
Securing the field: a CBOR-based lightweight PKI framework for Smart agriculture

Vellaipandi, M.^{1,2}, Bharathi, B.², Gobinath, K.³, Soundra Pandian, K. K.⁴ and Marshal, R.^{3*}

¹Standardization Testing and Quality Certification Directorate, India; ²Sathyabama University, India; ³Indian Computer Emergency Response Team, India; ⁴Controller of Certifying Authorities, India.

Vellaipandi, M., Bharathi, B., Gobinath, K., Soundra Pandian, K. K. and Marshal, R. (2026). Securing the field: a CBOR-based lightweight PKI framework for Smart agriculture. *International Journal of Agricultural Technology* 22(5):2477-2496.

Abstract The growth of smart agriculture has enhanced the food production efficiency and sustainability. However, it has also expanded the attack surface to different cyber security threats. The inherent limitations in smart agriculture devices and their environment limit the adoption of cyber security measures. Deployment of Public Key Infrastructure (PKI) in smart agriculture devices can enhance the security of the smart agriculture systems. However, traditional PKI frameworks are built for implementation in systems with large computational power. This limits their adoption in smart agriculture systems. To address these challenges, a transition toward Concise Binary Object Representation (CBOR) and the CBOR Object Signing and Encryption (COSE) standard is enhanced the security of smart agriculture devices. The proposed framework provides a scalable, binary-first security roadmap that can be practically implemented to safeguard the smart agriculture systems in resource-constrained environments.

Keywords: Concise Binary Object Representation (CBOR), Digital certificate, Public Key Infrastructure (PKI), Internet of Things (IoT), Smart agriculture

Introduction

Smart agriculture powered by data-driven technologies play a major role in global food production. By integrating smart sensors, autonomous machinery, and real-time data analytics, the agriculture sector is empowered with technologies and solutions that can be used for large scale farming. The data driven analytics empower the precision farming approach and enhance the effective utilization of resources like water and fertilizers and productivity (Latino *et al.*, 2024; Ahmed *et al.*, 2024; Dutta *et al.*, 2025). Smart agriculture also contributes to the reduction of chemical footprint of farming operations and helps the food systems to adapt to the challenges of climate transformation (Holzinger *et al.*, 2024; Bhansali *et al.*, 2024; Choudhary *et al.*, 2025).

* **Corresponding Author:** Marshal, R.; **Email:** marshalrgj@gmail.com

The increasing adoption of smart technologies in agricultural systems has made cybersecurity as a key pillar of food security. The reliance on networked sensors, automated irrigation and harvesting systems has also expanded the attack surface for cyber threats. Cyber-attacks targeting agriculture systems have the potential to disrupt food supplies and disable critical machinery (Bissadu *et al.*, 2024; Sharma and Mishra, 2025; Kumar and Faisal, 2024). A successful cyberattack on a large-scale smart farm can lead to significant impact such as economic losses, physical damage to equipment, contamination of crops and misuse of automated chemical dispensers.

Strengthening the cyber security of smart agriculture requires strict implementation of cyber security frameworks (Campoverde-Molina and Luján-Mora, 2024; Zanella *et al.*, 2020). However, the distributed nature of networks, limited device capabilities, lack of awareness has complicated the security of smart agriculture devices. The use of Public Key Infrastructure (PKI) in agricultural enterprises can be a viable solution to address the different challenges. However, the traditional PKI architectures were developed for traditional computers and devices with large computational capability and power. The internet connectivity in smart agriculture farms and remote areas also present a key challenge on the adoption of PKI. These challenges restrict their scalability and maintenance in smart agriculture devices. However, in the recent past, several approaches have been attempted to make light weight PKI architectures that can facilitate the adoption of PKI in smart agriculture systems.

In this work, a detailed survey is made on the different security measures that can be adopted in smart agriculture, their challenges and the possible way forward that can be followed to enhance the cyber security of smart agriculture. The study also explores about CBOR (Concise Binary Object Representation). CBOR provides a lightweight, compact format certificate that can be easily adopted by resource-constrained devices and low-bandwidth networks. They can be adopted to overcome the limitations of traditional X.509 certificates. In this study, a transition toward CBOR and CBOR Object Signing and Encryption (COSE) standard is proposed to secure IoT devices, drones, and autonomous machinery that are used in smart agriculture farms.

Smart agriculture threats

Cyber-attacks on smart agriculture have transitioned from simple threats to large scale operational threats. Cyberattacks targeting smart agriculture has become a serious concern as the sector is increasing the adoption of digital technologies such as smart sensors, drones, automated irrigation systems, and cloud-based platforms. These technologies help farmers to improve their

productivity, but they also introduce vulnerabilities in the systems and expands the threat landscape. Just-in-Time (JIT) supply chains and automated Farm-to-Table logistics are driven by modern, data-driven approach to food distribution. These approaches minimize inventory, reduces waste, and enhances freshness by delivering products shortly after harvest or production. However, these approaches rely on Artificial Intelligence (AI), Internet of Things (IoT), and localized systems to create a "pull-based" system, where the actual consumer demand drives the supply chain. With the rise in adoption of these approaches and smart devices, the attacks and threats targeting the sector are also rising with every passing year. The smart devices that are connected to the internet are often deployed in remote areas with poor cybersecurity practices and they make them attractive targets for cybercriminals (Bhansali *et al.*, 2024; Choudhary *et al.*, 2025; Bissadu *et al.*, 2024). This section explores the different cyber security threats and Figure 1 presents the key cyber security threats that are targeting the smart agriculture systems.

Ransomware attacks

Most of the agriculture sector products are time sensitive and perishable in nature. This forces them to maintain a high up time. Even a short downtime can cause crop spoilage, livestock loss, and major financial damage. Threat actors attack management systems such as irrigation, livestock monitoring, and supply-chain platforms. The access to these time sensitive critical systems is denied by threat actors and they demand ransom in return. These entry point of these attacks are mostly social engineering attacks and exploitation of software vulnerabilities.

IoT device hijacking

Smart agriculture systems use devices such as soil sensors, weather monitors, and livestock trackers. These devices are often secured poorly with authentication or outdated firmware. The use of default or weak credentials are exploited by threat actors to gain control. Once compromised, the devices are used as bots or disabled by the threat actors. Infected devices often lead to poor farming decisions and reduce the productivity.

Sensor data manipulation

The reliance on the data collected by the smart devices also makes them as one of the attractive targets for threat actors. Attackers inject false or manipulated data into agricultural systems, such as incorrect soil moisture or weather

readings. The automated systems that take decisions based on the sensor data can be forced to make harmful decisions such as over-irrigation, under-watering, and improper fertilizer application that can damage the crops.

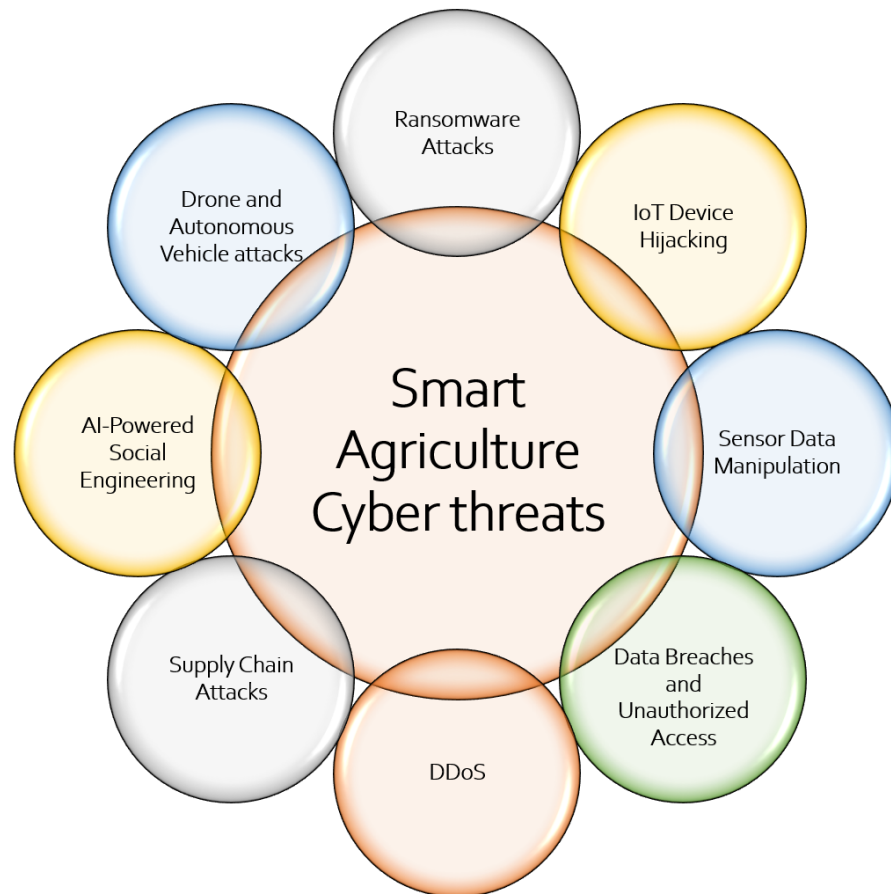


Figure 1. Smart Agriculture Cyber Threats

Data breaches and unauthorized access

The data processed and collected in smart agriculture systems have a lot of potential uses and applications. Threat actors try to gain access to sensitive agricultural data, including production records, financial data, and proprietary farming strategies. Successful attacks lead to privacy violations, financial loss, and misuse of competitive information.

Supply chain attacks

Threat actors attempt to enter into smart agriculture systems by compromising agricultural software providers or equipment manufacturers. By inserting malicious code into updates or firmware, threat actors gain access to multiple farms at once. Since these software updates are made through trusted connections, these threats are hard to detect and mitigate compared to other attacks.

Distributed denial of service (DDoS) attacks

The lack of proper measures to mitigate Distributed Denial of Service (DDoS) attacks with limited hardware resources is also exploited by threat actors. DDoS attacks target farm management platforms, cloud dashboards, and logistics systems. These attacks prevent real-time monitoring, disrupts communication, delays operations and product distribution.

AI-powered social engineering

The rise of Artificial Intelligence (AI) powered social engineering attacks are hard to detect, and they are used as entry points for different types of attacks. These attacks predominantly target the non-technical staff who are involved in the use of smart agriculture systems. These attacks are used to bypass security systems and to do different types of malicious activities, such as data exfiltration and ransomware attacks.

Drone and autonomous vehicle attacks

Drones and autonomous farming equipment are also targeted to alter their operations, causing unsafe behaviour, incorrect spraying, or intentional destruction of farmland. Threat actors manipulate GPS signals used by these devices to misguide machinery, disrupt planting or harvest patterns leading to collisions or physical damage on farms.

Challenges in smart agriculture cyber security

The implementation and adoption of cyber security measures in smart agriculture systems face a lot of practical challenges. This section explores them in detail. These challenges limit the adoption of cyber security measures in smart farms and systems to build secure and resilient smart agriculture systems

(Zanella *et al.*, 2020; Taji and Ghanimi, 2024; Bravi and Liroy, 2025; Rao *et al.*, 2021). The summary of challenges is presented in Figure. 2.



Figure 2. Challenges in Cyber Security adoption

Technical and infrastructural barriers

Farms that are located in rural areas face unreliable internet connectivity and inconsistent power supply. The connectivity issues impact the continuous secure connections that needs to be established for continuous real time monitoring. The integration with outdated legacy systems makes the networks more vulnerable to cyber-attacks. The legacy systems require expensive add-on solutions for security in smart devices with resource-constraints. Implementing strong encryption or advanced security protocols can strain these devices and it a trade-off needs to be achieved between performance and security.

Economic and financial constraints

Advanced security tools such as intrusion detection systems, encryption technologies, and secure network infrastructure are expensive. Small and medium-scale farmers consider cyber security costs as optional rather than looking at it as an essential element. Many low-cost agricultural technologies prioritize usability and affordability over security. As a result, devices are inherently vulnerable to cyber threats.

Lack of awareness

The lack of cybersecurity awareness and digital literacy among farmers and technology operators hinders the adoption of cyber security. Most of the users are not aware of the potential cyber security risks and they neglect the basic cybersecurity practices.

Technical expertise

The lack of awareness and digital literacy is further augmented by shortage of skilled professionals having the understanding of cybersecurity as well as agricultural systems. This lack of dual expertise impacts the installation, management, and maintenance of secure agriculture systems.

Lack of standardization and interoperability

The lack of standardization with different manufacturers using different protocols complicates the matter further. This is further worsened with the lack of interoperability which makes it difficult to implement consistent security measures across all devices and platforms within a farm. The lack of implementation of secure communication mechanisms by low-cost devices also increases the vulnerability of the devices.

Complex and distributed farm environments

Smart agriculture systems are highly distributed, and they have numerous interconnected devices spread across large geographical areas. This distributed environment makes it more difficult to manage and secure such complex environments. As a result, firmware updates, security patches, and system monitoring gets delayed or ignored, leaving systems vulnerable to attacks.

Lack of visibility

The lack of visibility into the devices connected into the networks makes it difficult to monitor the endpoints and establish secure communication. Such lack of visibility also limits the patch management process and updating systems to reduce the risk of vulnerabilities. This can be further worsened by lack of restriction to connect devices into the network. Use of compromised devices in the network by users who are not aware of the cyber security measures can act as an entry point for the attackers.

Physical security risks

Unlike traditional IT systems housed in secure facilities, agricultural devices are mostly placed in open environments. This makes them susceptible to physical tampering, theft, hardware-level attacks and environmental threats. The lack of physical security can lead to deployment of compromised devices that can be used as an entry point to the systems.

Low perceived risk and adoption resistance

Many users still underestimate the likelihood and impact of cyberattacks in smart agriculture. This low perception of risk leads to negligence in adopting cybersecurity measures. Since the benefits of security are not always immediately visible the users show lesser interest in the adoption of cyber security tools and policies as they are expensive.

Supply chain vulnerabilities

Dependence on third-party vendors for hardware, software, and services introduces the supply chain risks. A vulnerability in any part of the supply chain can impact multiple farms simultaneously. The lack of maintenance of inventory and secured supply chain procurement enhances the supply chain risks and increases the risk surface.

PKI in smart agriculture

The integration of Public Key Infrastructure (PKI) in smart agriculture can provide a robust security framework for managing digital identities across a decentralized network of devices. Smart agriculture systems rely on a variety of systems such as autonomous tractors, soil sensors, drone fleets, and irrigation systems. Being an interconnected “system of systems” it requires the interconnected systems to work in coordination. In such an interconnected

environment, PKI can serve as the foundational “trust engine” that can prevent unauthorized access, data tampering, and cyberattacks on smart agriculture operations (Vellaipandi *et al.*, 2023; El-Hajj and Beune, 2024; Höglund *et al.*, 2020; Höglund and Raza, 2021; Rosu and Graur, 2025). Public Key Infrastructure (PKI) in IoT provides a secure foundation by issuing unique digital certificates (X.509) to devices by replacing vulnerable credentials. These certificates enable mutual authentication (mTLS) and ensure only verified devices are connect to networks and protect the data integrity and confidentiality during transmission. The key features of PKI are presented in Figure 3.

Device identity and authentication

PKI enables device identity and authentication by issuing a unique digital certificate to every IoT device or piece of machinery. A private key securely generated and stored within a tamper-proof chip. A corresponding public key is embedded in a digital certificate to verify this identity. This ensures that the devices can cryptographically verify whether the data is coming from a legitimate source.

Secure data integrity

By digitally signing the data, PKI guarantees that information remains authentic during transmission. This ensures the data integrity and prevents manipulation of data. PKI facilitates end-to-end encryption and protects data both at rest and in transit. It ensures that the integrity of data by preventing tampering.

Encrypted command and control

PKI facilitates the encrypted command and control by securing communication channels between the devices. This encrypted communication ensures that only authorized commands are executed by the devices. Unlike standard web browsing, IoT devices use mutual Transport Layer Security (mTLS), where both the device and the server verify each other's certificates before exchanging data. This ensures a "secret handshake" is made and prevents unauthorized eavesdroppers from accessing communication streams.

Secure over-the-air (OTA) updates

PKI is used to sign software updates, and it ensures that devices only install legitimate and authorized code. This Secure OTA updates prevent the

introduction of malware at the edge devices connected to a network and ensures that only legitimate software is installed at the devices.

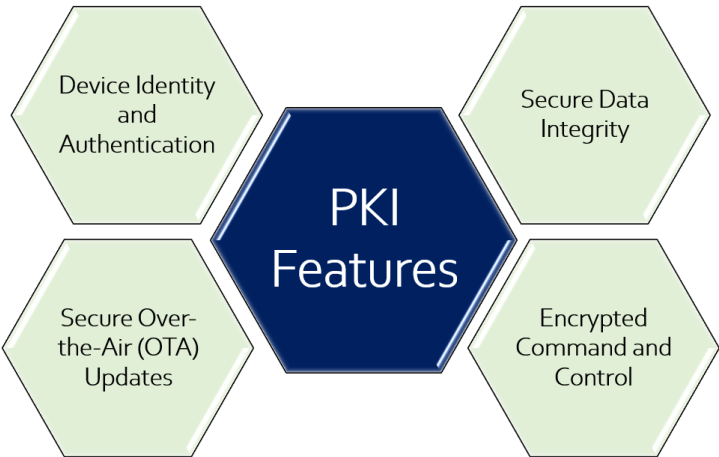


Figure 3. PKI key features



Figure 4. PKI Advantages

PKI for cyber security

Device authentication and rogue device prevention

By issuing a unique digital certificate to each device, PKI ensures that only trusted sensors, drones, or machinery communicate in the smart agriculture network. This reduces the risks associated with rogue or compromised devices and simplifies the integration of legacy equipment with modern smart systems. The key advantages of using PKI in smart agriculture from a cyber security perspective is presented in Figure 4.

Secure communication in distributed environments

The encrypted and certificate-based communication in PKI enables authentication across the devices connected in the distributed network. They ensure that the sensitive data remains protected from interception or manipulation by malicious actors, even in remote locations.

Ensuring data integrity

The AI-driven analytics and automated systems rely on accurate information for decisions in irrigation, planting, and yield prediction. The digital signature by PKI at the source, provides authenticity and prevents unauthorized modifications. Hence, PKI helps to maintain operational accuracy and reliability.

Secure updates and maintenance

The location of smart device in remote areas across vast regions makes maintenance and update a challenge in smart agriculture systems. The secure over-the-air (OTA) update by PKI with digital signature of the firmware and software facilitate secure installation. Devices verify these signatures before installation and ensuring their legitimacy. It reduces the risk of malware and supply chain attacks.

Access control and user authentication

The certificate-based authentication by PKI restricts access to authorized users and mitigates risks associated with social engineering, human error and insider threats. This prevents the unauthorized access to sensitive systems.

Secure supply chain integration

The digital identity verification of supply chain partners including vendors, distributors, and software providers can be achieved by using PKI. It helps to reduce the threats originating from compromised supply chain partners and enhances the overall resilience of the agricultural ecosystem.

Scalability for future growth

The adoption of AI and cloud-based services is on the rise and PKI can help the scaling of such environments in a secured manner as it can support thousands of digital identities. Its hierarchical certificate management ensures to have consistent security across all devices and platforms. This flexibility and support make them a sustainable and robust cyber security solution for both small and large-scale agricultural operations.

Digital certificates for PKI in smart agriculture- challenges

PKI digital certificate is an electronic document that uses cryptography to bind a public key to an entity's identity. The digital certificates are issued by trusted Certificate Authorities (CAs). A Certificate Authority (CA) verifies the identity of the applicant, often through a Registration Authority (RA). Once verified, the CA issues a signed digital certificate. The certificate is used to prove the identity and to exchange keys for secure communication. Compared to traditional IT environments, smart agriculture requires lightweight, efficient, and scalable PKI solutions (Fugkeaw *et al.*, 2026; Jagdish *et al.*, 2025; Rao *et al.*, 2026). PKI implementation in smart agriculture faces a few practical challenges as presented in Figure 5.

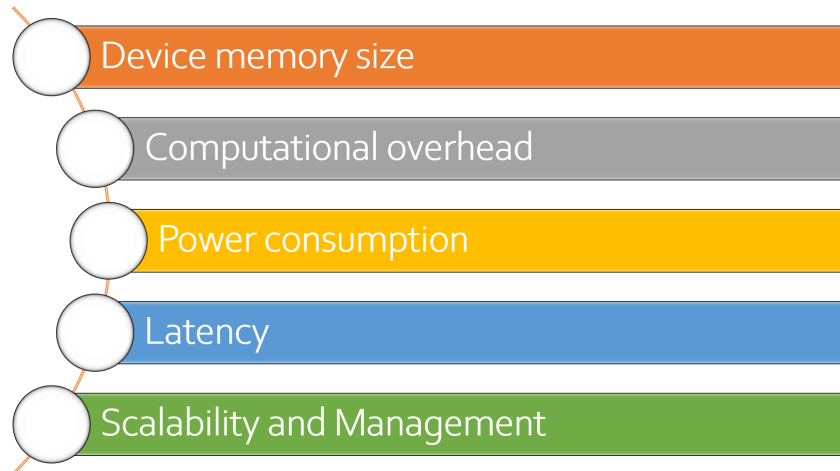


Figure 5. PKI Challenges

Device memory size

Digital certificates act as the pillar of PKI as they provide authentication, encryption, and secure communication. Traditional X.509 certificates used in

PKI use Abstract Syntax Notation One (ASN.1) encoding. These certificates are verbose and occupy hundreds of bytes in the memory. The size of the certificate limits their performance in resource constrained devices.

Computational overhead

Parsing traditional ASN.1 X.509 certificates is CPU-intensive process and it requires significant RAM. Storing a full certificate chain and its associated libraries for validation can exceed the available RAM/Flash of smart devices. Certificate Revocation Lists (CRL) contain every revoked serial number. Devices cannot download massive Certificate Revocation Lists (CRLs), and real-time OCSP (Online Certificate Status Protocol) checks can create a single point of failure.

Power consumption

Frequent communication between IoT devices, gateways and cloud platforms is essential for real-time monitoring. Large certificate sizes increase the data transmitted with every handshake or update. This increases the consumption of bandwidth and energy. The traditional PKI design was built for web servers and laptops. The continuous transmission and computation of certificate validity can result in increased energy usage, or operational failures, making traditional certificates impractical for many farm-deployed sensors, drones, or autonomous machinery. These challenges impact the operation of battery-powered field devices.

Latency

Large certificates can exceed the Maximum Transmission Unit (MTU) of these networks and they require packet fragmentation. Introduction of fragmentation can increase the likelihood of data loss, latency, and increases the energy consumption due to multiple radio transmissions. Large certificate transmission becomes challenging over low-bandwidth networks. Exchanging large certificates during device authentication or handshake processes can take several seconds and introduce high latency in the communication process. In time-sensitive scenarios, such as emergency frost-protection irrigation or autonomous drone operations, these delays can impact the farm productivity and automation reliability. Checking if a certificate is still valid is nearly impossible at the edge.

Scalability and management

Managing the status of thousands of certificates in real-time creates a massive computation overhead on the CA (Certificate Authority). Traditional PKI relies on manual CSR (Certificate Signing Request) generation, and this limits the scalability in large environments with devices located at remote areas. IoT deployments often involve hardware from multiple vendors. Getting different manufacturers to agree on a single root CA or cross-certification standard is a significant hurdle.

CBOR for smart agriculture PKI

To overcome these limitations discussed in the previous section, the industry has shifted from traditional protocols towards building a native Lightweight PKI architecture. ECQV (Elliptic Curve Qu-Vanstone) framework is an implicit certificate scheme, and the certificate contains reconstruction data and user information for construction of public key. The device's public key in ECQV is mathematically derived by combining the certificate with the CA's public key and the certificate size is approximately 40–60 bytes. However, ECQV is implicit and the public key is calculated from the certificate. This requires the verifier to already have the CA's public key and perform extra elliptic curve computation. Edwards-curve Digital Signature Algorithm (EdDSA) provides high-speed signing and small signature sizes. EdDSA is resistant to several side-channel attacks that are common in field-deployed sensors. However, EdDSA requires significant CPU cycles and has to parse a messy text-based format to find the signature leading to energy consumption. CBOR (Concise Binary Object Representation) offers a compact, efficient, and scalable encoding standard that enables secure, lightweight digital certificates suitable for the unique requirements of smart agriculture (Rix *et al.*, 2016; Lemogue *et al.*, 2023). CBOR allows for streaming Parsing, and a device can begin validating a signature while it is reading from the buffer rather than having to load a massive certificate into limited RAM first. The key advantages of CBOR are presented in this section and Figure 6.

Compact and efficient encoding

Compared to verbose ASN.1 structures, CBOR maps certificate fields to small integer keys, and compresses X.509 certificate. This significant payload compression allows the certificate to fit within a single network frame and

eliminates the need for packet fragmentation. This helps to reduce the number of packets and delay in resource constrained networks.

Low processing overhead and hardware compatibility

Parsing CBOR-encoded certificates requires minimal CPU cycles and low memory. This facilitates quick certificate verification even in resource constrained devices. This reduced computational overhead helps to conserve battery life of the smart devices. By reducing certificate size, computational requirements, and transmission overhead, CBOR ensures smooth and reliable operation for battery-powered smart devices.

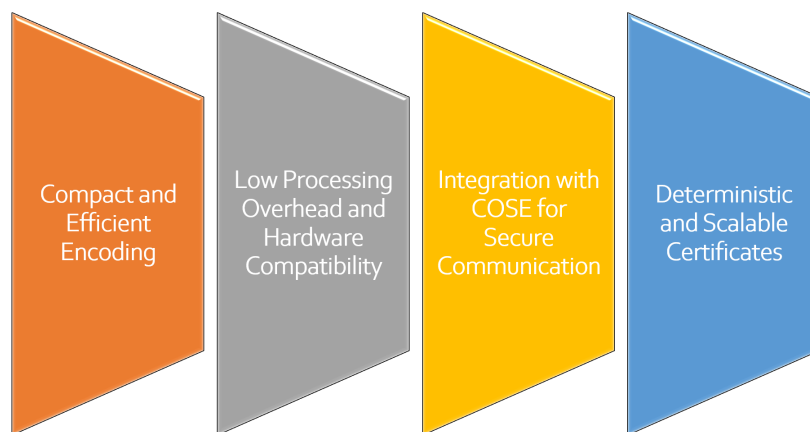


Figure 6. CBOR advantages

Integration with COSE for secure communication

CBOR integrated with the COSE (CBOR Object Signing and Encryption) standard enables compact and secure certificate handling (Vellaipandi *et al.*, 2026; Iglesias-Urkia *et al.*, 2019). Devices can use CWTs (CBOR Web Tokens) instead of full certificate chains to prove its identity and authorization. CBOR also supports protocols like EDHOC (Ephemeral Diffie-Hellman Over COSE) to establish secure connections efficiently compared to traditional TLS handshakes.

Deterministic and scalable certificates

CBOR supports canonical encoding with each piece of data having a single, deterministic representation. This simplifies the hashing and signing of

certificates in low-power hardware and they eliminate the need for complex canonicalization required by XML or JSON formats. In addition to that, CBOR's compact and lightweight design allows easy scalability with zero-touch onboarding, automated renewal, and revocation of thousands of devices without overwhelming gateways or network resources.

Practical approach for CBOR adoption

To facilitate adoption of CBOR in smart agriculture systems, a practical approach is proposed in this section. The proposed approach as presented in Figure 7 provides a secure adoption of CBOR in smart agriculture by integrating a binary-first security lifecycle which is tailored for resource-constrained environments.

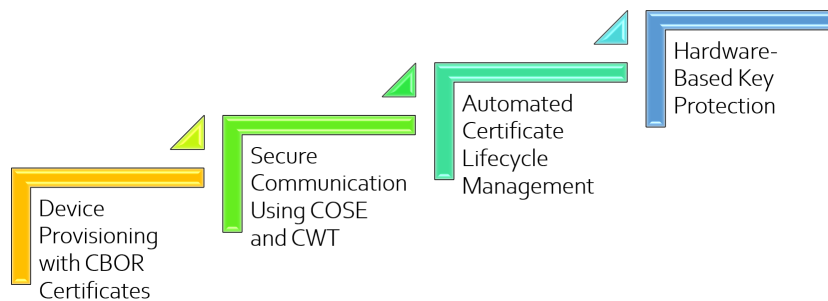


Figure 7. CBOR for Smart Agriculture

Device provisioning with CBOR certificates

The first step is device provisioning with CBOR certificates. Each of the smart device needs to be provided with a compact CBOR certificate that contains a public key and identification metadata. These certificates can be preloaded at the factory or deployed via zero-touch provisioning using EST payloads over secure CoAP (EST-coaps). This can enable large-scale farms to onboard thousands of devices efficiently without manual intervention. This can ensure that every device is uniquely identifiable and trusted from the moment it is connected to the network.

Secure communication using COSE and CWT

Secure communication channels should be established using CBOR along with COSE. COSE can allow the devices to sign and encrypt messages efficiently using lightweight algorithms. Lightweight key exchange protocols like EDHOC

(Ephemeral Diffie-Hellman Over COSE) can be used to establish session keys with fewer messages and reduced latency. CBOR Web Tokens (CWTs) can be used to replace traditional API keys and large certificates.

Automated certificate lifecycle management

Verify the credentials using cached COSE-signed tokens in devices located at remote locations. It does not require continuous connectivity to a central server and can provide seamless renewal, revocation, and offline validation. It can reduce the downtime and ensure continuous security even in low-bandwidth or intermittent networks. This can also enable automatic key rotation over narrow-bandwidth links without packet fragmentation or failure. It helps to have an automated certificate lifecycle management, even if there are thousands of devices located in remote locations.

Hardware-based key protection

Secure Elements (SEs) or Physically Unclonable Functions (PUFs) can securely store the private keys within devices. These keys can prevent the exposure of sensitive cryptographic material. This approach can allow low-power resource constrained devices to operate securely over extended periods of time. Standardization of data payloads with Sensor Measurement Lists (SenML)-CBOR can further enable efficient anomaly detection at gateways.

Conclusion

Cybersecurity has become indispensable in smart agriculture due to the widespread adoption of smart devices, automated machinery, drones, and cloud-based farm management systems. The cyber security of these interconnected technologies is essential for decision-making and precision farming. However, there are several practical challenges in the adoption of cyber security measures. The study proposes the adoption of a CBOR-enabled PKI across device provisioning, secure communication, certificate lifecycle management, and hardware protection. By adopting the proposed methodology, smart agriculture systems can establish a strong, scalable, and resilient security framework. The proposed approach can ensure that every device has a verifiable identity, secure data, safe command execution, and secure integration of legacy or third-party systems. The proposed approach is robust and practically implementable for adoption by smart agriculture systems. By replacing traditional, heavy text-based protocols with the proposed approach, large-scale farming operations can

achieve a high level of cyber-resilience without sacrificing the energy efficiency or bandwidth of their smart devices.

Conflicts of interest

The authors declare no conflict of interest.

References

- Ahmed, B., Shabbir, H., Naqvi, S. R. and Peng, L. (2024). Smart agriculture: Current state, opportunities, and challenges. *IEEE Access*, 12:144456-144478.
- Bhansali, K., Akki, P., Heeneth Sai, A. V., Bodepudi, N. D. and Krishnan, A. (2024). Smart agriculture: IoT-based smart application for agriculture. 2024 2nd International Conference on Networking and Communications (ICNWC), Chennai, India, pp.1-12.
- Bissadu, K., Hossain, G. and Vajpayee, P. (2024). Agriculture 5.0 cybersecurity: Monitoring agricultural cyber threats with digital twin technology. 2024 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, pp.0252-0258.
- Bravi, E. and Liroy, A. (2025). Securing IoT devices: An overview. 2025 IEEE Symposium on Computers and Communications (ISCC), Bologna, Italy, pp.1-6.
- Campoverde-Molina, M. and Luján-Mora, S. (2025). Cybersecurity in smart agriculture: A systematic literature review. *Computers & Security*, 150:104284.
- Choudhary, V., Guha, P., Pau, G. and Mishra, S. (2025). An overview of smart agriculture using Internet of Things (IoT) and web services. *Environmental and Sustainability Indicators*, 26:100607.
- Dutta, M., et al. (2025). Internet of Things-based smart precision farming in soilless agriculture: Opportunities and challenges for global food security. *IEEE Access*, 13:34238-34268.
- El-Hajj, M. and Beune, P. (2024). Lightweight public key infrastructure for the Internet of Things: A systematic literature review. *Journal of Industrial Information Integration*, 41:100670.
- Fugkeaw, S., Chansudsuk, C., Wongmasa, N. and Vipittragan, P. (2026). ChainDrone: Lightweight group authentication and audited data transfer for drone swarms with blockchain integration. *IEEE Open Journal of the Communications Society*, 7:1923-1940.
- Holzinger, A., Fister, I., Fister, I., Kaul, H.-P. and Asseng, S. (2024). Human-centered AI in smart farming: Toward Agriculture 5.0. *IEEE Access*, 12:62199-62214.
- Höglund, J., Lindemer, S., Furuheid, M. and Raza, S. (2020). PKI4IoT: Towards public key infrastructure for the Internet of Things. *Computers & Security*, 89:101658.

- Höglund, J. and Raza, S. (2021). LICE: Lightweight certificate enrollment for IoT using application layer security. 2021 IEEE Conference on Communications and Network Security (CNS), Tempe, AZ, USA, pp.19-28.
- Iglesias-Urkia, M., Casado-Mansilla, D., Mayer, S., Bilbao, J. and Urbieto, A. (2019). Integrating electrical substations within the IoT using IEC 61850, CoAP, and CBOR. IEEE Internet of Things Journal, 6:7437-7449.
- Jagdish, B. V., I. A., Vikas, M. N., A. M. and Naik, C. (2025). Decentralised IoT authentication using blockchain and machine learning: The trust circle framework. 2025 International Conference on Inventive Computation Technologies (ICICT), Kirtipur, Nepal, pp.1765-1770.
- Kumar, S. and Faisal, M. (2024). Critical review of cybersecurity risks in precision agriculture. 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, pp.1-7.
- Latino, M. E., Menegoli, M. and Corallo, A. (2024). Agriculture digitalization: A global examination based on bibliometric analysis. IEEE Transactions on Engineering Management, 71:1330-1345.
- Lemogue, A., Martinez, I., Toutain, L. and Bouabdallah, A. (2023). Towards flexible and compact encoded DNS messages using CBOR structures. 2023 IEEE International Performance, Computing, and Communications Conference (IPCCC), Anaheim, CA, USA, pp.228-235.
- Rao, A. K., Singh, B. K., Kamana, Yadav, S. K. and Jaiswal, M. (2026). AgriSmartNet: A quantum-inspired secure framework for smart sensing, clustering, and PPO-SADS decision-making in precision agriculture. Sustainable Computing: Informatics and Systems, 101340.
- Rao, V. V., Marshal, R. and Gobinath, K. (2021). The IoT supply chain attack trends—vulnerabilities and preventive measures. 2021 4th International Conference on Security and Privacy (ISEA-ISAP), Dhanbad, India, pp.1-4.
- Rix, T., Detken, K.-O. and Jahnke, M. (2016). Transformation between XML and CBOR for network load reduction. 2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), Offenburg, Germany, pp.106-111.
- Roşu, A. P. and Graur, O. A. (2025). Towards minimal certificates for federated space public key infrastructure. 2025 Security for Space Systems (3S), Noordwijk, Netherlands, pp.1-12.
- Sharma, B. and Mishra, R. K. (2025). A review of the cyber security risks in AI powered smart agriculture 4.0. 2025 2nd International Conference on Advanced Computing and Emerging Technologies (ACET), Ghaziabad, India, pp.1-6.

- Taji, K. and Ghanimi, F. (2024). Enhancing security and privacy in smart agriculture: A novel homomorphic signcryption system. *Results in Engineering*, 22:102310.
- Vellaipandi, M., Bharathi, B., Gobinath, K. et al. (2026). A novel CBOR based CA certificate for IoT device security. *International Journal of System Assurance Engineering and Management*. DOI:10.1007/s13198-026-03200-4
- VellaiPandi, M., Bharathi, B., Gobinath, K. and Pandian, K. K. S. (2023). Significance of secure Internet of Things device certification – An authentication perspective. *2023 Innovations in Power and Advanced Computing Technologies (i-PACT)*, Kuala Lumpur, Malaysia, pp.1-6.
- Zanella, A. R. A., Silva, E. and Albini, L. C. P. (2020). Security challenges to smart agriculture: Current state, key issues, and future directions. *Array*, 8:100048.

(Received: 7 May 2025, Revised: 4 July 2026, Accepted: 6 September 2026)