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

An Efficient Multiuser Authentication and Data Transformation Technique for Smart Agriculture Using Cryptography

Bilas Haldar[1], Prabin Kumar Jha[2], Partha Kumar Mukherjee*[3]

Submitted:11/03/2024 **Revised**: 26/04/2024 **Accepted**: 03/05/2024

Abstract: The dynamic advancements in smart agriculture, coupled with the integration of advanced technologies are revolutionizing the agricultural sector. This transformation is enhancing efficiency, precision, and sustainability, leading to unprecedented improvements in crop management and yield optimization. However, the proliferation of digital interfaces and interconnected systems in this domain necessitates a heightened focus on ensuring the confidentiality, integrity, and authenticity of agricultural data. This research contributes to the advancement of secure agricultural technologies, fostering a dependable foundation for the evolution of smart agricultural practices. The work proposed a robust framework for ensuring the security of smart agriculture systems through advanced multiuser authentication and key generation techniques using Secure Elliptic Curve Cryptography (SECC). The framework's robustness is underscored by its ability to withstand evolving cyber threats and provide a resilient foundation for safeguarding sensitive agricultural data. Additionally, it represents innovative data encryption and decryption techniques using the suggested SECC methodology. Furthermore, this work conducts a comparative analysis between the Elliptic Curve Cryptography (ECC) based approach and the proposed SECC methodology in terms of enhanced performance and security. The results of this research work, highlight the substantial potential of data in agriculture to enhance the effectiveness and efficiency of smart farming services. It introduces an advanced secure defense strategy providing the protection of data and operational integrity against potential cyber threats through suggested SECC techniques. Moreover, the work represents a novel prevention strategy designed to safeguard against unauthorized access control attacks in the realm of smart agriculture.

Keywords: *Decryption, Encryption, Key Generation, SECC, Security Defense Strategy, Unauthorized Access Control Attack*

1. Introduction

The agricultural sector has undergone a remarkable transformation fueled by the emergence of smart agriculture in recent years. This innovative approach involves the integration of diverse digital technologies and interconnected systems, including satellite imagery, drones, IoT-based sensors, and automated machinery. These advancements are not only enhancing the precision and efficiency of farming practices but are also promoting sustainable agricultural practices. Smart agriculture is paving the way for optimized resource management, improved crop yields, and reduced environmental impact by leveraging real-time data and advanced analytics. However, the rapid digitization and network connectivity inherent in smart agriculture introduce complex security challenges. The vast amount of sensitive data generated and exchanged within these systems is susceptible to cyber threats. It poses significant risks to the confidentiality, integrity, and authenticity of agricultural information. Such vulnerabilities not only jeopardize operational efficiency but also threaten the very foundation of food security and safety. In light of these challenges, there is a pressing need for robust security mechanisms capable of protecting against man-in-the-middle attacks, unauthorized access, data breaches, and other cyber threats.

Addressing this critical issue, the present research endeavors to contribute significantly to the advancement of secure agricultural technologies. At the heart of this endeavor is the development of a robust security framework designed to protect smart agriculture systems from a myriad of cyber threats. This framework employs advanced multiuser authentication and key generation techniques, utilizing SECC to ensure the highest level of data security. The proposed multi-user authentication mechanism not only accommodates the varied profiles of users but also establishes a secure gateway, permitting only authorized entities access to pivotal agricultural data. Moreover, this work pioneers innovative encryption and decryption methods tailored for the agricultural sector, employing the SECC methodology to safeguard data transmission against evolving cyber threats.

This paper outlines the pressing need for enhanced security measures in smart agriculture, detailing the proposed SECC-based framework's capacity to provide a resilient defense against cyber threats. Through a comparative analysis of the proposed SECC framework and traditional

[1] *Department of Computer Science and Engineering, The Neotia University, Sarisha, Diamond Harbour Road, South 24 Parganas, West Bengal- 743368, India. bilashaldar@tnu.in, bilasphd2020@gmail.com*
[2] *Department of Robotics and Automation, The Neotia University, Sarisha, Diamond Harbour Road, South 24 Parganas, West Bengal-743368, India. prabinkumar.jha@tnu.in*
[3] *Department of Computer Science and Engineering, The Neotia University, Sarisha, Diamond Harbour Road, South 24 Parganas, West Bengal-743368, India. parthakumar.mukherjee@tnu.in, partha.mukh68@reduffmail.com*
** Corresponding Author Email: parthakumar.mukherjee@tnu.in, partha.mukh68@reduffmail.com*

Elliptic Curve Cryptography (ECC) approaches this research aims to demonstrate the superior performance and security features of the SECC methodology. The ultimate goal is to establish a secure, dependable foundation for the continued evolution of precision farming and smart agricultural practices, ensuring the protection of data and operational integrity against potential cyber threats. The work presents a novel security strategy designed to prevent unauthorized access control attacks, thereby reinforcing the resilience of smart agriculture systems in the face of growing cyber security challenges.

Objectives

The primary objectives of this research work are as follows:

1. To analyze the current state of smart agriculture, identifying key vulnerabilities and challenges in the security of interconnected systems and digital interfaces.
2. To design and develop a comprehensive security framework leveraging SECC. This framework specifically addresses the unique needs of smart agriculture systems through multiuser authentication and secure key generation techniques.
3. To innovate data encryption and decryption techniques utilizing the proposed Secure Elliptic Curve Cryptography methodology for smart agriculture applications.
4. To conduct a comparative performance and security analysis between the traditional ECC method and the proposed SECC methodology.
5. To introduce an advanced secure defense strategy for protecting agricultural data and operational integrity against potential cyber threats using the SECC technique.
6. To implement a novel strategy for preventing unauthorized access control attacks within smart agriculture.

The paper is organized according to the following structure: Section 2 provides a comprehensive review of relevant literature about the current landscape of smart agriculture. Section 3 presents our innovative methodology for ensuring the security of smart agriculture systems. Section 4 showcases simulation results and offers a discussion of the proposed methodology. Section 5 conducts a comparative analysis of the performance metrics achieved by our methodology against existing approaches. Furthermore, Section 6 explained security analysis and the application of our proposed approach in smart agriculture. To conclude, Section 7 presents insightful remarks, bringing closure to the paper.

2. Literature Review

The integration of digital technologies in agriculture, known as smart farming or precision agriculture, has significantly transformed traditional farming practices. However, this evolution brings about substantial security challenges that need to be addressed to protect agricultural systems from various cyber threats. Recent studies have introduced innovative approaches to key exchange, authentication, encryption, and decryption mechanisms reflected in smart applications. This literature review highlights significant advancements in cryptographic protocols and key management strategies that underpin the security of contemporary and emerging digital communication systems in smart agriculture. Yazdinejad et al. [1] extensively discussed the security challenges in Smart Farming and Precision Agriculture. The authors identified several types of cyberattacks that threaten these domains, including Man-In-The-Middle, Ransomware, Denial of Service, Botnets, and SQL injection. Ferrag et al. [2] introduced a deep learning-based intrusion detection system designed to mitigate DDoS attacks in Agriculture 4.0. Alyahya et al. [3] presented the Cyber Secured Framework for Smart Agriculture (CSFSA), which provides an authentication scheme for IoT devices. Jagadeeshwar et al. [4] introduced innovative safety mechanisms by employing Asymmetric Key Cryptography with the Related Key Security technique.

Friha et al. [5] examined emerging technologies for IoT-based smart agriculture, emphasizing the importance of addressing security concerns alongside technological advancements. Kethineni et al. [6] implemented an enhanced deep learning framework that addresses the challenges of data encryption and intrusion detection in smart agriculture. Singha et al. [7] proposed a secure communication system for wireless sensor networks in smart agriculture, where each communication step is encrypted using suitable cryptographic algorithms. Haldorai et al. [8] surveyed smart agriculture, focusing on various processing techniques and the integration of diverse technologies to enhance agricultural practices. Alex et al. [9] explored the deployment of IoT-based technologies and machine learning techniques in agriculture. Vangala et al. [10] analyzed potential attacks and threats, proposing an architecture for smart farming that is independent of underlying technologies. Kumari et al. [11] introduced a mutual authentication framework, leveraging elliptic curve cryptography, designed for two users in a secure communication network. Nikooghadam et al. [12] used elliptic curve cryptography to create a novel two-factor authentication and key agreement technique for the Session Initiation technique (SIP). Abduljabbar et al. [13] significantly advanced the existing literature with their contribution, unveiling a novel elliptic curve cryptography-based scheme that showcased formal security under the rigorous Burrows–Abadi–Needham (BAN) logic.

Jouini et al. [14] presented a novel authentication mechanism for IoT devices, integrating blockchain smart contracts into smart farming to enhance the security and reliability of device authentication. Samaranayake et al. [15] contributed by exploring an approach that leverages emerging technologies to improve the efficiency of applying for and receiving decisions on financing for rural farmers. Olakanmi et al. [16] focused on securing UAV-routed data transmission between farm-wide wireless sensor networks (FWSN) and the cloud server or ground base station in agricultural settings. Mahalingam et al. [17] designed a hybrid Recurrent Neural Elliptical Curve Blockchain (RNECB) technique to securely store sensed agricultural data in the cloud server. Kumar et al. [18] developed an IoT-based smart ecosystem for agriculture, evaluating their framework and demonstrating its potential to transform agricultural practices through enhanced connectivity and data driven decision-making. Itoo et al. [19] ventured into the realm of smart agriculture monitoring systems, offering a distinctive perspective by introducing a privacy-preserving and efficient key agreement framework. Truong et al. [20] explored a provable elliptic curve cryptography-based authentication scheme. This unique approach enables users to register with a trusted center, gaining authorization to access various service providers. Ametepe et al. [21] directed their attention to the creation of a secure service architecture tailored for data transmission within intelligent networks, with a specific application to crop monitoring in agricultural fields. Shuai et al. [22] presented an authentication scheme based on a public key-based cryptosystem, showcasing effectiveness against Man-in-the-Middle (MitM) and replay attacks. However, their study identified limitations, including vulnerabilities to privileged insider threats, user impersonation, and Ephemeral Secret Leakage (ESL) attacks.

Tian et al. [23] implemented a signature-based privacy-preserving methodology, aiming to address certain security issues. The technique does not ensure the anonymity and untraceability of the communication parties, and vulnerabilities to ESL attacks still exist. Kamble et al. [24] contributed to the field with the development of an efficient and provably secure lightweight authentication and key establishment protocol. Chae et al. [25] developed a protocol lacking user and device anonymity due to the public exchange of Internet Protocol (IP) addresses. Furthermore, the computation overhead associated with public key cryptography in digital signatures and certificates poses additional challenges, making it susceptible to various attacks [26]. Wu et al. [27] and Srinivas et al. [28] presented protocols with their own set of vulnerabilities, ranging from user anonymity violations to smart card loss attacks. Wu et al. [29] introduced a methodology that addressing certain issues, incurred high computation costs due to its reliance on bilinear pairing operations [30]. Kebotogetse et al. [31] developed a lightweight Elliptic Curve Authentication Scheme (ECCAS) that utilizes a bilinear map to construct an ideal elliptic curve.

The extensive literature review reveals a significant advancement in integrating digital technologies within the agricultural sector, particularly through smart farming and precision agriculture. While numerous studies have proposed various solutions to enhance the security of agricultural systems, several critical gaps and areas requiring further research have been identified. The research gaps focus on developing a holistic security framework that can seamlessly incorporate intrusion detection, secure communication protocols, and robust authentication mechanisms is essential. The literature review covers various applications and advancements in elliptic curve cryptography for enhancing security in multiple domains such as smart agriculture and secure communication networks. However, smart agriculture faces unique security threats, such as targeted attacks on critical infrastructure or theft of sensitive crop yield data. Addressing these gaps proposed work contributes significantly to the development of more robust, efficient, and secure multi-user authentication, and data exchange systems for smart agriculture using the SECC technique. This adaptive approach ensures the scalability and flexibility of the security system across the smart agriculture ecosystem.

3. Proposed Methodology

The proposed methodology centers on the development and implementation of a Secure Elliptic Curve Cryptography technique for enhancing the security of smart agriculture systems. This methodology is structured into several key phases such as multiparty key generation, authentication, encryption, and decryption techniques. Each phase is designed to address specific aspects of the security challenges within the context of smart agriculture. The SECC employed as a pivotal element in our proposed methodology, is a form of public-key cryptography leveraging the mathematical intricacies of elliptic curves over finite fields. It is founded on algebraic concepts related to elliptic curves over Galois Fields (GF), which may manifest as binary fields GF(2^n) or prime fields GF (P). The elliptic curves over the prime finite field FP, where $P > 3$ is an odd prime number, the equation defining the curve is given by $y^2 = (x^3 + a \times x + b) \% P$, with parameters a, b, and P characterizing the curve.

This SECC methodology offers a secure framework for parties involved in smart agriculture to exchange cryptographic keys and perform various cryptographic operations. Elliptic curves play a pivotal role in generating private and public keys, as well as in encrypting and decrypting messages. At the core of our methodology is the development of innovative data encryption and decryption techniques based on SECC. These techniques are designed

to provide a high level of data protection, ensuring that agricultural data remains confidential and tamper-proof during storage and transmission.

Cryptographic schemes built upon secure elliptic curve cryptography hinges on the inherent difficulty of solving elliptic curve discrete logarithms. This methodology aims to deliver a robust, secure, and adaptable framework that can safeguard smart agriculture systems against unauthorized access and cyber threats. In the context of SECC, the scalar multiplication process is pivotal, wherein an integer x and a point $P \in FP$ lead to the addition of P to itself x times, resulting in a point $Q = xP \in FP$. The discrete logarithm of point Q to base P, denoted as $\boldsymbol{k = Log_p Q}$ entails determining the value of x. This innovative approach is set against the backdrop of smart agriculture, characterized by the strategic utilization of advanced technologies and data analytics to optimize farming processes, enhance productivity, and minimize resources.

3.1 Key Generation

The pivotal key generation phase plays an important role in the creation of encryption, decryption, and authentication keys using SECC for the smart agriculture system. The suggested key generation process generates a pair of keys, comprising the public key and the private key. These keys collectively serve as the foundation for securing communications, maintaining data integrity, and enabling authentication within the smart agriculture framework. The public key is specifically designed to encrypt messages, producing unintelligible ciphertext, while the private key plays a crucial role in decrypting these messages. This key generation process involves creating a unique set of keys for each user denoted as $'U_{user}'$ incorporating arithmetic operations, a customized SECC technique, and modular arithmetic operations. It is worth noting that the parameter $'N_{max}'$ representing the maximum limit, must adhere to the requirement of being a prime number. This ensures the robustness of the generated keys that contribute to the overall security and effectiveness of the smart agriculture authentication system. An explanation of the key generation technique is presented in Algorithm 1.

Algorithm 1. Generation of keys using SECC technique

Require: Prime number Q_{secc}, Real numbers a_{agri}, b_{agri}

Ensure: N_{max} represents the maximum limit

1: Generate a prime number Q_{mecc} and points on the elliptic curve in KGP_{mecc}

2: Generate two constant real numbers such as a_{agri} and

b_{agri}

3: Select two distinct prime numbers such as $PQ1$ and $PQ2$

4: Calculate the value of $N_{agri} = PQ1 \times PQ2$

5: Calculate the value of $\phi(N_{agri}) = (PQ1-1) \times (PQ2-1)$

6: Generate points in KGP_{mecc} using $y^2 = (x^3 + a_{agri} \times x + b_{agri}) \% Q_{secc}$

7: Select a random point as G_{agri} from KGP_{mecc}

8: $PN_{user} \in GCD(PN_{user}, \phi(N_{agri})) = 1$ and $(1 < PN_{user} < N_{max})$

9: $Q_{user} = PN_{user} \times G_{agri}$

10: $PN_{agri} \in GCD(PN_{agri}, \phi(N_{agri})) = 1$ and $PN_{user} \neq PN_{agri}$ and $(1 < PN_{agri} < N_{max})$

11: $Q_{agri} = PN_{agri} \times G_{agri}$

12: Select the number of users as U_{user}

13: Generate U_{user} prime numbers, constituting a set

$Q1_{user}, Q2_{user}, Q3_{user}, Q4_{user}, \ldots\ldots\ldots QU_{user.}$

14: $I = 1$

15: **while** $I \leq QU_{user}$ **do**

16: $KD_{user}[I] = PN_{user} \times Q[I]_{user}$

17: $I = I + 1$

18: **end while**

19: $K_{user} = PN_{user} \times Q_{agri}$

20: $K_{agri} = PN_{agri} \times Q_{user}$

21: Return $KD_{user}, K_{user}, K_{agri}$

22: Exit

3.2 Authentication

Authentication within smart agriculture, employing Secure Elliptic Curve Cryptography, revolves around validating the identities of users within the agricultural system. The SECC offers a secure and efficient authentication technique utilizing public and private keys. This transformation process recon- structs the original key and also concurrently verifies users. Initially, users input their respective keys and apply the proposed authentication algorithm to regenerate a key, employing the greatest common divisor method. The subsequent step entails comparing the regenerated key with the original key. The successful authentication is confirmed if the regenerated key matches the original key, while unsuccessful authentication is declared otherwise. In this operation, the recipient dynamically generates both a public key and a private key. Subsequently, the receiver uses its private key to decrypt the received message in the

decryption process. The algorithm for the authentication technique is represented in Algorithm 2.

Algorithm 2. Authentication using the SECC technique

Require: Private key of user PN_{user} and Receiver key

$KD_{receiver}$

Ensure: $min_{threshold}$ denotes the minimum number of user

1: Fetch the values for $KD_{user}, PN_{user}, KD_{agri}$
2: Get authenticated user keys $KD_{receiver}$
3: $Count = 0$
4: **while** (I in $KD_{receiver}$) **do**
5: **if** (I match KD_{user}) **then**
6: $KD_{col}.append(I)$
7: $count = count + 1$
8: **end if**
9: $I = I + 1$
10: **end while**
11: Len = length(KD_{agri})
12: $Flag$ =0
13: **if** ($count > min_{threshold}$) **then**
14: $I = 1$
15: **while** ($I < Len$) **do**
16: $AU_{user} = GCD(KD_{col}[I], KD_{col}[I + 1])$
17: **if** ($AU_{user} \neq PN_{user}$) **then**
18: $Flag$ =1
19: Goto step 26
20: **end if**
21: $I = I+1$
22: **end while**
23: **else**
24: Exit
25: **end if**
26: **if** ($Flag \neq 1$) **then**
27: Print ("Authentication Successful")
28: **else**
29: Print ("Authentication unsuccessful")
30: **end if**
31: Exit

3.3 Encryption

Encryption stands as the foundational process for encoding a message, a crucial step in safeguarding it and restricting access solely to authorized entities. In the context of smart agriculture, where advanced technologies are harnessed to optimize farming practices, the implementation of encryption holds paramount importance in securing communications and data. The proposed encryption technique is used to encrypt authentication keys and agriculture data files. It employs a public key for encryption that is generated in the key generation process. The technique also performed elliptic curve point addition and multiplication operations to enhance the security of data transformation.

Algorithm 3. Encryption using the SECC technique

Require: Input data file M_{input} , Public key

Ensure: Points on the elliptic curve in KGP_{agri}

1: Input agriculture data file M_{input}
2: Select the block size indicated as PB
3: **while** (PM in M_{input}) **do**
4: $File_{MPA}$ += ASCII(PM)
5: **end while**
6: Len = Length ($File_{MPA}$)
7: $count = 0$
8: **while** K in (Len, PB) **do**
9: $MPB[K]$ += $File_{MPA}$
10: $count = count + 1$
11: **end while**
12: Retrieve the receiver's public key of the Q_{agri}
13: Retrieve the elliptic curve point G_{agri} from KGP_{agri}
14: Generate a random value as AKP_{user}, $\in 1 < AKP_{user} < N_{max}$
15: $PKI = 1$
16: **while** $PKI \leq count$ **do**
17: $Cipher1_{user} = AKP_{user} \times G_{agri}$
18: $Cipher2_{user} = MPB[PKI] + (AKP_{user} * Q_{agri})$
19: **end while**
20: Return ($Cipher1_{user}, Cipher2_{user}$)
21: Exit

The Python programming language is used to implement the suggested encryption technique. The pseudocode for the encryption technique is represented in Figure 1.

```
def SECC_Encryption(name):
    file_ = open(name,'rb')
    temp=''
    for i in file_:
        temp+=i.decode('ISO-8859-1')
    C1x = Qk * Qx
    C1y = Qk * Qy
    C2x = Qk * bx
    C2y = Qk * by
    Et1 = chr(C2x)
    Et2 = chr(C2y)
    In = [ord(c) for c in B]
    Bi = [bin(x) [2:].zfill(8) for x in In]
    Bii= ','.join(Bi)
    data = Bii
    key = Ebb
    Ekb = [bin(x)[2:].zfill(8) for x in out_arr]
    Dekripsi_xor = ''.join([chr(int(x, 2)) for x in Ekb])
```

Fig. 1. Pseudocode for encryption technique

3.4 Decryption

Decryption in cryptography serves as the inverse operation to encryption, involving the transformation of ciphertext back into plaintext through the suggested SECC algorithm. This process is instrumental in retrieving the original and intelligible information from the encrypted data. It contributes to the secure and efficient handling of sensitive agricultural data within the framework of smart agriculture. This decryption algorithm outlines the systematic process of decrypting a message, constructing a descriptor, subtracting points, and reversing big integers to ASCII numbers. It is a recon- version of ASCII numbers into strings to obtain the original plaintext message.

Algorithm 4. Decryption using the SECC technique

Require: Ciphertext data file $Cipher1_{user}$, $Cipher2_{user}$, private key

Ensure: Points on the elliptic curve in KGP_{agri}

1: Retrieve ciphertext message $Cipher1_{user}$, $Cipher2_{user}$

2: Read the receiver's private key PN_{agri}

3: Get block size PB same as the encryption block.

4: Read number of subblocks as *count* from Algorithm 3

5: $K = 1$

6: **while** $K \leq count$ **do**

7: $V_{datax} = Cipher1_{user}[K] \times PN_{agri}$

8: $V_{data} = Cipher2_{user}[K] - V_{datax}$

9: V_{datam} = convertdecimal (V_{datax}) 10: **end while**

11: **while** PM in V_{datam} **do**

12: $FilePdec$ = ASCIICharacter(PM)

13: **end while**

14: Return $FilePdec$

15: Exit

Figure 2 illustrates the workflow diagram of the proposed SECC methodology, detailing key generation, authentication, encryption, and decryption techniques. Initially, two unique random prime numbers are generated, followed by the creation of points on an elliptic curve using the equation $y^2 = x^3 + a \times x + b$. Subsequently, public and private keys are generated for users and agriculture servers. The suggested key generation methodology produces multiple distinct keys for each valid user denoted as $Q1_{key}$. The proposed encryption approach encrypted keys before the transformation. The agriculture server receives keys from valid users and regenerates the original keys. The server regenerates the secret key referred to as $Q2_{key}$ upon receiving multiple keys from users. Successful authentication at the first level is determined by matching $Q1_{key}$ with $Q2_{key}$, while a mismatch results in unsuccessful authentication. Additionally, a threshold value is generated upon receiving a minimum number of authenticated user keys. Successful authentication occurs when the threshold value matches with private keys otherwise, authentication is deemed unsuccessful.

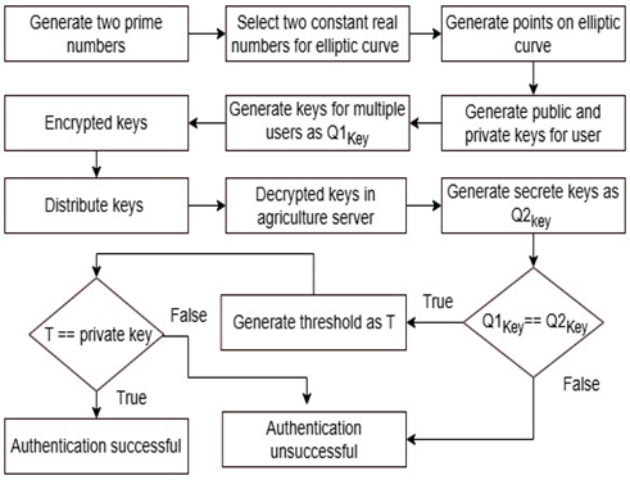


Fig. 2. Workflow diagram of the suggested SECC technique

4. Results and Discussion

This section showcases the outcomes obtained through the implementation of our proposed methodology. The development of a multiuser authentication technique provides a reliable solution against security threats in smart agriculture. The performance of the SECC technique is evaluated under various scenarios that highlight its robustness against potential security vulnerabilities. The SECC demonstrated efficiency in data encryption and decryption processes that ensure a secure communication

channel within a smart agriculture system. The efficiency of the suggested method extends to diverse file types that encompass large-size files. The results underscore the effectiveness of SECC in providing a strong cryptographic foundation for protecting sensitive agricultural information. This result ensures the capability of the proposed technique to safeguard sensitive information from unauthorized access.

Table 1. Key generation and regeneration time of the SECC methodology

Number of bits of prime numbers	***Key generation time (Second)***	***Key regeneration time (Second)***
7	0.2410904	0.1468078
10	0.3055334	0.1795418
14	0.3288754	0.2018005
17	0.3504902	0.2472077
20	0.4071637	0.2512503
24	0.4744303	0.2803021
27	0.5089006	0.3136643
30	0.5818327	0.3536291
34	0.7225547	0.4180559
37	0.7810534	0.4510523
40	0.8212382	0.5018034

Table 1 represents the key generation times of the proposed methodology across the number of bits of prime numbers. The key generation and regeneration time showcased efficiency and strength in facilitating secure communication among multiple users in the smart agriculture domain. The first column of the table denotes the number of bits of prime numbers which varies from 7 to 40. The key generation time using the proposed SECC technique showcases the second column from the left in the same table. There has been variability in the timeframe, with values ranging from 0.2410904 to 0.8212382 seconds. It highlights the computational complexity involved in dealing with larger prime numbers which is an essential factor in ensuring the security of the key generation technique. The key regeneration time of the suggested techniques varies from 0.1468078 to 0.5018034 seconds. Across all bit lengths, key generation times are consistently higher than key regeneration times. This suggests that the proposed SECC methodology is more efficient in regenerating keys than generating them from scratch. It is beneficial in dynamic environments where keys need to be frequently updated or regenerated.

Table 2. Encryption and decryption time of the SECC methodology

Data file size (MB)	***Encryption time (Second)***	***Decryption time (Second)***
11	167.1245	282.8755
22	235.8213	391.8012
30	272.2022	665.6707
42	364.1674	728.4452
55	475.4835	1104.3182
63	604.5683	1442.2543
75	726.1566	1552.2430
82	928.6230	1791.3708
90	1259.9154	1976.5865
97	1476.8941	2249.8235

This work presents encryption and decryption time analyses for diverse file types and sizes employing the suggested robust technique in Table 2. The proposed encryption and decryption techniques presented a formidable defense against potential data compromise during transmission. The leftmost column of Table 2 denotes the file sizes in megabytes (MB), ranging from 11 MB to 97 MB. The adjacent column illustrates the corresponding encryption durations using the proposed Secure Elliptic Curve Cryptography technique. Experimental results indicate encryption times ranging from 167.1245 to 1476.8941 seconds. Furthermore, the final column showcases the decryption times associated with the SECC methodology. Notably, the work elucidates that the time required for decryption exhibits variability within the range of 282.8755 to 2249.8235 seconds. A notable aspect of the results is the significant difference between encryption and decryption times, with decryption consistently taking longer than encryption across all data sizes. This suggests that the decryption process may involve more complex computations or steps than encryption, highlighting an area for potential optimization in the SECC methodology. Results indicated superior security and efficiency metrics for the proposed SECC approach in smart agriculture.

Experimental Setup

The experimental setup for this research employs the SECC methodology, executed using Python 3.11 on a 64-bit Microsoft Windows 10 platform. The hardware configuration includes an Intel Core™ i3-4160 processor operating at 3.6 GHz, complemented by 8 GB of DDR4 RAM. This setup ensures sufficient computational power and memory capacity to effectively implement and test the SECC methodology.

Table 3. Configuration details of the experimental setup

Simulation Parameters	Configuration
Host Operating System	Microsoft Windows 10, 64-bit
Host Primary Memory	8 Gigabytes DDR4
Programming Platform	Python 3.11
Host CPU	Intel Core TM i3 processor 4160
Processing Speed	3.6 GHz

5. Performance Analysis and Comparison

This section conducts a performance analysis, comparing key generation time, encryption time, and decryption time of the proposed methodologies. A detailed time analysis comparison between the modified ECC and the novel SECC approach is presented in the subsequent tables. Data tables and graphs provided in this section provide valuable insight into the performance of both methods across multiple types and sizes of data. The evaluation is enhanced by incorporating comprehensive tables and graphs, which provide a holistic view of what is happening with the algorithms. These metrics include key generation time, encryption time, and decrypting time. A comparative analysis between the proposed SECC methodology and the modified ECC methodology within smart agriculture systems revealed the superior performance of the novel approach. The outcomes underscored the potential of the SECC approach to outperform traditional methods, further solidifying its efficacy in securing smart farming services.

Figure 3 visually represents the data from Table 1, utilizing continuous solid and dashed lines. The graph illustrates the random generation of private keys, showcasing their impact on the overall process. An analysis reveals that an incremental increase in the number of bits of prime numbers correlates with a gradual rise in key generation time. Similarly, the key regeneration time exhibits a gradual increase with higher values of private keys. This discrepancy is attributed to the inherently higher computational complexity involved in the key generation process. The encryption process that involves key generation, demands more computational resources, resulting in a comparatively prolonged duration for key generation.

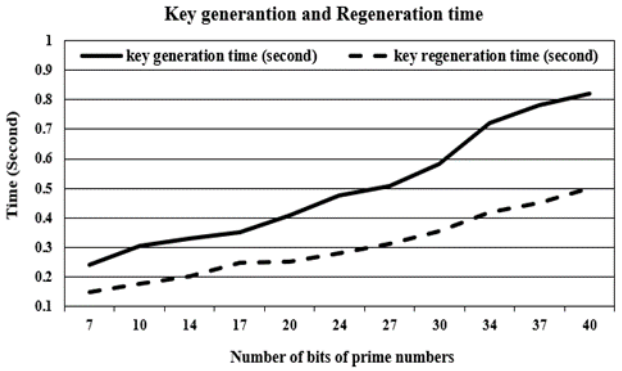


Fig. 3. Comparative analysis of key generation and regeneration time of the SECC technique

A visual representation of the encryption and decryption times of Table 2 is provided in Figure 4 using the proposed SECC methodology with continuous solid and dashed lines. The solid line corresponds to encryption time, while the dashed line signifies decryption time. Observations from the graph reveal fluctuations in decryption time, exhibiting both increases and decreases. This variability is influenced by the randomly generated private key values, as reflected in the graphical representation. The encryption time, in contrast, demonstrates a gradual increase, emphasizing the steady computational effort required for the encryption process.

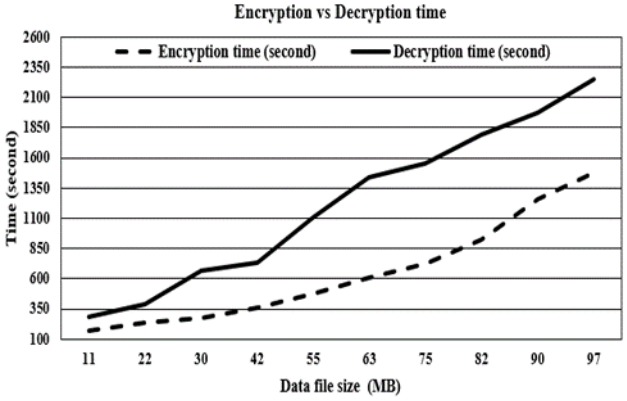


Fig. 4. Comparative analysis of encryption and decryption time of the SECC technique

Notably, decryption time exhibits exponential growth with larger file sizes. The graph highlights a critical point where, after a certain threshold, implementation becomes challenging due to significantly higher decryption times compared to encryption times. This elevated decryption time contributes to the robust security of our proposed methodology. The graph also visually conveys the intensive mathematical computations inherent in the proposed methodology. The correlation between computation complexity and decryption time is evident, emphasizing the meticulous nature of the security measures integrated into the system. Overall, this graphical representation provides insights into the dynamic relationship between file size, encryption time, and decryption time, affirming the robustness and security of the proposed SECC

methodology.

Table 4. Comparison of encryption times between the SECC and the modified ECC method

Data file size (MB)	*Proposed SECC (Second)*	*Modified ECC (Second) [32]*
11	167.1245	321.12
22	235.8213	543.42
30	272.2022	705.245
42	364.1674	820.1434
55	475.4835	1058.6701
63	604.5683	1182.3108
75	726.1566	1422.7892
82	928.623	1754.1808
90	1259.9154	1904.2601
97	1476.8941	2101.8934

A comparative analysis is conducted to assess the efficiency of encryption techniques between the SECC and Modified Elliptic Curve Cryptography [32] methodologies. Table 4 displays a comparative analysis of encryption times for the proposed SECC and modified ECC techniques. The second column details the encryption times achieved with the proposed SECC methodology, ranging from 167.1245 to 1476.8941 seconds. In contrast, the third column showcases encryption times using a modified ECC algorithm, fluctuating between 321.1200 and 2101.8934 seconds. The suggested methodology takes less encryption time than the modified ECC algorithms. The proposed SECC method demonstrated enhanced strength and efficiency in facilitating secure communication among multiple users. This comparison sheds light on the effectiveness of the SECC approach in addressing key exchange challenges in smart agriculture.

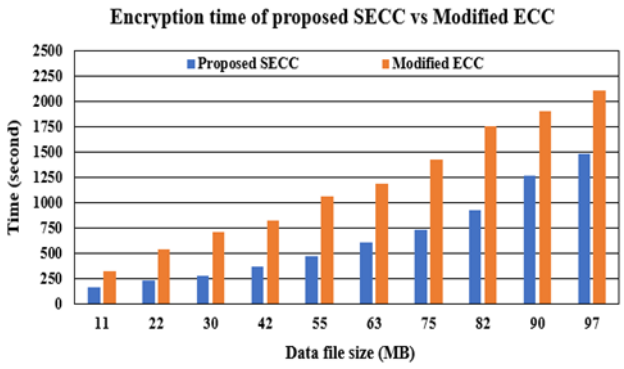


Fig. 5. Encryption time comparison of the proposed SECC and modified ECC methodology

Figure 5 visually represents the comparison outlined in Table 4. The blue bars depict the encryption times achieved with the proposed SECC methodology, while the orange bars represent the encryption times associated with modified ECC techniques [32]. It is evident that the proposed SECC methodology consistently results in shorter encryption times compared to the modified ECC methodology. Thus, the findings affirm that the proposed SECC methodology is faster than the modified ECC methodology. The outcomes of the comparative analysis highlighted the substantial potential of the proposed SECC methodology in enhancing the overall effectiveness and efficiency of smart farming services. This assessment is pivotal for understanding the real-world implications and practical benefits of adopting the proposed framework in smart agriculture systems.

Table 5. Comparison of decryption times between the SECC and the modified ECC method

Data file size (MB)	*Proposed SECC (Second)*	*Modified ECC (Second) [32]*
11	282.8755	402.5017
22	391.8012	547.4108
30	665.6707	806.3725
42	728.4452	1053.226
55	1104.3182	1641.2311
63	1442.2543	2012.8502
75	1552.243	2364.8405
82	1791.3708	2507.9073
90	1976.5865	2703.3405
97	2249.8235	3078.0153

The decryption times of the suggested SECC and modified ECC [32] approaches are contrasted in Table 5. The suggested SECC methodology's decryption time, which ranges from 282.8755 to 2249.8235 seconds, is shown in the second column. The decryption time using a modified ECC technique is shown in the third column from the left. There is a range in the encryption time from 402.5017 to 3078.0153 seconds. Measure the decryption time and reliability improvements facilitated by the SECC approach. Assess the methodology's ability to address concerns related to unauthorized access and data breaches.

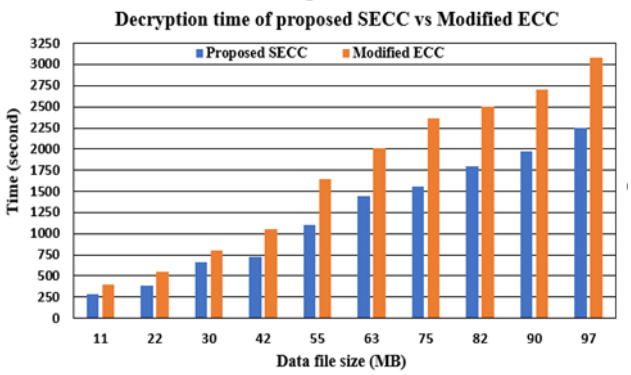


Fig. 6. Decryption time comparison of the proposed SECC and modified ECC methodology

Figure 6 displays the graphical depiction of Table 5. The blue bars in this image indicate the decryption time using the suggested SECC methods, whereas the orange bars show the decryption time using modified ECC [32]. Thus, it can be concluded that the suggested SECC technique requires less time for decryption than the ECC approach with changed decryption time. According to the suggested methodology's outcome, the modified technique is slower than the suggested methodology. The improved security measures and performance metrics position the SECC framework as a promising advancement in the field of secure agricultural technologies, providing a dependable foundation for the evolution of precision farming practices.

6. Security Analysis and Application

Data transformation and authentication processes must be thoroughly assessed for security vulnerabilities using Secure Elliptic Curve Cryptography. The SECC techniques renowned for their robust security features and comparatively compact key sizes, hinge their security on the complexity of the Elliptic Curve Discrete Logarithm Problem. It evaluates the robustness of the multiuser authentication mechanism in verifying the legitimacy of users within the smart agricultural system. The mathematical complexity of the proposed methodology assesses its resilience against various cyber security attacks. The deliberate use of random points on an elliptic curve further fortifies the methodology against potential security threats. The large random prime number selection and harder points addition technique increase more complexity and security of the key generation process of the SECC technique. The harder encryption and decryption technique resilience against cyber threats targeting sensitive agricultural data.

6. 1 Man-in-the-Middle (MITM) attack

A man-in-the-middle (MITM) attack occurs when an intruder intercepts, modifies, and retransmits messages between two parties, making them believe they are communicating directly with each other. The proposed SECC-based authentication techniques mitigate this threat by ensuring secure initial communication and verifying the identity and public key pair of the user, preventing any adversary from tampering with this information. In this approach, the user's private key components are PN_{user} and Q_{user}. The methodology involves selecting two distinct large prime numbers, *PQ1* and *PQ2*. The value of PN_{user} is determined such that $PN_{user} \in GCD(PN_{user}, \phi(N_{agri})) = 1$ and $(1 < PN_{user} < N_{max})$. The value of ϕ(Nagri) is calculated as $\phi(N_{agri}) = (PQ1 - 1) \times (PQ2 - 1)$. The private key, Q_{user}, is computed as $Q_{user} = PN_{user} \times G_{agri}$, where G_{agri} is a randomly selected point on the elliptic curve calculated using $y^2 = (x^3 + a_{agri} \times X + b_{agri}) \% Q_{secc}$. To enhance the security of the multi-user authentication process, keys are generated using $KD_{user}[I] = PN_{user} \times Q[I]_{user}$, where *I* ranges from 1 to QU_{user}. The authentication methodology employs a minimum threshold to ascertain the required number of valid users. This is expressed as $AU_{user} = GCD(KD_{col}[I], KD_{col}[I + 1])$, where *'count'* tracks the number of valid users. If the count exceeds the minimum threshold and $AU_{user} \neq PN_{user}$, authentication fails; otherwise, it succeeds.

This two-level authentication technique provides robust security. An attacker would face significant difficulty accessing the system because generating the authentication keys requires knowledge of the complex mathematics involved in 'G_{agri}' point generation. The private key's value depends on $\phi(N_{agri})$, which is derived from the large prime numbers *PQ1* and *PQ2*. Generating these primes through a backtracking process is exceedingly difficult, making an MITM attack infeasible. The detailed key generation and authentication methodologies are presented in Algorithms 1 and 2, demonstrating the robustness of the proposed SECC-based authentication techniques against man-in-the-middle attacks.

6. 2 Unauthorized Access Control Attack

An Unauthorized Access Control Attack is a cyberattack where an intruder exploits vulnerabilities in access control systems to gain unauthorized entry to resources or sensitive data. In the context of agriculture, unauthorized access to critical information such as crop and farm data, weather forecasts, and financial records can lead to serious privacy breaches and misuse of valuable data. The suggested multi-user authentication technique is recommended to counter such threats in smart agriculture. This method enhances security by requiring multiple authentication factors, thereby bolstering defenses against unauthorized access control attacks. Additionally, the proposed encryption technique is used to transfer data over the network. The proposed approach involves employing mathematical operations that ensure strong security during data transformation. A random value, AKP_{user}, within the range $(1 < AKP_{user} < N_{max})$, is generated for encryption. Data values are encrypted using $Cipher1_{user} = AKP_{user} \times G_{agri}$ and $Cipher2_{user} = MPB[PKI] + (AKP_{user} * Q_{agri})$, where Q_{agri} is

determined during the key generation process. During decryption, values are computed using $V_{datax} = (Cipher1_{user}[K] \times PN_{agri})$ and $V_{data} = (Cipher2_{user}[K] - V_{datax})$. This process ensures data integrity and confidentiality. Importantly, breaking the data values would require knowledge of the private key PN_{agri}, which is generated uniquely during the key generation phase and cannot be reconstructed through backtracking methods. This inherent security measure prevents unauthorized access to the data. This methodology, integrating multi-user authentication and strong encryption techniques, provides robust security against unauthorized access control attacks. The SECC technique, illustrated in Algorithm 5, serves as a comprehensive prevention strategy that fortifies the security posture against potential threats in smart agriculture.

Algorithm 5. Unauthorized access control prevention strategy using SECC technique

Require: User ID, password, and agriculture data

Ensure: key generation, encryption, decryption, and authentication technique

Input UID_{farmer}, $PASS_{farmer}$, $Data_{agri}$

$UKEY_{farmer}$ = Keygeneration(UID_{farmer}, $Pass_{farmer}$)

if ($UKEY_{farmer} == NULL$) **then**

  Print ("Key generation unsuccessful")

  Goto step 1

else

  $Distribute_{keys} = Encryption(UKEY_{farmer})$

  if ($Distribute_{keys} \neq 1$) **then**

    Print ("Key Encryption Unsuccessful")

    Exit

  else

    Print ("Key Encryption successful")

  end if

end if

$MKEY_{farmar} = Authentication(Distribute_{keys})$

if ($MKEY_{farmar} == 1$) **then**

Print("Authentication successful")

$C_{data} = Encryption(Data_{agri})$

if ($C_{data} == NULL$) **then**

  Print("Data encryption unsuccessful")

else

$Cdata_{agri} = AgricultureDatabaseServer(C_{data})$

Print("Encrypted data store in database")

$Decryption(Cdata_{agri})$

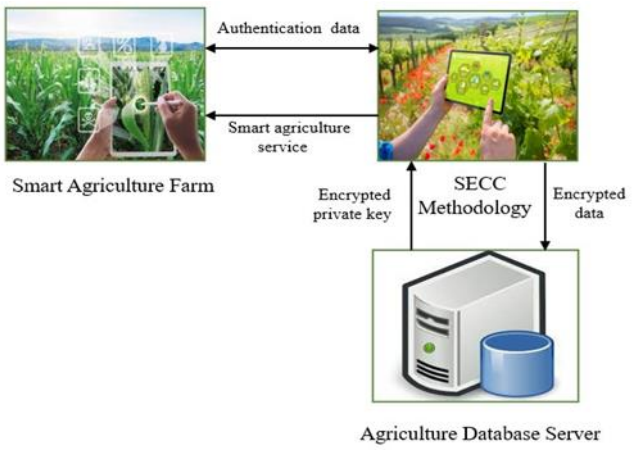
end if

end if

Exit

6.3 Application in Smart Agriculture

Smart agriculture utilizes advanced technologies to enhance the efficiency, productivity, and sustainability of farming operations. It leverages a combination of Information and Communication Technologies, automation, and sensors to optimize decision-making and resource utilization in farming. The proposed SECC technique is used in smart agriculture to improve security in a smart agriculture system. The application of SECC in smart agriculture contributes to building a secure and resilient foundation for precision farming practices, safeguarding data, and ensuring the reliable operation of interconnected agricultural systems. The proposed conceptual framework is illustrated in Figure 7 using the SECC technique. These frameworks are designed to effectively mitigate cyber threats within the realm of smart agriculture. The SECC technique is employed to ensure the secure transmission of sensitive data between devices within smart agriculture systems. This encompasses the encryption of sensitive agricultural data and authentication information using the robust SECC methodology. Furthermore, the multi-user authentication schemes are instrumental in verifying the identities of individuals interacting with the smart agriculture system.



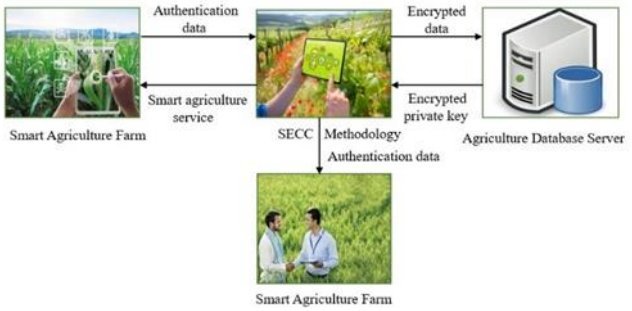


Fig. 7. Smart agriculture conceptual framework using the SECC methodology

Agriculture database server plays a crucial role in modern farming practices that enable efficient data management, and decision-making processes. The farmer provides authentication data in a smart agriculture farm system. The authentication data are encrypted through the SECC technique. This encrypted data is subsequently transmitted to the agricultural database server. The agriculture database server serves as a robust foundation for managing, analyzing, and retrieving agricultural data for smart agriculture systems. The database server sends the encrypted private key to the SECC methodology. The SECC methodology then decrypts the data value and verifies user authenticity through a multi-user authentication technique. It provides service to the user after successful authentication.

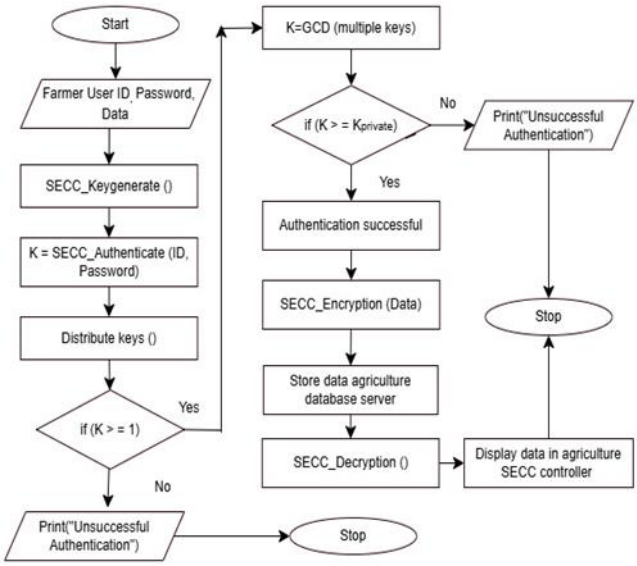


Fig. 8. Security defense strategy in smart agriculture

Figure 8 showcases the security defense strategy of the proposed methodology in smart agriculture The proposed key generation, authentication, encryption, and decryption techniques can be applied in smart agriculture to ensure secure communication, confidentiality, and data integrity. The key generation techniques generate a public and private key pair using the SECC technique for each entity involved in smart agriculture. The private key should be securely stored on the device. The multiple public keys are distributed to all the authenticated users. The suggested SECC authentication methodology is used to establish a secure authentication process. It generates the value of K in the authentication technique. It compares the value of K with $K_{private}$. If it is the satisfied condition the authentication is successful otherwise authentication unsuccessful. The proposed authentication provided higher security to access data value from unauthorized users. After successful authentication, SECC encryption methodology is used to encrypt sensitive smart agriculture data to ensure confidentiality during transmission. Then data values are stored in the agriculture database server. After decryption data values view in the agriculture SECC controller. The suggested decryption process provided robust security for data transformation in smart agriculture.

7. Conclusion

This research underscores the critical importance of securing agricultural data amidst the rapid evolution of smart agriculture. The integration of cutting-edge technologies has undoubtedly revolutionized farming practices, yet it also brings forth challenges regarding data confidentiality, integrity, and authenticity. This work contributes significantly to addressing these challenges through the development of a robust security framework utilizing Secure Elliptic Curve Cryptography. The proposed methodology presents innovative multiuser authentication and key generation techniques. This work introduces novel stronger encryption and decryption techniques using SECC methodology. It is paramount for the sustainability and advancement of smart agriculture farming systems. The comparative analysis demonstrated the faster performance, efficiency, and enhanced security features of the SECC methodology over traditional ECC approaches for encryption and decryption times. This underscores the importance of adopting robust and innovative security measures to protect sensitive agricultural data. Furthermore, this research introduces a novel security defense strategy along with a smart agriculture conceptual framework employing the SECC technique. The framework's resilience stands out as an important highlight as it shows that it can survive changing cyber threats and provides an adequate foundation for conserving sensitive agricultural data. The suggested unauthorized access control prevention strategy contributes to preventing unauthorized access control attacks and provides more security for data transformation.

The future direction of the research work incorporates advanced cryptography and machine learning algorithms to enhance anomaly detection and intrusion prevention capabilities within smart agriculture systems. This can involve training models on historical attack patterns to predict and prevent future security breaches in smart agriculture systems.

Conflicts of interest

The authors confirm that this article's contents have no conflict of interest.

Acknowledgments

The authors would like to acknowledge there are no financial support funds.

References

[1] A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, H. Karimipour, E. Fraser, A. G. Green, C. Russell, and E. Duncan, "A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures," Applied Sciences, vol. 11, no. 16, p. 7518, 2021.

[2] M. A. Ferrag, L. Shu, H. Djallel, and K.-K. R. Choo, "Deep learning- based intrusion detection for distributed denial of service attack in agriculture 4.0," Electronics, vol. 10, no. 11, p. 1257, 2021.

[3] S. Alyahya, W. U. Khan, S. Ahmed, S. N. K. Marwat, and S. Habib, "Cyber secure framework for smart agriculture: Robust and tamper- resistant authentication scheme for iot devices," Electronics, vol. 11, no. 6, p. 963, 2022.

[4] M. Jagadeeshwar, D. Shanthi, M. P. "Automated Data Security Model Using Cryptography Techniques in Cloud Environment". International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 3, pp. 1910-7, 2024.

[5] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of things for the future of smart agriculture: A comprehensive survey of emerging technologies," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 4, pp. 718–752, 2021.

[6] K. Kethineni and P. Gera, "Iot-based privacy-preserving anomaly detection model for smart agriculture," Systems, vol. 11, no. 6, p. 304, 2023.

[7] A. Singha, N. Mumenin, N. I. Akhter, M. S. H. Moon, and M. U. Ahmed, "A lightweight cryptographic scheme to secure wsns in agriculture," in Proceedings of Trends in Electronics and Health Informatics: TEHI 2021, pp. 615–624, Springer, 2022.

[8] A. Haldorai, S. Murugan, and M. Balakrishnan, "Significance of ai in smart agriculture: Methods, technologies, trends, and challenges," Artificial Intelligence for Sustainable Development, pp. 3–25, 2024.

[9] N. Alex, C. Sobin, and J. Ali, "A comprehensive study on smart agriculture applications in india," Wireless Personal Communications, vol. 129, no. 4, pp. 2345–2385, 2023.

[10] A. Vangala, A. K. Das, V. Chamola, V. Korotaev, and J. J. Rodrigues, "Security in iot-enabled smart agriculture: Architecture, security solutions, and challenges," Cluster Computing, vol. 26, no. 2, pp. 879–902, 2023.

[11] A. Kumari, M. Yahya Abbasi, V. Kumar, and A. A. Khan, "A secure user authentication protocol using elliptic curve cryptography," Journal of Discrete Mathematical Sciences and Cryptography, vol. 22, no. 4, pp. 521–530, 2019.

[12] M. Nikooghadam and H. Amintoosi, "A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol," Security and Privacy, vol. 3, no. 1, p. e92, 2020.

[13] Z. A. Abduljabbar, V. O. Nyangaresi, H. M. Jasim, J. Ma, M. A. Hus- sain, Z. A. Hussien, and A. J. Aldarwish, "Elliptic curve cryptography- based scheme for secure signaling and data exchanges in precision agriculture," Sustainability, vol. 15, no. 13, p. 10264, 2023.

[14] O. Jouini and K. Sethom, "A blockchain based authentication mechanism for iot in agriculture 4.0," in International Conference on Advanced Information Networking and Applications, pp. 67–76, Springer, 2023.

[15] P. Samaranayake and P. Ranasinghe, "Improving agriculture financing opportunities for farmers using blockchain technology: A proof-of- concept development and case scenario illustration," in Emerging Tech- nologies in Business: Innovation Strategies for Competitive Advantage, pp. 193–218, Springer, 2024.

[16] O. O. Olakanmi, M. S. Benyeogor, K. P. Nnoli, and K. O. Odeyemi, "Uav-enabled wsn and communication framework for data security, acquisition and monitoring on large farms: A panacea for real-time precision agriculture," in Advanced Technology for Smart Environment and Energy, pp. 17–33, Springer, 2023.

[17] N. Mahalingam and P. Sharma, "An intelligent blockchain technology for securing an iot-based agriculture monitoring system," Multimedia Tools and Applications, vol. 83, no. 4, pp. 10297–10320, 2024.

[18] C. Senthil kumar and R. Vijay Anand, "Security in iot-enabled smart agriculture systems," in Communication Technologies and Security Challenges in IoT: Present and Future, pp. 279–300, Springer, 2024.

[19] S. Itoo, A. A. Khan, M. Ahmad, and M. J. Idrisi, "A secure and privacy-preserving lightweight authentication and key exchange algorithm for smart agriculture monitoring system," IEEE , 2023.

[20] T.-T. Truong, M.-T. Tran, A.-D. Duong, P.-N. Nguyen-Pham, H.-A. Nguyen, and T.-N. Nguyen, "Provable user authentication scheme on ecc in multi-server environment," The Journal of Supercomputing, vol. 79, no. 1, pp. 725–761, 2023.

[21] A. F.-X. Ametepe, S. A. R. Ahouandjinou, and E. C. Ezin, "Secure encryption by combining asymmetric and symmetric cryptographic method for data collection wsn in smart agriculture," in 2019 IEEE International Smart Cities Conference (ISC2), pp. 93–99, IEEE, 2019.

[22] M. Shuai, L. Xiong, C. Wang, and N. Yu,"A secure authentication scheme with forward secrecy for industrial IoT using rabin cryptosystem" Computer Communications,vol.160 pp.215–227, 2020.

[23] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted internet of drones," Journal of Information Security and Applications, vol. 48, p. 102354, 2019.

[24] A. Kamble, V. Gaikwad, and J. Tembhurne, "A provably lightweight mutually authentication and key establishment protocol using extended chaotic map for telecare medicine information system," International Journal of Information Technology, pp. 1–17, 2023.

[25] C.-J. Chae and H.-J. Cho, "Enhanced secure device authentication algorithm in p2p-based smart farm system," Peer-to-peer networking and applications, vol. 11, pp. 1230–1239, 2018.

[26] V. O. Nyangaresi, Z. A. Abduljabbar, K. A.-A. Mutlaq, J. Ma, D. G. Honi, A. J. Aldarwish, and I. Q. Abduljaleel, "Energy efficient dynamic symmetric key based protocol for secure traffic exchanges in smart homes," Applied Sciences, vol. 12, no. 24, p. 12688, 2022.

[27] F. Wu, L. Xu, S. Kumari, and X. Li, "A new and secure authentication scheme for wireless sensor networks with formal proof," Peer-to-Peer Networking and Applications, vol. 10, pp. 16–30, 2017.

[28] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," Ad Hoc Networks, vol. 54, pp. 147–169, 2017.

[29] H.-T. Wu and C.-W. Tsai, "An intelligent agriculture network security system based on private blockchains," Journal of Communications and Networks, vol. 21, no. 5, pp. 503–508, 2019.

[30] I. Q. Abduljaleel, Z. A. Abduljabbar, M. A. Al Sibahee, M. J. J. Ghrabat, J. Ma, and V. O. Nyangaresi, "A lightweight hybrid scheme for hiding text messages in colour images using lsb, lah transform and chaotic techniques," Journal of Sensor and Actuator Networks, vol. 11, no. 4, p. 66, 2022.

[31] Otisitswe Kebotogetse. "A Secured Elliptic Curve Cryptography Authentication Scheme for Advanced Metering Infrastructure Communication". International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 3, 2024, pp. 4182-8,. 2024.

[32] D. Natanael, D. Suryani, et al., "Text encryption in android chat applications using elliptical curve cryptography (ecc)," Procedia Computer Science, vol. 135, pp. 283–291, 2018.