International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

# Digital Forensics in Agriculture: A Systematic Analysis of Security Challenges, Tools, and Applications in Smart Farming

Himanshu Shukla, Abhishek Verma
Department of Information Technology, College of
Technology, Govind Ballabh Pant University of Agriculture
and Technology, Pantnagar, India
himanshusgnps@gmail.com, abhishekverma09062000@gmail.com

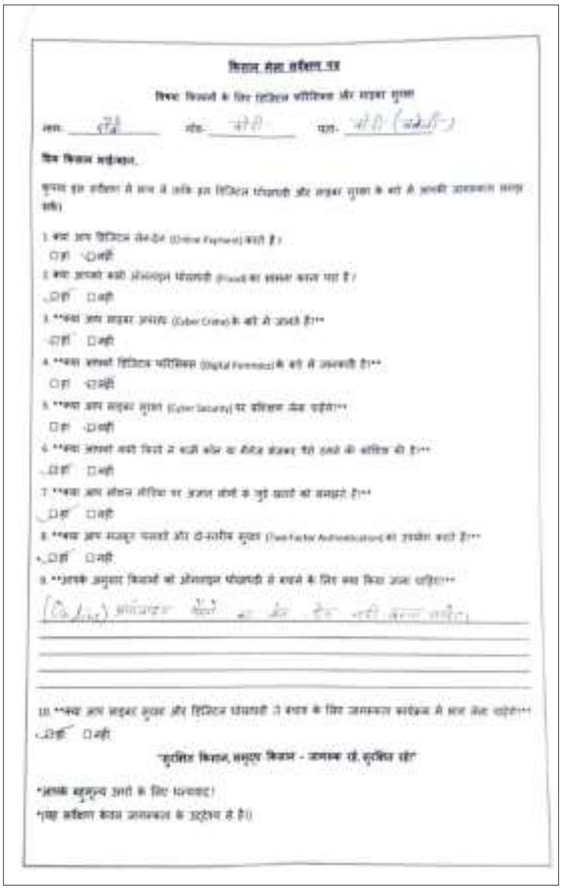
## Abstract

The emergence of Agriculture 4.0 has led to a significant transformation in farming practices through the integration of smart technologies, including Internet of Things (IoT) devices, drones, autonomous machinery, and cloud-based platforms. While these advancements have enhanced operational efficiency and data-driven decision-making, they have also introduced complex cybersecurity risks and digital vulnerabilities. In response to these threats, digital forensics has become an essential discipline for identifying, collecting, analyzing, and preserving digital evidence within agricultural systems. This paper presents a comprehensive and systematic analysis of the current state of digital forensics in agriculture, drawing upon literature published between 2018 and 2024. It explores the unique forensic challenges posed by heterogeneous Ag-IoT environments, limited tool compatibility, real-time data volatility, and legal considerations. Emerging technologies such as artificial intelligence, machine learning, blockchain, and drone forensics are examined for their potential to enhance forensic capabilities in smart farming contexts. Real-world case studies are analyzed to illustrate practical challenges and gaps in forensic readiness. The review concludes by identifying critical areas for future research, emphasizing the need for scalable forensic frameworks, specialized training, and robust policy development to support secure and resilient agricultural ecosystems.

***Keywords:*** *Digital forensics, Smart agriculture, IoT forensics, Cybersecurity, Blockchain; Drone forensics, Forensic readiness, AI in forensics, Ag-IoT security*

## 1. Introduction and Survey

The agricultural sector is undergoing a transformative shift through the integration of digital technologies, commonly referred to as Agriculture 4.0. This revolution is characterized by the adoption of Internet of Things (IoT), cloud computing, remote sensing, artificial intelligence (AI), and big data analytics to enhance productivity, sustainability, and decision-making in farming practices. While these advancements are accelerating efficiency and innovation across the agricultural value chain, they also introduce new and evolving cybersecurity risks. As farms become increasingly connected through smart devices and automated systems, the attack surface for cyber threats has expanded significantly. Incidents such as ransomware attacks on agricultural software providers and unauthorized access to critical sensor networks highlight the sector's vulnerability. These threats not only jeopardize operational continuity but can disrupt national food supply chains and compromise sensitive agricultural data. In this context, digital forensics emerges as a critical discipline. It provides the tools and methodologies necessary to detect, investigate, and respond to cyber incidents in smart farming environments. However, the application of digital forensics in agriculture remains underexplored. This paper presents a systematic analysis of security challenges, forensic tools, and practical applications in the context of Agriculture 4.0. To incorporate ground-level insights, a field survey was conducted with farmers during the 117th Kisan Mela at Pantnagar University in 2025. Participants from diverse regional backgrounds shared cybersecurity concerns and digital risks encountered in smart farming. Their responses are supported with visuals and case-based figures to contextualize the digital forensic challenges.



किसान मेला सर्वेक्षण पत्र

विषय: किसानों के लिए डिजिटल फॉरेंसिक और साइबर सुरक्षा

नाम: [illegible] गाँव: [illegible] पता: [illegible]

प्रिय किसान भाई/बहन,

कृपया इस सर्वेक्षण में भाग लें ताकि हम डिजिटल धोखाधड़ी और साइबर सुरक्षा के बारे में आपकी जागरूकता समझ सकें।

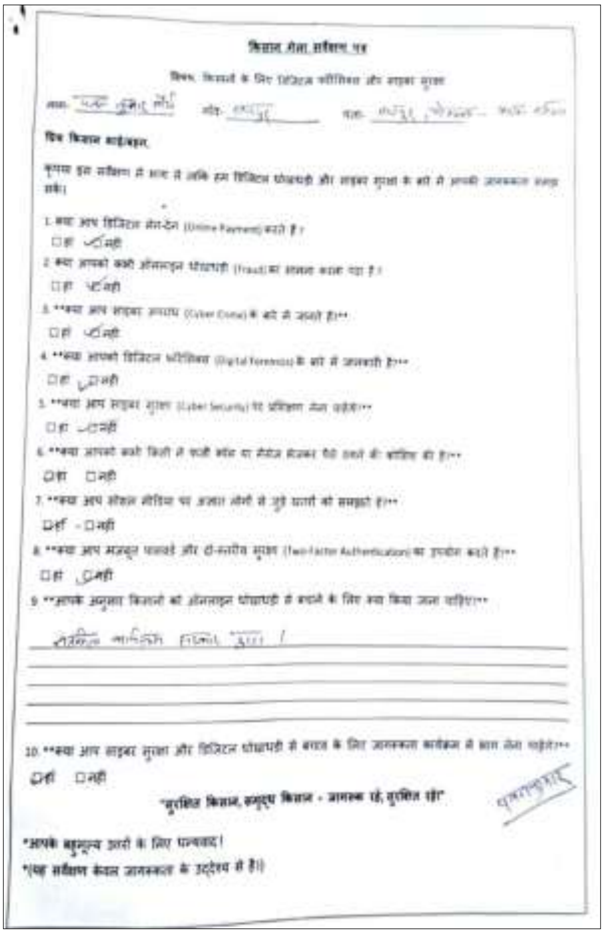
1. क्या आप डिजिटल लेन-देन (Online Payment) करते हैं?
□ हाँ ☑ नहीं
2. क्या आपको कभी ऑनलाइन धोखाधड़ी (Fraud) का सामना करना पड़ा है?
☑ हाँ □ नहीं
3. **क्या आप साइबर अपराध (Cyber Crime) के बारे में जानते हैं?**
☑ हाँ □ नहीं
4. **क्या आपको डिजिटल फॉरेंसिक (Digital Forensics) के बारे में जानकारी है?**
□ हाँ ☑ नहीं
5. **क्या आप साइबर सुरक्षा (Cyber Security) पर प्रशिक्षण लेना चाहेंगे?**
□ हाँ ☑ नहीं
6. **क्या आपको कभी किसी ने फर्जी कॉल या मैसेज भेजकर पैसे ठगने की कोशिश की है?**
☑ हाँ □ नहीं
7. **क्या आप सोशल मीडिया पर अजनबी लोगों से जुड़े खतरों को समझते हैं?**
☑ हाँ □ नहीं
8. **क्या आप मजबूत पासवर्ड और दो-स्तरीय सुरक्षा (Two-Factor Authentication) का उपयोग करते हैं?**
☑ हाँ □ नहीं
9. **आपके अनुसार किसानों को ऑनलाइन धोखाधड़ी से बचाने के लिए क्या किया जाना चाहिए?**

(Online) ऑनलाइन पैसों [illegible] नहीं करना चाहिए।

10. **क्या आप साइबर सुरक्षा और डिजिटल धोखाधड़ी से बचाव के लिए जागरूकता कार्यक्रम में भाग लेना चाहेंगे?**
☑ हाँ □ नहीं

"सुरक्षित किसान, समृद्ध किसान - जागरूक रहें, सुरक्षित रहें!"

*आपके बहुमूल्य उत्तरों के लिए धन्यवाद!
*(यह सर्वेक्षण केवल जागरूकता के उद्देश्य से है।)



किसान मेला सर्वेक्षण पत्र

विषय: किसानों के लिए डिजिटल फॉरेंसिक और साइबर सुरक्षा

नाम: [illegible] कुमार [illegible] गाँव: [illegible] पता: [illegible]

प्रिय किसान भाई/बहन,

कृपया इस सर्वेक्षण में भाग लें ताकि हम डिजिटल धोखाधड़ी और साइबर सुरक्षा के बारे में आपकी जागरूकता समझ सकें।

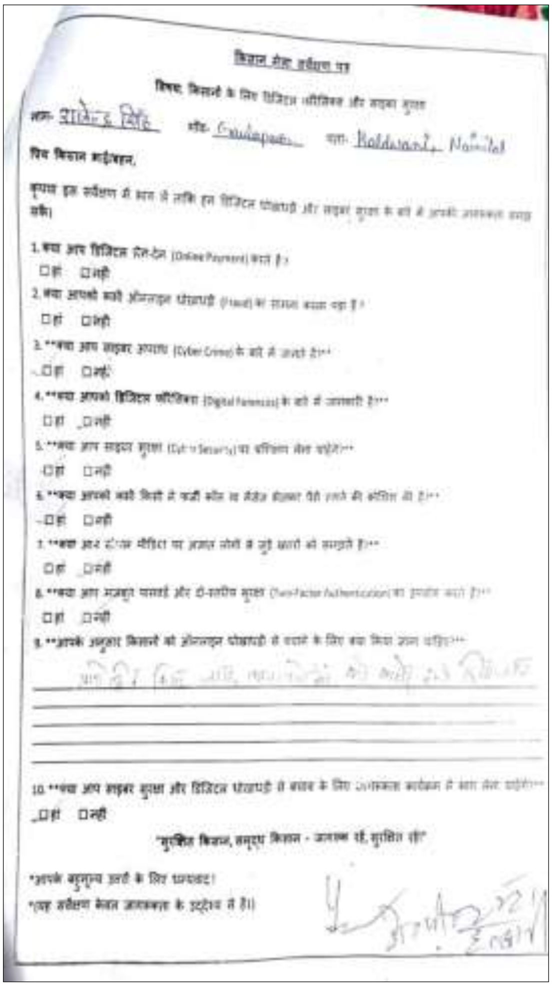
1. क्या आप डिजिटल लेन-देन (Online Payment) करते हैं?
□ हाँ ☑ नहीं
2. क्या आपको कभी ऑनलाइन धोखाधड़ी (Fraud) का सामना करना पड़ा है?
□ हाँ ☑ नहीं
3. **क्या आप साइबर अपराध (Cyber Crime) के बारे में जानते हैं?**
□ हाँ ☑ नहीं
4. **क्या आपको डिजिटल फॉरेंसिक (Digital Forensics) के बारे में जानकारी है?**
□ हाँ ☑ नहीं
5. **क्या आप साइबर सुरक्षा (Cyber Security) पर प्रशिक्षण लेना चाहेंगे?**
□ हाँ ☑ नहीं
6. **क्या आपको कभी किसी ने फर्जी कॉल या मैसेज भेजकर पैसे ठगने की कोशिश की है?**
☑ हाँ □ नहीं
7. **क्या आप सोशल मीडिया पर अजनबी लोगों से जुड़े खतरों को समझते हैं?**
☑ हाँ □ नहीं
8. **क्या आप मजबूत पासवर्ड और दो-स्तरीय सुरक्षा (Two-Factor Authentication) का उपयोग करते हैं?**
□ हाँ ☑ नहीं
9. **आपके अनुसार किसानों को ऑनलाइन धोखाधड़ी से बचाने के लिए क्या किया जाना चाहिए?**

[illegible]

10. **क्या आप साइबर सुरक्षा और डिजिटल धोखाधड़ी से बचाव के लिए जागरूकता कार्यक्रम में भाग लेना चाहेंगे?**
☑ हाँ □ नहीं

"सुरक्षित किसान, समृद्ध किसान - जागरूक रहें, सुरक्षित रहें!"

*आपके बहुमूल्य उत्तरों के लिए धन्यवाद!
*(यह सर्वेक्षण केवल जागरूकता के उद्देश्य से है।)



किसान मेला सर्वेक्षण पत्र

विषय: किसानों के लिए डिजिटल फॉरेंसिक और साइबर सुरक्षा

नाम: [illegible] सिंह गाँव: Gaulapar पता: Haldwani, Nainital

प्रिय किसान भाई/बहन,

कृपया इस सर्वेक्षण में भाग लें ताकि हम डिजिटल धोखाधड़ी और साइबर सुरक्षा के बारे में आपकी जागरूकता समझ सकें।

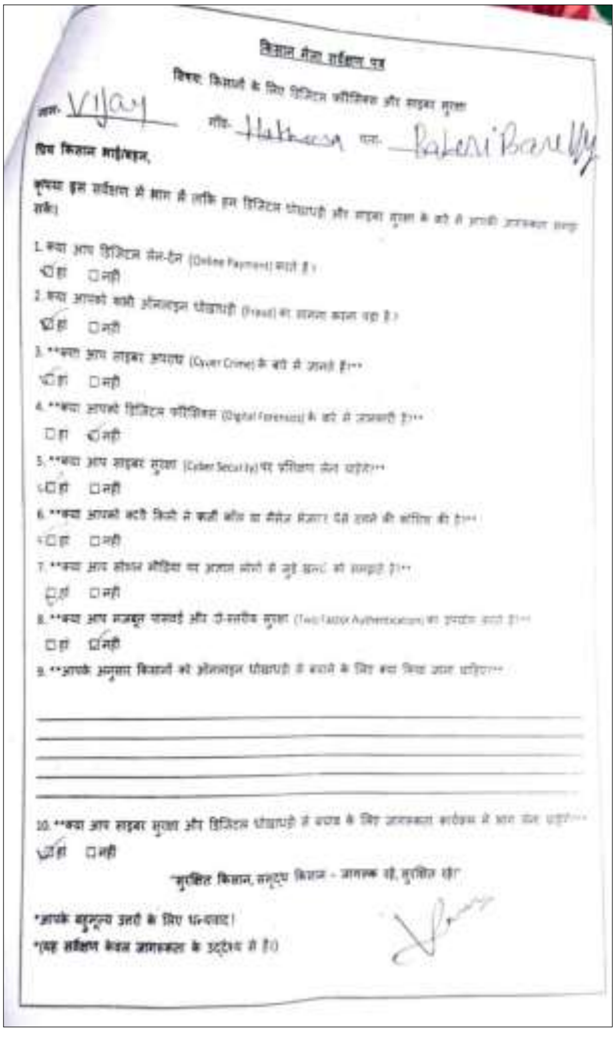
1. क्या आप डिजिटल लेन-देन (Online Payment) करते हैं?
□ हाँ □ नहीं
2. क्या आपको कभी ऑनलाइन धोखाधड़ी (Fraud) का सामना करना पड़ा है?
□ हाँ □ नहीं
3. **क्या आप साइबर अपराध (Cyber Crime) के बारे में जानते हैं?**
☑ हाँ □ नहीं
4. **क्या आपको डिजिटल फॉरेंसिक (Digital Forensics) के बारे में जानकारी है?**
□ हाँ ☑ नहीं
5. **क्या आप साइबर सुरक्षा (Cyber Security) पर प्रशिक्षण लेना चाहेंगे?**
☑ हाँ □ नहीं
6. **क्या आपको कभी किसी ने फर्जी कॉल या मैसेज भेजकर पैसे ठगने की कोशिश की है?**
☑ हाँ □ नहीं
7. **क्या आप सोशल मीडिया पर अजनबी लोगों से जुड़े खतरों को समझते हैं?**
□ हाँ ☑ नहीं
8. **क्या आप मजबूत पासवर्ड और दो-स्तरीय सुरक्षा (Two-Factor Authentication) का उपयोग करते हैं?**
□ हाँ ☑ नहीं
9. **आपके अनुसार किसानों को ऑनलाइन धोखाधड़ी से बचाने के लिए क्या किया जाना चाहिए?**

[illegible]

10. **क्या आप साइबर सुरक्षा और डिजिटल धोखाधड़ी से बचाव के लिए जागरूकता कार्यक्रम में भाग लेना चाहेंगे?**
☑ हाँ □ नहीं

"सुरक्षित किसान, समृद्ध किसान - जागरूक रहें, सुरक्षित रहें!"

*आपके बहुमूल्य उत्तरों के लिए धन्यवाद!
*(यह सर्वेक्षण केवल जागरूकता के उद्देश्य से है।)



किसान मेला सर्वेक्षण पत्र

विषय: किसानों के लिए डिजिटल फॉरेंसिक और साइबर सुरक्षा

नाम: Vijay गाँव: Hathesa पता: Paheri Bareilly

प्रिय किसान भाई/बहन,

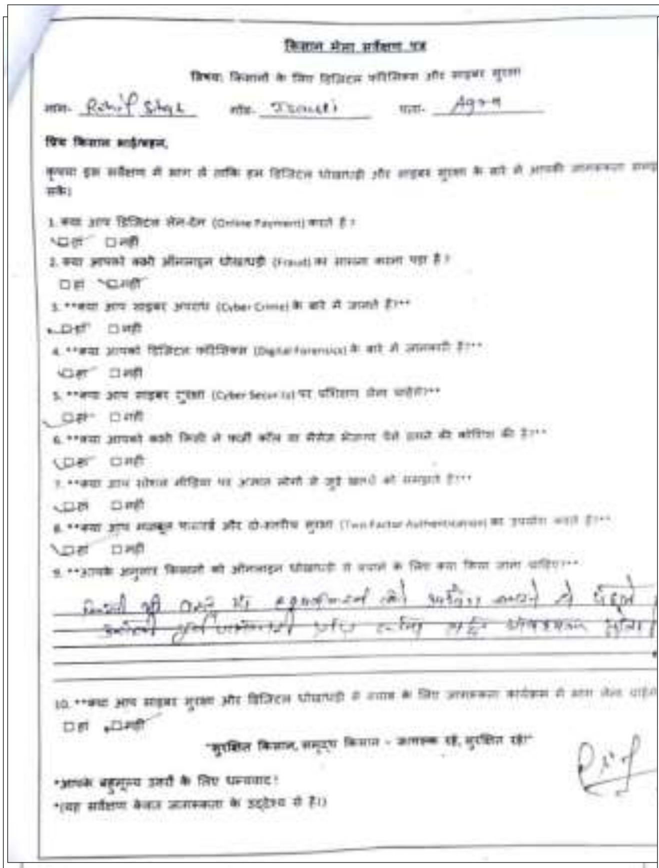
कृपया इस सर्वेक्षण में भाग लें ताकि हम डिजिटल धोखाधड़ी और साइबर सुरक्षा के बारे में आपकी जागरूकता समझ सकें।

1. क्या आप डिजिटल लेन-देन (Online Payment) करते हैं?
☑ हाँ □ नहीं
2. क्या आपको कभी ऑनलाइन धोखाधड़ी (Fraud) का सामना करना पड़ा है?
☑ हाँ □ नहीं
3. **क्या आप साइबर अपराध (Cyber Crime) के बारे में जानते हैं?**
☑ हाँ □ नहीं
4. **क्या आपको डिजिटल फॉरेंसिक (Digital Forensics) के बारे में जानकारी है?**
□ हाँ ☑ नहीं
5. **क्या आप साइबर सुरक्षा (Cyber Security) पर प्रशिक्षण लेना चाहेंगे?**
☑ हाँ □ नहीं
6. **क्या आपको कभी किसी ने फर्जी कॉल या मैसेज भेजकर पैसे ठगने की कोशिश की है?**
☑ हाँ □ नहीं
7. **क्या आप सोशल मीडिया पर अजनबी लोगों से जुड़े खतरों को समझते हैं?**
☑ हाँ □ नहीं
8. **क्या आप मजबूत पासवर्ड और दो-स्तरीय सुरक्षा (Two-Factor Authentication) का उपयोग करते हैं?**
□ हाँ ☑ नहीं
9. **आपके अनुसार किसानों को ऑनलाइन धोखाधड़ी से बचाने के लिए क्या किया जाना चाहिए?**

10. **क्या आप साइबर सुरक्षा और डिजिटल धोखाधड़ी से बचाव के लिए जागरूकता कार्यक्रम में भाग लेना चाहेंगे?**
☑ हाँ □ नहीं

"सुरक्षित किसान, समृद्ध किसान - जागरूक रहें, सुरक्षित रहें!"

*आपके बहुमूल्य उत्तरों के लिए धन्यवाद!
*(यह सर्वेक्षण केवल जागरूकता के उद्देश्य से है।)



किसान मेला सर्वेक्षण पत्र

विषय: किसानों के लिए डिजिटल फॉरेंसिक और साइबर सुरक्षा

नाम- Rohit Singh   गाँव- Jhauli   पता- Agra

प्रिय किसान भाई/बहन,

कृपया इस सर्वेक्षण में भाग लें ताकि हम डिजिटल धोखाधड़ी और साइबर सुरक्षा के बारे में आपकी जागरूकता समझ सकें।

1. क्या आप डिजिटल लेन-देन (Online Payment) करते हैं ?
☑ हां □ नहीं

2. क्या आपको कभी ऑनलाइन धोखाधड़ी (Fraud) का सामना करना पड़ा है ?
□ हां ☑ नहीं

3. **क्या आप साइबर अपराध (Cyber Crime) के बारे में जानते हैं?**
☑ हां □ नहीं

4. **क्या आपको डिजिटल फॉरेंसिक (Digital Forensics) के बारे में जानकारी है?**
☑ हां □ नहीं

5. **क्या आप साइबर सुरक्षा (Cyber Security) पर प्रशिक्षण लेना चाहेंगे?**
☑ हां □ नहीं

6. **क्या आपको कभी किसी ने फर्जी कॉल या मैसेज भेजकर पैसे ठगने की कोशिश की है?**
☑ हां □ नहीं

7. **क्या आप सोशल मीडिया पर अज्ञात लोगों से जुड़े खतरों को समझते हैं?**
☑ हां □ नहीं

8. **क्या आप मजबूत पासवर्ड और दो-स्तरीय सुरक्षा (Two-Factor Authentication) का उपयोग करते हैं?**
☑ हां □ नहीं

9. **आपके अनुसार किसानों को ऑनलाइन धोखाधड़ी से बचाने के लिए क्या किया जाना चाहिए?**

किसानों को नए से equipment को अपडेट करने से पहले उनको पूर्ण जानकारी और इसके लिए सही प्रशिक्षण सुविधा

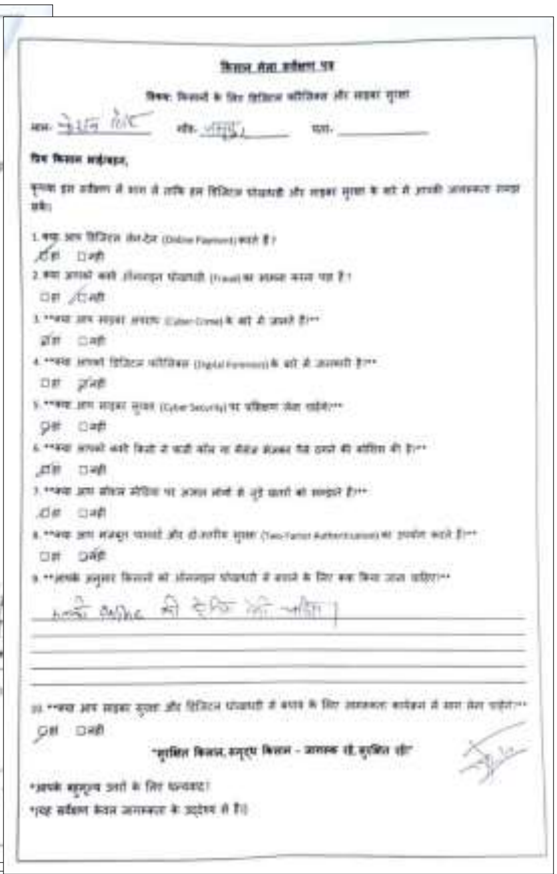
10. **क्या आप साइबर सुरक्षा और डिजिटल धोखाधड़ी से बचाव के लिए जागरूकता कार्यक्रम में भाग लेना चाहेंगे?**
□ हां ☑ नहीं

"सुरक्षित किसान, समृद्ध किसान - जागरूक रहें, सुरक्षित रहें"

Rif

*आपके बहुमूल्य उत्तरों के लिए धन्यवाद!

*(यह सर्वेक्षण केवल जागरूकता के उद्देश्य से है।)



किसान मेला सर्वेक्षण पत्र

विषय: किसानों के लिए डिजिटल फॉरेंसिक और साइबर सुरक्षा

नाम- जेठन सिंह   गाँव- [illegible]   पता-

प्रिय किसान भाई/बहन,

कृपया इस सर्वेक्षण में भाग लें ताकि हम डिजिटल धोखाधड़ी और साइबर सुरक्षा के बारे में आपकी जागरूकता समझ सकें।

1. क्या आप डिजिटल लेन-देन (Online Payment) करते हैं ?
☑ हां □ नहीं

2. क्या आपको कभी ऑनलाइन धोखाधड़ी (Fraud) का सामना करना पड़ा है ?
□ हां ☑ नहीं

3. **क्या आप साइबर अपराध (Cyber Crime) के बारे में जानते हैं?**
☑ हां □ नहीं

4. **क्या आपको डिजिटल फॉरेंसिक (Digital Forensics) के बारे में जानकारी है?**
□ हां ☑ नहीं

5. **क्या आप साइबर सुरक्षा (Cyber Security) पर प्रशिक्षण लेना चाहेंगे?**
☑ हां □ नहीं

6. **क्या आपको कभी किसी ने फर्जी कॉल या मैसेज भेजकर पैसे ठगने की कोशिश की है?**
☑ हां □ नहीं

7. **क्या आप सोशल मीडिया पर अज्ञात लोगों से जुड़े खतरों को समझते हैं?**
☑ हां □ नहीं

8. **क्या आप मजबूत पासवर्ड और दो-स्तरीय सुरक्षा (Two-Factor Authentication) का उपयोग करते हैं?**
□ हां ☑ नहीं

9. **आपके अनुसार किसानों को ऑनलाइन धोखाधड़ी से बचाने के लिए क्या किया जाना चाहिए?**

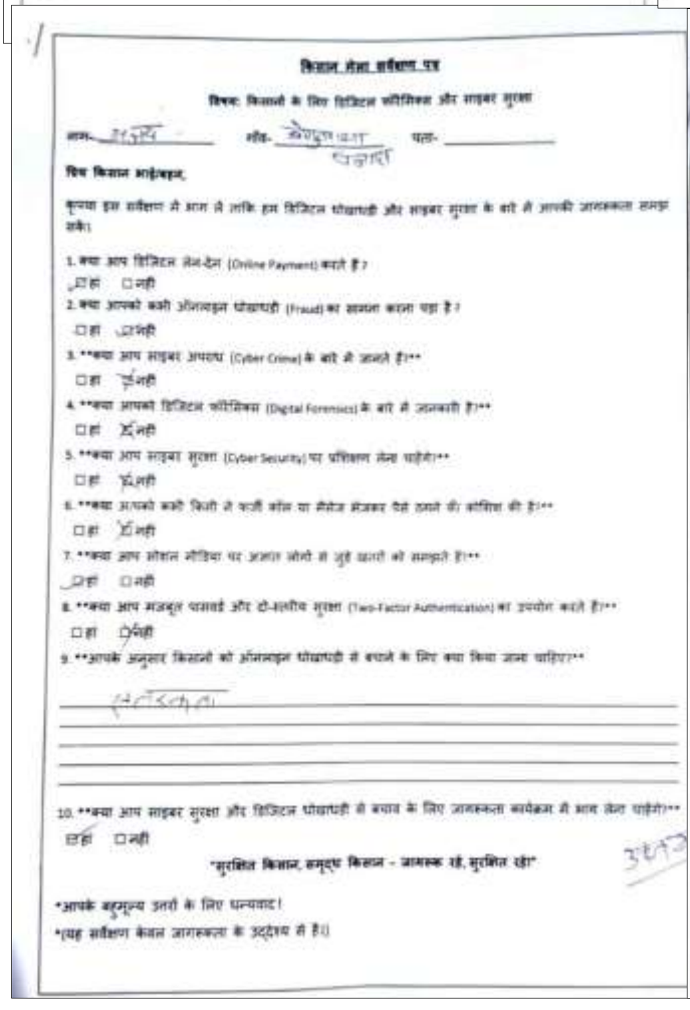
इन्हें Online की ट्रेनिंग दी जाना।

10. **क्या आप साइबर सुरक्षा और डिजिटल धोखाधड़ी से बचाव के लिए जागरूकता कार्यक्रम में भाग लेना चाहेंगे?**
☑ हां □ नहीं

"सुरक्षित किसान, समृद्ध किसान - जागरूक रहें, सुरक्षित रहें"

*आपके बहुमूल्य उत्तरों के लिए धन्यवाद!

*(यह सर्वेक्षण केवल जागरूकता के उद्देश्य से है।)



किसान मेला सर्वेक्षण पत्र

विषय: किसानों के लिए डिजिटल फॉरेंसिक और साइबर सुरक्षा

नाम- अरुण   गाँव- बेगुमपुरा पंजाबी   पता-

प्रिय किसान भाई/बहन,

कृपया इस सर्वेक्षण में भाग लें ताकि हम डिजिटल धोखाधड़ी और साइबर सुरक्षा के बारे में आपकी जागरूकता समझ सकें।

1. क्या आप डिजिटल लेन-देन (Online Payment) करते हैं ?
☑ हां □ नहीं

2. क्या आपको कभी ऑनलाइन धोखाधड़ी (Fraud) का सामना करना पड़ा है ?
□ हां ☑ नहीं

3. **क्या आप साइबर अपराध (Cyber Crime) के बारे में जानते हैं?**
□ हां ☑ नहीं

4. **क्या आपको डिजिटल फॉरेंसिक (Digital Forensics) के बारे में जानकारी है?**
□ हां ☑ नहीं

5. **क्या आप साइबर सुरक्षा (Cyber Security) पर प्रशिक्षण लेना चाहेंगे?**
□ हां ☑ नहीं

6. **क्या आपको कभी किसी ने फर्जी कॉल या मैसेज भेजकर पैसे ठगने की कोशिश की है?**
□ हां ☑ नहीं

7. **क्या आप सोशल मीडिया पर अज्ञात लोगों से जुड़े खतरों को समझते हैं?**
☑ हां □ नहीं

8. **क्या आप मजबूत पासवर्ड और दो-स्तरीय सुरक्षा (Two-Factor Authentication) का उपयोग करते हैं?**
□ हां ☑ नहीं

9. **आपके अनुसार किसानों को ऑनलाइन धोखाधड़ी से बचाने के लिए क्या किया जाना चाहिए?**

जागरूकता

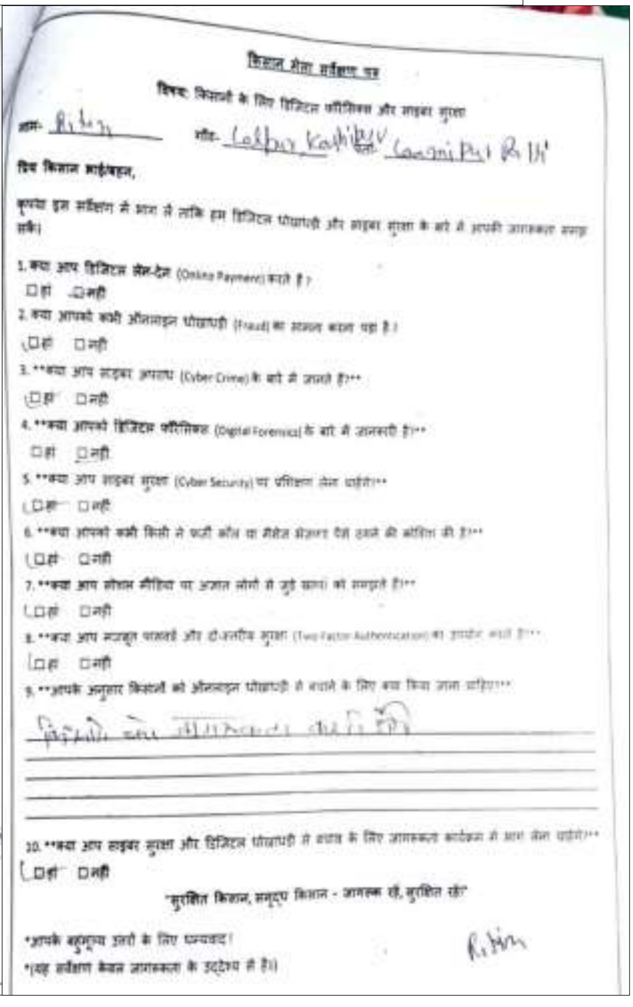
10. **क्या आप साइबर सुरक्षा और डिजिटल धोखाधड़ी से बचाव के लिए जागरूकता कार्यक्रम में भाग लेना चाहेंगे?**
☑ हां □ नहीं

अरुण

"सुरक्षित किसान, समृद्ध किसान - जागरूक रहें, सुरक्षित रहें"

*आपके बहुमूल्य उत्तरों के लिए धन्यवाद!

*(यह सर्वेक्षण केवल जागरूकता के उद्देश्य से है।)



किसान मेला सर्वेक्षण पत्र

विषय: किसानों के लिए डिजिटल फॉरेंसिक और साइबर सुरक्षा

नाम- Ritin   गाँव- Lakhu Kathkav   पता- Lanni Pur Rithi

प्रिय किसान भाई/बहन,

कृपया इस सर्वेक्षण में भाग लें ताकि हम डिजिटल धोखाधड़ी और साइबर सुरक्षा के बारे में आपकी जागरूकता समझ सकें।

1. क्या आप डिजिटल लेन-देन (Online Payment) करते हैं ?
□ हां ☑ नहीं

2. क्या आपको कभी ऑनलाइन धोखाधड़ी (Fraud) का सामना करना पड़ा है ?
☑ हां □ नहीं

3. **क्या आप साइबर अपराध (Cyber Crime) के बारे में जानते हैं?**
☑ हां □ नहीं

4. **क्या आपको डिजिटल फॉरेंसिक (Digital Forensics) के बारे में जानकारी है?**
□ हां ☑ नहीं

5. **क्या आप साइबर सुरक्षा (Cyber Security) पर प्रशिक्षण लेना चाहेंगे?**
☑ हां □ नहीं

6. **क्या आपको कभी किसी ने फर्जी कॉल या मैसेज भेजकर पैसे ठगने की कोशिश की है?**
☑ हां □ नहीं

7. **क्या आप सोशल मीडिया पर अज्ञात लोगों से जुड़े खतरों को समझते हैं?**
☑ हां □ नहीं

8. **क्या आप मजबूत पासवर्ड और दो-स्तरीय सुरक्षा (Two-Factor Authentication) का उपयोग करते हैं?**
☑ हां □ नहीं

9. **आपके अनुसार किसानों को ऑनलाइन धोखाधड़ी से बचाने के लिए क्या किया जाना चाहिए?**

किसानों तक जागरूकता पहुँचानी चाहिए

10. **क्या आप साइबर सुरक्षा और डिजिटल धोखाधड़ी से बचाव के लिए जागरूकता कार्यक्रम में भाग लेना चाहेंगे?**
☑ हां □ नहीं

"सुरक्षित किसान, समृद्ध किसान - जागरूक रहें, सुरक्षित रहें"

*आपके बहुमूल्य उत्तरों के लिए धन्यवाद!

Ritin

*(यह सर्वेक्षण केवल जागरूकता के उद्देश्य से है।)

## 2. Background and Literature Review

### 2.1 What is Digital Forensics?

Digital forensics is the process of identifying, collecting, preserving, analyzing, and presenting digital evidence in a legally acceptable manner. Traditionally used in criminal investigations and cybersecurity, digital forensics enables investigators to trace unauthorized access, detect malicious activities, and ensure the integrity and admissibility of digital evidence [3]. It encompasses various branches, including computer forensics, mobile device forensics, network forensics, and memory forensics. In recent years, digital forensics has extended into non-traditional domains such as agriculture, where cyber-physical systems are increasingly used.

### 2.2 What is Smart Agriculture or Ag-IoT?

Smart agriculture, often referred to as **Agriculture 4.0**, integrates advanced technologies such as IoT, AI, drones, blockchain, and big data analytics into farming practices. The Ag-IoT (Agricultural Internet of Things) specifically involves deploying interconnected sensors, actuators, and edge devices to monitor soil conditions, livestock, weather, crop health, and machinery in real time [2]. These technologies aim to improve productivity, sustainability, and resource management, but also expose farms to significant cybersecurity risks.

### 2.3 Recent Literature (2018–2024)

Research over the past several years has explored the convergence of digital forensics and smart systems. Deep learning applications in agriculture have been reviewed, highlighting early uses of AI relevant to forensic data analysis [7]. To secure data archiving in IoT systems, emphasizing traceability and integrity—key concerns in digital forensics.

Vasilaras examined AI in mobile forensics, stressing transparency and explainability in investigative tools[10]. Shukla and other analyzed mobile forensic tools and noted their limitations in adapting to evolving platforms[9]. Alenezi discussed challenges in smart environments, including data heterogeneity and real- time evidence handling[1].

To ensure evidence integrity, proposed a blockchain-based forensic framework[4]. Lutta and other reviewed IoT forensics, highlighting tool gaps and data collection difficulties[8]. Dunsin and all emphasized the potential of AI and ML in automating digital investigations but noted limited focus on agriculture- specific applications[6].

### 2.4 Gaps in the Literature

Despite a growing body of research on digital forensics in cyber-physical and IoT environments, there is a noticeable gap in studies specifically addressing agricultural applications. Smart farming infrastructures differ from industrial or corporate IoT systems due to their decentralized nature, environmental exposure, and domain- specific data formats. The lack of tailored forensic frameworks, insufficient awareness of forensic readiness among agricultural stakeholders, and the absence of case studies on forensic investigations in agricultural settings represent significant gaps.

This paper aims to bridge these gaps by providing a focused analysis of digital forensics in agriculture, evaluating existing tools and methods, and identifying critical challenges and opportunities for research and implementation.

## 3. Forensic Challenges in Agricultural Systems

As agriculture increasingly adopts smart technologies, forensic investigators face a range of domain-specific challenges when addressing cyber incidents in these environments. Unlike traditional IT infrastructures, smart farming ecosystems present unique complexities due to the nature of devices, data, and operational settings.

### 3.1 Heterogeneous Devices and Data Formats

Smart agriculture employs a wide array of interconnected devices, including soil sensors, weather stations, autonomous tractors, drones, and livestock trackers. These devices are often produced by different manufacturers and operate on proprietary firmware, leading to high heterogeneity in hardware interfaces, data structures, and communication protocols [1] [2]. This diversity significantly complicates the acquisition, parsing, and normalization of digital evidence.

Forensic investigators must account for multiple standards such as LoRaWAN, Zigbee, Bluetooth Low Energy (BLE), and custom APIs, making device identification and compatibility a non-trivial task. Without standardized logging and evidence formats, data correlation across devices becomes increasingly challenging.

### 3.2 Limited Forensic Tools for Ag-IoT

Most existing digital forensic tools are designed for conventional IT environments and lack compatibility with low-power, resource-constrained Ag-IoT devices. The absence of specialized forensic frameworks for smart farming limits investigators' ability to conduct live analysis or extract reliable evidence from resource constrained devices [8]. [6]Additionally, due to the decentralized and often remote deployment of these devices, physical access for forensic imaging can be impractical or delayed, risking evidence loss.

### 3.3 Real-Time Data Volatility

Agricultural systems rely heavily on real-time data streams for decision-making, such as automated irrigation, disease prediction, and livestock monitoring. These data streams are volatile, ephemeral, and frequently overwritten or discarded due to storage limitations. As a result, the window for capturing volatile evidence is extremely narrow[10]. In the absence of pre-configured forensic readiness strategies—such as remote logging or live data replication—valuable digital traces may be lost permanently before any investigation begins.

### 3.4 Legal and Privacy Concerns

The collection and analysis of digital evidence in agricultural settings raise serious legal and privacy issues. Forensic investigations may involve accessing sensitive operational data, such as production volumes, GPS coordinates, or proprietary farming algorithms. Without appropriate legal frameworks or consent mechanisms, evidence handling may violate farmers' privacy rights or breach data protection regulations such as the General Data Protection Regulation (GDPR) in Europe [4].

Furthermore, the **ownership and jurisdiction of Ag-IoT data**—particularly when using third-party cloud services—can become ambiguous, hindering lawful seizure or examination of evidence. These legal uncertainties necessitate the development of clear policies around evidence acquisition, chain of custody, and data governance in smart farming contexts.

## 4. Case Studies and Reported Incidents

While digital forensics in agriculture is still an emerging field, several real-world cyber incidents demonstrate the vulnerabilities in smart farming infrastructures and the pressing need for forensic readiness. These cases highlight the diversity of threats—ranging from ransomware and firmware exploitation to data manipulation— and provide insights into the challenges investigators face in agricultural environments.

### 4.1 Talman Ransomware Attack on the Wool Industry (Australia, 2020)

**Incident :**In 2020, Talman, an Australian agricultural software provider, suffered a ransomware attack that brought wool auctions across Australia and New Zealand to a halt [2].

**Impact:**The incident led to a week-long disruption of trading activities, resulting in an estimated AUD $60–$80 million in financial losses. Key operational data was rendered inaccessible, severely affecting supply chains.

**Forensic Analysis:**Lack of centralized logging and forensic readiness made it difficult to identify the source of the attack or preserve digital evidence. Investigators struggled with incomplete log data and system inconsistencies.

**Outcome or Resolution:**The event prompted industry-wide discussions on enhancing backup systems and implementing cyber incident response strategies, but highlighted the lack of digital forensic frameworks in agricultural IT environments.

### 4.2 John Deere Tractor Hacking Demonstration (DEF CON, 2022)

**Incident :** In 2022, a cybersecurity researcher known as "Sick Codes" demonstrated a successful root access hack into a John Deere tractor system at DEF CON, revealing deep vulnerabilities in smart agricultural machinery [2].

**Impact:** Although performed ethically, the demonstration showed that attackers could potentially hijack tractor operations, alter firmware, and compromise embedded systems.

**Forensic Analysis:** The tractor's firmware lacked forensic logging capabilities, and there were no built-in mechanisms for auditing unauthorized changes. This illustrated a broader issue of insufficient forensic traceability in Ag-IoT equipment.

**Outcome or Resolution:** The manufacturer acknowledged the issues and pledged to improve security. The case highlighted the urgent need for forensic-by-design hardware in agricultural machinery.

### 4.3 Simulated Breach of Smart Irrigation Systems (Middle East, Research Simulation)

**Incident:** A simulated red-teaming exercise tested the resilience of smart irrigation systems controlling thousands of hectares. The team demonstrated an attack through vulnerable cloud-based dashboards [1].

**Impact:** The attack showed how easily water supplies could be manipulated, threatening crops and agricultural sustainability. It raised concern over the potential for nation-state attacks on food systems.

**Forensic Analysis:** The absence of secured audit trails and limited data logging made it impossible to fully reconstruct the attacker's path or actions during the simulation.

**Outcome or Resolution:** The study recommended secure design practices, including immutable logging and forensic readiness in cloud interfaces, as a means of improving post-incident investigation.

### 4.4 Unauthorized Access to GPS-Enabled Harvesting Systems (USA, 2021)

**Incident:** In 2021, several farmers in the U.S. reported suspicious activities in their GPS-controlled harvesters, including erratic navigation and yield misreporting.

**Impact:** Potential manipulation of GPS and data settings raised concerns about operational sabotage and data integrity loss, threatening crop management decisions and insurance claims.

**Forensic Analysis:** Due to the lack of encrypted communication and weak authentication, the source of interference could not be verified. Absence of forensic data logs made attribution impossible.

**Outcome or Resolution:** The incident led to increased farmer awareness of cybersecurity and pushed vendors to enforce firmware updates and default credential changes.

## 5. Emerging Tools and Techniques

As agriculture adopts interconnected technologies, digital forensics must adapt to address the unique challenges of smart farming. Emerging tools such as AI/ML, blockchain, IoT forensics platforms, and drone forensics offer promising capabilities to enhance forensic readiness in Agriculture 4.0 environments.

### 5.1 AI and Machine Learning

AI and ML support digital forensics by automating anomaly detection, pattern recognition, and timeline reconstruction. In agriculture, these technologies can process unstructured data from sensors, logs, and surveillance systems, aiding the identification of irregular activities. [6] highlight AI's potential in managing high-volume data and reducing human bias in investigations.

### 5.2 Blockchain for Evidence Integrity

Blockchain offers a tamper-proof method for preserving digital evidence. Its immutable and distributed structure supports a secure chain of custody. [4] proposed a blockchain -based evidence framework suitable for agricultural systems, where sensor and transaction data are distributed. This enhances trust and traceability during investigations.

### 5.3 IoT Forensics Platforms

Traditional forensic tools often fail to address the constraints of Ag-IoT systems, which involve diverse, lowpower, and remote devices. [8] emphasize the need for platforms with edge analytics, standardized metadata handling, and remote acquisition features tailored to smart farming devices.

### 5.4 Drone Forensics

Drones in agriculture generate valuable forensic data, such as GPS logs, images, and telemetry. Extracting this data is essential in incidents involving unauthorized drone use or data manipulation.

[10] recommend incorporating UAV data into broader forensic workflows to support traceability and incident analysis. Together, these tools form the foundation for a proactive, integrated forensic architecture tailored to modern agriculture's needs.

| Technology | Application in Agriculture | Forensic Benefit | Reference |
|---|---|---|---|
| **AI/ML** | Analysis of sensor data, image recognition for anomalies, livestock tracking logs | Automated evidence detection, timeline reconstruction, pattern recognition | [6] |
| **Blockchain** | Logging of transactions from IoT devices, smart contracts for machine<br>operation tracking | Immutable chain of custody, data integrity assurance, tamper-proof logging | [4] |
| **IoT Forensics** | Evidence collection from smart irrigation, soil sensors, machinery controllers | Real-time log acquisition, support for heterogeneous protocols and<br>metadata | [8] |
| **Drone Forensics** | Recovery of GPS data, flight paths, and onboard video from UAVs used in field<br>monitoring | Location and time correlation, investigation of unauthorized drone<br>access | [10] |

## 6. Discussion and Challenges

The integration of digital technologies in agriculture has created new opportunities for efficiency but has also introduced complex cybersecurity risks. This review reveals several emerging patterns, successes, and persistent gaps in the application of digital forensics within smart farming ecosystems. A shortage of trained forensic professionals in rural regions limits incident response and forensic analysis capacity. This skills gap is further compounded by a general lack of cybersecurity awareness among agricultural workers and stakeholders, which hampers early detection and effective mitigation of cyber threats. Without adequate training and awareness programs tailored to the unique challenges of Ag-IoT environments, farms remain vulnerable to attacks and may struggle to maintain forensic readiness [5].

### Trends and Emerging Solutions

A key trend is the growing reliance on AI/ML, blockchain, and IoT forensics to address the challenges posed by data volume, device heterogeneity, and real-time analysis [6][4]. These technologies offer potential for automated anomaly detection, secure evidence logging, and scalable investigation across smart farm infrastructures. Additionally, platforms tailored for drone and sensor data analysis are emerging to support field-level forensic investigations.

### Gaps and Limitations

Despite promising developments, practical adoption remains limited. Real-world case studies (e.g., Talman ransomware, GPS harvesting incidents) reveal a widespread lack of forensic readiness, poor logging mechanisms, and limited support for evidence preservation. Many forensic tools are not optimized for resourceconstrained Ag- IoT devices or the distributed nature of large farms [8].

### Key Challenges and Open Issues

**Scalability**: Most forensic frameworks are not built to manage the scale and diversity of large agricultural operations spread across remote locations.

**Skills Gap**: A shortage of trained forensic professionals in rural regions limits incident response and forensic analysis capacity.

**Integration with Traditional Practices**: Many farms operate in hybrid digital-traditional models, making seamless forensic integration difficult without disrupting legacy workflows.

**Legal and Ethical Barriers**: Data privacy, unclear ownership of farm data, and jurisdictional constraints (especially with cloud services) complicate lawful evidence handling [1].

### Future Scope for Research

Future research must focus on developing lightweight forensic tools designed specifically for Ag-IoT devices and constrained environments. There is also a need for:

- **Standardized forensic frameworks** for agriculture, including guidelines for evidence preservation and logging.
- **Integration of forensic-by-design principles** into farm equipment, drones, and smart dashboards.
- **Legal and ethical frameworks** tailored to the agricultural domain, especially concerning drone surveillance, environmental data, and farmer privacy.
- **AI models trained specifically on agricultural data** to support incident detection, anomaly correlation, and automated reporting.
- **Field-based validation** of forensic tools in real farm environments to bridge the gap between theory and practice.

## 7. Conclusion

As agriculture evolves into a data-driven, interconnected domain through the adoption of smart farming technologies, the risks posed by cyber threats have become increasingly significant. This review highlights the critical role of digital forensics in securing agricultural systems by enabling the detection, investigation, and response to cyber incidents. The integration of AI/ML, blockchain, IoT forensics platforms, and drone data analysis offers promising avenues for enhancing forensic capabilities in this domain. However, current tools and practices remain limited in their ability to scale across large farms, accommodate diverse devices, or integrate with traditional farming practices. The lack of skilled professionals, poor forensic readiness, and absence of standardized protocols continue to impede progress. Case studies illustrate these gaps and emphasize the need for proactive measures. To address these challenges, policy reforms are needed to define clear regulations around digital evidence collection, data ownership, and privacy in agricultural contexts. Simultaneously, there is a strong need for the development of specialized forensic frameworks tailored to the unique characteristics of smart farming ecosystems. These frameworks must be scalable, lightweight, and adaptable to resource-constrained environments while ensuring compliance with legal and ethical standards.

In conclusion, securing the future of Agriculture 4.0 depends not only on technological innovation but also on embedding forensic-by-design principles and fostering a culture of cybersecurity awareness within the agricultural sector.

### References

[1]. Alenezi, A. M. (2023). *Digital forensics in the age of smart environments: A survey of recent advancements and challenges*. *Forensic Science International:*

*Digital Investigation, 45*, 301655. https://doi.org/10.1016/j.fsidi.2023.301655

[2]. Bui, H. T., Aboutorab, H., Mahboubi, A., Gao, Y., Sultan, N. H., Chauhan, A., Parvez, M. Z., Bewong, M., Islam, R., Islam, Z., Camtepe, S. A., Gauravaram, P., Singh, D., Babar, M. A., & Yan, S. (2024). *Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems*. *Computers & Security, 140*, 103754. https://doi.org/10.1016/j.cose.2024.103754\Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*(3rd ed.). Academic Press.

[3]. Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. (2020). *Study and implementation on the application of blockchain in electronic evidence generation*. *Forensic Science International: Digital Investigation, 35*, 301001. https://doi.org/10.1016/j.fsidi.2020.301001

[4]. Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). *Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review*. *Computers in Industry, 135*, 103566. https://doi.org/10.1016/j.compind.2022.103566

[5]. Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2023). *A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response*. *Forensic Science International: Digital Investigation, 49*, 301717. https://doi.org/10.1016/j.fsidi.2023.301717

[6]. Kamilaris, A., & Prenafeta-Boldú, F. X. (2018). *Deep learning in agriculture: A survey*. *Computers and Electronics in Agriculture, 147*, 70–90. https://doi.org/10.1016/j.compag.2018.02.016

[7]. Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bastaki, B. B. (2021). *The complexity of internet of things forensics: A state-of-the-art review*. *Forensic Science International: Digital Investigation, 38*, 301210. https://doi.org/10.1016/j.fsidi.2021.301210

[8]. Shukla, U., Mandal, B., & Kiran, K. V. D. (2022). *Perlustration on mobile forensics tools*. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2022.02.321

[9]. Vasilaras, A., Papadoudis, N., & Rizomiliotis, P. (2024). *Artificial intelligence in mobile forensics: A survey of current status, a use case analysis and AI alignment objectives*. *Forensic Science International: Digital Investigation, 49*, 301737. https://doi.org/10.1016/j.fsidi.2024.301737