International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

TECHECOSYS- IoT-Based Agriculture with the Blockchain Initiative

[1]Surya M., [2]S. Manohar

Submitted: 10/12/2023 **Revised**: 14/01/2024 **Accepted**: 31/01/2024

Abstract: The objective of this work is to enhance Secure IoT initiated platform for Agriculture domain with the support of MIRACL architecture to implement security. The effective monitoring and agricultural management is carried out with IoT sensors. The sensors are integrated to evaluate environmental factors like soil, temperature and humidity to create techno eco system to create an architecture name TECHECOSYS that integrated block chain, IoT for agriculture ecosystem. The architecture proven to be secure as it deals with MIRACL secure platform that provide extensive cloud secure platform for agri data integrations.

Keyword: *TECHECOSYS, Block chain agri, Secure IoT, Ecosystem*

1. Introduction

Smart secure sensing for IoT-based agriculture refers to the effective monitoring and management of agricultural activities through the Internet of Things (IoT) and sophisticated sensing technologies [1]. Farmers may now collect real-time data on a wide range of parameters, including crop health, soil moisture, temperature, and humidity [2]. Because of the introduction of blockchain technology, the agricultural IoT ecosystem now has an extra layer of security and transparency. Blockchain can help enhance agricultural product supply chain traceability. Customers may have more confidence in the provenance, quality, and safety of the produce if crucial data points at each stage of production, processing, and distribution are recorded on the blockchain. This transparency has the potential to reduce instances of fraud, minimize outbreaks of foodborne diseases, and improve overall food safety. A variety of agricultural processes may be automated and streamlined using smart contracts developed on the blockchain. Smart contracts, for example, may be used to automatically carry out actions depending on predefined parameters, such as activating irrigation systems when soil moisture falls below a certain threshold. These self-executing contracts eliminate the need for middlemen and reduce the likelihood of human error. Traditional centralized systems can be harmed by single points of failure and cyberattacks. Blockchain, on the other hand, operates as a decentralized network that distributes data across several nodes [5]. Because of its decentralized design, the system becomes more robust, ensuring consistent data availability and making it more resistant to assaults.

Blockchain technology, popularized by cryptocurrencies such as Bitcoin, is a decentralized, distributed ledger system that protects the immutability and integrity of data. Blockchain technology can help with a variety of difficulties in agriculture, including data security, trust, and transparency [3]. In the following ways, the blockchain method can improve smart, secure sensing in IoT-based agriculture: The capacity of blockchain to provide an immutable, tamper-proof record of transactions is its defining characteristic. This means that, in the context of agriculture, sensor data collected from various IoT devices may be safely stored on the blockchain [4]. The integrity of the data is ensured since any changes can be traced back to their original source. Farmers, suppliers, distributors, and consumers may now exchange data in an open, transparent, and secure manner thanks to blockchain technology. Farmers may retain their privacy while increasing collaboration and confidence by selectively sharing sensor data with the relevant parties via blockchain.

Although the use of blockchain technology considerably enhances smart secure sensing in IoT-based agriculture, there are various challenges to overcome. These include energy needs for mining operations, blockchain network scalability, and the need for interoperability standards across multiple IoT devices and blockchain platforms. Smart, secure sensing in IoT-based agriculture may improve data security, create trust, enable transparent transactions, and raise the efficacy of agricultural activities across the supply chain by utilizing blockchain technology.

Need for IoT in Agriculture

As a result of the Internet of Things (IoT), the agriculture business is evolving and revolutionizing. The following are some key reasons why IoT in agriculture is essential: Crop Monitoring and Management, Livestock Monitoring and Management, Precision Irrigation, Smart

[1,2] *Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani campus, Chennai, Tamilnadu, India*
[1]*sm3589@srmist.edu.in*, [2] *manohars@srmist.edu.in*

Greenhouses, Weather Monitoring and Forecasting, Pest and Disease Management, Farm Equipment Monitoring.

a) To provide localized weather information, weather stations and sensors may be incorporated into IoT networks. This data may help farmers make educated decisions about pest management, irrigation, and crop planting. Accurate weather forecasting helps with crop optimization, lowers losses caused by bad weather, and improves overall farm management.

b) The continuous monitoring of crops enabled by IoT-based technology allows for the early detection of diseases, pests, and nutritional deficiencies. Connected sensors can detect atypical plant growth patterns, changes in leaf color, and the presence of insects, alerting farmers and allowing them to take precautionary measures. Quick action may be taken to minimize crop losses and reduce the need for chemical treatments with the aid of this early warning system.

c) IoT enables precision farming techniques by collecting real-time data from a range of sensors and devices put in the field. Farmers may measure and analyze data such as soil moisture, temperature, humidity, light levels, and crop health [6]. This data-driven technology may optimize resource management, such as water, fertilizers, and pesticides, increasing agricultural yield while decreasing expenses.

d) Sensor-equipped Internet of Things (IoT) devices can monitor farm animals' health, behavior, and location. Remote monitoring of vital indicators such as body temperature, heart rate, and eating patterns allows for quicker medical intervention in times of disease or distress. Tracking systems based on the IoT also enhance grazing patterns and prevent animal theft and loss.

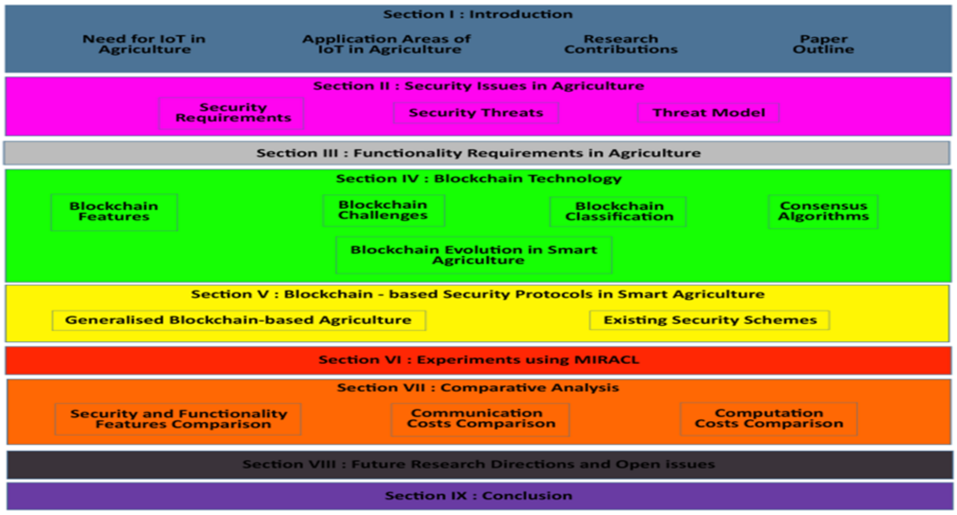

Fig. 1. Roadmap of the paper

IoT technology has expanded the openness and traceabili ty of the agricultural supply chain.Stakeholders may hav e a thorough understanding of the origin, quality, and ma nagement of agricultural commodities by recording and documenting data at each stage, from production to distri bution.This increases food safety, reduces fraud, and boo sts consumer confidence.IoT devices and sensors provide valuable information on how resources are used and accessible on the farm. Farmers may adjust fertilizer delivery based on crop demands, optimize irrigation schedules based on soil moisture levels, and monitor animal health and behavior. This helps to reduce resource waste, conserve water, reduce environmental impact, and improve overall performance.

e) Thanks to the IoT, farmers can monitor and manage agricultural activities remotely, even from afar. Automation systems and linked devices may control machinery and equipment in greenhouses, as well as watering, temperature, and humidity. Farmers may focus on strategic decisions while decreasing operational expenses and labor costs by offering remote access and automation. Figure 1 show the road map for the research.

Agriculture may use IoT to transition from traditional farming practices to data-driven, productive, and sustainable practices. Farmers benefit from the use of IoT technology in a variety of ways, including resource optimization, productivity enhancement, cost reduction, risk mitigation, and contributing to a more resilient and long-lasting agricultural environment.

Research Contributions

A few noteworthy research fields and their contributions are listed below:

Researchers are growing increasingly interested in how blockchain technology is being used in agriculture. The potential of blockchain technology to increase data security, transparency, and trust in IoT-based agricultural systems has been investigated. Creating blockchain frameworks, implementing smart contracts, and researching the benefits of decentralized, immutable ledgers for supply chain traceability and secure data sharing are all examples of research contributions in this domain. Farm automation and robotics Research on the use of IoT in robotics and farm automation is ongoing. Researchers have used IoT connections and data processing capabilities to construct drones, robotic systems, and autonomous agricultural robots. These advancements will allow large-scale agricultural operations to be monitored, harvested, and planted autonomously, increasing output and requiring less labor overall. Algorithms and models for analyzing agricultural data have been created as a result of research in data analytics and decision support systems. These systems provide farmers with useful information and recommendations for better resource management, crop planning, and disease management. Researchers' use of machine learning and data mining methodologies has increased the efficacy and precision of agricultural decision-making processes. The research objective has been to use IoT to promote sustainable agricultural systems. This includes investigating battery-saving sensor technologies, optimizing resource utilization using IoT-based precision agricultural approaches, and developing environmentally friendly pest and disease control systems. Researchers have also investigated the combination of IoT technology and renewable energy sources in order to produce energy-independent and sustainable farming systems.

Research has been conducted to establish dependable and effective IoT network infrastructures for agriculture. This includes researching wireless communication protocols, network architectures, and connection choices that may handle the unique challenges of agricultural areas. Reliable and scalable IoT network infrastructures ensure smooth communication and data transfer between sensors, devices, and applications in the agricultural IoT ecosystem. Research has aided in the construction and development of sensor technology for agricultural applications. This entails developing and deploying sensors to monitor factors such as crop health, soil moisture, temperature, and humidity. These advancements have made it feasible to collect data in agricultural conditions more precisely and quickly.These are only a few examples of IoT-based agricultural research contributions. Researchers from all around the world are working hard to find innovative answers to the difficulties and possibilities presented by the convergence of IoT and agriculture. The field is always evolving.

2. Security Issues in Agriculture Environment

Physical security, cyberthreats, and biosecurity problems are just a few of the numerous security concerns that may occur in an agricultural context. As the agriculture sector becomes more connected and dependent on technology, cyber threats are becoming a serious concern. Cybercriminals may attempt to gain unauthorized access to farm management systems, data, or control systems, disrupting operations, stealing important data, or causing financial damage [7]. Biosecurity threats, such as the introduction of pests, pathogens, or invasive species, can have an impact on agricultural ecosystems. These threats have the potential to harm crops, injure livestock, and devastate the agricultural ecosystem as a whole. It is critical to implement proper biosecurity measures to minimize or decrease such risks. The agricultural supply chain includes various processes, from production and processing to distribution. Any point in the supply chain that is prone to fraud, manipulation, or contamination might jeopardize the food's quality and safety. Farmers and agricultural workers face a number of safety risks when working on farms, including mechanical accidents, chemical exposure, and livestock-handling injuries. Making sure there are adequate safety measures and training may help decrease these risks. Livestock theft is a major worry for farmers and ranchers. Horses, lambs, and other animals are easily stolen, resulting in considerable financial losses. Rusting, or the theft of cattle, is a common problem in many locations. Agricultural equipment and gear are routinely left unattended in remote places, leaving them vulnerable to theft. Furthermore, mishandling or tampering with machinery can result in accidents and property damage. Agricultural operations necessitate the use of expensive machinery, equipment, and crops. Farmers may incur significant financial losses as a result of stolen tools, machinery, or harvested crops. Vandalism to infrastructure and property can also disrupt operations and cause damage. Agricultural operations are particularly vulnerable to natural disasters such as floods, droughts, wildfires, and storms due to their dependency on meteorological conditions. These events have the ability to severely damage crops, infrastructure, and machinery, resulting in massive financial losses.

Security concerns in the agricultural environment must be handled by a mix of preventative measures, technical advancements, staff training, and stakeholder involvement. Physical security measures, robust cybersecurity protocols, promoting biosecurity legislation, and being prepared for crises may all help to protect the agriculture sector from possible attacks. [8][9].

3. Functionality Requirements in Agriculture Environment - Techecosys

Several functional requirements are required for productive and efficient agricultural operations. These criteria may vary depending on the kind of agriculture, such as crop farming, livestock husbandry, or horticulture. Here are some examples of standard agricultural functional requirements.

The TECHECOSYS blockchain application. We used blockchain technology in this project. Customers can see exactly where the items on the shelf originated from. The project's purpose is to show people how their everyday items make their way from the farm to the market. There are three sorts of users in the project. The three groups are customers, users, and miners. When all users log on to the system, they establish a P2P network connection with other users. Customers are the key users of the system. Customers can use the product name to search the system for any product. Customers only use the search section when there has been no customer input into the system [11].

Weather has a significant influence on agricultural activities. Farmers may utilize real-time weather monitoring, projections, and alerts to plan operations, regulate irrigation, protect crops from adverse weather, and maximize resource use. Because agriculture typically involves working outside, having mobile access to important activities is critical. Mobile apps or web interfaces that allow farmers and agricultural personnel to access data, do activities, and get notifications on their mobile devices may result in increased productivity and flexibility. In agriculture, collaboration among numerous stakeholders, such as farmers, agronomists, suppliers, and purchasers, is widespread. Functionalities that promote communication, information sharing, and collective decision-making can improve agricultural operations' coordination and performance. Users may only prepare and deliver blocks for chain addition to TECHECOSYS. Miners may be looked at as TECHECOSYS servers. The system has too many servers if there are too many miners. Customers and users can connect any miners to the system. All data communication takes the form of packets. All packets are delivered to and processed by miners. Manual labor is not required for miners. The mechanism does all of the miners' labor in the back. Human error decreased as a consequence, and time was saved. The Python programming language and Python modules were used to develop this project. This system may only be accessed and registered for by users. To achieve these functionality requirements, a variety of technologies, such as farm management software, sensor networks, Internet of Things (IoT) devices, data analytics tools, and mobile applications, can be employed [12]. The use of such technologies can help to optimize agricultural operations, boost productivity, and promote sustainable farming practices.

4. Techecosys Evolution

Blockchain technology has the potential to revolutionize smart agriculture by boosting transparency, traceability, and efficiency across a wide range of agricultural processes [13]. Here is a timeline of how blockchain technology in smart agriculture has evolved.

Smart contracts built on blockchain technology TECHECOSYS may automate and expedite a wide range of agricultural processes, such as farmer-buyer agreements, payment settlements, and the transfer of digital assets. These self-executing contracts can eliminate middlemen, reduce transaction fees, and enable faster, more secure payments. By utilizing blockchain, smart agriculture may streamline supply chain activities such as inventory management, logistics, and quality control. Blockchain's decentralized transparency and real-time visibility into inventory levels allow for more exact demand estimation while also reducing delays. Blockchain-based systems can enable peer-to-peer trade and decentralized marketplaces for agricultural commodities. Small-scale farmers can reduce costs while increasing market access by engaging directly with customers, negotiating pricing, and eliminating traditional intermediaries and waste.

Farmers, researchers, suppliers, and distributors are just a few of the players in the agricultural ecosystem that can now share data in a safe and decentralized manner owing to blockchain technology. It encourages cooperation and data security while facilitating the exchange of insightful knowledge, scientific breakthroughs, and best practices for improved agricultural outcomes. Blockchain technology may be used to produce and trade digital tokens that represent carbon credits in order to encourage climate-smart agriculture. Farmers that implement sustainable practices can be awarded tokens that can be exchanged or sold as an incentive, increasing carbon sequestration and environmental care. Blockchain-based systems can improve the efficacy and transparency of agricultural insurance operations. Smart contracts can automate payouts depending on specified triggers, such as weather conditions or crop failure, lowering administrative costs while increasing payout accuracy.

IoT and blockchain can collaborate in smart agriculture systems. IoT devices may gather actual data on environmental conditions, soil dampness, crop health, and livestock monitoring. This data may be safely stored on the blockchain to maintain data integrity and allow data-driven decision-making for precision agriculture. Blockchain-based systems can improve the efficacy and transparency of agricultural insurance operations. Smart contracts can automate payouts depending on specified triggers, such as weather conditions or crop failure, lowering administrative costs while increasing payout accuracy.

Table 1: Existing Blockchain Their Applications

Consensus mechanism	Resource	Applications
Ripple	Not applicable	XRP
PBFT	Not applicable	Tendermint
PoW	Concurrent Application	Ethereum
PoS	Digital Certificate	PeerCoin
DPoS	Currency	BitShared Ark EOS
PoB	Currency	PeerCoin
PoL	SGX	Luckychain
PoA	Computations	BitShared Ark EOS
PoET	Intel SGX	Ethereum
PoSp	Storage space	Storj

Table 2: Attacks on Existing Applications

Attack	Affected Method	Affected Module
mining	PoW	Blocks privately Affect Mining
DDos	PoS	Blocks Networks
Sweetener attack	PoS	Nodes broken
Masqurade	PoS	Fake Transaction
Phishing	PoS	Values Change Data Theft

Blockchain technology may be used to create agricultural data marketplaces where farmers can safely sell or share their data with agricultural technology vendors, academia, and other stakeholders. This encourages data-driven innovation and allows farmers to commercialize their data while maintaining control over how it is utilized. As blockchain technology advances, its implementation in smart agriculture has the potential to totally transform the industry, making it more transparent, effective, and sustainable [14]. To effectively realize the benefits of blockchain in smart agriculture, issues such as scalability, interoperability, and data protection must be addressed.

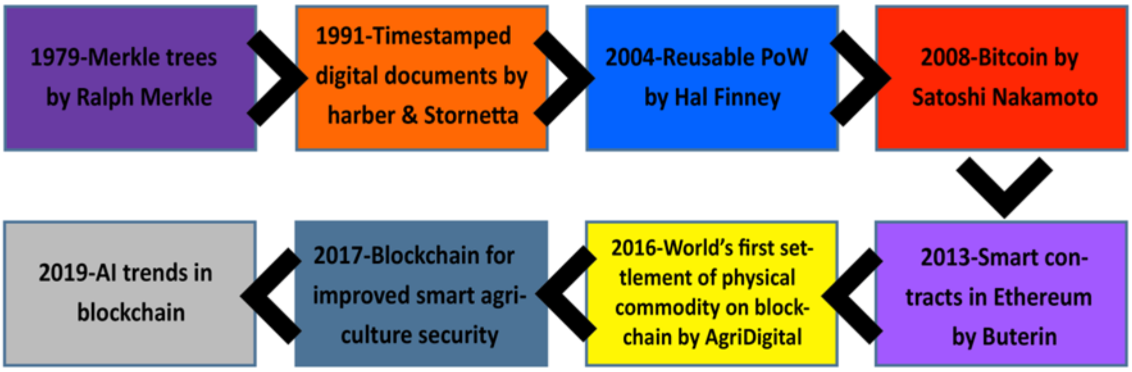

Fig 2. Evolution of blockchain

5. Security Models in Smart Agriculture

Smart agriculture systems can be made more secure and resilient by using blockchain-based security standards [15]. Here are some instances of how blockchain can be used for agricultural security. Figure 2 show the evolution of blockchain

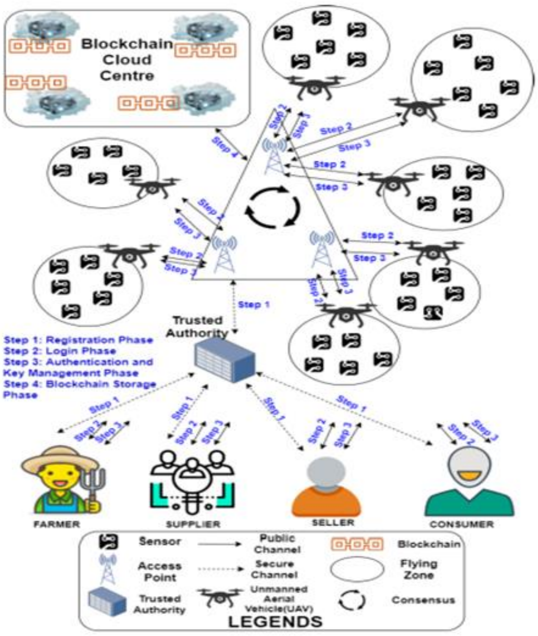

Fig 3. General architecture for TECHECOSYS.

Because blockchain is decentralized and unchangeable, the data saved on it cannot be modified or interfered with. This characteristic can be used to secure critical agricultural data such as sensor readings, supply chain records, or certification certificates. These documents are stored on the blockchain, making it more difficult for unscrupulous actors to alter or falsify data and allowing for a reliable audit trail. Figure 3 depicts the use of cloud-assisted blockchain in smart sensing. Contrary to popular belief, block chain applications employ a P2P architecture rather than a client-server architecture. We first encountered blockchain with the advent of Etherum in our lives. Despite the fact that blockchain applications are becoming increasingly popular throughout the world, our country is only now hearing about them. The term "block chain" refers to a data security structure. The block chain, which has gained popularity in the field of crypto currency mining, has begun and will continue to grow into several industries today. The World Wide Web's conventional architecture employs a client-server network. Because the server is a centralized database controlled by a number of administrators with rights, TECHECOSYS saves all of the essential information in one place, making it easy to update. Unlike client-server applications, data is saved in the system and not in a single location. Any user may readily access system data, and any user can become a miner (such as a database). Simply issue a be-miner request to any TECHECOSYS node, and all nodes will be joined.

Blockchain may be used in smart agriculture to maintain secure identification and access. By utilizing cryptographic keys and digital signatures, blockchain can provide secure authentication and authorization operations. Farmers, agricultural laborers, and other stakeholders' unique identities may be recorded on the blockchain, ensuring that only authorized individuals can access and interact with the system. Blockchain-based, verifiable tracking systems employed by huge corporations are almost non-existent in our nation. TECHECOSYS employs blockchain to track merchandise on their shelves. demonstrates where and how a product arrives on the market shelf. Contrary to popular belief, there is a P2P network architecture in the background rather than a client-server design, and any user in the system can freely examine the data submitted into the system. Data breaches and single points of failure are common with traditional centralized data storage solutions. Data breaches and single points of failure are common with traditional centralized data storage solutions. Smart agricultural systems can achieve data redundancy and resilience by utilizing a distributed blockchain network. When data is dispersed over several network nodes, it is more difficult for attackers to compromise or modify it. For a number of purposes, smart agriculture employs self-executing agreements known as "smart contracts," which are kept on the blockchain. However, the security and trustworthiness of smart contracts must be ensured. Blockchain-based security procedures can help reduce the risk of vulnerabilities and attacks by evaluating the code and logic of smart contracts.

Blockchain technology has the potential to make the agricultural supply chain more secure and transparent. When every transaction and movement of items is registered on the blockchain, it is easier to trace the origin, handling, and quality of agricultural products. This transparency increases overall supply chain security by making it simpler to detect and prevent fraud, counterfeiting, and unauthorized changes. Blockchain-based technologies have the potential to enable multiple parties to safely communicate sensitive agricultural data. By utilizing encryption techniques and access restrictions, blockchain may provide fine-grained control over data sharing and ensure that sensitive information is only available to authorized parties. Blockchain-based systems can serve as a tamper-proof ledger for security-related occurrences and events. When security events, warnings, and system adjustments are stored on the blockchain, it is easier to detect possible security breaches, analyze problems, and launch effective incident response systems.

Table 3: Execution Time (In Milliseconds) Of TECHECOSYS

Time Variation	Average time (ms)
T_{bp}	3.899
T_{h}	1,012
T_{exp}	0.012
T_{eca}	1.011
T_{ecm}	0.134
$T_{ecsiggen}$	0.446
$T_{ecsigver}$	2.170
T_{senc}	1
T_{sdec}	2
T_{mul}	0.06
T_{add}	0.02

To apply blockchain-based safety measures in smart farming, careful design, integration, and stakeholder involvement are required, as consensus procedures, encryption standards, identity management frameworks, and regulatory compliance must be considered to ensure the efficiency and scalability of blockchain-based security solutions in the agricultural context.

6. Result Comparison

TECHECOSYS uses MIRACL (Multiprecision Integer and Rational Arithmetic Cryptography Library) is a cryptography library that provides a variety of functions for safe data protection and communication. I don't have access to particular data on MIRACL testing, but I can provide a broad overview of MIRACL and other related cryptographic libraries' possible uses and applications. When we look at the structure of the block chain, we see that it is made up of blocks, and each block in the chain retains the hash information of the preceding block, indicating that it is linked to the prior block. In this scenario, it allows for more secure data storage. Blocs are made up of four parts in this scheme. Hash, Previous Hash, Transaction, and Timestamp are all valid. It is similar to an encrypted private ID. A hash is data that has been encrypted using certain standards. The sha256 and sha1 algorithms are commonly employed. This project uses the Sha256 hash technique. Figure 4 shows the Project applied in TECHECOSYS.

Pseudo code as

```
def _createFarmStand(_name: String[256], _location: String[512], _wallet: address) -> bool:
    #check data
    assert len(_name) <= 256, 'Name must be less than 256 characters.'
    assert len(_location) <= 512, 'Location must be less than 512 characters.'
    assert _wallet == self.owner, 'Address does not match contract owner.'
    assert self.stand_created == False, 'Farm stand already created on this contract.'
    #create farmStand object
    new_stand: farmStand = farmStand({
        name: _name,
        location: _location,
        wallet: _wallet
    })
    #track farm stand
    self.standInfo[0] = new_stand
    #set creation boolean
    self.stand_created = True
    #return success boolean
    return True
def _transferOwnership(_from: address, _to: address) -> bool:
    #ensure the person changing it is the owner
    assert _from == self.owner, 'Only the owner may transfer ownership.'
    assert _to != ZERO_ADDRESS, 'You may not transfer ownership to a ZERO_ADDRESS.'
    #transfer ownership
    self.owner = _to
    #return success boolean
    return True
```

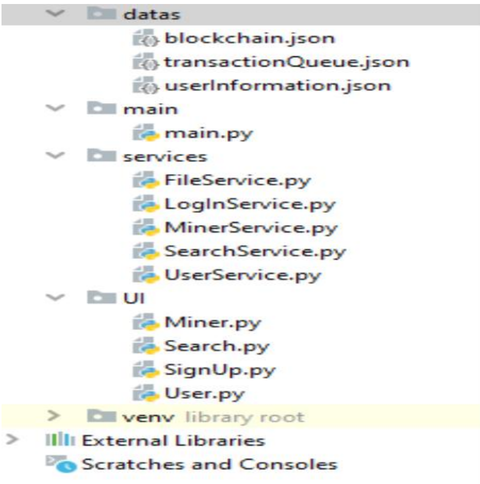

Fig 4. TECHECOSYS Farm module

MIRACL can secure data transport between various components of smart agricultural systems. This entails encrypting data at the source, securely transmitting it via networks, and then decrypting it when it arrives at its destination. This protects sensitive data from unauthorized access and eavesdropping. MIRACL may be used to establish secure access control strategies in smart agriculture systems. It enables the creation and verification of digital signatures and certificates to identify persons or devices and ensure that only authorized parties have access to critical resources or perform certain activities. MIRACL may be used to create privacy-preserving techniques in situations where several entities must collaborate and analyze data without revealing private information. The actual data saved in the chain is referred to as a transaction. In this system, it is transaction ID, farm ID, farm name, number, from place to place, and operation date. Users make a request for transaction addition to all miners. All miners that receive the request compete to add the transaction to the chain. This competition is known as Proof of Work. There is a hash standard that is generally updated on a regular basis. In TECHECOSYS, miners continually enter data into a hash function and even employ brute force to enter this data. To win the race, the first ten digits of the output of this function must be zero, and it must be completed within 10 minutes. If one miner completes the task before the others, the transaction will be added to the blockchain.

TECHECOSYS may be used to establish secure communication channels between various smart farm system components. Secure connectivity between IoT devices, edge devices, and cloud platforms is required to avoid unauthorized access or data interception. These are the primary: user interface, services, and data. This directory contains the main.py file. Farm's UI files are located in the UI folder. Miner.py, Seacrh.py, SignUp.py, and User.py are examples. The Services folder contains all of the user's operation functions. This folder contains the files MinerService.py, gfarmService.py,ownerService.py, and LogInService.py. These files include all of the project's functional work. Finally, the Datas folder contains all of the system data. Blockchain.json, userInformation.json, and transactionQueue.json are made files in there. The most significant file for this system is blockchain.json, which contains the primary system data. Blockchain.json repository userInformation.json just stores user information, and transaction data is stored in TransactionQueue.json placed below. Fig 5. Shows Blockchain Farm Module

{"hash": "76fe9f55b7403e76dfa399bd550a80028e519958ba1e169a3142b7a616c8ach",

"previousHash": "76fe9f55b7403e76dfa399bd550a80028e519958ba1e169a3142b7a616c8cdbe",

"transaction": {

"transactionId": "TRN91198",

"FarmId": "Cofee",

"FarmName": "Jarvis",

"Number": 400,

"fromPlace": "xyz warhouse, rize,merkez",

"toPlace": "rpls warhouse, trabzon,merkez",

"date": "20230231127"

},

"timestamp": "20230231127"

}


```
def searchBlockchain(key):
    senderPacket = []
    block = []
    with open('/datas/blockchain.json','r') as file:
        block = json.load(file)
        for i in block:
            trans = i['transaction']
            name = trans['productName']
            if key == name:
                senderPacket.append(i)
    return senderPacket
```

Fig 5. Search Block Chain Farm module

It's vital to remember that the individual experiments performed using MIRACL or cryptographic libraries are determined by the study's or application's criteria and goals. Researchers and developers may leverage MIRACL's capabilities to construct secure communication, data protection, and privacy-preserving tactics in smart agriculture and other domains where data security is critical.

7. Comparative Analysis

Certainly, it can compare TECHECOSYS and OpenSSL, another cryptographic library, in a comparison. A popular open-source library called OpenSSL provides a wide range of cryptographic functions and protocols. The following table compares MIRACL and OpenSSL based on various criteria:

Table 4: Application area identification

Existing	Attributes	Working Functionality
Chaganti *et al.*	CIA	Common Security
Vangala *et al.*	Authentication and Authentication	Wireless Sensor Network
Aldhyani *et al.*	Client	PKI

Freyhof *et al.*	Preserving privacy	PKI
Yao *et al.*	Traceability	VANETs
Kaur *et al.*	CIA	VANETs
Islam and Shin	Authorized Access	IoD Healthcare
Chen *et al.*	Messages	Smart Agriculture
Wu and Tsai	Email	Smart Agriculture
Zhou *et al.*	Mutual Authentication	PKI

The objectives and use cases that MIRACL and OpenSSL target are different. In contrast to OpenSSL, which provides a wider range of cryptographic features, MIRACL focuses on effective multiprecision arithmetic cryptographic operations. Figure 6 show the Challenges in smart agriculture.

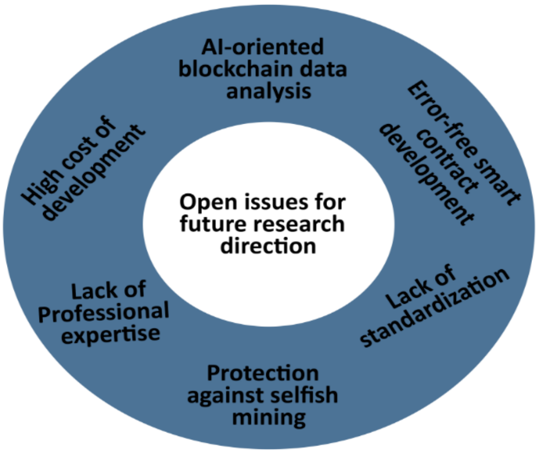

Fig 6. Future Research direction.

The decision between the two is based on the particular project requirements, the required level of complexity, and the support and documentation choices. Developers should assess their unique demands, performance requirements, and community support to determine which library is best for their cryptography needs. The result observations of MIRACL are shown in the following figures 7, 8, 9, 10 and 11 sensor in IOT.

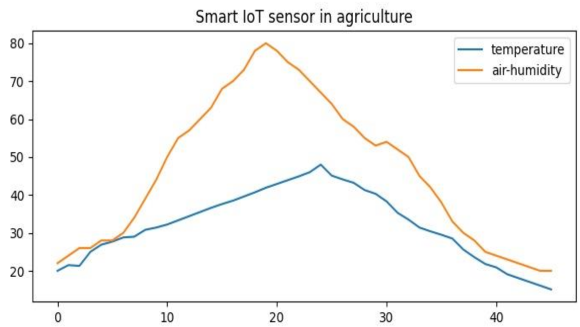

Fig 7: Temperature and humidity sensor comparison

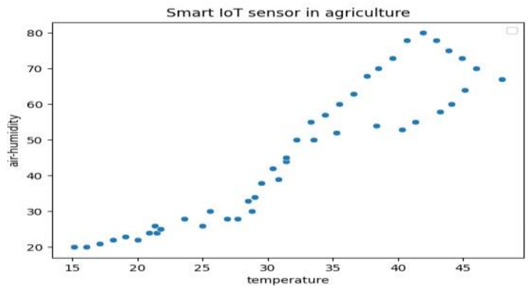

Fig 8: Increase in air humidity vs. temperature

Fig 7 and 8 gives the comparison analysis of temperature and humidity measures using IoT sensor. Both temperature and humidity are interlinked through the process is shared using blockchain technology.[16]

The variations in the sensors are monitored and observed using the distributed channel concepts that focused on temperature and humidity measures.[18]

The minute variations are clearly observed and subject the forecast analysis.

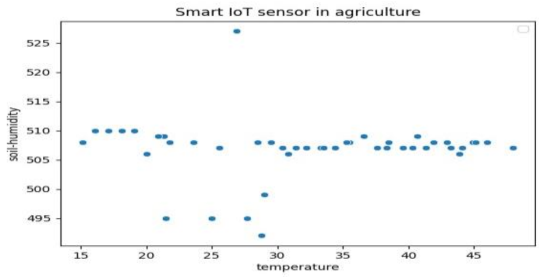

Fig 9: Balancing temperature and humidity

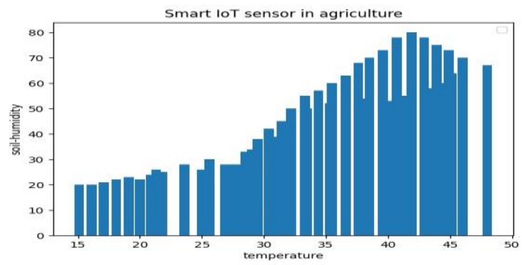

Fig 10: Humidity variations in Sensors

Fig 9 and Fig 10 shows the growth analysis of the yield against temperature and humidity and also highlight the impact of environmental factors that influence it.

Each channel is secured with the support of block chain technology and the growth factors are analyzed accordingly. Fig 11 and Fig 12 shows the temperature sensor data frame and final Blockchain test result.[19]

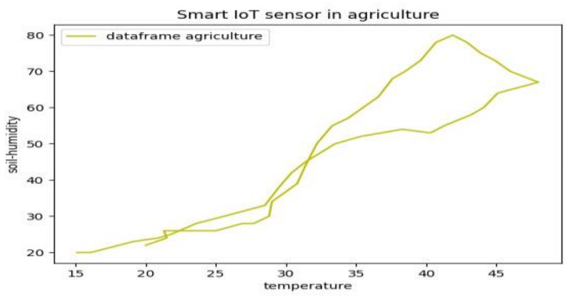

Fig 11: Temperature sensor data frame

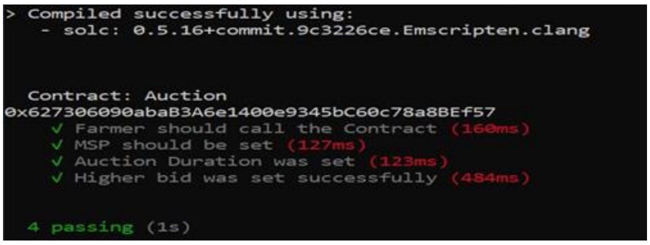

Fig 12: Security factors against sensor data frame

Security plays a major role and the impact is clearly shown based on the indication of the graph shown above. Hence the combined factors of blockchain along with IoT sensors gives secure precession agriculture as defined by MIRACL.[17]

8. Conclusion and Future Research Directions

Finally, TECHECOSYS's deployment of smart sensors, IoT technologies, and blockchain in the agriculture business enables a revolutionary and efficient farming system. Farmers may now remotely monitor and control critical components of their operations, guaranteeing optimal crop growth conditions. Furthermore, the adoption of blockchain technology ensures safe data storage, resulting in transparency and confidence in the agricultural supply chain. This not only benefits farmers by lowering the danger of fraud and boosting traceability, but it also offers customers assurance of food quality and safety. Furthermore, the integration of smart sensors and IoT technologies enables real-time data analysis, resulting in better informed decision-making and higher agricultural output.

Future research in the field of cryptography and secure communication for smart agriculture might focus on the following areas: As data collection and sharing become increasingly widespread in smart agriculture, privacy protection becomes more crucial. Future research might look at advanced privacy-preserving techniques, including differential privacy, safe multi-party computing, and homomorphic encryption, to enable secure data analysis and collaboration without jeopardizing sensitive information. Standardization is critical to the compatibility, interoperability, and security of smart agriculture systems. To encourage smooth integration and secure interoperability among various agricultural technologies, future research can focus on developing agricultural-specific standards and protocols that address issues such as data formats, communication methods, and security requirements.

Smart agriculture must enhance authentication and access control to avoid unauthorized access and assure data security. A future study might look at novel authentication approaches, biometrics, and complex access control models to improve the security and usability of authentication procedures in agricultural systems. Smart agriculture systems are vulnerable to a variety of cybersecurity threats, including malware, data breaches, and denial-of-service assaults. To successfully mitigate and manage emerging threats, future research should focus on the creation of robust cybersecurity frameworks that integrate threat intelligence, anomaly detection, and incident response methodologies.

These research routes are intended to address the security concerns and emerging challenges in smart agriculture. Researchers may help to create safe and sustainable agricultural systems by pushing the boundaries of encryption, privacy-preserving approaches, secure computing, and resilient frameworks.

Reference

[1] Chaganti, Rajasekhar, et al. "Blockchain-based cloud-enabled security monitoring using Internet of Things in smart agriculture." Future Internet 14.9 (2022): 250.

[2] Sinha, Bam Bahadur, and R. Dhanalakshmi. "Recent advancements and challenges of Internet of Things in smart agriculture: A survey." Future Generation Computer Systems 126 (2022): 169-184.

[3] Pyingkodi, M., et al. "Sensor based smart agriculture with IoT technologies: a review." 2022 international conference on computer communication and informatics (ICCCI). IEEE, 2022.

[4] Vangala, Anusha, et al. "Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges." Cluster Computing 26.2 (2023): 879-902.

[5] Zeng, Hui, et al. "An IoT and Blockchain-based approach for the smart water management system in agriculture." Expert Systems 40.4 (2023): e12892.

[6] Kethineni, Keerthi, and G. Pradeepini. "Intrusion detection in internet of things-based smart farming using hybrid deep learning framework." Cluster Computing (2023): 1-14.

[7] Aldhyani, Theyazn HH, and Hasan Alkahtani. "Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model." Mathematics 11.1 (2023): 233.

[8] Alahmadi, Adel N., et al. "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture." Sensors 22.9 (2022): 3520.

[9] Freyhof, Mark. "Cybersecurity of Agricultural Machinery: Exploring Cybersecurity Risks and Solutions for Secure Agricultural Machines." (2022).

[10] He, Leilei, et al. "IoT-based urban agriculture container farm design and implementation for localized produce supply." Computers and Electronics in Agriculture 203 (2022): 107445.

[11] Ouafiq, El Mehdi, Rachid Saadane, and Abdellah Chehri. "Data Management and Integration of Low Power Consumption Embedded Devices IoT for Transforming Smart Agriculture into Actionable Knowledge." Agriculture 12.3 (2022): 329.

[12] Aanjankumar S, Poonkuntran S. Peer-2-Peer Botnet manage SDT security algorithm. In 2016 IEEE Interna-tional Conference on Computational Intelligence and Computing Research ICCIC (2016), pp. 1-5.

[13] Xie, Dongbo, et al. "Actuators and sensors for application in agricultural robots: a review." Machines 10.10 (2022): 913.

[14] Akella, Gopi Krishna, et al. "A Systematic Review of Blockchain Technology Adoption Barriers and Enablers for Smart and Sustainable Agriculture." Big Data and Cognitive Computing 7.2 (2023): 86.

[15] Aanjankumar S, Poonkuntran S. An efficient soft compu-ting approach for securing information over GAME-OVER Zeus Botnets with modified CPA algorithm. Soft Computing. (2020) Nov;24(21):16499-507.

[16] Padhy, Sasmita, et al. "AgriSecure: A Fog Computing-Based Security Framework for Agriculture 4.0 via Blockchain." Processes 11.3 (2023): 757.

[17] Alam, Shadab. "Security Concerns in Smart Agriculture and Blockchain-Based Solution." 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON). IEEE, 2023.

[18] Anitha, T., S. Aanjankumar, S. Poonkuntran, and Anand Nayyar. "A novel methodology for malicious traffic detection in smart devices using BI-LSTM–CNN-dependent deep learning methodology." Neural Computing and Applications 35, no. 27 (2023): 20319-20338.

[19] Aanjanadevi, S., S. Aanjankumar, K. R. Ramela, and V. Palanisamy. "Face Attribute Convolutional Neural Network System for Data Security with Improved Crypto Biometrics." Computer Systems Science & Engineering 46, no. 1 (2023)