. When reading or writing the data from or to the edges, the end devices search for the nodes close to the key attribute values using buckets inside the networks to identify the nodes [4, 20]. The S/Kademlia algorithm is used for DHT in IPFS to register the nodes whenever a file gets uploaded and links to nodes through an identifier for file retrieval.

4.3 Data Security through IOTA Tangle

The IOTA Tangle has built two-layer solutions called L2 for dealing with the data. The first one is built for MAM, and the second is with STREAMS. The Tangle with MAM has two protocols to traverse and authenticate the data in the distributed ledger network. These protocols mainly work on the principle of cryptography. With the help of Masked Authenticated Messaging (MAM) in the IOTA Tangle network, it allows any device to publish data in the transactions but only read the data of authorized devices. The IOTA introduces

the concept of zero-value transactions, here, the first protocol is responsible for transactions, but the data transactions are authenticated. MAM is a second protocol that helps in protecting the data and verifies its authenticity. With MAM, data channels can avoid malicious attempts or fake data because only the owner has the right to publish data into the channel. As data is published into its respective channel, a channel ID is received that acts as the identifier, which allows other devices to connect to retrieve the data. There are three different channel modes: public, private, and restricted. In the public channel mode, the transaction uses the root of the Markle tree as the address; therefore, whichever device gets access to the channel ID can decrypt the data using the address as the decryption key. In private mode, the Markle tree's root is hashed; hence, only those devices with the original root can decrypt the data. Lastly, restricted channels will include both pre-shared keys and the root of the Markle tree. Only devices with information regarding both pre-shared keys and Markle tree roots can decrypt the data. The application for IOTA tangle can be developed using quantum-proof cryptography, and javascript language [21]. The second is the STREAMS [22] tool that helps in structuring and navigating the data securely through Tangle. It is basically a framework to develop applications through secure cryptographic messaging and allows any device to order messages with integrity and immutability. A publisher device takes control of the messages to be sent by everyone else and makes the messages private by using public key encryption. Any device, called a subscriber, can consume and pull and publish the information from the Tangle as opposed to MAM where only a channel owner can publish the data [23].

4.4 Novel Architecture for CroPAiD

An IoT device used to collect data from agricultural fields is referred to as the Internet-of-Agro-Things (IoAT). The IoAT is equipped with all the capabilities of networking (WiFi, LoRa, Bluetooth) to communicate the data through IOTA Tangle. There are several endpoints between the target device and the IOTA gateway. Fig. 5 shows the state-of-the-art architecture design for the current system CroPAiD.The edge layer is responsible for fetching the data from the internet things and sharing the agricultural data among servers. The edges interface with higher networking, space, and energy supplies and provide management and monitoring services with multiple sensor nodes and other gateways. The servers store, process, and visualize data moving from edges. The architecture presents an edge layer as a communication medium between sensors and servers. A distributed storage technology-IPFS is embedded into the edge along IOTA Tangle that serves as a gateway between IoT devices and servers. With distributed storage on edge, the limitations of IOTA, such as double spending and other attacks, are evaded. Each agricultural sensor data file is transmitted to IPFS to generate a hash, as explained in subsection 4.2, through its unique content identifier. A Merkle-directed acyclic graph (Merkle-DAG) calculates a root that can retrieve the original file from the segments. The distributed storage hash of the crop's sensor data is then moved toward the Tangle residing in the edge. The IOTA node receives the hash from the IPFS and further secures it by generating Tangle hashes using MAM and STREAMS tools, as discussed in subsection 4.3 above. The distributed ledger technology is feasible for point-point, point-multipoint, and multipoint-multipoint communications between various sensor devices on the field and multiple servers.

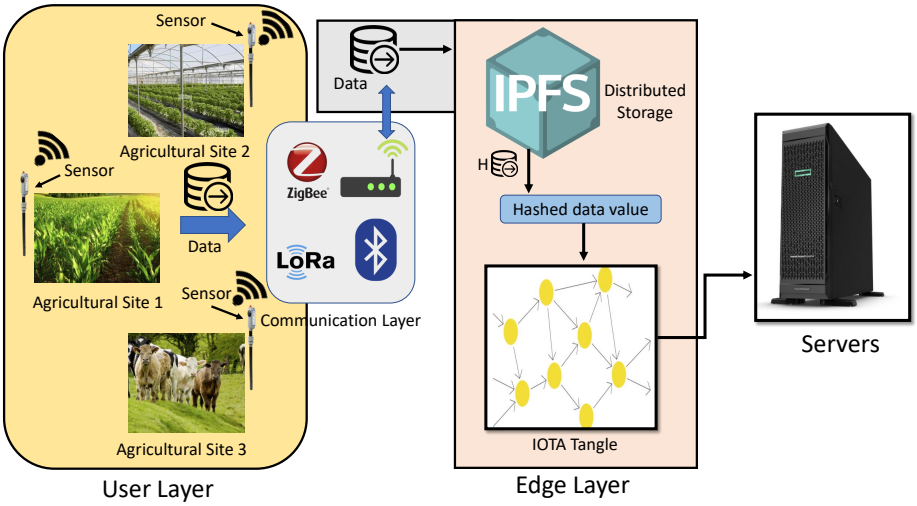


Fig. 5. CroPAiD Novel Architecture with IPFS and IOTA Tangle.

5 Proposed Algorithms for CroPAiD System

The data from the Internet of Things moves toward the edge layer that has both Distributed Storage-IPFS (DS) and IOTA Tangle systems implemented. algorithm 1 presents phases in transferring crop data(C_d) to IPFS and generating 256 kb buffer files to give a root hash at the end. In the edge distributed storage system (DS_E), both private (DS_{pr}) and public keys (DS_{pu}) are generated to incorporate access control through digital signatures and signing crop data files. The IPFS converts the crop data (C_d) into a 256kb buffer file (C_d) and signs the buffer file ($C_{dbf265\ KB}$)to get a root hash file of the crop data ($H(C_dC_{bf})$) where H denotes the hash of the crop data file.

Algorithm 1 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.

Each input data present in the Tangle creates the following fields: data-length, data, public key, private key, index, index-next, sign, and auth-sign. The IOTA tangle generates a seed (S_d) from a random source and produces a key pair for input data using the edwards25519 curve algorithm. Each input data calculates the index and the index-next via private and public keys. The hash of the public key is the index, and the hash of the public key for the following input data is the index-next. A different key pair is generated for the next input data from another random source, and for hashing, the algorithm used in IOTA is BLAKE2b [24]. Computing index and index-next are significant because they help in continuous data streaming, data ownership, verification, and authentication. A digest 'd' is given by hashing the data, data-length, public key, and index-next. The sign field is then calculated by signing the digest with the private key. This will be helpful in verification later for the user. If the user has to verify the data, compare the hash and sign field values with the public key in the input data. If both are equal, then the data is verified correctly. The sign field helps in only verification of the data but does not give authenticity or the author's identity. The field auth-sign is calculated by the key pair associated with the sensor device. This authorization signature is calculated by the private key of the IoT device and stored in a hardware source along with the public key certificate. To validate and see the authentication of the data, the user compares the signature with the public key through a trusted third-party certificate authority. The algorithm 2 and the Fig. 6 show the flow of Crop data in the Edge layer between IPFS and IOTA Tangle in detail and explains how the data is moved, verified, and authenticated in Tangle.

'$H(C_{dbf265\ KB})$' is taken as the input data to the Tangle ledger System. We represent that input data '$H(C_{dbf265\ KB})$' in the following algorithm as 'In_{iota},' data-length as '$In_{iota}len$,' the public key as '$In_{tangle}Pukey$,' private key as'$In_{tangle}Prkey$,' index as 'I' and next-index as 'n-I,' sign field as 'sign' and auth-sign as '$auth_{sign}$.' For Hashing and digest, we represent with letters 'H' and 'd'.

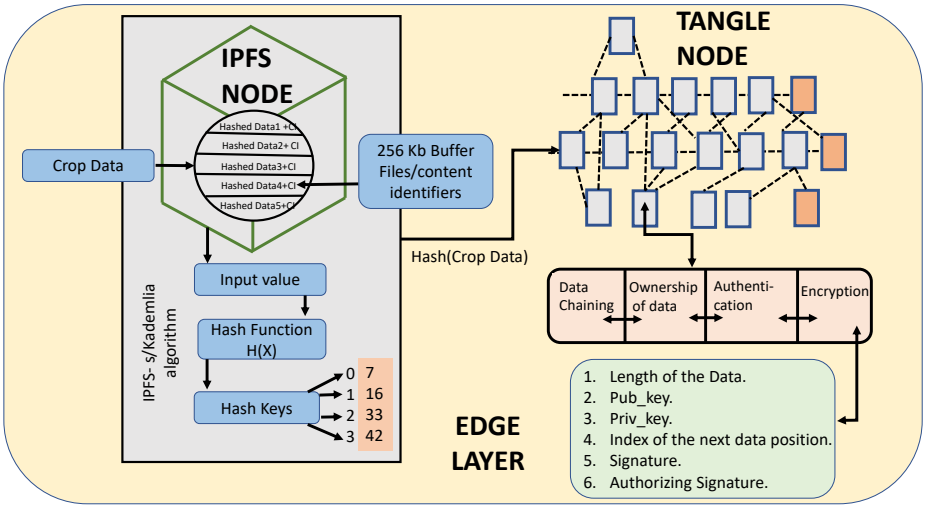


Fig. 6. CroPAiD detailed Data flow in the Edge layer between IPFS and IOTA Tangle.

Algorithm 2 Crop Data File in IOTA Tangle.

We represent $H(C_d)_{ipfs}$ coming from ipfs as input data to IOTA as Tangle(In_{iota}).
$In_{iota} \longrightarrow In_{iota}$, In_{iota}len, In_{tangle}Prkey, In_{tangle}Pukey, ind,
nex-ind,sign $auth_{sign}$.
Random Source $\longrightarrow S_d$.
$S_d \longrightarrow In_{tangle}$Prkey, In_{tangle}Pukey.
H(In_{tangle}Pukey)$\longrightarrow$ I.
A different key pair is generated for the next input data (Next-In_{iota}) from another random source.
The key pair from the next input data is (Next-In_{tangle}Prkey) and (Next-In_{tangle}Pukey).
H(Next-In_{tangle}Pukey) $\longrightarrow$ n-I.
A digest d is calculated for signature.
d= H((In_{iota}) + (In_{iota}len) + (In_{tangle}Pukey) + (n-I).
sign= signature(d + In_{tangle}Prkey)
if H(In_{iota})==sign+In_{tangle}Pukey **then**
    Verification Success.
else
    Process End.
    For authorization, we need the public(IoT_{Pukey}) and private keys (IoT_{Prkey})of the IoT device.
    $auth_{sign}$ = signature(IoT_{Prkey})
    if $auth_{sign}$== signature(IoT_{Pukey}) **then**
        Authentication Success.
    else
        Process End.
    end if
end if
Repeat the steps from 1 through 25 whenever a file is moved from IPFS in the edge layer.

6 Implementation and Validation

To implement the current system, we have taken the source code from Github and modified the code to our needs for the CroPAiD application. The application is designed using javascript; hence we use Node.js as an environment for executing our JS programs. In this application, it is mainly used to create, open, read, write, delete, and close files that reside on the server. Node.js is installed in both the application program interface and client programs to test and deploy the application. We modified and configured the local .json file of the application program interface (api) with the network settings of the node provider, IPFS node, and the database using dynamoDbConnection services provided through Amazon web services. Once the api is configured, the API server starts in the development mode as shown in Fig. 7. For the client mode to execute, we installed the node.js inside the client directory and configured the local.json file with the required fields of API endpoint URL, ipfs gateway URL, and the URL for tangle explorer. After client configuration, the client connects to the API server to open the front-end web browser.

The front end of the application is designed using React javascript. The user interface of the CroPAiD application is given in Fig. 8(a) and the Figure.8(b) shows the front-end design for uploading the crop data files.A hash is generated once the file gets uploaded to IPFS as shown in

Fig. 7. Connecting to api and Client Programs.

the Fig. 9(a) and files can be retrieved from IPFS and IOTA Tangle hashes as shown in Fig. 9(b). Thus, we implement and validate the application and record the DDS and IOTA hash results.

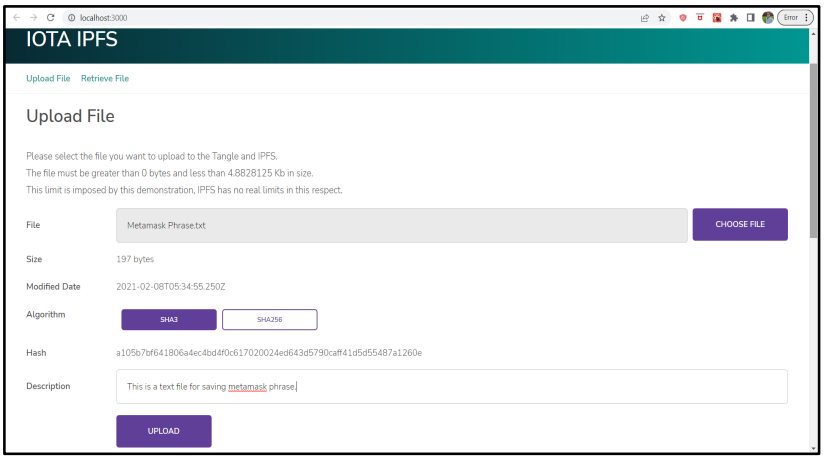
6.1 Datasets

The agricultural datasets we used are from the Kaggle [25] source. Each data belonged to different vegetables and fruits containing images of healthy and diseased crops. These data collected are sensitive and usable for further research and analysis in bringing improvements in farming and are also beneficial in the field of agricultural science. We uploaded the crop data in the current application to test and validate. Table 2 demonstrates different crop statistics we used for the present paper.

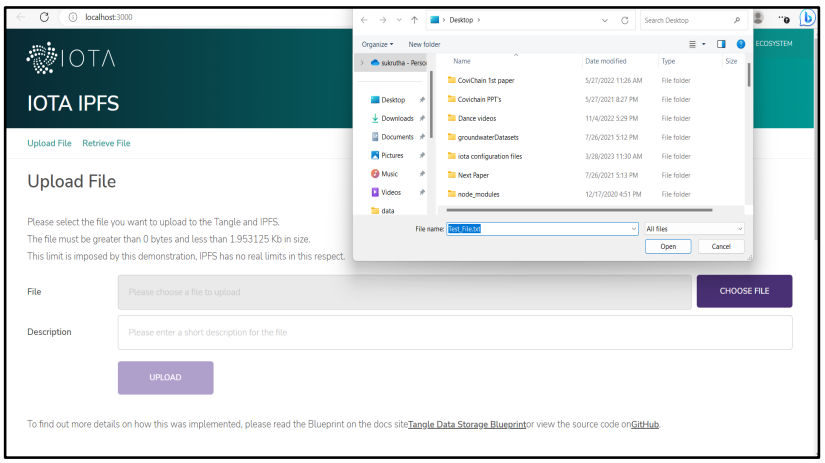
The Fig.10 shows some sample dataset images we used for storing and sharing in the CroPAiD application through IPFS and IOTA. When a crop gets infected, it damages and changes all the primary functions of the food that can harm humans when consumed. This type of crop infected data is beneficial in predicting future crop damage and helps improve crop yield. Therefore, 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. The Fig. 10(a), 10(b), 10(c), 10(d), 10(e), 10(f) show pictures of a healthy crop and a diseased crop of apple, potato, cherry, corn, grape and tomato correspondingly.

6.2 Experimental Results

To obtain the results for the current application, we have used Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz, 32.0 GB RAM as the edge layer. We have deployed the application logic of IPFS and IOTA tangle in this edge system. We upload the crop data file to the IPFS node to get the hash of the file, as shown in the Table 3. The IPFS hash file generated does not have the time stamp but avoids duplicates and double-spending attacks on the data transferred. The application further takes the IPFS hash as an input to the IOTA node to give another hash from the tangle platform. The Table 3 shows the double hashes produced by both IPFS and Tangle. The application has been tested with different sizes of crop data to produce two hashes with both technologies. Once both the hashes were received from the application, we used the message unique ID to retrieve the original file. The time to upload the files was very minimal, and the data transactions costs were zero compared to blockchain latencies and transaction fees. The paper we implement combines distributed storage IPFS and IOTA Tangle successfully, resulting in higher data security with reduced energy consumption nullifying the limitations of central, cloud, conventional database, and blockchain systems.



(a) User Interface.

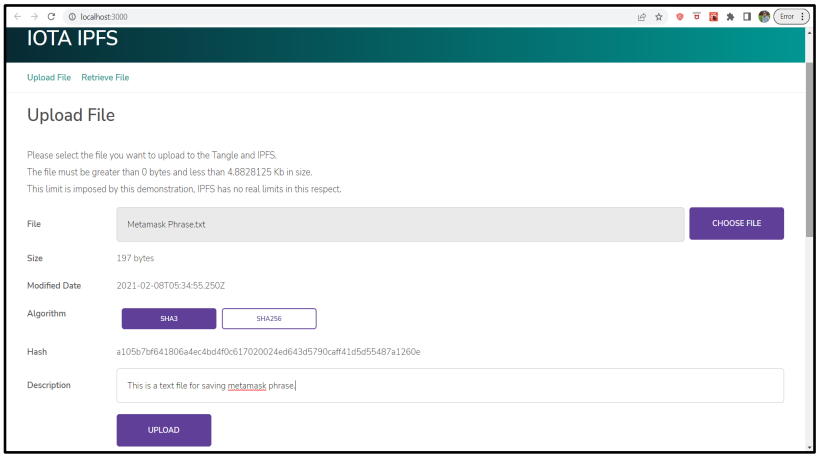


(b) File Uploading

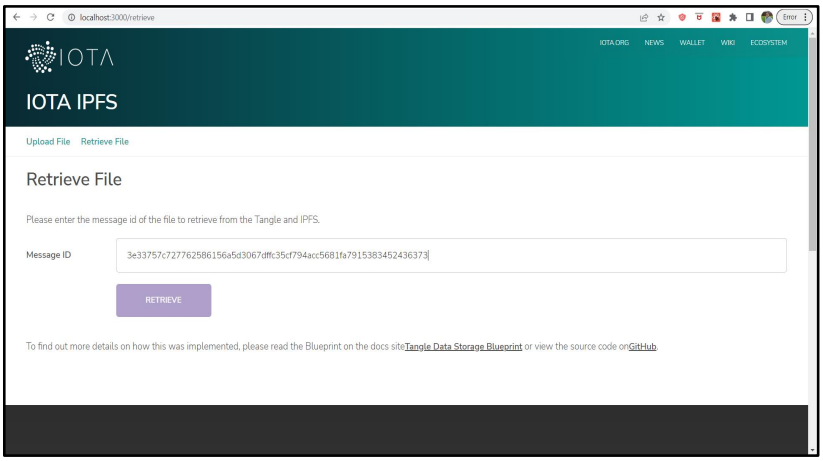
Fig. 8. CroPAiD Application User Interface.

7 Conclusions and Future Research

The paper suggests a state-of-the-art model that combines distributes storage-IPFS and the IOTA Tangle for managing the quality and integrity of the agricultural crop sensor data. The paper resolves various issues raised by traditional database, cloud, central, and blockchain storage systems, that include data security, privacy, integrity, and overcoming bottlenecks and latencies of conventional platforms. The Tangle uses tools such as MAM and STREAMS for communication and to secure the data received from the distributed storage system. In this paper, we also propose a novel architecture using an edge between the sensor things and the servers. The system can further be improvised with automation for taking in real-time data towards the edge IOTA Tangle systems.



(a) Hash of the File.



(b) File Reteiving

Fig. 9. Implementation of CroPAiD Application.

References

1. Farooq, M.S., Riaz, S., Abid, A., Abid, K., Naeem, M.A.: A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. IEEE Access **7**, 156237–156271 (2019). https://doi.org/10.1109/ACCESS.2019.2949703
2. Ivanov, I.: Cyber Security and Cyber Threats: Eagle VS "New Wars"? Academia.edu (2018). URL `https://www.academia.edu/38462737/CYBER_SECURITY_AND_CYBER_THREATS_EAGLE_VS_NEW_WARS_`
3. Henry, R., Herzberg, A., Kate, A.: Blockchain Access Privacy: Challenges and Directions. IEEE Security & Privacy **16**(4), 38–45 (2018). https://doi.org/10.1109/MSP.2018.3111245
4. Musharraf, M.: What is InterPlanetary File System (IPFS)? (2021). URL `https://www.ledger.com/academy/what-is-ipfs`

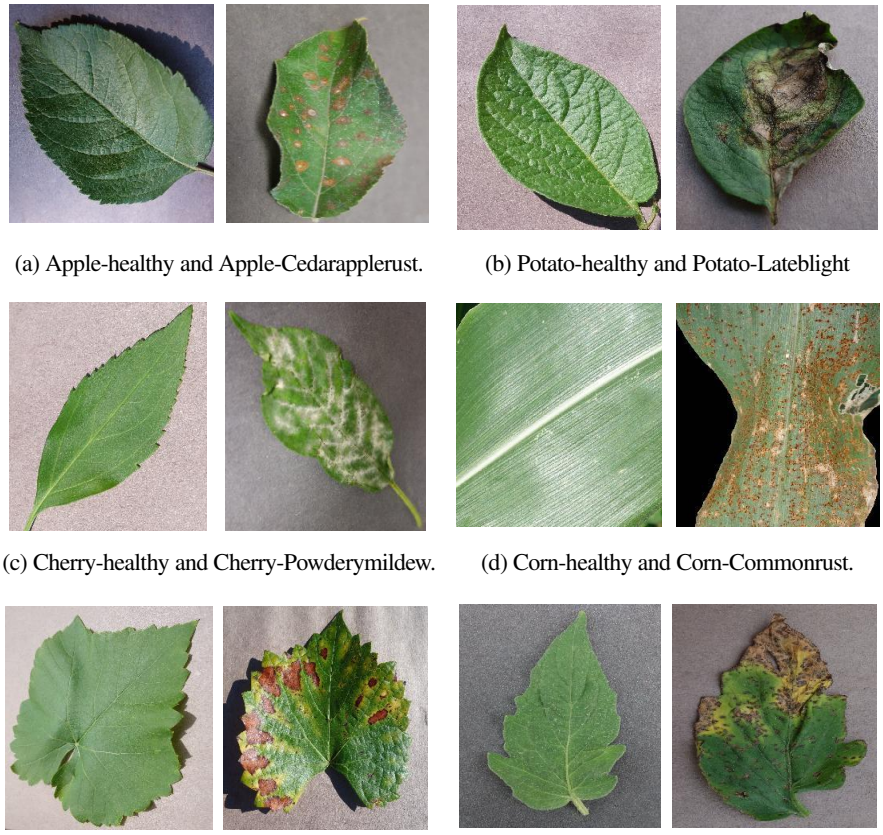
Table 2. Datasets for CroPAiD

Data Name	Dataset Size	Compressed Data Size	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	11.41 MB	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(Black-Measles)	28.6 MB	27.30 MB	https://www.kaggle.com/datasets /divumarcus/plant-health
Peach-healthy	6.16 MB	5.74 MB	https://www.kaggle.com/datasets /divumarcus/plant-health
Peach-Bacterialspot	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-Bacterialspot	30.5 MB	27.5 MB	https://www.kaggle.com/datasets /divumarcus/plant-health

5. Vangipuram, S.L.T., Mohanty, S.P., Kougianos, E., Ray, C.: G-DaM: A Distributed Data Storage with Blockchain Framework for Management of Groundwater Quality Data. Sensors **22** (2022). https://doi.org/10.3390/s22228725
6. Vangipuram, S.L.T., Mohanty, S.P., Kougianos, E., Ray, C.: agroString: Visibility and Provenance through a Private Blockchain Platform for Agricultural Dispense towards Consumers. Sensors **22**(21) (2022). https://doi.org/10.3390/s22218227. URL https://www.mdpi.com/1424-8220/22/21/8227
7. Yang, X., Li, M., Yu, H., Wang, M., Xu, D., Sun, C.: A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products. IEEE Access **9**, 36282–36293 (2021). https://doi.org/10.1109/ACCESS.2021.3062845
8. Yi, W., Huang, X., Yin, H., Dai, S.: Blockchain-based approach to achieve credible traceability of agricultural product transactions. Journal of Physics: Conference Series (2021). https://doi.org/10.1088/1742-6596/1864/1/012115. URL https://dx.doi.org/10.1088/1742-6596/1864/1/012115
9. Bapatla, A.K., Mohanty, S.P., Kougianos, E.: sFarm: A Distributed Ledger Based Remote Crop Monitoring System for Smart Farming. In: Internet of Things. Tech-

Table 3. Hashes generated through IPFS and Tangle

File Name	Reduced Size	IPFS Hash	Tangle Hash	Txn Time (Sec)
Apple-healthy	23.8 MB	QmXWpe6Q5v9qH7Wwgr5HH5BmB78Q2u4wPWFd7NkvooFZrP	SKJYF76R3947IRYREIU598475FHKEUR834759IFKR30WPWEKDSVLDKFROIRFHDKJ	35
Apple-Cedarapplerust	2.9 MB	QmYuERUhBu8fuXRab7RkWwDqDZKHcn8DpkUwpopaNMjAB3	GZSDUAYR87R675RWRYGJDHFU9586ERUFJBLDIR4395035RTHGKVJS579048EOIHK	3.45
Cherry-healthy	14.06 MB	QmPRkovGVUgYx2uehy1g5QHwqECXpd1NoCXAsUehznjU5t	JHSGFUY5R635RWGFJSHVET875985WIGDSHVLUSP5T98FHDVJDOYW8R76487RITHK	21
Cherry-Powdery mildew	11.41 MB	QmTy9g2ENwSP66DV2qkUP7XchCd9AQmaznM8saZbvz1xcY	CMVNGGF653RFHHKJLLOUUERWEQSCCBBJH87966453FDJGHKJUYRTEESXZVFMHKJO	7
Corn-healthy	13.39 MB	QmZkM4ymQCXKThLhY6igBMPxcjwaNauGj6Khvnr1rfuHNh	LQREWRR5473FCVVNGH67892DHGNCSK53FHSFFKJOIWRW9345FDGERSBHYUKIOUQW	14
Corn-Commonrust	16.72 MB	QmVCm8uXgyvnQEfvCbDpPxZ95XNuTySir7thRMMLfoNzFi	FR5476HYHKHNCVZSA338687UYKJNGGFTR544333DEHGJUIIPKNMNBBFVDFSEW4YU	12.34
Grape-healthy	6.29 MB	QmX1ohMDQqRqtvDGPYVGZjyfVx3zuVEKTXxKRmj6VJxc75	MNXBFYO5I73RGKLD7879HSJRY764934UTWJHEUFQJO7GDAPOLKLKOIUSDWKN-MND4	5.13
Grape-Esca(Black-Measles)	27.30 MB	QmZw4X69QyptuNWjbA3o6NWAK6x9veeb3CcXZdPWQV6qcY	D564837HTYCBHGDJDUR7595HFYE54658THG84658HRI746595RHFI76HJGDTYRIR	37
Peach-healthy	5.74 MB	QmUCANWk22uX6JCBew8SCRXXDbMfruXyfCj7YJmSJesmYz	MNZCJHARU8473EIDHKSJFLJG9485029QPWADJSLKFWORIAJFKZJFKSDJLLKPLSKJ	4.61
Peach-Bacterial spot	29.89 MB	QmdWXdTy8LaTHaLwFAPe49FCBd5eiijaM43kMd16yj13S7	BVKJSDYFIWUR23OUOQFHSKDLSEORIQPOWASJCDK-FLKI KDFIY98T4OIP4O549TIDH	43.2
Potato-healthy	3.05 MB	QmenHxheRqXnXE57DmL6Ncgvr3pTJ9Edg9KFXW58ei5R6z	XJSTF346TIUWFH7W6457VISU6WILQURW87RIFI8479WRIUFLSJKAS511OQALSJWP	3.52
Potato-Lateblight	16.5 MB	QmbY6uwyER8WYXbzC8ES9xS6iXumSyK2oy757EgUp2gcxR	U6785GHFVDBXDSEWR5687IJKGNBMCVXDSWQUTIOUPIKBMNVVDGTR6E4R7T8987JJ	23.4
Tomato-healthy	35.29 MB	QmTozqarvDLCzaqXrt2895H9jBVPsiFx12JedBc9Jy4NFA	VDFER4557YHGDDSXZMNKJOU865GGJJLDVXVGSAWUWOIWNVHZFQ5E7TIUGVJHIFJH	61.3
Tomato-Bacterial spot	27.5 MB	Qmbzvc2Pk4qN9vR13vvvuFhWiDNhWjhTtMEB12PUcDZwGP	MBSJAOEUGD7847KI387HOWSKDHGVXMSLE-DUR6E6R9TUWSBXKBOFIF8EE6RWFSBVK	38.6



(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.

Fig. 10. Sample Images of Crop Condition Dataset.

nology and Applications. Springer International Publishing (2022). URL https://doi.org/10.1007/978-3-030-96466-5_2

10. Nakanishi, R., Zhang, Y., Sasabe, M., Kasahara, S.: IOTA-Based Access Control Framework for the Internet of Things. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 87–95 (2020). https://doi.org/10.1109/BRAINS49436.2020.9223293
11. Ghaffaripour, S., Miri, A.: Parasite Chain Attack Detection in the IOTA Network. In: 2022 International Wireless Communications and Mobile Computing (IWCMC) (2022). https://doi.org/10.1109/IWCMC55113.2022.9824318
12. Calicioglu, O., Flammini, A., Bracco, S., Bellù, L., Sims, R.: The Future Challenges of Food and Agriculture: An Integrated Analysis of Trends and Solutions. Sustainability **11** (2019). https://doi.org/10.3390/su11010222
13. Wolf, S.A., Wood, S.D.: Precision Farming: Environmental Legitimation, Commodification of Information, and Industrial Coordination. Rural Sociology (1997). https://doi.org/10.1111/j.1549-0831.1997.tb00650.x

14. Demestichas, K., Peppes, N., Alexakis, T.: Survey on Security Threats in Agricultural IoT and Smart Farming. Sensors **20** (2020). https://doi.org/10.3390/s20226458
15. West, J.: A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies. Journal of Agricultural & Food Information **19**(4), 307–330 (2018). https://doi.org/10.1080/10496505.2017.1417859
16. Devendra, C.: Climate Change Threats and Effects: Challenges for Agriculture and Food Security. ASM Series on Climate Change (2012). URL https://pdf.usaid.gov/pdf_docs/PBAAK550.pdf
17. Elijah, O., Rahim, S.K.A., Sittakul, V., Al-Samman, A.M., Cheffena, M., Din, J.B., Tharek, A.R.: Effect of Weather Condition on LoRa IoT Communication Technology in a Tropical Region: Malaysia. IEEE Access **9**, 72835–72843 (2021). https://doi.org/10.1109/ACCESS.2021.3080317
18. An, W., Wu, D., Ci, S., Luo, H., Adamchuk, V., Xu, Z.: Chapter 25 - Agriculture Cyber-Physical Systems. In: Cyber-Physical Systems, Intelligent Data-Centric Systems, pp. 399–417. Academic Press (2017). https://doi.org/https://doi.org/10.1016/B978-0-12-803801-7.00025-0
19. Popov, S.: The Tangle. Tangle White Paper (2018). URL https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf
20. Lundkvist, D.C., Lilic, J.: An Introduction to IPFS (2016). URL https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0
21. Foundation, I.: mam.js (2021). URL https://github.com/iotaledger/mam.js
22. Foundation, I.: IOTA Streams (2021). URL https://www.iota.org/solutions/streams
23. Palmieri, A., Vilei, A., Castanier, F., Vesco, A., Carelli, A.: Enabling Secure Data Exchange through the IOTA Tangle for IoT Constrained Devices. Sensors, MDPI. (2022). https://doi.org/10.3390/s22041384
24. Saarinen, M.J., Aumasson, J.P.: The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC) (2015). URL https://www.rfc-editor.org/rfc/rfc7693.html
25. Srivastava, D.: Plant Health (2020). URL https://www.kaggle.com/datasets/divumarcus/plant-health