Mesopotamian journal of Cybersecurity
Vol.4,No.3, **pp**. 1–21
DOI: https://doi.org/10.58496/MJCS/2024/012; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Enhancing Electronic Agriculture Data Security with a Blockchain-Based Search Method and E-Signatures

Duaa Hammoud Tahayur[1], Mishall Al-Zubaidie[1,*]

[1] Department of Computer Sciences, Education College for Pure Sciences University of Thi-Qar, Nasiriyah 64001, IRAQ

ARTICLE INFO

Article history
Received 04 Jun 2024
Accepted 15 Aug 2024
Published 09 Sep 2024

Keywords
Agriculture apps
Blockchain Signatures
EAA
Optimal solution
Uncle-block attack

ABSTRACT

The production of digital signatures with blockchain constitutes a prerequisite for the security of electronic agriculture applications (EAA), such as the Internet of Things (IoT). To prevent irresponsibility within the blockchain, attackers regularly attempt to manipulate or intercept data stored or sent via EAA-IoT. Additionally, cybersecurity has not received much attention recently because IoT applications are still relatively new. As a result, the protection of EAAs against security threats remains insufficient. Moreover, the security protocols used in contemporary research are still insufficient to thwart a wide range of threats. For these security issues, first, this study proposes a security system to combine consortium blockchain blocks with Edwards25519 (Ed25519) signatures to stop block data tampering in the IoT. Second, the proposed study leverages an artificial bee colonizer (ABC) approach to preserve the unpredictable nature of Ed25519 signatures while identifying the optimal solution and optimizing various complex challenges. Advanced deep learning (ADL) technology is used as a model to track and evaluate objects in the optimizer system. We tested our system in terms of security measures and performance overhead. Tests conducted on the proposed system have shown that it can prevent the most destructive applications, such as obfuscation, selfish mining, block blocking, block ignoring, blind blocking, and heuristic attacks, and that our system fends off these attacks through the use of the test of the Scyther tool. Additionally, the system measures performance parameters, including a scalability of 99.56%, an entropy of 60.99 Mbps, and a network throughput rate of 200,000.0 m/s, which reflects the acceptability of the proposed system over existing security systems.

1. INTRODUCTION

Governments must enact laws and take important steps to improve agricultural food safety by utilizing identity verification and traceability systems. Food safety is an essential human right. Accurate data transmission via network servers is emphasized, underscoring the vital role that agricultural goods play in preserving the population's food supply and encouraging the adoption of sustainable and fruitful farming practices. Enhanced agricultural productivity is linked to both economic growth and national development. Increasing food production can reduce reliance on imports, increase regional economic growth, encourage the sustainable development of rural areas, and improve food security. Food safety provenance and identity verification all contribute to bolstering customer confidence in the food system and supplying them with wholesome and safe products. As a result, preserving the nutritional value of food is a significant task that calls for collaboration among the relevant businesses, the government, and the agricultural sector. Food security and confidence in the global food supply network can be improved by passing the necessary laws and putting in place efficient tracking and identity verification systems [1]. Blockchain is among the most cutting-edge technologies [2]. It has been investigated together with its effects on the agricultural sector and its products [3]. This approach uses blocks to establish openness in the agricultural product supply chain. Food safety and supply chain transparency are important issues that require serious consideration. Big data is used to gather data from customers, distributors, and manufacturers. Ownership transfers and item tracing along the entire supply chain are handled by blockchain technology [4]. Blockchain technology is revolutionizing the agricultural tracking industry as well as other service applications, such as finance, healthcare, and the Internet of Smart Things (IoT). The majority of app development techniques currently in use are based on well-known blockchain platforms such as Ethereum, Bitcoin, and Hyperledger Fabric [5]. The ability of blockchain technology to trace an item along the supply chain is among its most advantageous applications. Because of its advantages, the scientific community has been interested in learning more about the possible uses of blockchain technology (BCT) in the supply

[*] *Corresponding author. Email: mishall_zubaidie@utq.edu.iq*

chain industry [6]. In addition to fortifying the supply chain and managing and overseeing risk mitigation strategies, this technology has the potential to prevent security breaches. When combined, cryptocurrencies and the Worldwide Web of Things have been shown to be cost-effective and time-saving tactics that generate many data. These data are analysed via advanced deep learning (ADL) techniques [7, 8]. Electronic agriculture using the IoT and machine learning. Agriculture-related difficulties and issues can be resolved with the use of contemporary technologies such as machine learning, deep learning, and the IoT [9-11]. IoT devices, including sensors, can be used to track and evaluate water usage as well as detect the temperature and humidity of the soil. Artificial intelligence (AI)-powered drones can also be utilized in smart agriculture to collect high-resolution photos for crop inspection and analysis. The quality of transplant results can be enhanced by combining the IoT and deep learning techniques. The agriculture industry can become more productive and effective by utilizing an integrated suite of electronic applications offered by the IoT. These applications include automatic irrigation control systems that ensure that the proper amount of water is applied, as well as smart water management systems that use sensors to detect soil moisture and water flow. To meet agricultural demands, the state of agriculture should be considered through the use of sensors to measure temperature, humidity, and illumination, as well as surveillance cameras to detect plant diseases and pests. Additionally, there are applications to enhance the management of agricultural inputs, including the ability to remotely control agricultural equipment, sensors to assess the levels of pesticides and fertilizers, and intelligent control systems to distribute these inputs effectively. To provide suggestions for the best agricultural practices and aid in productivity prediction and long-term planning, this also entails gathering and evaluating agricultural data utilizing integrated monitoring systems and specialized apps. These IoT-integrated electronic applications assist farmers in managing their farms more profitably, boosting yield, reducing expenses, and protecting natural resources. The primary objectives are to issue laws and implement identity verification and product traceability systems to improve agri-food safety. Advanced technologies such as blockchain and big data analytics can be used to increase agricultural supply chain security. The IoT and machine learning technologies can be applied to solve agricultural problems and improve productivity [8].

The importance of the management of agricultural produce output and food safety supplies in the food supply chain is the primary goal for agriculture companies. Recently, this has been accomplished by utilizing technologies such as blockchain technology for transaction tracking and information gathering from manufacturers, suppliers, and counterparties and by utilizing goods via the supply chain's guideline tools for producing food in a safe way. Any toolkit's most crucial decisions are those that have an immediate impact on food safety. By using big data and blockchain technology to precisely and accurately trace products along the supply chain, food safety can be guaranteed [12]. Security issues can arise in real-world applications when blockchain is employed as a platform to manage traceable application data. There are increasing attacks on agricultural applications, as shown in Figure 1, which require technology to provide security and performance [13]. Protecting agricultural data transmitted via the IoT is extremely important for preserving agricultural products, as any change to these data, such as environmental identifiers, soil types, seed types, production quantities, fruit quality, fruit types, etc., will negatively affect the resources of agricultural companies and even the economies of countries. The arrival of accurate agricultural data from the sender to the recipient will greatly preserve agricultural crops and prevent damage to products. The protection of agricultural data is closely linked to the economy at the level of agricultural institutions and countries, which motivates us to design an efficient system that prevents various attacks and implements procedures with high performance.

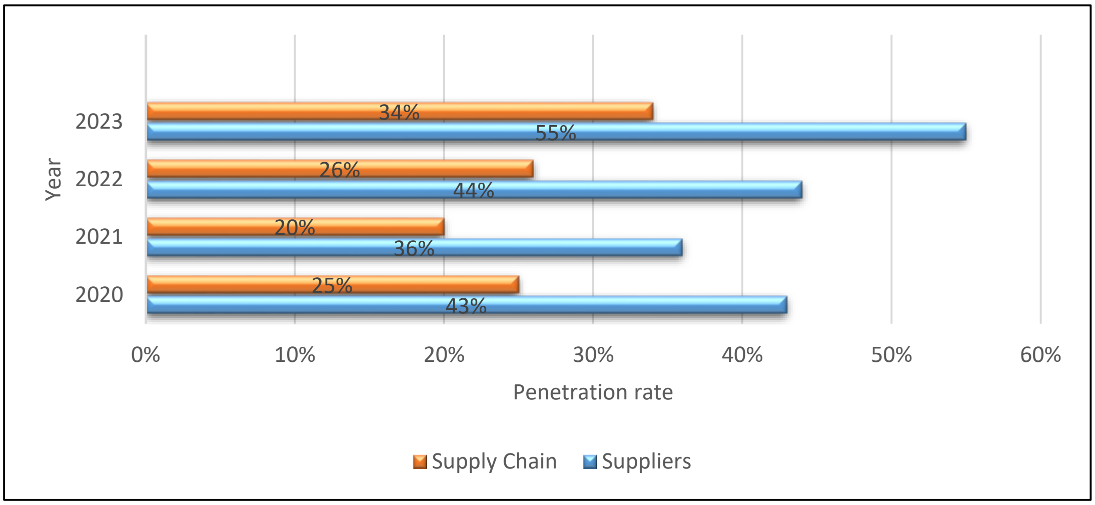


Fig. 1. Penetration rates for electronic agricultural applications based on the IoT

E-agricultural applications are not secure enough to prevent various types of data attacks. Additionally, blockchains may have poor data security, high demand for data storage, and inefficient query performance. The following issues could arise in real-world applications when employing blockchain as a platform to manage traceable application data. Users obtain more access to the underlying storage system, as there are more nodes and data. Moreover, the data storage system's functionality and efficiency are severely strained by it. The blockchain verifies its data via hashes, which may be insufficient to repel data tampering attacks. Using strong signatures to prevent the modification of data in the blockchain is a very large challenge. Public key signatures provide better handling of the blockchain in terms of scaling users and nodes. Each device has two keys: public and private. A message is signed by the sender via the public key during data transfer, and only the recipient with this particular public key may verify and obtain accurate data [14, 15]. Furthermore, the randomness used with blockchain and hashing may not be sufficient to support data transmitted or stored via EAA-IoT. By filling security gaps in blockchain technology, electronic agriculture applications can greatly improve agricultural application products, services, and prosperity [15]. For the security breach case study, several examples illustrate the breach of agricultural data worldwide. For example, the Federal Bureau of Investigation (FBI) noted in its 2023 Internet Crime Complaint Center (IC3) Report that 2,825 attack reports totaling approximately $59.6 billion in damage were recorded across all industries. Of these, 1,193 complaints are associated with 16 important infrastructure sectors that have been recognized, comprising the food and agricultural sectors. Because of their critical position in the food supply chain, the importance of accurate data, and the time-sensitive nature of their operations, agricultural cooperatives have recently been the target of a variety of cyberattacks against agricultural data. Attacks during prime times have the potential to seriously impair the availability of necessities such as fertilizer and seeds, which would have an impact on planting schedules and, eventually, the food chain and the investigation of agricultural data. Such assault patterns have been noted by the FBI, with many occurrences documented throughout the autumn 2021 harvest and prior to the 2022 planting season. Owing to pressure to preserve supply chain integrity, attack actors may view these cooperatives as more ready to pay the ransom, making them attractive targets (FBI, 2021, 2022) [16]. Our principal contributions are listed below:

- Edward's digital signatures algorithm (Ed25519) is based on the technology of the blockchain instead of the secure hash algorithm (SHA-256) to ensure that data tampering is prevented. To our knowledge, this contribution is novel and has not been used before in the EAA-IoT.
- ADL and ABC are used to find the randomness and optimal solution and support the performance and security of the proposed system. To our knowledge, there is no system that combines the ADL, ABC, blockchain and Ed25519 algorithms to support EAA-IoT security.
- Provide an extensive analysis of security (attacks theoretical analysis and Scyther test) and performance parameter analysis (execution time, scalability, entropy, network throughput, and blockchain performance), as well as the proposed system performance and limitations in EAA-IoT.

The following are the key ideas, which provide a concise overview of the paper structure. An overview of security threats and e-agriculture is provided in Section 1. We present the relevant literature on our research issue in Section 2. The methods of the suggested e-agriculture approach are illustrated in Section 3. Section 4 describes the proposed methodology. Section 5 provides details of our theoretical security analysis, and Section 6 examines the security analysis with Scyther. Section 7 illustrates the performance findings. We describe the findings and implications of the study. The conclusion is presented briefly in Section 8.

2. RELEVANT WORKS

Research has been conducted on the use of signature methods and the blockchain in e-agriculture applications; however, there are still many security drawbacks and usability difficulties with the current approaches. A brief investigation of recent research on the subject of our study is provided in this section.

Jacolin et al. [1] employed deep learning and machine learning methods to detect plant problems. The diseases of plants can have a considerable influence on food yields, and early identification is crucial. They analysed the benefits and drawbacks of various plant disease segmentation approaches, such as the cut-off method, clustering technique, edge detection technique, and regional technique. More research and development are still needed to find effective solutions based on machine learning and deep learning to accurately and reliably monitor and diagnose plant diseases. However, they noted that these standard methods have drawbacks and might not be sufficiently precise. Li et al. [2] presented a solution to protect privacy in blockchain technology by ring signature technology. Data storage applications for privacy focus on the ring signature on an elliptical curve and use the complete anonymity of the ring signature to ensure the data security and identity privacy of users in the blockchain. The method it uses ring signature technology, and it is easy to store data to provide advanced privacy for this technology. The results provided high protection and privacy for the identities of users in blockchain applications. However, the researchers did not mention any specific evaluations or comparisons of performance and did not analyse the security of the proposed system. The system proposed by Chatterjee and Singh [3] makes use of the idea of BCT smart contracts. The parties to the transactions are managed by all the entities involved in the BCT-based supply chain network. They claimed that to preserve high levels of traceability and transparency across the supply chain ecosystem, all transactions are documented. Additionally, a group signature technique is employed when misuse is discovered. The system's total performance is tested via three metrics: transaction efficiency, system risk reduction, and participant trust. Their system's implementation results in a measurement of transaction efficiency that takes into account latency, throughput, average execution time, and gas cost. Nevertheless, the group signature technique is very expensive to perform for EAA-IoT applications. Additionally, the researchers here did not enhance security and did not address possible attacks on the system.

Taji and Ghanimi [4] introduced a system for homomorphic signcryption based on hyperelliptic curve (HEC) for IoT-enabled agriculture. They noted that, in comparison with other methods, their HEC-based signcryption methodology improves security while requiring less computation and transmission overhead. Additionally, their solution meets the requirements of confidentiality, integrity, and availability triad while providing efficient performance in resolving privacy preservation concerns. Their suggested solution improves practicality and adaptability for agricultural situations by reducing computing and communication costs by approximately 95.08% and 87.28%, respectively. Nevertheless, their system lacks the features offered by blockchain, such as management, distribution, transparency, and integration, which indicates that their system relies on traditional methods. Additionally, the problem of using signcryption has several limitations and drawbacks in its implementation, including the complexity of the algorithms and the infrastructure used to create and verify the signature. A BCT-based system for data security was introduced by Aljabri et al. [5]. In this system, blocks are created via the Rivest, Shamir, and Adleman (RSA) signatures. To train and test their system, they first choose the BCT-secured data and divide it into training and testing datasets via differential evolution (DE). The verified system may also include a deep belief network (DBN) for attack prediction. The simulation objective is to assess the classification accuracy and safety. However, when RSA signatures are used, the minimum length of the keys used is 1024 bits, which negatively affects their system performance. Moreover, another problem is the modification of sensitive data, which threatens the data stored on servers.

Yourong Chen et al. [6] presented a proposal called the “miner revenue optimization algorithm based on a Pareto artificial bee colony in a blockchain network”, which aims to optimize the revenue of offensive mining pools and miners under block-blocking attacks in blockchain networks. Researchers have used an algorithm called the "Pareto artificial bee colony" to solve this problem. The solution methods include the following operations: Calculating the evaluation value, calculating the probability of selection, the random exchange process, the transformation process, and the Pareto dominance method. They also used the “watcher bees,” “explorer bees,” and “scout bees” processes to achieve the optimal solution. The simulation results revealed that their proposed algorithm was able to find a suitable action strategy that decreased the difference and variability value of the income solution set while increasing the minimum, average, and evaluation values of the best possible solution for each attack miner pool. The suggested method performed better than other existing algorithms, such as the nondominated sorting genetic algorithm II (NSGA2) and multiple objective particle swarm optimization (MOPSO). The pain in the research may be related to achieving a balance between increasing the revenues of offensive mining pools, ensuring the necessary revenues for each mining pool and its miners, and overcoming block-blocking attacks that reduce the overall revenues of offensive mining pools. There may be challenges in ensuring that revenues are distributed fairly and efficiently between the preparers in the mining pool and the pool manager. Product tracking information for each company is then linked to a useful chain (segmentation indicators). The system has demonstrated its ability to provide comprehensive data information and transmit it in a useful series. It included simultaneous use of security and privacy chains of product data, high power savings, and meeting the requirements of all participants in the tracking system. The main problem is mitigating the effects of ban attacks on the revenues of the mining complex and not eliminating attacks against the system. Striking this delicate balance appears to be an ongoing challenge that the researchers were not able to fully resolve in this work. To confirm data integrity in cloud storage, Kumar and Bandanadam [7] intended to suggest a BCT-based public auditing system. Initially, users upload their data to the cloud and then retrieve it as needed. The enhanced EL-GAMAL (IEL-GAMAL) encryption method is used by their system to encrypt user data, which are then uploaded via the BCT blocks to the cloud service provider (CSP). When a user needs to confirm the information included in cloud storage, they request a public audition to produce evidence of the encrypted block kept in the BCT. However, the EL-GAMAL algorithm with long keys is expensive because of system performance overhead. In addition, the authors did not provide an analysis of important parameters in electronic applications, such as entropy and scalability. Additionally, in their proposed system, they dealt with hacking attacks but did not present the results of their analysis.

A thorough system for protecting dynamic agricultural data produced by internet-connected loT devices was proposed by Vardhan et al. [8]. Three primary elements comprise the suggested system: advanced AI principles, intrusion detection and prevention systems (IDPSs), and a honeycomb architecture. To decrease single points of failure and increase data resilience, the honeycomb design combines distributed storage with decentralized control, offering a solid basis. Inaccurate inferences drawn from a single false data point might have an impact on the sustainability and overall growth of the agriculture industry. Using the suggested cybersecurity system would help agriculture stakeholders protect the confidentiality and integrity of their data, which would increase the industry's resilience to cyberattacks and increase confidence in the reliability of analysis. To ensure the sustainability and resilience of agricultural data ecosystems in the face of rising cyber threats, the results of this study are anticipated to benefit farmers, researchers, and policymakers, among other stakeholders in the agricultural sector. Nonetheless, their proposed system did not rely on a robust signature algorithm that prevents data tampering attacks. Moreover, their system's security against the latest attacks was not analysed to prove its applicability in the context of EAA-IoT. Arvind Panwar et al. [12] examined the potential uses of BCT in agriculture, including managing the supply chain, handling payments, and product certification. It also looks at the difficulties and constraints of using blockchain technology in the agricultural industry, addressing problems with interoperability, scalability, and regulatory frameworks. Systematic reviews and meta-analyses (PRISMA) were used to carry out the systematic literature review. A method used in research is meta-analysis. The outcomes highlight the noteworthy and advantageous effects of BCT on farming. An alliance of government agencies, business executives, and tech experts promotes the widespread application of the BCT scheme in farming. The potential of the financial system is to revolutionize the agriculture sector by offering a secure and transparent platform for supply chain management. Underlines the requirements for clear regulations, stakeholder involvement, and technical expertise for the effective application of BCT in farming. In summary, together with suggestions for its successful application, the report offers a comprehensive review of the possible uses of blockchain technology to address issues facing the agricultural sector. The main problem is that scalability needs to be addressed for the effective application of blockchain technology in agriculture. Scaling blockchain solutions to handle high volumes and complex processes for the agricultural sector remains an ongoing challenge.

Hassan Khan et al. [14] offered a thorough analysis that looked at how blockchain technology might be used with sixth-generation (6G) mobile networks. They looked into consensus methods, deployment, and blockchain-powered 6G network services. It also looks at the possible advantages and difficulties of combining digital currencies with 6G, including how they can affect power consumption, scalability, and security. A summary of ongoing 6G projects and standardization efforts is also provided. Researchers have investigated several avenues for 6G, blockchain technology, and related research. They proposed applying the long-term nature, decentralized governance, privacy, and openness of blockchain technology to address trust issues in the development of 6G networks. Examine how blockchain technology enables 6G services for sharing resources, integrity, secrecy, access control, and authentication. Analysing consensus techniques for 6G network Blockchain-as-a-service (BaaS) architectures Analyse how consensus techniques affect 6G scalability, security, and power usage. They address architectural elements, service models, and technology challenges after carefully analysing the current situation. Blockchain offers creative solutions to trust-related issues in the design of 6G networks. Blockchain-powered 6G connections can effectively manage resource sharing, improve privacy and security, and offer safe access control and authentication. The security concerns that they pose risks to the IoT system are not adequately addressed. Changxiong Yang et al. [15] presented an editable blockchain technique for preserving agricultural product traceability data. They claim that the immutability of blockchain technology limits the application of blockchain-based tracking mechanisms while rendering changing permissions for sharing information or removing inaccurate data challenging. The strategy enables businesses to encrypt data to safeguard privacy and adds chameleon hash software to provide data-altering capabilities. It employs a distributed block-releasing method to increase productivity and makes threshold release procedures easier to implement to prevent single failure point issues. The technology also establishes systems of accountability to identify bad actors. Accountability mechanisms have been implemented to detect malicious parties. The suggested system outperforms blockchain-based tracking remedies in terms of building blocks and granting speed. The proposed scheme offers more versatility in terms of data management and access control than conventional permanent blockchain. To overcome the shortcomings of the current agricultural item traceability structures, they proposed an editable method based on blockchain technology, with an emphasis on data updates, access control, and enhancing efficiency. The main loophole is data privacy concerns. Researchers point to the need for data protection and privacy.

Ghassan Faisal Albaaji et al. [17] explained that blockchain technology affects Iraq's food supply systems and farming. It outlines initiatives and projects; discusses the broad ramifications, difficulties, and possible advantages; and evaluates the project's maturity. Blockchain technology has promise for establishing an open food supply network and offering a trustworthy source of information regarding the conditions of farms, agricultural contracts, and stockpiles. Many initiatives are in motion to use blockchain technology for a variety of food products and problems. A more comprehensive AI-based framework that incorporates blockchain technology has a great deal of potential to be more effective. The farming industry and farms themselves are nevertheless hindered by several issues and limitations that prevent widespread implementation. Their study investigated the possible advantages of using blockchain technology architecture to improve food safety and implement sustainable agricultural practices through increased transparency, traceability, and data management. It uses a case study to investigate the uses and implications of a distributed ledger framework for Iraqi agriculture. Blockchain innovation can create an open food supply chain and provide a reliable source of information about agricultural stocks, conditions in the agricultural sector, and other related issues. Several projects are underway to use blockchain technology for a range of food products and problems that the Iraqi agriculture sector faces. AI-based frameworks and blockchain integration have considerable potential for success. Agricultural systems and their widespread use among farmers still face several challenges and barriers. There are potential negative gaps that widespread adoption of blockchain technology could have on food supply systems and agricultural practices in Iraq. More research and analysis may be needed for stronger hash algorithms. A named data networking (NDN), which is a data network security method based on blockchain-based and certificate-less electronic signatures, was proposed by Li Bing et al. [18]. CLDS-B, or the "Secure Mechanism backed up by certificateless Digital Signatures and Blockchain," is the name of their proposed system. To guarantee data integrity and authentication in NDN networks, CLDS-B employs certificateless digital signatures. To stop the use of fake public keys, CLDS-B ties the data identifier to the public key and resolves the issue of key exposure to private keys. Blockchain technology is used by CLDS-B to manage cryptographic data decentralizedly, making it resilient to single failures of nodes. Do not need a certificate to use a digital signature. To manage decentralized cryptographic data, blockchain technology is employed. While it is marginally less effective than other secure NDN systems, CLDS-B simulations demonstrated that it beats a standard NDN system. Security investigations and verification demonstrated the resilience of CLDS-B to key divulgence threats. In situations where a high degree of security is necessary, CLDS-B is regarded as a competitive solution. Nonetheless, complex procedures in their proposal lead to performance measures that may be less effective.

Amal Abdel-Ahmadi et al. [19] identified distributed denial of service (DDoS) assaults in IoT networks and provided an overview of recent research on the use of machine learning (ML) and deep learning (DL) models. They studied the overview of IoT devices, security issues, and the connection between fog and cloud computing for the IoT. The value of DDoS attack detection in IoT networks is identifying DDoS assaults with ML/DL and other approaches. Nonetheless, it examines recent research that has employed various ML and DL models to identify denial-of-service threats in the IoT, including supervised learning models (e.g., decision trees, random forests, and support vector machines). Models of unsupervised learning, such as anomaly detection and clustering. They studied deep learning models, including convolutional and recurrent neural networks. The combination of several ML/DL models can increase the accuracy of detection. One of the main challenges is the lack of representative and complete IoT-DDoS datasets. The resource limitations of IoT devices can be addressed by integrating fog/edge computing with ML/DL models. The main problem that researchers have not yet been able to solve fully is the lack of comprehensive and high-quality datasets for training and evaluating machine learning and deep learning models to detect various attacks in IoT networks. Table I shows the results of previously proposed methods.

Table I**.** PREVIOUS PROPOSED WORKS

Study and year of publication	**Used methods**	**Drawbacks**
C. Jacolin et al. [1], 2022	Using deep learning and machine learning methods to detect plant diseases.	More research and development are still needed to find effective solutions based on machine learning and deep learning to accurately and reliably monitor and diagnose plant diseases.
Li et al. [2], 2020	The solution was based on using the elliptic signature over an entire curve.	The researchers did not mention any specific evaluations or comparisons of performance and did not analyse the security of the proposed system.
Chatterjee and Singh [3], 2023	They have adopted an agriculture system that includes group signatures and blockchain.	The researchers did not enhance security or address possible attacks on the system. Additionally, the group signature technique is very expensive to perform for EAA-IoT applications.
Taji and Ghanimi [4], 2024	Researchers depended on homomorphic signcryption based on hyperelliptic curves (HEC) for IoT-enabled agriculture.	Their system lacks the features offered by blockchain such as management, distribution, transparency, and integration, which indicates that their system relies on traditional methods. Additionally, the problem of using a signcryption has some limitations and drawbacks in its implementation, including the complexity of the algorithms and infrastructure to create and verify the signature.
Aljabri et al. [5], 2024	They used blockchain and RSA in their system.	Using RSA signatures means that the minimum length of the keys used is 1024 bits, which will negatively affect their

		system’s performance. Additionally, another problem is the modification of sensitive data big threat to data stored on servers.
Yourong Chen et al. [6], 2021	Researchers used the Pareto Artificial Bee Colony (PABC) algorithm to optimize the revenues of offensive mining pools and miners subject to ban attacks in blockchain networks.	The main problem is mitigating the effects of ban attacks on the revenues of the mining complex and not eliminating the attacks against the system. Striking this delicate balance appears to be an ongoing challenge that the researchers were not able to fully resolve in this work.
Kumar, and Bandanadam [7], 2024	It uses EL-GAMAL and BCT-based public auditing system.	EL-GAMAL algorithm with long keys is expensive for systems performance overhead. In addition, the authors did not provide an analysis of important parameters in electronic applications such as entropy and scalability. Additionally, in their proposed system, they dealt with hacking attacks but did not present the results of their analysis.
Vardhan et al. [8], 2024	Dynamic agricultural data produced by internet-connected loT devices and blockchain was adopted that includes advanced AI principles, IDPS, and honeycomb.	Their proposed system did not rely on a robust signature algorithm that prevents data tampering attacks. Moreover, their system's security against the latest attacks was not analysed to prove it through applicability in the context of EAA-IoT.
Arvind Panwar et al. [12], 2023	The study used the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology to conduct a systematic review of the literature on BCT applications in the agricultural sector.	The main problem is that scalability needs to be addressed for the effective application of blockchain technology in agriculture. Scaling blockchain solutions to handle high volumes and complex processes for the agricultural sector remains an ongoing challenge.
Hassan Khan et al. [14], 2024	Using blockchain to enable 6G services in the areas of resource sharing, integrity, confidentiality, access controls, and authentication.	Not treated adequately security concerns that they pose risks to the IoT system.
Changxiong Yang et al. [15], 2024	This technology offers the Chameleon hash, which provides the ability to change the recorded data if necessary.	The main problem is data privacy concerns. Researchers point to the need for data protection and privacy.
Ghassan Faisal Albaaji et al. [17], 2024	Use of blockchain technology to create a more transparent and accessible food supply chain by providing a distributed and decentralized ledger of information.	Negative potential gaps that widespread adoption of blockchain technology could have on food supply systems and agricultural practices in Iraq. More research and analysis may be needed.
Li Bing et al. [18], 2024	Using blockchain technology CLDS-B uses blockchain technology to manage cryptographic data in a decentralized manner.	The main research problem is that performance measures may be less effective.
Amal Abdel-Ahmadi et al. [19], 2023	Methods used to detect Distributed Denial of Service (DDoS) attacks in IoT networks using Machine Learning (ML) and Deep Learning (DL) models.	The researchers have not been able to solve yet fully is the lack of comprehensive and high-quality datasets for training and evaluating machine learning and deep learning models to detect DDoS attacks in IoT networks.

3. E-AGRICULTURE BACKGROUND AND SIGNATURE METHODS

This section provides a brief background on security techniques in e-agriculture.

3.1 Consortium Blockchain

Blockchain consortia may offer a wide range of advantages and uses in the context of IoT and e-agriculture applications. The safety and provenance of agricultural products and foods may be tracked from field to table via blockchain technology to establish a transparent and shared record. The provenance of agricultural products, manufacturing, distribution, and storage procedures, as well as details regarding safety and quality, are readily available to farmers, manufacturers, product distributors, and final customers. Distributed resource administration water, land, and agricultural equipment are examples of common resources in agriculture that can be distributed and organized via blockchain technology. Participants in the blockchain network may swiftly and openly carry out the operations of registration, verification, and distribution in addition to having access to precise data about resource utilization. Precise observations of the environment and climate farms can use technology to collect data from connected sensors, such as systems that monitor the quantity of fertilizer, humidity, and temperature. These data are kept on a shared blockchain so that researchers and farmers may analyse and use them to make more informed choices on the basis of estimations of changes in the climate and the environment around them. By increasing food safety, it is possible to build an extensive system that guarantees food safety via blockchain technology [20, 21]. Blockchain technology makes manufacturing, transportation, retention, and verification data captureable. It is a helpful tool for monitoring and identifying leading sources as a result. Blockchain can be used to develop a comprehensive framework that guarantees food safety, which will increase food safety. Blockchain is a useful tool for tracking and locating possible origins of food contamination because it stores data on production, distribution, conservation, and verification. IoT-connected sensors can also focus on transportation and storage conditions, helping to identify health issues while they have a chance to affect the quality of food. Facilitation of financial transactions: Blockchain technology has the potential to simplify agricultural industry acquisitions. Smart contracts that are built around cryptocurrency and blockchain technology can be used to create digital payment systems. Farmers, buyers, and suppliers can all carry out quick, easy, and transparent financial transactions [22]. When used for e-agricultural applications, the use of blockchain has the potential to greatly increase process transparency, efficiency, and security in the agricultural industry. Increasing agricultural output, producing better-quality items, and enhancing food security are achieved through improving cooperation among relevant parties and offering accurate and dependable data sources.

3.2 Advanced Deep Learning (ADL)

A subfield of machine learning called "advanced deep training" analyses enormous amounts of data and applies neural networks with deep connections to address challenging issues. The general quality, productivity, and efficiency of the e-agricultural industry could be enhanced by the implementation of deep learning techniques. Deep neural networks can be used to identify pests and diseases of plants. This enables the system to identify ailments accurately and respond quickly to treat them. Agricultural yield and performance forecasting. Deep learning systems can forecast possible yields and enhance yield projections by integrating past information with water, soil, and climate factors. To accurately predict future crop yields, algorithms that use deep learning can be employed to assess complicated correlations between several factors. By regulating itself and analysing the farming system, deep neural networks can be used to handle ecological management systems and irrigation for the benefit of agriculture. Deep learning models are constructed using sensor data, such as humidity, light, and temperature data. These models enable the best possible productivity through decision-making and environmental control [23]. Deep learning evaluation of sensors and data collection can maximize the use of farm assets such as water and fertilizer while consuming more resources. Deep learning algorithms can identify trends in resource consumption and provide targeted recommendations for increasing output and reducing waste.

3.3 Artificial Bee Colonization (ABC) Algorithm

Maximizing efficiency is the aim of the strategy used to artificially and naturally pollinate crops with constructed colonies of honey in digital crops. The application of blockchain technology improves immunization process security and transparency. The artificial bee settlement hypothesis, which uses artificial bees to spread pollen across plants, is the foundation of the algorithm. Because these robotic bees are equipped with sensors and Bluetooth, they are able to identify specific plants and precisely document their state [24]. These data are kept in a distributed file system to guarantee both security and transparency. These data can be used by researchers and farmers to assess how better pollination techniques can increase agricultural productivity. Blockchain technology also offers a way to verify the existence and identity of robotic bees in the field. They can also be used to guarantee the authenticity and quality of agricultural products by tracking them.

The replica bee colony is made up of three kinds of bees: scout bees, which randomly look for food; employed bees, which are linked to specific food sources; and observer bees, who watch the hired bees move in the hive to obtain food. Scout bees and observers are included in the group of unemployed bees. Finding all available food sources is the first job assigned to scout bees. Then, both working and bystander bees take advantage of the sweetness of sources of food, and eventually, this unrelenting exploit will wear them out. After that, a worker bee, when the food supply runs out, becomes a scout bee, searching for a new food source. The amount of honey in the food supply is associated with the quality (fitness) of the practical solution, which is the position of the source of nourishment in this metaheuristic algorithm [25]. The total amount of sources of food and hired bees is often equal because each hired bee is linked to a single food source (solutions).

3.4 Ed25519 Signature

One kind of digital signature used in the field of digital security is the Ed25519 signature [26]. Blockchain technology, which is the foundation of many electronic agriculture applications, is utilized. Blockchain technology is an information recording system that uses a network of interrelated blocks to securely and openly record information. Each block on the blockchain is signed by digital signature technology, which ensures the security and authenticity of the data. The digital signature technique known as Ed25519 is based on the extreme Kirby curve, and its compact switch size and quick processing speed make it suitable for use in high-performance applications, such as agricultural electronic applications. In regard to electronic farming, the Ed25519 signature can be used for several purposes. It can be used to sign sensitive information regarding agricultural productivity or crops, enable data verification, and stop data manipulation. Increased security and trust in the transmission of information and digital recording of agricultural activities can result from the use of the Ed25519 signatures on the basis of electronic applications for agriculture.

3.5 IoT with E-Agriculture Application

Since it is directly linked to and improves farming and crop management, the network of things, or IoT, is regarded as one of the technologies utilized in the field of computer applications in agriculture (e-agriculture). Sensors and devices that gather and exchange various types of agricultural data have connected the Worldwide Web with Things, or the IoT for brief, to computer programs for agriculture or e-agriculture [27, 28]. For farms, agricultural fields, and other locations, data are gathered and transformed into information that can be evaluated and comprehended. Using this information for better oversight of their crops, farmers can decide whether to irrigate their crops, how to take care of their vegetation, and how to effectively control pests. In response to continuous sensor data, this system can modify the temperature, water distribution, and lighting. Farmers and agricultural experts can communicate with one another online and share advice and knowledge, which can improve farming practices and increase productivity. The Internet of Things, also known as the IoT, technologies have been combined with e-agriculture apps to improve the management of crops and production by making it easier to collect, monitor, analyse, and use agricultural data. This technology helps increase agricultural productivity and offers creative alternatives.

4. A NOVEL METHOD FOR E-AGRICULTURE EMPLOYING MODERN TECHNOLOGIES

In this section, we present an enhanced system that employs Ed25519 signatures and the ABC algorithm along with proprietary blockchain technology and cutting-edge deep learning to track the provenance of food commodities in the agricultural products sector. Well, give a quick overview of electronic farming techniques. Figure 2 generally describes the proposed methodology and the role of the adopted algorithms in the proposed system. First, the ADL algorithm is used to analyse the collected data related to electronic agriculture. The deep learning algorithm helps extract complex properties and patterns from data, leading to a deeper understanding and more accurate predictions. ADL can reveal subtle relationships and trends within e-agriculture data. Ed25519 is used as an efficient digital signature algorithm to ensure the integrity and authenticity of the data contained in each block in BCT. Ed25519 provides efficient and secure digital signatures to protect blocks from tampering or unauthorized alteration. This algorithm helps maintain the integrity of e-agriculture-related data within each block in the collected data. By simulating the foraging behavior of bees, the ABC algorithm can find optimal solutions for the data and improve the accuracy of the analysis. The ABC algorithm parameters are associated with keys to generate signatures. Private keys and e-farming parameters are used to create digital signatures. These keys and parameters ensure the authenticity and integrity of the data associated with e-agriculture. It uses these parameters as its input. ABC parameters such as colony size, learning rate, and number of iteration cycles are set and optimized via these keys and parameters. After digital signatures are created via private keys and parameters, these signatures are added to blocks. The improved ABC parameters ensure the accuracy and reliability of the digital signatures associated with each block. This leads to increased safety and security of data stored in blocks related to EAA-IoT.

4.1 Examining Dataset-Based E-Agricultural Application

There are numerous advantages to using IoT technology in e-agriculture applications. Temperature, humidity, and illumination are just a few of the variables that may be measured with electronic and digital sensors. To make precise predictions, quick learning techniques are applied to the data analysis. The environmental conditions and plant needs are considered when intelligent electronic computers are used. By timing the water flow at the ideal moment, the flat ring helps maximize irrigation effectiveness and reduce water use. Assets in agriculture may be tracked via radio frequency identification (RFID), sensing, and Internet technologies because they allow for exact location and condition tracking, which improves supply chain and warehouse management. Through the process of gathering sensitive data online and organizing them into datasets, farmers can acquire important information regarding crop performance and the factors they wish to create. Changes in industrial engineering, agriculture, and the environment can be made with the use of these datasets. To diversify agricultural production, enhance quality, and lower finite expenses such as water, we use Internet apps with agricultural applications. Members will also be able to adopt a data- and analytics-driven approach. Since kaggle.com provided the datasets for our preliminary assessments of the suggested approach, we utilized them in our research [15].

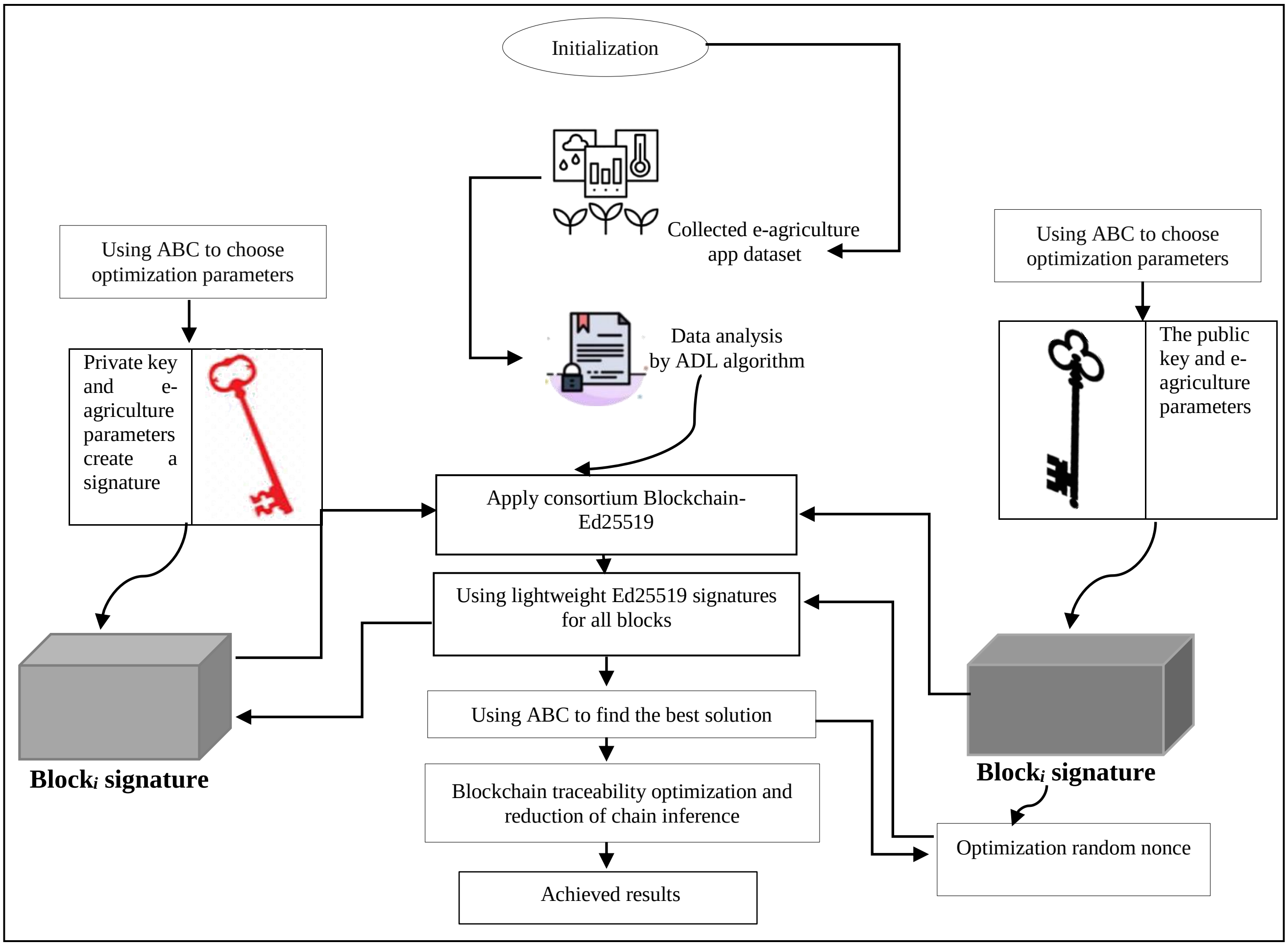

Initialization
Collected e-agriculture app dataset
Using ABC to choose optimization parameters
Using ABC to choose optimization parameters
Private key and e-agriculture parameters create a signature
Data analysis by ADL algorithm
The public key and e-agriculture parameters
Apply consortium Blockchain-Ed25519
Using lightweight Ed25519 signatures for all blocks
Using ABC to find the best solution
Blockchain traceability optimization and reduction of chain inference
Achieved results
Block$_i$ signature
Block$_i$ signature
Optimization random nonce

Fig. 2. General proposed methodology for e-agriculture applications

4.2 Advanced Deep Learning (ADL)

Conventional deep neural networks have limitations. Advanced depth architecture for intelligent action (ADL) fills these gaps. These transitory connections enable nonsequential information to move between layers by transferring data between nonadjacent layers. The network can handle big data and more complex problems more easily because of these horizontal links. The ADL architecture's nonsequential deep neural network design makes use of several parallel channels for information flow, improving model performance. We propose the integration of these modern methods. We integrate blockchain technology with the worldwide web of things, IoT, and ADL. To estimate food demand and supply, we provide a hybrid model that combines techniques from a genetic algorithm (GA), a recurrent neural network (RNN), and prediction models such as long short-term memory (LSTM) and a gated recurrent unit (GRU). Furthermore, we simultaneously tune this hybrid model parameter. Hundreds of kilograms of agricultural produce are transported daily from various farmer markets to towns, where they arrive at centers for dealing with and purchasing bulk agricultural goods. The proposed method uses blockchain technology to create online documentation for each food product, ensuring safety. Users may easily obtain information on the product market, cost, manufacturing, quality, and other aspects through the system. Using the Worldwide Web of Things for e-agriculture applications has many benefits. Electronic and digital sensors can identify several factors that affect plant growth, such as temperature, humidity, and sunlight. By adding horizontal and cross-layer connections, the advanced depth infrastructure for smart action (ADL) expands the capabilities of traditional deep neural networks. By sending data between nonadjacent levels, these transitory connections allow nonsequential information to flow between layers. This architecture's horizontal connectivity allows it to address more complex problems and larger data volumes with greater efficiency. Model performance is improved by using many parallel channels for information flow, which is made possible by the network's deep, nonsequential design. We suggest fusing these modern techniques with blockchain and IoT technology. We suggest the use of a hybrid model based on RNN algorithms along with a cutting-edge GA and prediction models such as the GRU and LSTM to estimate the supply and demand for food. Weighted example techniques are used to optimize these hybrid model parameters. There are numerous advantages to employing the IoT in e-agriculture applications. Temperature, humidity, and sunlight are a few examples of variables that can be detected via electronic and digital sensors to impact plant growth. To examine the data, deep learning methods are used. Smart e-agriculture systems that leverage the IoT can incorporate sophisticated deep learning methods such as LSTM, CNN, and GRU. Temperature, humidity, light level, and plant conditions are just a few types of agricultural data that may be gathered by IoT-connected sensors. Important patterns and elements in these visual data, such as pictures of plants or the agricultural landscape, can be identified via CNNs. Using LSTM networks, time series analysis is performed on agricultural data, including temperature and humidity data, over time. This aids in anticipating alterations in the surrounding environment and notifies farmers beforehand. The GRU is used to make wise decisions. To make informed agricultural decisions, sensory data and future projections are integrated via GRU networks. The GRU, for example, can be used to find the best time for projections via current data. The merged CNN, GRU, and LSTM parts form an integrated deep learning model. The program generates recommendations for agriculture or early warnings on the basis of inputs of IoT-sensed data. With this integrated approach, e-agriculture applications based on the IoT can benefit from the advantages of each deep learning technology. This approach has the potential to greatly increase agricultural productivity, accuracy, and efficacy. Algorithm 1 illustrates the use of ADLs in the proposed system.

Algorithm 1: ADL algorithm

```
Input
    Training agriculture dataset, test agriculture dataset
Output
    Dataset validation, neural network model
Training Data ← Collect training agriculture Data ()
Training Data ← Clean data (training Data)
Training Data ← Format data (training Data)
Split Data (training data, test data, validation data)
Model ← Design model ()
Training model (model, training Data)
Evaluate model (model, test data)
Adjust parameters (model, validation Data)
Predict new data (model)
```

4.3 Blockchain Consortium Foundation on Ed25519 Signatures

Our suggested e-agriculture solution uses blockchain technology in conjunction with Ed25519 signatures to offer a strong defense against attempts to counterfeit agricultural data. EdDSA (Edwards curve digital signature algorithm), which is based on indigo curve encryption technology, is the foundation for the Ed25519 digital signature method. The following justifies the widespread preference and usage of Ed25519 signatures in the suggested electronic agriculture. Ed25519 offers a very high degree of protection. They are built to resist powerful assaults from a variety of hostile attacks, including active strikes. Ed25519 offers excellent computational and resource efficiency. Its speedy creation and verification of signatures make it appropriate for use in a variety of applications, including those involving memory and processing-constrained devices. The network's member dedication to the event lends a high degree of legitimacy and dependability. Blockchain technology facilitates decentralized sharing, which is tracked across many networked devices and recognized by a registry. Blockchain provides resistance against illegal activity and data manipulation. As a result, network users can more easily agree and work together technically since the network registry is updated through collaborative decision-making and authority participation. One significant benefit of using agreement technology in blockchain is the generation of anonymous data. The network's members feel that encouraging contributions to group decision-making via communication fosters trust among users. Our suggested solution combines blockchain technology with Ed25519 signatures to offer significant protection against agricultural data fabrication threats. The Edwards curve digital signature technique, which is based on elliptic curve cryptography, provides the foundation for the Ed25519 digital signature technique.

For a number of reasons, Ed25519 is recommended and frequently utilized in suggested electronic agriculture. First, it has enhanced security because it is built to fend off a variety of threats, including active attacks and efforts to tamper with agricultural data, and Ed25519 offers a high level of protection. Ed25519 is distinguished for its high computational and resource-use efficiency. Second, it facilitates the quick creation and validation of signatures and can be applied to e-agricultural applications, even on devices with constrained memory and processing power. Authenticity and dependability. With Ed25519 signatures, the blockchain achieves a high degree of validity and dependability. Blockchain operates in a decentralized fashion, utilizing a distributed and interactive ledger to record participation and transactions among numerous devices that are part of the network. Figure 3 displays the blockchain structure of the proposed system. In addition to security and credibility, a high degree of credibility is achieved through the network participants' promise of the event being unable to be altered or faked: Utilizing Ed25519 signatures helps lower the possibility of agricultural data forgeries and manipulation. Digital signatures improve security and transparency in the agricultural system by enabling transactions to be validated and certified. Agricultural data forgery attempts can be thwarted with great security by using blockchain technology in conjunction with Ed25519 signatures. Ed25519 signatures can be combined with a blockchain in our proposed system to provide a reliable verification mechanism and high reliability in recording agricultural transactions and data on the network. Concepts related to digital signatures are formed via the Ed25519 system: Ed25519 is a digital signature system that is designed to provide high security and good performance. Ed25519 uses a public key elliptic curve25519 to create digital signatures. Hash: Hash functions are used to obtain a digital fingerprint of certain data. In Figure 3, the block structure contains several elements. First, hash numbers are indicated, such as “#2790 Hash”, “#2791 Hash”, and “#2792 Hash”. Each hash number contains a message digest that contains the hash output. These hash numbers are used to uniquely identify the data. The hash output is used to verify data integrity. ABC private key and ABC public key: A private key is used to sign data. The public key is used to verify the authenticity of the digital signature. ABC is used in our proposal to support random optimization of keys. After that, the hash and keys are used to generate Ed25519 signatures, thus protecting the block data from changes and tampering. “Track ABC blocks” refers to following or tracking specific blocks. "Time for necessity, ABC random nonces" refers to the use of random numbers for certain purposes to maintain confidentiality or security. All of these above elements are included in e-transactions. In the second block, the e-transaction elements of the first block are verified. The validity and integrity of these transactions should be verified; otherwise, the block is rejected. Finally, the quality of training conducted on the system is evaluated via ADL. Algorithm 2 shows the merging of Ed25519 signatures with the blockchain into a system. Table II lists the types of blockchains that are based on the Ed25519 signature [29, 30, 31].

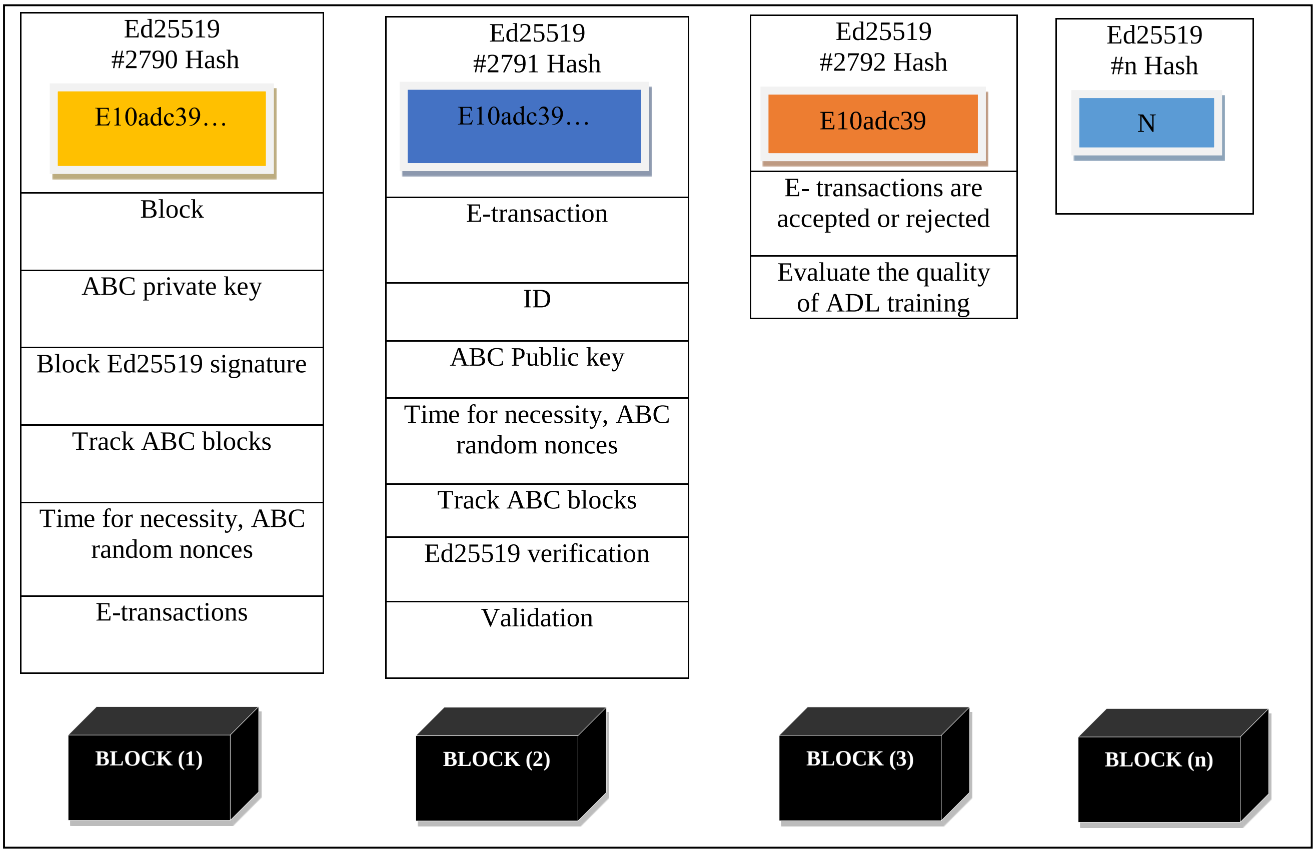


Fig. 3. Block structure in our proposed system

```
Algorithm 2: Ed25519 is signature with blockchain
Input
   Block e-agriculture parameters, agriculture data
Output
    verification Block parameters
  Private Key ← Generate Private Key ()
  Public Key ← Generate Public Key (Private Key)
 //Sign the agriculture data using the private key
  Hash = Hash Function (agriculture data)
  $r$ ← Scalar Multiply (Base Point, private Key)
  $s$ ← (hash + $r.x$) * Inverse (private Key, Modulo)
  Send block Ed25519 signature to next block
 //Verify the signature using the public key
  Hash = Hash Function (agriculture data)
 Is Valid = Verify Signature (Public Key, message, ($r$, $s$))
       if it is Valid: "The signature is valid"
       else: "The signature is not valid"
```

Table II. CLASSIFICATION BLOCKCHAIN BASED ON THE SIGNATURE

Blockchain Types	**Description**
Public	• It is consistent with signature nature as a distributed and transparent technology. They provide easy access and sharing for farmers and consumers. However, they may be complex and slow for some e-agriculture applications that require fast transaction speeds. • There are few privacy safeguards and transactions and data are exposed to the public. • Signatures are considered secure, but they may be more vulnerable to certain attacks, such as hash attacks, compared to newer signature schemes.
Private	• Customizability for agricultural needs, transaction speed, and access control. However, more centralized, it may be less transparent for consumers and less compatible with the Ed25519 signature. • Because all transactions and data are managed by the organization, it provides the maximum level of privacy. • Although the signature algorithms employed in consortium blockchains provide more sophisticated security protections than those used in private blockchains, they are nevertheless widely regarded as safe.
Consortium	• It has flexibility in customization, speed of transactions, and a degree of decentralization and transparency. It matches well with the signature nature of Ed25519. Best suited for e-farming applications with the use of Ed25519 signature may be the consortium blockchain. It provides the right balance between customization and speed on the one hand, and transparency and decentralization on the other hand. It also aligns well with the nature of Ed25519 signature as a distributed and secure technology. Consortium blockchain provides advantages over public blockchain such as improved scalability, enhanced privacy, and faster finality. While consortium blockchain provides advantages over private blockchain such as improved access control, data confidentiality, and efficiency. • Because transactions and data may be limited to approved parties, it provides superior privacy control. • Strong security features including ease of implementation and resistance to various attacks are provided by these signature algorithms based consortium blockchain.

4.4 Algorithms for selecting the best possible method for selecting bee colonies

The algorithms are inspired by how bees consume nectar. They collaborate or work in groups to gather the most nectar possible. Without an automated central control system, the outcomes can exercise the complex system and carry out the operation process. There might be a different, more successful solution. The block result optimization problem is solved via the ABC algorithm. By creating a group of artificial bees that represent the potential keys of the signature, the ABC could optimize the key parameters in the Ed25519 signature. The artificial bee signature is first encrypted via a random key, and then its performance is assessed via performance metrics, including key size and security strength. Several times until the best key is picked and used as the solution for the signing procedure, the key with the highest performance criterion value is chosen. Additionally, to support the security of agricultural keys and data, we use ABC in our proposed system to create random and optimum nonces. Additionally, the asset securitization of agricultural records via blockchain and ABC lowers the risk of leakage and enhances the security of agricultural data. The interests of farm enterprises must be protected, which is very important. A blockchain is used, with numerous dispersed nodes taking part. The solutions discovered by the ABC are signed via Ed25519 signatures. Additionally, the proposed system uses ABC to find the best block positions for agricultural data and traceability optimization to reduce chain inference. Algorithm 3 shows the use of ABC with Ed25519 signatures in our proposed system. In general, there are several algorithms for obtaining optimal solutions, such as tiger beetle optimization (TBO) [32] and particle swarm optimization (PSO). Table III shows a comparison of ABC, TPO, and PSO [33, 34] and explains the reasons for choosing ABC. It is clear from the table that ABC is the best suitable choice for our proposed system.

Algorithm 3: ABC algorithm with Ed25519 signatures

```
Input
    Problem, criteria, solution array, bee array, agriculture data
Output
    the best solution, random nonces, random keys pair
 1 Define the problem or improvement required in the electronic agriculture system
     problem ← 'Improve crop production';
 2 Define the criteria and variables that will be used to measure the quality of solutions
     criteria ← 'Productivity, resource efficiency, water availability, cost, biodiversity';
 3   Represent the potential solutions using artificial bees in the colony
      Set Length (solutions, Num Solutions);
      Loop NumSolutions
         solutions[i]: = Generate Solution ();
  4 Evaluate the proposed solutions using the defined criteria
      Loop NumSolutions
          Evaluate Solution(solutions[i])
  5 Update the positions of artificial bees based on the proposed solutions and their evaluations
      Loop NumSites-1
          sites[i]. Update Site(solutions)
  6 Repeat the process to obtain the optimal solution
      Loop Num Iterations
        Loop NumSites
            sites[i]. Search ()
  7 Analyse and document the results
     Best solution ← Get the best solution (solutions)
     Analyse and document results (best solution)
  8 Assigning the best solutions to Ed25519 and blockchain
     Private key ← best solution, public key ← best solution
     Block traceability ← is the best solution, random nonce ← best solution
```

Table III. COMPARISON OF THE ARTIFICIAL BEE COLONY ALGORITHM AND THE NEW TIGER BEETLE ALGORITHM, BASED ON THE SIGNATURE OF ED25519

Artificial Bee Colonizes (ABC)	**Tiger Beetle Optimization (TBO)**	**Particle Swarm Optimization (PSO)**
It is characterized by a more random nature in searching for solutions due to imitating the behavior of artificial bees.	It is characterized by a less random nature due to imitating the hunting behavior of predatory beetles.	Fish schools and bird groups' social dynamics provide inspiration for PSO which is characterized by a less random nature.
Produces more diverse solutions due to the random behavior of the bees.	This may produce less diverse solutions due to the focus on catching prey.	PSO might lead to a narrower range of solutions being investigated, particularly if the particles converge in one area of the search space.
May be more stable due to diversity in solutions and avoid falling into local solutions.	May be less stable due to the focus on hunting and falling into local solutions.	In PSO, the exploration depends on the particles' ability to move around the search space, which may be more susceptible to the specific parameter settings and the convergence behavior that less stable of the algorithm.
Enjoys high performance.	Performance is less than ABC.	Performance is less than ABC.
Security is high and on par with the New Tiger Beetle Optimization (TBO) Algorithm	Security is high and on par with ABC Algorithm	Security is less than ABC and TBO.
Numerous optimization issues, such as function optimization, scheduling, and engineering design, have been effectively solved with ABC.	TBO has not yet been researched and used to the same extent as ABC.	PSO has not yet been researched and used to the same extent as ABC.
ABC is more robustness.	TBO is less robustness than ABC and PSO.	PSO is more robustness.

5. SECURITY ANALYSIS

In this section, we demonstrate security analysis through attack analysis and testing of the Scyther verification tool.

5.1 Attack analysis

- **Jamming Attacks:** This attack impedes or interrupts the blockchain data transmission mechanism. A blockchain impact can occur when a jamming attack causes blocks to be lost or delayed in the system. Our solution employs consortium blockchain technology to thwart jamming attempts.

- **Selfish mining attack:** Increased benefits for attackers at the expense of other users of the system are the goal of this attack. To increase their chances of deciphering the upcoming blocks and mining more money, attackers choose to keep the blocks they discover rather than broadcasting them to the network. This weakens the blockchain's general safety and effectiveness and compromises the system. By leveraging the Ed25519 signature method and the synthetic bee colony algorithm, our method prevents selfish mining attacks and improves system performance.

- **Block discarding attack:** During this assault, network administrators reject valid blocks that are displayed. As a result, attackers have the power to select which blocks are uploaded to the chain and to reject legitimate transactions. The system's ability to consistently secure and carry out transactions is jeopardized by this attack. Our approach prevents data modification in the online Farm Stuff network by using the Ed25519 signature, thus facilitating the block-discarding attack.

- **Block withholding attack:** Hackers disable network advertisements for the components they find during this attack. Instead of broadcasting the block to share it with other miners, they keep it to themselves. Because they can mine more blocks while running against resistance, this increases their chances of earning more money. This strike upsets the system equilibrium and disrupts the usual block completion procedure**.** Our approach employs a sophisticated deep-learning algorithm to counteract block-withholding assaults.

- **Uncle-block attack:** This attack makes use of the blockchain uncle blocks. Our method prevents manipulation of Bechtel data in the IoT system by employing artificial bee colony techniques and the Ed25519 signature to counter uncle block attacks.

- **Inference attacks:** Seek to retrieve private data from the system by using existing data or inferences drawn from it. Hackers can extract sensitive information with the aid of inference attacks. Our system employs the ABC algorithm to thwart inference assaults.

5.2 Security Analysis via Scyther

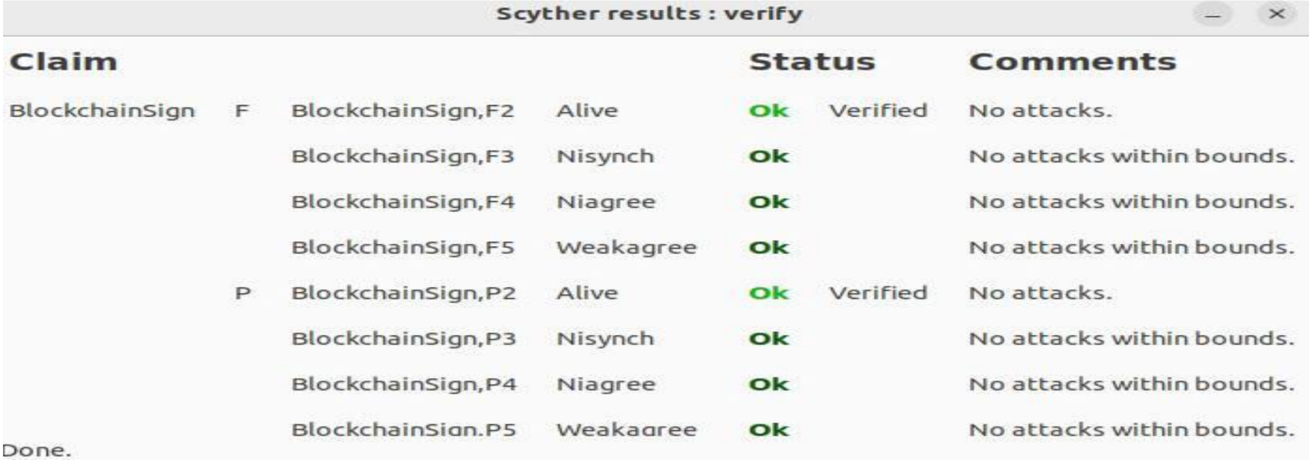
We make use of Scyther, an effective tool for cryptographic protocol validation. Owing to its sophisticated features, this application can lead to quick verification and tracking of attacks. Without the need for approximation approaches, it efficiently verifies the majority of procedures for an infinite number of meetings and ensures that all attacks detected are genuine assaults on the model. Scyther allows users to undertake unrestricted verification or identify attacks. Among various tools for protocol analysis, Scyther is unique in that it combines the benefits of model checking (attack discovery and terminating) and abstraction-based techniques (unrestricted validation) or argument proving. Moreover, Scyther has cutting-edge capabilities such as complete profiling and attack selection that are absent from other programs [35]. It can be used as a graphical user interface, a command line interface, or a backend for analysis programs that employ Python interface functions. To detect attacks on information and confirm the authenticity and confidentiality of that information, Scyther analyses security requirements for a range of protocols. This information can be used for production or consumption processes, transmission and reception between F and P, or between businesses or organizations. This tool verifies signatures, verifies particular signatures, and uses data via attributes that adhere to security standards, such as Weakagree, Nisynch, Alive, and Niagree.

5.2.1 Scyther and E-Agriculture Blockchain Apps

We evaluate our proposed method's effectiveness with the Scyther tool. We used the Security Protocols Describing Linguistics (SPDL) in the Scyther software to obtain our protocol roles ready for analysis. Here, we communicate to the F and P servers via a sequence of commands. To facilitate communication between entities and validate security needs, we simulate our suggested protocol between role events. Weakagree, Nisynch, Niagree, and Alive are among the tested events. Scyther transmit () and rec () instructions allow us to evaluate e-farming requests and identify potential security flaws or attacks. Our protocol satisfies security criteria, as evidenced by the findings. Protocol security is achieved by the use of digital signatures, which guarantee information secrecy and availability for all involved parties. This data contract specifically relates to commitment. In our proposed protocol, for example, F and P agree to share a specific set of information, and the grower and farmer's details are shared as follows: The proposed protocol achieves assurance of noninjectable agreement. The parties' message integrity can be guaranteed in this way. Nisynch: To ensure that the protocol is resistant to attack, the suggested protocol achieves a nonsynchronization guarantee.

5.2.2 Results of the Scyther Test

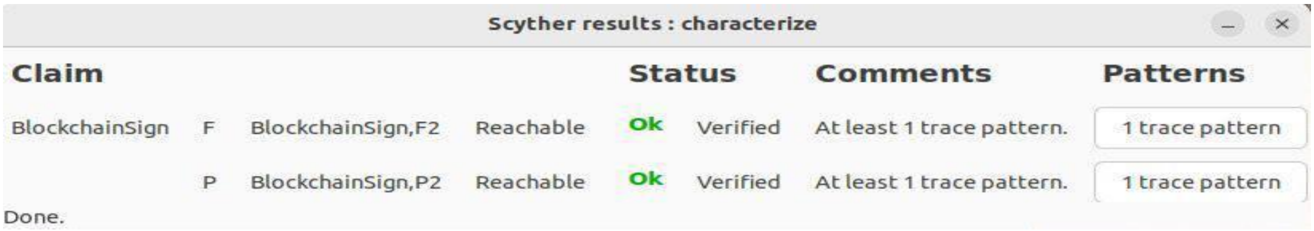
In this instance, we evaluate the e-farming technique suggested by the Scyther tool. The test results of our protocol for the events "Alive", "Niagree", "Weakagree", and "Nisynch" are shown in Figure 4. The test demonstrates the secrecy of the F and P requests, private keys (skP, skF), and public keys (pkF, pkP). It clarifies that the purchases are safe. Without any threats or attacks directed against the network entities, security parameters sent e-farming directives, or F data over the network, they are transferred between network entities (F and P). Our suggested protocol is resistant to attacks in the field of study. Figure 5 shows the results of the respective paradigms.



```
Scyther results : verify

Claim                                                    Status          Comments
BlockchainSign  F  BlockchainSign,F2  Alive        Ok    Verified   No attacks.
                   BlockchainSign,F3  Nisynch      Ok               No attacks within bounds.
                   BlockchainSign,F4  Niagree      Ok               No attacks within bounds.
                   BlockchainSign,F5  Weakagree    Ok               No attacks within bounds.
                P  BlockchainSign,P2  Alive        Ok    Verified   No attacks.
                   BlockchainSign,P3  Nisynch      Ok               No attacks within bounds.
                   BlockchainSign,P4  Niagree      Ok               No attacks within bounds.
                   BlockchainSign,P5  Weakagree    Ok               No attacks within bounds.
Done.
```

Fig. 4. Application of the Scyther tool to validate the suggested security protocol



```
Scyther results : characterize

Claim                                                Status          Comments                     Patterns
BlockchainSign  F  BlockchainSign,F2  Reachable      Ok    Verified  At least 1 trace pattern.    1 trace pattern
                P  BlockchainSign,P2  Reachable      Ok    Verified  At least 1 trace pattern.    1 trace pattern
Done.
```

Fig. 5. Description of the defined role in the proposed system

6. PERFORMANCE ANALYSIS

The proposed Java was used to implement system algorithms in Ubuntu 18.04.6 LTS. The PC in question has an Intel$^{(R)}$ Core$^{(TM)}$ i7-6600U CPU, which is the 9th generation, and 8.00 MB of RAM. We implemented all our algorithms 100 times in Java to evaluate them explicitly and extract results accurately. The numerical data obtained via Microsoft Excel sheets in Ubuntu were then analysed to create performance figures and graphs, which will be briefly discussed later. Figure 6 depicts the training and testing times of the advanced deep learning algorithm that helps us collect, analyse, predict, and extract data that we use in the field of electronic agriculture applications. Figure 7 depicts the Ed25519 signatures and signature validation of the proposed system. This process is repeated 100 times. From the results in Figure 7, verification operations consume less execution time than signature operations do, which is consistent with existing research results; the difference is that our Ed25519 signature implementation has adequate performance for e-agriculture applications. Figure 8 shows the operation of the ABC algorithm before and after the generation of the random nonces, random private/public, and block traceability optimization to improve its results and test it 100 times to evaluate the eligibility of this algorithm in supporting e-agriculture. In Figure 9, blockchain technology is used, information is stored in a set of blockchain blocks (1 block, 3 blocks, 5 blocks, 7 blocks, and 10 blocks), and the validity of information and changes is confirmed through a verification and approval process. The reduced security threats in EEA-IoT and the initial results were appropriate, as shown in the figures. Finally, Figures 10 and 11 show the performance of our proposed system, including the blockchain before and after ABC randomization of the system. Table IV shows a comparison of the parameters used in the proposed system and existing systems. In this table, we compare the performance parameters with those of existing systems that are closest to our research topic, even though the environments are different. The comparison clearly shows that our system outperforms modern quality systems in terms of entropy, network productivity and scalability parameters.

6.1 Entropy

In the context of digital signature algorithms, the word “entropy” is employed. The integrity and validity of digital data or documents online can be verified with the use of a digital signature. Standard deviation, or entropy, is a crucial component in digital signature algorithms. The potential noise or disorder in data is measured by entropy. Entropy is significant in the context of digital signature algorithms because the algorithms need to be able to produce distinct, random signatures for every message or document to make signatures hard to counterfeit. This can lead to the creation of signatures that are predictable or repetitive, which leaves signatures open to manipulation and falsification. To make digital signatures more secure, dependable, and challenging to forge, digital signature algorithms must use strong random sources and maintain a degree of entropy. The entropy rate in our system was 60.99 Mbps.

6.2 Network Productivity

The amount of data that can be sent over a communications network in a specific period of time is measured as the network throughput. It reflects the speed and efficiency with which data can be transferred over a network. The amount of data that is transferred over a network in a given period of time is referred to as the network throughput. The system's effectiveness and capacity depend on the use of the Ed25519 signature. Network throughput is affected by several factors, such as the speed of execution of the signature algorithm and the size of the signed data. Our proposed system has a network throughput rate of 200000.0 m/s.

6.3 Scalability

The capacity of a protocol or method to manage and adjust to increasing workloads or sizes of data is known as scalability. Scalability, as it relates to the ABC, is the algorithm’s capacity to manage a growing number of objectives or issues to be solved. The scalability of this algorithm is crucial. Problem scale. An algorithm’s capacity to handle large numbers of objectives or variables may be required when solving a problem with many other factors. There are several competing objectives in the problem that need to be handled simultaneously. Conserve time and money. Time and resources may be saved if the technique is successfully scalable. One scaled version of the algorithm can handle all problems, saving time and money by eliminating the need to run numerous independent versions of the algorithm to address different problems. The scalability rate of our system was 99.56.

Table IV. A COMPARISON OF THE PARAMETERS USED IN THE SYSTEM

Parameters	Proposed Protocol Ratio	Previous Research
Scalability	99.56%	31% in [36]
Entropy	60.99 Mbps,	Achieving entropy is challenging due to a lack of resources [37]
Network Throughput	200000.0 m/s	400 s [38] 300 s [39]

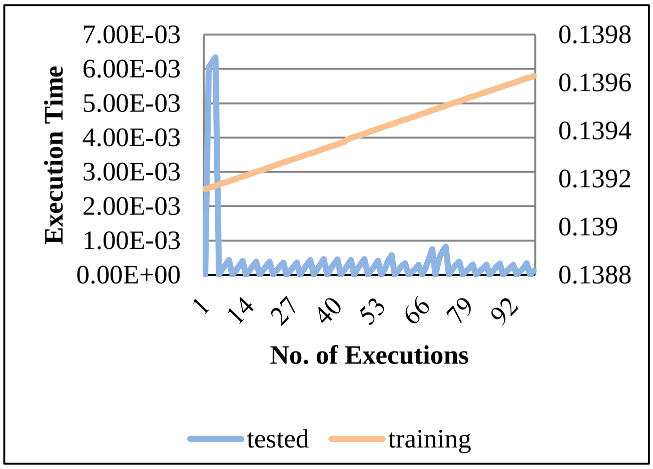


Fig. 6. Data analysis via advanced deep learning algorithms.

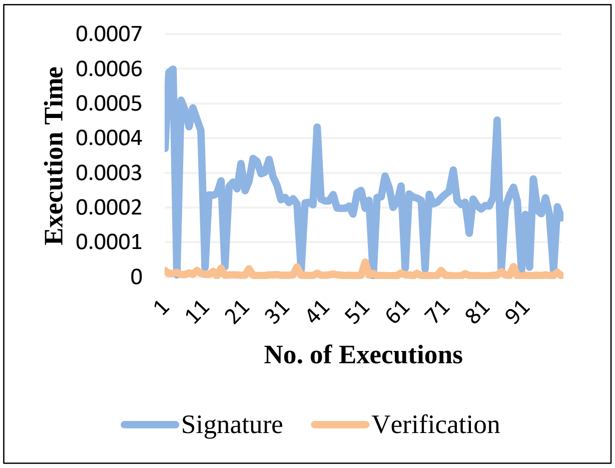


Fig. 7. Ed25519 operations for signature and verification.

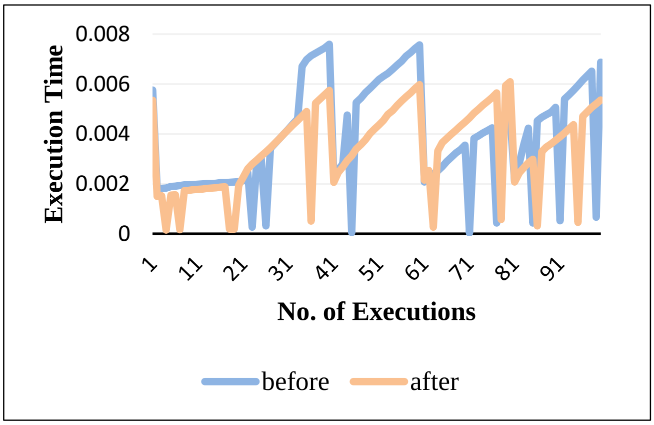


Fig. 8. Using the ABC algorithm and improving the system

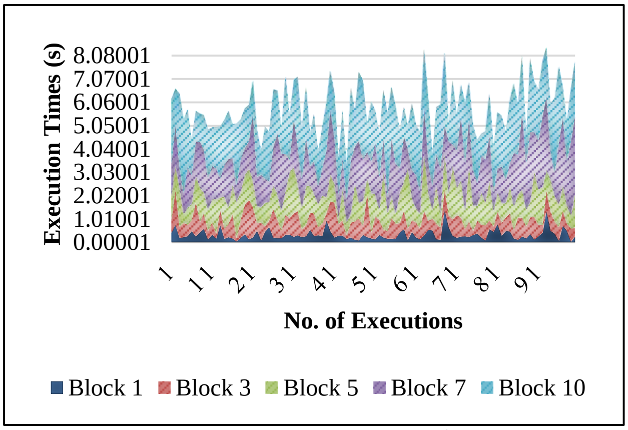


Fig. 9. Blockchain technology performance

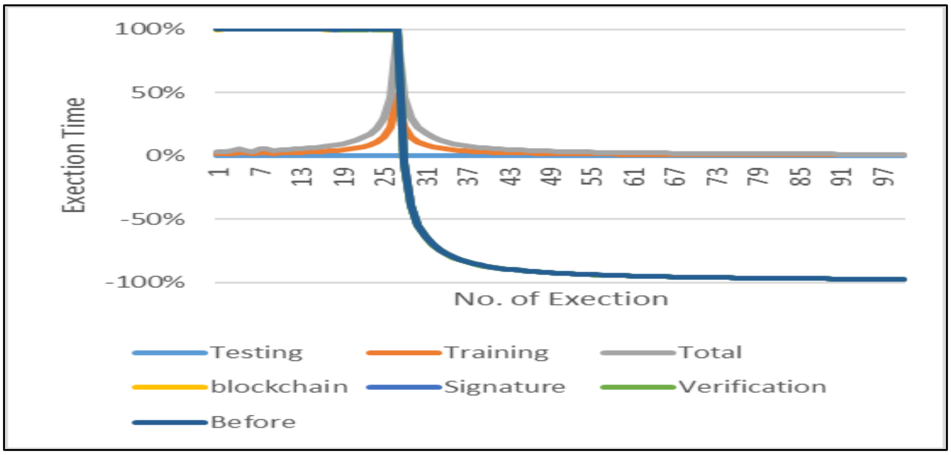


Fig. 10. System performance before ABC randomness

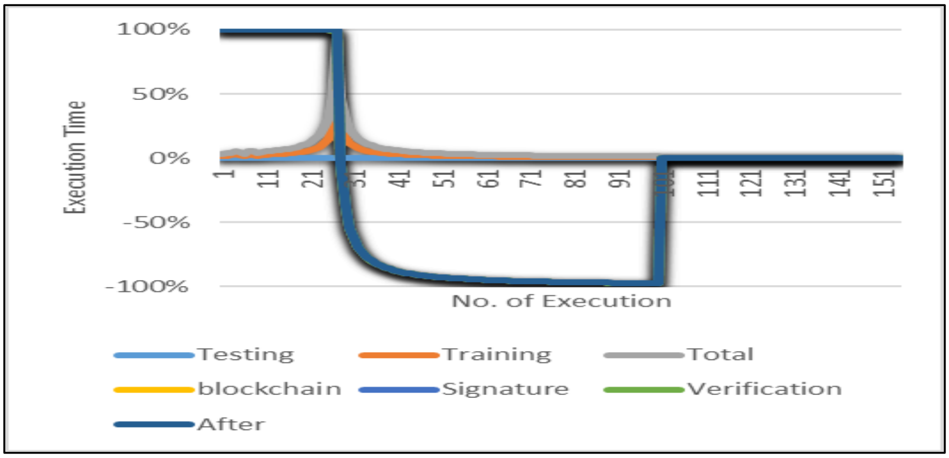


Fig. 11. System performance after ABC randomization

6.4 Study Limitations

EAA-IoT systems include several devices, such as computers and sensors. Our proposed system focuses on protecting the data of computers and servers and not sensors. Therefore, the first definition of our proposed system can be the performance metric of source-constrained sensors. For example, our system relies on Ed25519-SHA-512, which can be expensive for agricultural area data collection sensors, as an improvement to Ed25519 is required to accommodate the sensors. Our system was tested on 10 blocks in the blockchain. Second limitation: The results of the performance parameters may change depending on the size of the data and the number of blocks. Third, the fluctuation of the results of the ABC algorithm in improving the system may require improving this algorithm to extract more stable results. Finally, different farming environments and areas, collecting data and then transmitting them via the IoT in real applications can generate different performance results.

7. CONCLUSION

Farmers and agricultural businesses now urgently need to protect electronic agricultural application data, as the accuracy of agricultural product information has a significant effect on their resources and national economies. The improved system analyses, predicts, and tracks product provenance via ADL technology as a model. IoT application security can be enhanced, and data changes in BCT can be avoided by using blockchain blocks and Ed25519 technology to create digital signatures. Ed25519 is a fantastic option for data authentication in the IoT because of its appropriate key sizes, safe implementation, and understandable designs. Numerous risks aim to change or intercept data sent over the EAA-IoT or stored on it. Because sufficient security protection has not been incorporated in current research, electronic farming and related applications are susceptible to security threats. Compared with other techniques, ed25519 signatures are securely implemented and have low-key metrics. The artificial bee (ABC) approach, which controls the unexpected and unpredictable aspects of the process, can assist in optimizing many difficult issues and searching for the best solutions in Ed25519 IDs. To the best of our knowledge, this is the first time that Ed25519, blockchain, and ABC technologies have been integrated into EAA-IoT applications. In particular, we replaced Ed25519 in the blockchain instead of using SHA-256. Compared with those of previous studies, the benefits of the early performance of the proposed system demonstrate the possibility of its application in the field of the IoT. The results revealed that the signature verification process was faster than the signature process, as shown in Figure 7. Additionally, the proposed system is faster when using ABC randomness, as shown in Figure 8. In addition, the performance parameters (scalability 99.56%, entropy 60.99 Mbps, and network throughput 200000.0 m/s) were tested, and the superiority of our proposed system over existing methods was proven, as the results were suitable for EAA-IoT applications. Moreover, through the Scyther test for security, the system's ability to thwart all our research-scope attacks was demonstrated. For future work, we plan to adopt a fast hash algorithm within the Ed25519 signatures instead of SHA-256-like GLUON, which is very fast and could be very suitable for EAA-IoT applications. Collaboration with EAA-IoT stakeholders, such as farmers, distributors, and regulatory authorities, is one of the future plans to test the proposed system in real-world environments. Additionally, we plan to analyse the proposed system with big data and analyse improved ABC algorithms such as the multiobjective artificial bee colony (MOABC) algorithm in an attempt to obtain better performance and more stable results.

Conflicts of interest

The paper states that there are no personal, financial, or professional conflicts of interest.

Funding

The acknowledgements section of the paper does not mention any financial support from institutions or sponsors.

References

[1] C. Jacklin, and S. Murugavalli, "A comprehensive review of the detection of plant disease using machine learning and deep learning approaches," Measurement: Sensors, 24, 100441, 2022. https://doi.org/10.1016/j.measen.2022.100441.

[2] X. Li, Y. Mei, J. Gong, F. Xiang and Z. Sun, "A blockchain privacy protection scheme based on ring signature," IEEE Access, vol. 8, pp. 76 765-76 772, 2020. https://doi.org/10.1109/ACCESS.2020.2988973.

[3] K. Chatterjee, and A. Singh, "A blockchain-enabled security framework for smart agriculture," Computers and Electrical Engineering, 106, 108594, 2023. https://doi.org/10.1016/j.compeleceng.2023.108594.

[4] K. Taji, and F. Ghanimi, "Enhancing security and privacy in smart agriculture: A novel homomorphic signcryption system," Results in Engineering, 22, 102310, 2024. https://doi.org/10.1016/j.rineng.2024.102310.

[5] A. Aljabri, F. Jemili, and O. Korbaa, "Intrusion detection in cyber-physical system using RSA blockchain technology," Multimedia Tools and Applications, 83(16), 48119-48140, 2024. https://doi.org/10.1007/s11042-023-17576-z.

[6] Y. Chen, H. Chen, M. Han, B. Liu, Q. Chen, Z. Ma, and Z. Wang, "Miner revenue optimization algorithm based on Pareto artificial bee colony in blockchain network," Journal of Wireless Communications and Networking, 2021(1), 1-28, 2021. https://doi.org/10.1186/s13638-021-02018-x.

[7] R. P. Kumar, and S. R. Bandanadam, "Block chain-based decentralized public auditing for cloud storage with improved EIGAMAL encryption model," International Journal of Information Technology, 16(2), 697-711, 2024. https://doi.org/10.1007/s41870-023-01599-8.

[8] R. Vardhan, R. Kumar, and P. Supraja, "Intelligent fortification of agricultural data integrity," In 2024 2nd International Conference on Networking and Communications (ICNWC) (pp. 1-8). IEEE, 2024. https://doi.org/10.1109/ICNWC60771.2024.10537380.

[9] M. Al-Zubaidie, and W. A. Jebbar, "Providing security for flash loan system using cryptocurrency wallets supported by XSalsa20 in a blockchain environment," Applied Sciences, 14(14), 6361, 2024. https://doi.org/10.3390/app14146361.

[10] S. A. Yousiff, R. A. Muhajjar, and M. H. Al-Zubaidie, "Designing a blockchain approach to secure firefighting stations based Internet of things"," Informatica, 47(10), 2023. https://doi.org/10.31449/inf.v47i10.5395.

[11] P. Chithaluru, F. Al-Turjman, R. Dugyala, T. Stephan, M. Kumar, and J. S. Dhatterwal, "An enhanced consortium blockchain diversity mining technique for IoT metadata aggregation," Future Generation Computer Systems, 152, 239-253, 2024. https://doi.org/10.1016/j.future.2023.10.020.

[12] A. Panwar, M. Khari, S. Misra, and U. Sugandh, "Blockchain in agriculture to ensure trust, effectiveness, and traceability from farm fields to groceries," Future Internet, 15(12), 404, 2023. https://doi.org/10.3390/fi15120404.

[13] E. Johns, "Cyber security breaches survey 2023," GOV.UK, 2023, available in https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023.

[14] K. Hasan, M. Sajid, M. Lapina, M. Shahid, and K. Kotecha, "Blockchain technology meets 6G wireless networks: A systematic survey," Alexandria Engineering Journal, 2024. http://dx.doi.org/10.1016/j.aej.2024.02.031.

[15] S. Yang, S. Li, W. Chen, and Y. Zhao, "A Redactable blockchain-based data management scheme for agricultural product traceability," Sensors, 24(5), 1667, 2024. https://doi.org/10.3390/s24051667.

[16] USDA, An official website of the United States government, "GIAC Cyber Security Discussion Paper," U.S. Department of Agriculture, 2024, available in https://www.ams.usda.gov/about-ams/giac-may-2024-meeting/cybersecurity#:~:text=AGCO%2C%20a%20major%20provider%20of,including%20a%20tractor%20assembly%20facility.

[17] A., G. Faisal, and S. S. Vinod Chandra. "Blockchain technology in agriculture: Digitizing the Iraqi agricultural environment," Environment, Development, and Sustainability, 2024. http://dx.doi.org/10.1007/s10668-024-04623-4.

[18] L. Bing, M. Zheng, and M. Maode, "A novel security scheme supported by certificateless digital signature and blockchain in named data networking," IET Information Security, Volume 2024, Article ID 6616095, 2024. http://dx.doi.org/10.1049/2024/6616095.

[19] A.A. Alahmadi, M. Aljabri, F. Alhaidari, D.J. Alharthi, G.E. Rayani, L.A. Marghalani, O.B. Alotaibi and S.A. Bajandouh, "DDoS attack detection in IoT-based networks using machine learning models: A survey and research directions," Electronics, 12, 3103, 2023. https://doi.org/10.3390/electronics12183103.

[20] M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," Symmetry, 15(1), 152, 2023. https://doi.org/10.3390/sym15010152.

[21] S. Zheng, and C. Jiang, "Consortium blockchain in shipping: Impacts on industry and social welfare," Transportation Research Part A: Policy and Practice, 183, 104071, 2024. https://doi.org/10.1016/j.tra.2024.104071.

[22] K. Rakhimberdiev, A. Ishnazarov, P. Allayarov, F. Ollamberganov, R. Kamalov, and M. Matyakubova, "Prospects for the use of neural network models in the prevention of possible network attacks on modern banking information systems based on blockchain technology in the context of the digital economy," In Proceedings of the 6th International Conference on Future Networks & Distributed Systems, pp. 592-599, 2022. https://doi.org/10.1145/3584202.3584291.

[23] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "REISCH: Incorporating lightweight and reliable algorithms into healthcare applications of WSNs," Applied Sciences, 10(6), 2007, 2020. https://doi.org/10.3390/app10062007.

[24] X. Zhou, Y. Wu, M. Zhong, and M. Wang, "Artificial bee colony algorithm based on multiple neighborhood topologies," Applied Soft Computing, 111, 107697, 2021. https://doi.org/10.1016/j.asoc.2021.107697.

[25] S. Aslan, "A comparative study between artificial bee colony (ABC) algorithm and its variants on big data optimization," Memetic Computing, 12(2), 129-150, 2020. https://doi.org/10.1007/s12293-020-00298-2.

[26] D. Owens, R. El Khatib, M. Bisheh-Niasar, R. Azarderakhsh, and M. M. Kermani, "Efficient and side-channel resistant Ed25519 on ARM Cortex-M4," IEEE Transactions on Circuits and Systems I: Regular Papers, pp. 2674 – 2686, 2024. https://doi.org/10.1109/TCSI.2024.3384414.

[27] M. Al-Zubaidie, and R. A. Muhajjar, "Integrating trustworthy mechanisms to support data and information security in health sensors," Procedia Computer Science, 237, 43-52, 2024. https://doi.org/10.1016/j.procs.2024.05.078.

[28] P. S. Solanki, and G. Joshi, "Internet of Things: A growing trend in India's agriculture and linking farmers to modern technology," In Precision Agriculture for Sustainability, Apple Academic Press, pp. 373-382, 2024.

[29] J. Xiao, Y. Jiao, Y. Li, and Z. Jiang, "Towards a trusted and unified consortium-blockchain-based data sharing infrastructure for open learning—TolFob architecture and implementation," Sustainability, 13(24), 14069, 2021. https://doi.org/10.3390/su132414069.

[30] S. Han, Z. Wang, D. Shen, and C. Wang, "A Parallel Multi-Party Privacy-Preserving Record Linkage Method Based on a Consortium blockchain," Mathematics, 12(12), 1854, 2024. https://doi.org/10.3390/math12121854.

[31] T. H. Yuen, "PAChain: Private, authenticated & auditable consortium blockchain and its implementation," Future Generation Computer Systems, 112, 913-929, 2020. https://doi.org/10.1016/j.future.2020.05.011.

[32] A. Saihood, M. A. Al-Shaher and M.A. Fadhel, "A new tiger beetle algorithm for cybersecurity, medical image segmentation and other global problems optimization," Mesopotamian Journal of Cybersecurity, 17–46, 2024. https://doi.org/10.58496/MJCS/2024/003.

[33] M. Farsi, J. A. Erkoyuncu, and A. Harrison, "A super simple life-cycle cost estimation model with minimum data requirement," TESConf 2020 - 9th International Conference on Through-life Engineering Services, 2020. https://dx.doi.org/10.2139/ssrn.3718042.

[34] Z. Bingul, O. Karahan, "Comparison of PID and FOPID controllers tuned by PSO and ABC algorithms for unstable and integrating systems with time delay," Optimal Control Applications and Methods, 39(4), 1431-1450, 2018. https://doi.org/10.1002/oca.2419.

[35] W. Jebbar and M. Al-Zubaidie, “Transaction security and management of blockchain-based smart contracts in e-banking-employing microsegmentation and yellow saddle Goatfish”, Mesopotamian Journal of CyberSecurity, 4(2), 1-19, 2024. https://doi.org/10.58496/MJCS/2024/005.

[36] R. Fotohi, and F.S. Aliee, "Securing communication between things using blockchain technology based on authentication and SHA-256 to improve scalability in large-scale IoT," Computer Networks, 197, 108331, 2021. https://doi.org/10.1016/j.comnet.2021.108331.

[37] N. Ullah, P. Meratnia, and J. Havinga, "A Lightweight random number generator for decentralized IoT applications," IEEE Access. 9, 34238-34251, 2021. https://doi.org/10.1109/ACCESS.2021.3061802.

[38] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," IEEE Transactions on Intelligent Transportation Systems, 23(7), 8857-8867, 2021. https://doi.org/10.1109/TITS.2021.3086976.

[39] J. Xiao, T. Luo, C. Li, J. Zhou, and Z. Li, Z. "CE-PBFT: A high availability consensus algorithm for large-scale consortium blockchain," Journal of King Saud University-Computer and Information Sciences, 36(2), 101957, 2024. https://doi.org/10.1016/j.jksuci.2024.101957.