Decentralized Block chain Provenance Security System using Secure Sharable Advanced Encryption Standard for Distributed Agriculture Information Security

S. Vijayaragavan[1], **E. PunarSelvam**[2], **N. Kuppurasu**[3]

Abstract

Agriculture is one of the great economical deal in food industry for rapid growth in developing new ideas across the world. Due to the agricultural development in food industry, supply chain, agro-farms, information are in the form of collective maintenance in centralized storage system on Agro-network. The centralized security system doesn't met the trust worthiness to provide the reliable data on agro-information sharing in network. To formalize the data structure to improve the trust management based on block chain data processing techniques which is to make reliable data provenance system. To improve the security system, to propose a Decentralized Block chain provenance security system (DBPSS) to build a reliable data security on agro information sharing on distributed network. In addition on data security we intent a secure sharable advanced Encryption standard (SSAES) to improve block chain collective information records in the form bi-circular shifted codes to represent the key security on data records. DBPSS allows the verified information sharing based on block header by each information sharing on distributed network. This security verifies the block chain key codes during each transaction by traceable authenticity to provide for authentication on distributed system. The proposed system ensures the reliability of the data in distributed system to make higher performance as well in agricultural information security.

KeyWords: Block chain, distributed system, agricultural data safety, cryptography security, Data sharing, Trust management.

DOI Number: 10.14704/nq.2022.20.8.NQ44698 **NeuroQuantology 2022; 20(8): 6738-6749**

[1] Professor, Department of Computer Science and Engineering, Muthayammal Engineering College (Autonomous),Namakkal - 637408,Tamil Nadu, India.
[2] Professor, Department of Information Technology, Muthayammal Engineering College (Autonomous), Namakkal - 637408, Tamil Nadu, India.
[3] Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore - 641 046, Tamil Nadu, India.

Introduction

In a developing agricultural resources, the Block chain should be performed by linking the block od data on the form spliited data called modules chain to audit units optimized for storing data. Since many of the commentaries are online block chain, and there are many authors, you can contribute to that lock mechanism by starting with Google Docs, a spreadsheet similar to the one described above. A small example of Block chain is that it has a unique feature that makes it an attractive technology for tracking something stored, tagged and stored, rather than complicated. Bit coin has since been one of the most popular projects in Block chain technology.

Forum in information security in Agriculture computing technology is widely used today to share the sources of Infrastructure, software, applications, and business implementations Figure 1. It moves application software stored in large data centers from server computers to a large distance such as databases. Creates customer data on a remote server and stored. The customer can then access data and access data using internet technology to save it. This technology provides web service on a reliable agriculture computing platform, but it also the challenge is many design and performance Issues such as security concerns. One of the biggest concerns is the storage of data security issues. Data stored in a remote server data integrity is not incredible. For example, data storage service providers may decide to cover consumer profit margins. As a result, server access rarely removes the customer. Knowledge of the need for customer needs to be followed by observing the data integrity of data retrieval.

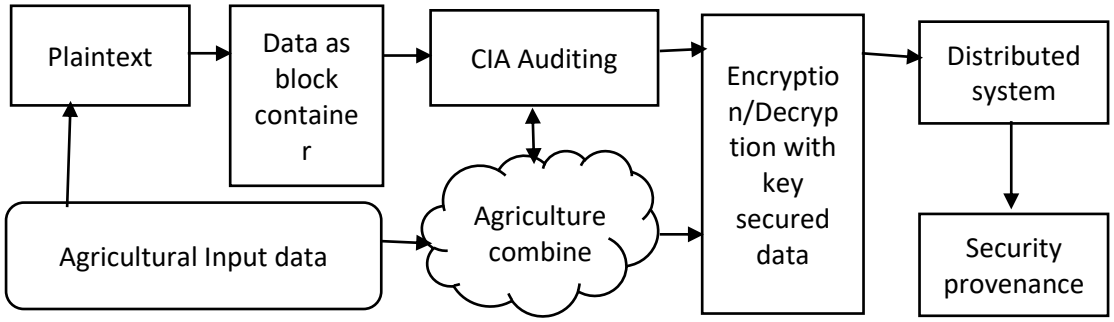

Figure 1 Information Security in Agriculture computing

Block chain is a digital transaction account book, maintained by a plurality of network computing machines that do not depend on a third party's trust. Each transaction data file is managed by a specific software platform that enables the processing of data, processing and storage and is stated in a human-readable format. In the structure of the original bit currency, each block has a heading of the time 2 link, exchange data, and a reference to the previous block. The hash, based on its content, is generated for each module, and the subsequent block title should be specified.

Cryptography is a combination of data mathematical handling (cryptosystem text) for both text (key). Convert text using the text encryption key encryption algorithm used. And the use of the decryption algorithm used to change the cursory text on the key chipper text. Key secured algorithms are required before creating the encryption and removal of unauthenticated block by retention [26]. During the encryption, there are three basic process-key generation, encryption and decryption process.

The problem is that many existing systems are solved by data integrity. They all fall into private-public censorship and censorship. The private audit program also provides capacity. When any public examination, allowing only the savings agriculture server to handle customer-based data while keeping any personal information. Employee General, The Client's Third Party Comptroller (TPA) Company is creating a public key. Done is stored on remote file server Customer informs about the stored file

monitoring and protection.

Literature review:

Block chain technology allows for more secure recording and digital transactions. Block chain is secure and transparent and available to all supply chain parties to create a common ledger system. For products related to agriculture [1][2]. Block chain technology can be sued to promote food security and prevent food fraud and to check the source and viability of agricultural produce and agricultural inputs. Block chain has the potential to improve detection and transparency because of all of them. Block chain technology can be used to achieve better prices, payment methods, registration and transparent subsidies of landowners to farmers [3]. Block chain technology has changed while questioning the main obstacle Information and Communication Technology (ICT) trust has changed our perception.

Improve while agriculture has proven sustainable development, information and communication technology capabilities. Agricultural knowledge is the permission of banks and other digital resources. FOA is recommended ICT Requirements. Recently, the communication technology monitoring system based on the promotion of agriculture in some areas. Farmers in such an area could be using a smart phone without having to go through their paddy field conditions. In this study, communication technology, water and effort, and nutrient load reduction were evaluated as evidence of the impact monitoring system [4][5].The Internet of Things (Population) extends to the Internet connection to achieve not just computers and humans, but most of the things in our environment. The impact of information sharing has the potential to improve the impact on our lives.

Block chain is a powerful technology, computing and management processes decentralized [6]. Block chain is a new tool for agricultural producers, supply chain management, food suppliers and retailers that can be used to integrate the distribution network to provide customers with information about the product. Block chain has ensured the safety of a separate, mutually exclusive, certification system from the World Table of Food and Agriculture Production Local Farms. Consumer confidence eroded by food fraud and major economic losses has steadily escalated into urgent problem makers, researchers, government, consumers and other stakeholders.

This technology is used to evaluate the feasibility of the block chain food supply chain and to ensure reliability [7]. Block chain Ledger and Related Technology (DLT) has proven network equity, digital currency and financial self-management help to transform a globally distributed platform that can transform from a centralized document sharing platform to potentially exciting,.Mostly they concentering Duplicated and Bookkeeping (DSBT) distributed and real estate assets [8][9].Contracts, exchanges, and their records provide the essential structure of the economic system, but they do not keep up with the digital transformation of the world.

They look like one of racing to capture the Formula's Supreme Freeze. Block chain is expected to solve this problem [10]. Food safety and quality assurance have become more and more difficult as the world has become more and more products. In particular, retailers, distributors and national regulatory authorities proved that finding food was more challenging.[11][12] The purpose of this paper is to present the findings of the Meat Investigation of Different Opinion Meat Supply Chain Partners (SCSS); it is a potential transparency and detection-like assessment block chain technology (BCT) Acceptable Potential System (TTS). Consumer Scale 141 Design / Method / TTS Approach for showing their views. [13] the also focused on the latest food safety education and business boom. In the supply chain series, the rapid development of internet technology, many new technologies are being used in the detection system [14][15].However, to date, almost all of these organizations are operating in monopolies, which are asymmetric, leading to problems of trust, such as fraud, corruption, fraud and falsification of information opacity. [16]

In addition, the failure of the centralized system is in danger of collapsing because a point collapse

can cause the entire system. Block chain technology can save a lot of intermediary costs by using structures in a decentralized way, and solving data monitoring and information security issues through an unauthorized timestamp [17]. Wireless sensor network research is a growing concern for the community and industry, because of its small size, this small "Smart Dust" piece offers ease of integration and a great advantage for "green" applications. Considering the green intelligent application environment, computing is a hot topic nowadays[18][19]. The event is likely to grow exponentially in terms of increasing the amount of knowledge that Linked Open Data (LOD) will publish for a serious review of all related warrants. This article briefly introduces the success of LOD development, the Block chain Key security (BLSK), and discusses the characteristics of measurement and performance.

Food safety in distributed problem which directly or indirectly affects the health, quality of life and quality of life of people because of information leakage without athenticity. It will have a major impact on the international economy, politics and society as a whole. As an effective means of security product quality management and control, many countries and territories are running a research, [20] development and diagnostic system. Sophisticated value chain running by using the technology of the agri-food value chain, key assurance to consumers that affordable, safe and adequate food, forage, fiber and fuel can be delivered in significant areas. Groundbreaking, [21] block chain Technology (BCT) has gained increasing acceptance and importance over the past few years. In the social and legal sectors such as finance, intellectual property and the supply chain network, different applications are implemented. Distributed ledger technology (DLT) and smart contracts offer a unique opportunity to bring greater efficiency, transparency and value recognition and information exchange in the agricultural sector [22]. By using digital logging, password and transaction processing and interoperability data storage.

Consumer awareness, as well as developing manufacturer internal quality requirements, is leading to new demands Supply Chain Detection. Existing centralized solutions suffer when not further from separate data storage. In recent years, discovery has emerged as an important tool for food safety and food quality assurance. On the other hand, repeatable system design requires a complete reflection and restructuring of the entire food supply chain referd Block chain based supply chain traceability (BSCT). Blockchain has been used to solve problems from different segments. [23] In agriculture, it is used to promote block chain as a food security and transaction time. Block chain technical requirements clearly compounded the interest of agricultural production and moderation. Block chain is the first to develop a decentralized crypto currency transaction and data management technologies. The reason is that without any central area of a third-party asset, block chain Security has the benefits of anonymity and data integrity it provides [24].

Greenhouse technology in agriculture such as remote monitoring and automation matters as a foundation (population) is growing steadily on the Internet. But it is still a major concern for security and privacy, coordinate mechanism of supply chain (Co-MSCM) due to the large spread of its network of properties. The purpose of this article is to explore the value of block chain technology as a solution for [25] creating and maintaining a reliable digital record. Access to appropriate financial services was considered a major challenge for many developing countries. Efforts to address these challenges include the conventional financial inclusion initiative, which will find its objectives to be effective in providing affordable, high-quality financial services to its target market in meeting popular financial needs.

Materials and methods

Block chain Security and Service Provider agriculture is the most important document among these which are still subject to further permission to manage the data that provides the level of key data in the place where only the work is allowed. Clients need block chain security on the effects of performance system and the agriculture providers have yet to find a number of methods to connect data to maintain their form

data. Maintaining the content of own content and then increasing the level of the analyzes and agricultures to document their information efficiency on encryption. To propose a Decentralized Block chain provenance security system (DBPSS) to build a reliable data security on agro information sharing on distributed network. In addition on data security we intent a secure sharable advanced Encryption standard (SSAES) to improve block chain

Because of the vast area of communication and use of a wide variety distributed secuirty need auditing verification, the most important security problem is because the point is to hack others to the agriculture data interest. Therefore, we focus mainly on the process of encryption and removal of security information using the Agriculture Computing It can be used here but still depends on a number verification on key standards, which can be somewhat safer for the entire data to focus on security concerns.

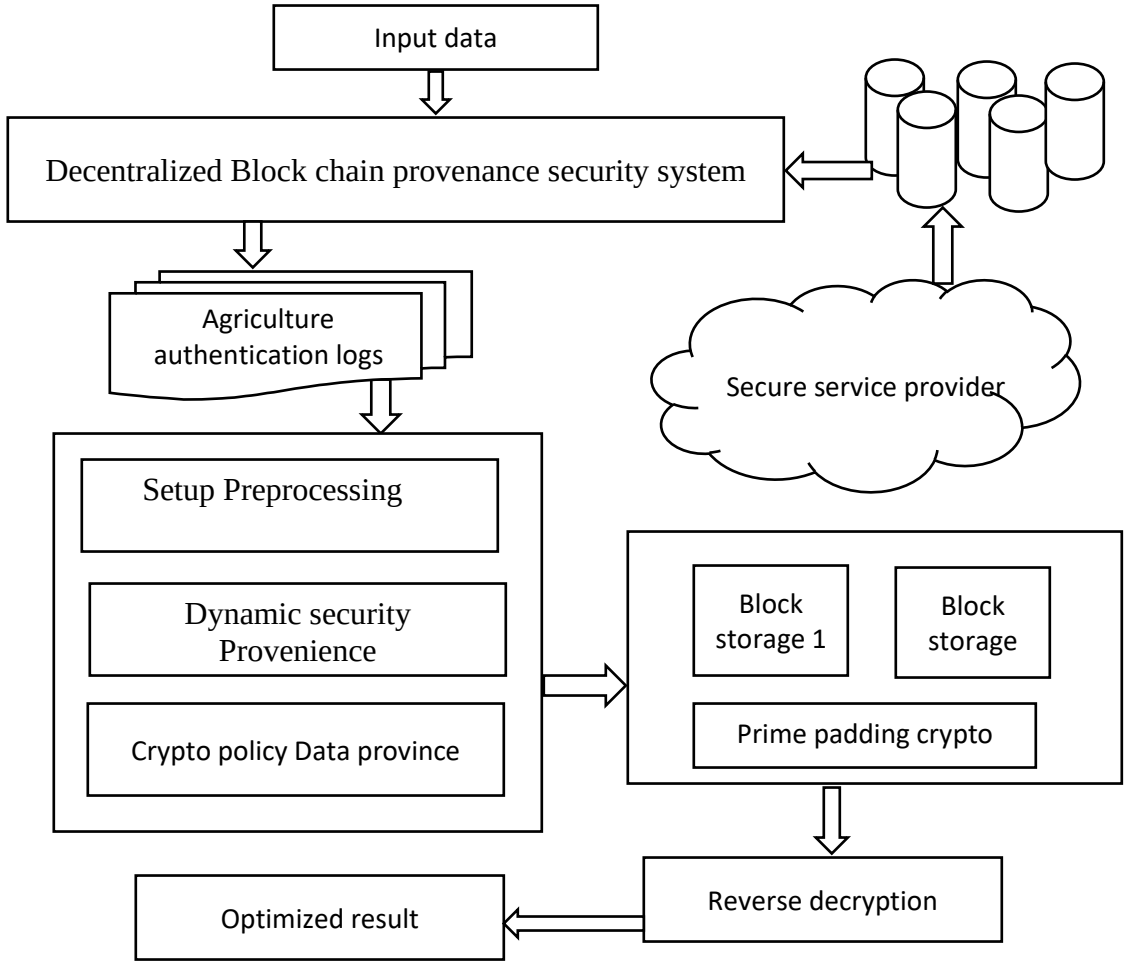

Figure 2 Architecture diagram for proposed system

A secure sharable advanced Encryption standard, a storage system based on the Secured sharable Prime factor encryption signature algorithm, is continuously monitored for the security of its stored data. It is proven to be based on data modeling (PDP) model concept. PDP model there is a challenge answer protocol. In the PDP model, the client uses agriculture monitoring and challenges to agriculture server challenges. The challenge blocks are subdivided into the remote file server and have the proof of its value for the selected Subcommittee volumes. The customer checks the proof that it is retrieved from the server and makes sure this remote agriculture storage file is correct to the server. The RSASS has two phases, i.e. system structure and

integrity.

Field Safety: (1) Due to the dynamic measurement, service essence agriculture computing models have the ability to use data agriculture platform applications and any standard infrastructure and security boundaries due to location transparency specializations. If a security breach involves, it is difficult to isolate a particular resource that has a physical threat or is left out.

(2) Agriculture computing service distributes agriculture services based on resources that may be owned by many providers, according to distribution models. If there is an interest paradox, it is difficult to sort out a united defense operation

(3) Multi-tenant agriculture and virtualized by the openness in sharing resources, such as access to user data and other unauthorized users.

(4) Agriculture Platform To meet massive information storage and provide fast access to a agriculture, agriculture security will also meet the need to use massive information processing operations.

Key features of security provenance system

1. It is a special trusted domain-based and boxes must manage a trusted agent in each domain. A Agriculture-based service provider resources are a trust management. 2. It distinguishes between two different roles in the agriculture: Designer designs for more customer deliveries and different credibility for the customer. 3. Relieve confidence Establishing Reliance on Reliability and Conducts Trust of One Kind of crypto Service. 4. The decision factor and refresh take time factor and factor transaction into account based on trust auditing.

3.1 Setup Preprocessing

This stage preprocess planning security tasks in agriculture systems, select how to effectively exploit resources to share other than duplicates and resources to utilize fully. At the same time, communication plays a major role in delaying agriculture planning delay, which leads to great waiting between security dispense but can cause idle time interval between processing units. In this thesis, a removal setup system uses efficient preprocess agriculture resources. Planning program, directed by outlier Map Previous coating time based planning is called a multi-agriculture duplicate systems algorithm and a new protocol is included in the secuirty of reconstructing tasks in the list. The copper time attempts to replicate photo insert the appropriate immediate security from removal of filled non filled verfrication of the current terminal of the processor selected in order to reduce its waiting time.

Algorithm

Step 1: Input raw data Rd {rd1,rd2,...rdn}

For each rd (record set□ Rs)

Check is Empty==NULL

Fill attribute Ac==nill to Rd

End for

Step 2: check distinct data Dt

For each attribute Dti in the data set

While (mismatch attribute (Ac) == Rd)

Remove record set from rd

Do

End for

Step 3: check numeric and non-numeric validated attributes fields

If Rd is a numeric attribute

Then hold discretize or eliminate the attribute;

If Rd is a non-numeric attribute Then

Hold Values □rd

Else

Remove the non-matched noise value

End if

End if

Step 4: keep raw data originate all fill case record fields

Step5: validation checks for ordered records

The preprocessing crude data for each record field arises with empty attributes as a regular field empty case. The above method of cleaning sanitizes the noise of raw data (Rs) values without which it originates in the form of distinct data acquisition.

3.2 Dynamic security Provenience

This condition is distributed in favor of the service provider distributed by the supervisory power servers. This company is considered semi-reliable. Private audit is system configuration. The model consists of two companies and the owner of the agriculture service provider information. This framework allows the information owner to only process the information to verify the information structure established by the repository server relating to the distribution and operation of the company. TPA wants a challenge to verify that it is at any time to verify the distant server information. Server has been certified by a source that retained that information. The correct evidence confirms that the encryption keys are used by the information matched by the tons and is generated by the right statement.

Algorithm:

Input: User Request Ur.

Output: Null

Start

Read user request Ur.

Identify the service claimed sc = Ur.Service

Identify list of Block services required SRl.

SRL =

For each service Si from SRL

Identify the list of attributes.

SA =

Perform Access blockClearance.

If true then

Allow Access.

Perform service level ABE.

Perform data management.

Else

Deny Access.

End

Stop.

The above discussed algorithm performs public auditing and verifies the trust of the user to allow or deny the user request.

Since the outsource information is naturally changing, it is necessary to set up a dynamic review of the Outsourcing Information Conference on Operations. Intuitive authenticators are used to achieve a standard transmission overhead in a general verification mode. In the previous procedures, the valuation will be recognized as the creditor's value as the same creditor and used to evaluate the distributed server through the process of evaluating the owner's permission to block the distributed server. The three equations are not replaced by three K, KP and KQ equations: ED = K 0 (n) +1 = K (p - 1) (Q - 1) +1 equation (5.1.1) = k (n - p (q 1) + 1 (5.1.5) + 1 (5.1.5) edp = kpho (p) + 1 = kp (p - 1) + 1 (5.1.6) edq = kqφ (q) + 1 = kq (q - 1) + 1. However, the insertions are limited to using the token value of the chunk that they may develop complex. Information needs to be chunky tags so that the real agriculture is the best in all of the subsequent scenarios where the information itself will be refreshed. As a result, the totally variable tag token function has to do with the valuation process to prevent them from fulfilling verification state.

3.3 Secured sharable Prime factor encryption

As an imaginary one can do, there is a need for encryption sources for longer forecasts for stronger security. Performance and safety level and safety levels measure the relationship between the ABE offers and the inspection to determine what level of security is secure sharable advanced Encryption standard. The coordinate-based encryption ABE is built on top of its security paired oriented cryptographic algorithmic base strength

1. Compute Two different Big Random Numbers are selected by B & K.

2. Block sharable Compute, n = k × p.

3. Extract chain links Predict: Phi (N) = (PQ-1) (Q-1).

4. Compute the prediction 1 <e

secure sharable advanced Encryption standard posses user B is encrypting an informative m, with which one decrypts the user. User needs to do the following to B:

- Receive a true public key (NA, EA).
- [0, NA - 1] to specify a full m message at

intervals.

• Select a random full g 1 <Q <NA, such as GCD (K, NA)) = 1.

• Compute C1 = k EA mod na. • Compute c2 = Foreign k mode.

• Send User A to encrypt text message (C1, C2).

Prime padding introduced an efficient add on bits of key embedding some security features, such as semantic encryption with protection against selective speech attacks. David's proposal was six times faster than Prime Pudding encryption. This project is an RSA-version of Prime Pad Encryption. That is, the sender chooses k ∈ Z ∗ n to encode a message m for an RSA system with general parameters (n, e).cipher text C = (A, B), where, A = k e (mod n) and B = m × (k + 1) e (mod n). Subscriber receiving the first computation by pressing Q = advertising (modn), and m = / (k + 1) e (mod n), retrieves. (Q + and (k + 1) emod n, due to distinguishability) This project is not semantically preserved. The big integer factor. The hardest attack is to send a lengthy enough public key encryption key length to the origin and structure of the well-arranged group of distributed net users, as the new factor and methods of improvement in the performance of the methods developed by the methods.

Data verification of reverse secured TPA auditing

After the secure sharable advanced Encryption standard third party audit (TPA) can verify the main padding data. When receiving a request from the client to verify tons of data, it sends an audit message to the service provider asking for a set of data sets for verifying auditing policy. The audit message contains status of the modules requested. Service provider sets a linear combination of blocks and applies to a mask. Serving as a service provider authenticator and tons of masked wires. Finally comparing mask modules from metadata from customer service provider and client.

To restore the default m from c2, the user must do a following:

• Resembles Use own private key dA and compute: c dA 1 = k mod nA.

• Estimates the Euclidean algorithm and calculate the unique integer s, 1 < s < nA, such that s ∗ k ≡ 1 (mod nA). • Compute c2 s = (meA k) s = (meA) k s = meA mod nA.

• Recover m, use the private key dA and compute :(meA) dA = m mod nA.

This prime padding reverse decryption is a strengthened version of encryption in order to secure protection. Zinc × zinc → {0, 1} L is a hash function: l let a safety parameter and hours. A = Q E, B = × (k + 1) e m, and H = h (m, k): A three m (A, B, H) of a database m. Here k is a random value. If the cipher is to be decoded, the receiver calculates: Q = ad (mod n), and m = b / (k + 1) e (mod n), then equality H tests? = H (m, k). If equality is satisfied, the information m is agreed; Otherwise, Cybertost rejected. This program does not seem to be aware of Cybertex, as it is a news probability, the ACCA is not safe against.

Result and discussion.

The block chain management resultant provides the execution of agricultural security standard implementation by testing parameters using performance analysis in encryption, decryption and auditing state. The projected Block chain based crypto policy in data security using trust key verification in distributed agriculture security environment. The verification begins the auditing source of owner data logs with outsourced encryption and decryption using distributed endpoint. The collection of different content file size executed at in different level time taken to execute the process of encryption-decryption duration and integrate with auditing point. The implementation was carried out through visual studio framework 4.0 with SQL server authentication. The resultant given below shows the performance of proposed security proves the higher efficiency.

Table 1: Details of processed parameters

Parameter	Value processed
Service provider	Agriculture service provider
Data processed	File Type, Clair text
File size	25 mb,50mb,75mb nearer
Number of users	1500

The above table 1 shows the parameters and the values taken to test the proposed system

implementation. This contains a agriculture service provider that is centralized to process the authentication with encrypted agriculture data. The data that are proceeding in the form of Clair content in different file size to test the security.

4.1 The impact of security analysis

The security depends on the process of encryption with key possess the auditing strategy to take the overall execution.

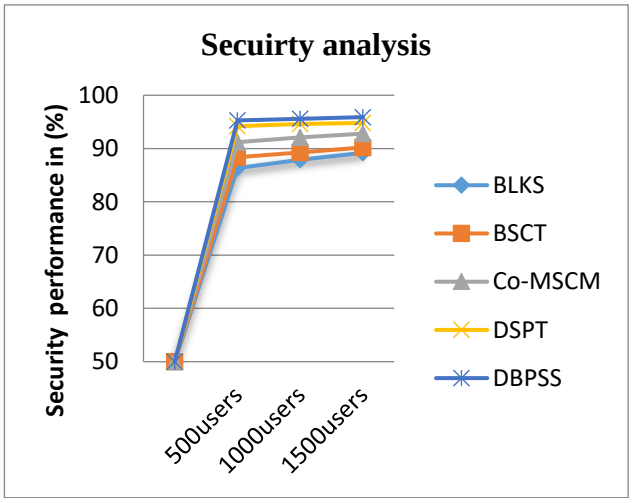

Figure 3: Comparison of security analysis

The above figure 3 shows the different methods produce the different level of user to do the security activity. The proposed system produce the higher impact security performance compared to the other dissimilar methods.

Table 2 Comparison of security analysis

	Comparison of security analysis				
Methods /users	BLKS	BSCT	Co-MSCM	DSPT	DBPSS
500users	86.3	88.4	91.2	94.2	95.3
1000users	87.9	89.3	92.1	94.6	95.6
1500users	89.2	90.2	92.8	94.8	95.9

The above table 2 shows a comparison of the Security analysis, and this can be tested with the total number of users that access the security with right authentication to access the data. The proposed system produces 95.9 % accuracy compared to the other methods. The proposed system proves the great performance of higher-end security with the improvement of standard crypto advanced efficient.

4.2 Impact of key auditing during encryption and decryption

The key verification proves the security to provide right authentication for whom have the right key to request the data. Time is taken to encrypt the data with key generation based on the size of the data. Similarly, the decryption has time taken to verify reverse encryption with verified key logs.

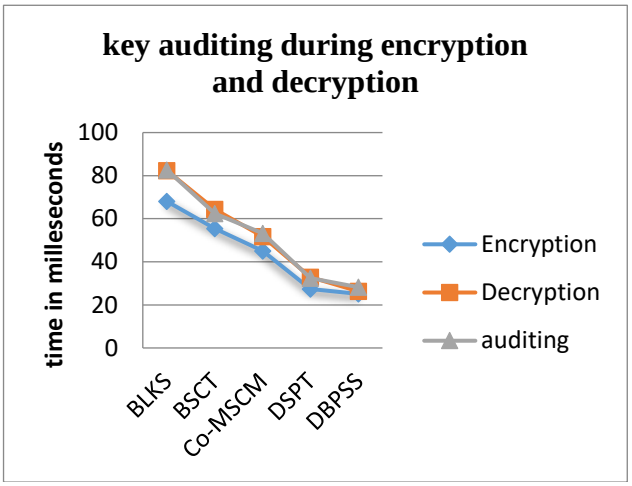

Figure 4: Comparison of key auditing execution

Figure 4, Shows the key audit of the state's ability to process execution between encryption and deletion of programs, meanwhile, is 25.1 ms. this implementation had much improved performance compared to previous methods.

Table 3 Comparison of key auditing performance

Methods/state	Comparison of key auditing execution during encryption and decryption				
	BLKS	BSCT	Co-MSCM	DSPT	DBPSS
Encryption	68.1	55.4	45.1	27.2	25.1
Decryption	82.4	64.2	51.8	32.3	26.3
Auditing	82.7	66.4	53.4	32.7	28.2

4.3 Impact of time complexity analysis

The overall time is taken to encrypt the data based on the size which depends on the process of execution. The time leads the fact with differential Clair content had the crypto policy security standard. The proposed system produces the lower time to process the data and improve the security which doesn't have time given to the intruders.

Time complexity (Ts)=

$$\frac{\text{Total number of blocks per bits} \times \text{two phase encryption}}{\text{time taken (s)}} \quad --(1)$$

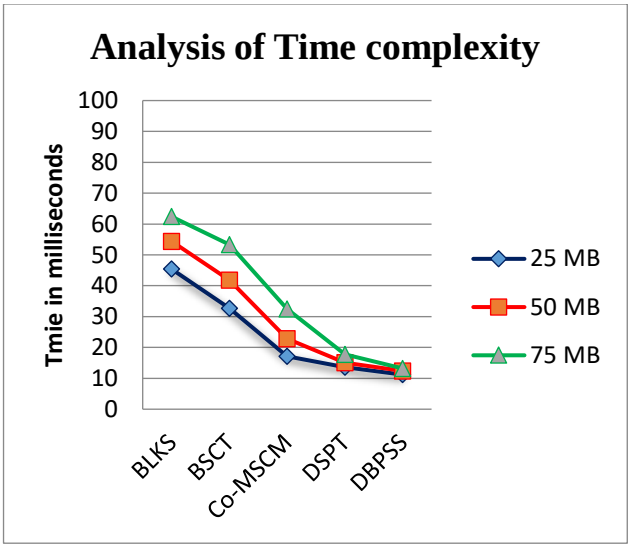

Figure 5: analysis of time complexity

The above Figure 5 shows the various file size to handle the encryption at mean time of evaluation by dissimilar methods, and proposed system P2ABE-SDA provides the least time 13.2 ms as well as previous cipher policy. This implementation had much improved performance compared to the previous steps.

Table 4 Comparison of time complexity

Methods/different Clair text file size	Comparison of time complexity				
	BLKS	BSCT	Co-MSCM	DSPT	DBPSS
25 MB	45.4	32.7	17.1	13.6	11.2
50 MB	54.4	41.8	22.8	15.1	12.4
75 MB	62.4	53.3	32.5	17.8	13.2

The above table 4 the proposed system shows a more complex time making comparisons that produce more improvement than other methods. The proposed system produces a less complicated time of execution than other methods.

4.4 Impact of false occurrence

The false occurrence is states of verification at the service level of integrity during key failed state, or encryption and decryption state.

Frequent occurrence state (FS) =

$$\frac{\text{Repeated block of the cipher}}{\text{Total number of cipher block occurrence}} \quad ----(2)$$

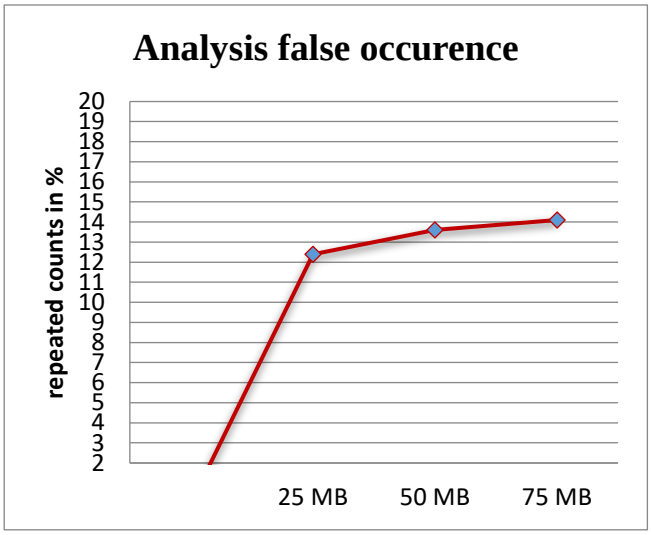

Figure 6: Comparison of false occurrence

The above Figure 6 shows the failed states to do the encryption whether data is encrypted during non-redundant evaluation with dissimilar methods. This shows evidently our implementation of proposed crypto method has produced active redundant false rate than previous methods

Table 5 comparison of false occurrence

Methods/different Clair text file size	Comparison of false occurrence				
	BLKS	BSCT	Co-MSCM	DSPT	DBPSS
25 MB	12.4	10.4	8.3	5.6	5.2
50 MB	13.6	11.2	9.1	6.1	5.6
75 MB	14.1	12.6	10.7	7.4	6.2

The above table 5 reviews the impact of execution at false evaluation of lower complexity by different methods. The projected method proves the least failure state in 5.2 % best evaluation to do the process quickly similar than other methods.

Conclusion

Data secrecy agriculture storage is a major problem. Privacy with encryption tools can be confirmed. In this paper, we are going to introduce a system that supports agriculture general storage of cryptosystems on a variety of classes that support a general key cryptosystem to suppress secret keys. Our proposed method defends the block chain chai security problematic factor t intense a Decentralized Block chain provenance security system (DBPSS) to improve the privacy and security system to build a reliable agricultural information shar9ing among on agro data's on distributed network. In addition on security proofs key enhancement depends on data security we sharing through secure sharable advanced Encryption standard (SSAES) to improve block chain. Proposed system improve the efficiency up to 95.9 % in security level although confidentiality information sharing rather than existing methods.

References

1. Mustafa Cem ALDAĞ, Bülent EKER,"How to Use Block chain Technology in Agriculture", International Conference on Service Systems and Service Management, Yr-2018, pp-1-9.
2. Yu-Pin Lin, Joy R. Pettway , Johnathan Anthony , Hussnain Mukhtar , Shih-Wei Liao, "Blockchain: The Evolutionary Next Step for ICT E-Agriculture",yr-2017,pp-1-12
3. Yoshida, K.; Tanaka, K.; Hariya, R.; Azechi, I.; Iida, T.; Maeda, S.; Kuroda, H. "Contribution of ict monitoring system in agricultural water management and environmental conservation". Yr. - 2016; pp. 359-369.
4. Atlam, Hany, Ahmed Alenezi, Madini Alassafi & Gary Wills. (June 2018). "Blockchain with Internet of Things: Benefits, Challenges, and Future Directions." Intelligent Systems and Applications, 6, 40-48.
5. Dr. Mariah Ehmke, Cole Ehmke, "Blockchain Technology Applications In The Wyoming Food System", International Farm Management Association Congress, 3 – 8 March 2019.pp.-1-12
6. Galvez, Juan F., J.C. Mejuto & J. Simal-Gandara. (2018). "Future challenges on the use of block chain for food traceability analysis" Trends in Analytical Chemistry. 107: 222-232.
7. Suvarna K. Kadam, "Review of Distributed Ledgers: The technological Advances behind cryptocurrency",yr-2018,pp.-1-6
8. Iansiti, Marco; Lakhani, Karim R. "The Truth about Blockchain". (January 2017). Harvard Business Review. Harvard University. Retrieved 2017-01-17.
9. Creydt, M., and M. Fischer, "Blockchain and more-Algorithm driven Food Traceability", yr-2019, pp.-1-6.
10. Tian, F. "A supply chain traceability system for food safety based on HACCP, block chain &

Internet of things." International Conference on Service Systems and Service Management (ICSSSM). IEEE.yr- 2017.,pp.-1-7
11. Yuan, H., H. Qiu, Y. Bi, S.H Chang, and A. Lam. 2019. "Analysis of coordination mechanism of supply chain management information system from the perspective of block chain." Information Systems and e-Business Management 1-23.
12. Aquino-Santos, Raul; Gonzalez-Potes, Apolinar; Edwards-Block, Arthur; Developing a New Wireless Sensor Network Platform and Its Application in Precision Agriculture, SENSORS, Vol. 11, No. 1, pp. 1192-1211, 2011.
13. Lukose, Dickson; World Wide Semantic Web of Agriculture Knowledge, JOURNAL OF INTEGRATIVE AGRICULTURE,Vol. 11, No. 5, pp. 769-774, 2012.
14. Tse, D., B. Zhang, Y. Yang, C. Cheng, and H. Mu. 2017. "Blockchain application in food supply information security." International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE. 1357-1361.
15. Zhao, G., S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B.M. Boshkoska. 2019. "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions." Computers in Industry 109: 83-99.
16. Sander, F., J. Semeijn, and D. Mahr. 2018. "The acceptance of block chain technology in meat traceability and transparency." British Food Journal 120 (9): 2066-2079.
17. Tribis, Y., A. El Bouchti, and H. Bouayad. 2018. "Supply Chain Management based on Blockchain: A Systematic Mapping Study." MATEC Web of Conferences (EDP Sciences) 200.
18. Tripoli, M, and J. Schmidhuber. 2018. "Emerging Opportunities for the Application of Blockchain in the Agri-food Industry." FAO and ICTSD: Rome and Geneva Licence: CC BY-NC-SA 3.
19. Martin Westerkamp, Fried helm Victor and Axel Kupper,"Block chain-based Supply Chain Traceability: Token Recipes model Manufacturing Processes", Telekom Innovation Laboratories, Technische Universidad Berlin, Germany,yr-2018,pp.-1-9.
20. F. Dabbene, P. Gay, and C. Tortia, "Traceability issues in food supply chain management: A review," Bio systems Engineering, vol. 120, pp. 65– 80, 2014.
21. Bermeo-Almeida O, Cardenas-Rodriguez M, Samaniego-Cobo T, Ferruzola-Gómez E, Cabezas-Cabezas R and Bazán-Vera W 2018 Blockchain in agriculture: A systematic literature review. Communications in Computer and Information Science 883 44-56.
22. Yli-Huumo, J., D. KO, S. Choi, S. Park, and K. Smolander. 2016. "Where is current research on block chain technology?—a systematic review." PloS one 11 (10).
23. Patil A S, Tama B A, Park Y and Rhee K 2018 "a framework for block chain based secure smart greenhouse farming. Lecture Notes in Electrical Engineering "474 1162-7.
24. Lemieux, Victoria Louise, 'Trusting Records: Is Blockchain Technology the Answer?' Records Management Journal, 26 (2016), 110–39.
25. Chinaka, Malvern, 'Blockchain Technology -- Applications in Improving Financial Inclusion in Developing Economies : Case Study for Small Scale Agriculture in Africa', 2016 <https://dspace.mit.edu/handle/1721.1/104542 > [accessed 21 May 2018]
26. Kumaresan, S., Shanmugam, V. Time-variant attribute-based multitype encryption algorithm for improved cloud data security using user profile. J Supercomput 76, 6094–6112 (2020). https://doi.org/10.1007/s11227-019-03118-8.