Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 2 (2025)

An Empirical Evaluation of Existing Methods used for Integrating Cybersecurity & Privacy Capabilities in Smart Farming Deployments

Mr. Ramesh Pandharinath Daund[1*],Dr. Mohd Junedul Haque[2] , Dr. Umesh Pawar[3]

[1*],[2],[3] Department of Computer Engineering School of Computer Science and Engineering Sandip University Nashik Maharashtra India.

[1*]ramesh.daund@gmail.com.

Article History:

Received: *02-08-2024*

Revised: *09-09-2024*

Accepted: *20-09-2024*

Abstract:

In the digital age, the imperative integration of Cybersecurity and Privacy Methods into Smart Farming systems has emerged as a critical concern. This necessity stems from the escalating reliance on Internet of Things (IoT) devices and cloud computing within the agricultural sector, which, while enhancing efficiency and productivity, concurrently elevates the vulnerability to cyber threats and privacy breaches. This paper embarks on a comprehensive review of the prevailing methodologies employed to fortify smart farming infrastructures against such vulnerabilities. Notably, it delves into a variety of approaches including, but not limited to, Advanced Encryption Standard (AES) for data security, Blockchain technology for ensuring data integrity and traceability, and Intrusion Detection Systems (IDS) for real-time monitoring of cyber threats. The review process adopted in this study is meticulous and multifaceted, encompassing a comparative analysis of these methods against a suite of evaluation metrics such as scalability, robustness, energy efficiency, and user privacy. This analytical framework not only elucidates the strengths and limitations of each method but also facilitates the identification of optimal cybersecurity and privacy-preserving solutions tailored to different smart farming scenarios. The implications of this work are manifold. By offering a systematic evaluation of cybersecurity and privacy methods, this paper contributes significantly to the body of knowledge, aiding stakeholders in the smart farming domain to make informed decisions regarding the deployment of security measures. Furthermore, it underscores the need for an ongoing evolution of these methods to combat emerging cyber threats effectively, thus ensuring the sustainability of smart farming practices in the digital era. Through this scholarly endeavor, the paper aims to pave the way for a more secure and privacy-compliant agricultural future, where technological advancements and cybersecurity measures coalesce seamlessly to enhance food security and farming efficiency.

Keywords: Smart Farming, Cybersecurity, Privacy Methods, Internet of Things (IoT), Blockchain Technology

1. Introduction

The advent of Smart Farming has revolutionized the agricultural landscape, offering unprecedented opportunities for efficiency, productivity, and sustainability. Leveraging the Internet of Things (IoT), cloud computing, and data analytics, Smart Farming enables precise agriculture, where decisions are data-driven, and resources are optimized. However, the integration of these digital technologies also introduces significant cybersecurity and privacy challenges. The vulnerability of smart farming systems to cyber-attacks and data breaches can have profound implications, not only compromising

the privacy and financial well-being of individual farmers but also threatening food security and safety at a global scale. This paper provides a comprehensive review of the cybersecurity and privacy methods currently employed in smart farming, analyzing their efficacy and identifying gaps in the existing frameworks.

The Introduction section of this paper begins by contextualizing the evolution of smart farming technologies and their critical role in modern agriculture. It highlights how digitalization has become a double-edged sword, enhancing operational capabilities while exposing agricultural data and IoT infrastructures to cyber threats. The paper then outlines the significance of cybersecurity and privacy in this domain, emphasizing the potential risks associated with inadequate protection measures. It proceeds to examine various cybersecurity and privacy methods tailored for smart farming, including encryption techniques, blockchain technology, and intrusion detection systems, among others.

The discussion extends to the comparative analysis of these methods against crucial evaluation metrics such as scalability, efficiency, robustness, and user privacy. This analytical approach not only sheds light on the current state of cybersecurity and privacy in smart farming but also sets the stage for identifying optimal solutions for diverse agricultural settings. Furthermore, the paper underscores the dynamic nature of cyber threats, advocating for adaptive and forward-looking security strategies that can evolve in tandem with emerging technologies and threat landscapes.

In doing so, this introduction lays the groundwork for a detailed exploration of the multifaceted challenges and solutions associated with integrating cybersecurity and privacy methods into smart farming. By providing a nuanced understanding of the intersection between digital agriculture and cybersecurity, the paper aims to catalyze further research and development efforts in this critical area, ensuring the resilience and sustainability of smart farming practices in the face of evolving cyber threats.

Motivation & Contributions

The motivation for this scholarly inquiry emanates from the burgeoning intersection of digital technologies and agriculture, epitomized by the concept of Smart Farming. As the agricultural sector increasingly adopts Internet of Things (IoT) devices, cloud services, and data analytics for enhanced productivity and sustainability, it concurrently encounters a spectrum of cybersecurity and privacy challenges. These challenges are not merely technical hurdles; they are pivotal concerns that bear on the economic viability of agricultural enterprises, the privacy and security of individual farmers, and, at a broader level, global food security and safety. Recognizing the gravity of these issues, this paper endeavors to dissect the landscape of cybersecurity and privacy within the context of smart farming, motivated by a pressing need to safeguard this critical infrastructure against cyber threats and privacy violations.

The core contribution of this research lies in its comprehensive review and analysis of existing cybersecurity and privacy methods tailored for the smart farming ecosystem. By meticulously evaluating a diverse array of techniques—ranging from encryption protocols and blockchain-based solutions to intrusion detection systems—the study not only maps the current security landscape but

also benchmarks these methods against vital performance indicators. This dual focus on cybersecurity and privacy is crucial; while cybersecurity aims to protect systems from malicious attacks, privacy measures ensure the confidentiality and integrity of data, addressing concerns that are paramount to farmers and stakeholders in the agricultural domain.

Further, this paper contributes to the academic and practical discourse by highlighting the nuanced requirements of smart farming systems, including the need for scalability to accommodate vast IoT networks, energy efficiency to sustain long-term deployments, and robustness to withstand sophisticated cyber threats. Importantly, it also emphasizes the dynamic nature of cyber threats, advocating for adaptive security measures that can evolve in response to new vulnerabilities and attack vectors for different scenarios.

In synthesizing these insights, the study not only advances the understanding of cybersecurity and privacy in smart farming but also proposes a framework for future research and development. It calls for a multidisciplinary approach that encompasses technological innovation, policy formulation, and stakeholder engagement, aiming to foster a secure, privacy-aware, and resilient smart farming infrastructure. Through its rigorous analysis and forward-looking recommendations, the paper aspires to contribute significantly to the body of knowledge, guiding the development of more sophisticated and effective cybersecurity and privacy solutions for the agricultural sectors.

2. In-depth review of existing Models

In the realm of Smart Farming, the convergence of modern technology and traditional agriculture has ushered in a new era of agricultural efficiency and productivity. Blockchain technology, with its inherent characteristics of transparency, immutability, and decentralization, emerges as a promising solution to address the challenges of data integrity, traceability, and security in Smart Farming environments [1]. A blockchain-based smart farming technology, as discussed in [1], provides farmers and stakeholders with a unified platform for accessing agricultural data samples. By leveraging smart contracts and consensus mechanisms, blockchain ensures the persistence, auditability, and integrity of data stored within blocks, thereby instilling confidence in the veracity of agricultural data samples. Furthermore, the authentication and key agreement mechanisms integrated into blockchain-based solutions facilitate secure communication and data exchange between IoT-enabled devices and gateway nodes [1].

The security and privacy challenges inherent in Smart Farming are multifaceted, necessitating comprehensive countermeasures to safeguard agricultural operations. In [2], the authors delineate three typical development modes of smart agriculture - precision agriculture, facility agriculture, and order agriculture - each characterized by distinct technological applications and security requirements. Authentication and access control mechanisms, privacy-preserving techniques, blockchain-based solutions for data integrity, cryptography, key management, physical countermeasures, and intrusion detection systems emerge as pivotal security countermeasures deployed across various smart agriculture modes [2]. Precision farming, with its potential for water conservation, increased productivity, and rural development, underscores the importance of secure and transparent data

management [3]. Blockchain technology, with its decentralized architecture and immutability, offers a reliable framework for storing and sharing farm data securely. AgroMobiBlock, as proposed in [3], presents an efficient blockchain-enabled authenticated key agreement scheme tailored to precision agricultural IoT networks. Through formal security analysis and simulation studies, AgroMobiBlock demonstrates resilience against a spectrum of cyber threats, ensuring the confidentiality and integrity of agricultural data [3].

The advent of Internet of Things (IoT) technologies has revolutionized agricultural practices, enabling real-time monitoring and management of farm resources [4]. However, the proliferation of IoT devices in smart farming landscapes necessitates robust intrusion detection mechanisms to mitigate cyber threats. Leveraging deep learning algorithms, EBWO-HDLID, as proposed in [5], offers an effective intrusion detection solution for IoT-based smart farming environments. By autonomously detecting unauthorized activities and anomalies, EBWO-HDLID ensures the security and reliability of agricultural systems [5].

The integration of Big Data (BD), Machine Learning (ML), and IoT technologies as per table 1, holds immense potential for optimizing rice production processes in smart agriculture [6]. Through a comprehensive survey of research on intelligent data processing in rice production, [6] elucidates the role of BD, ML, and IoT in various aspects of smart rice farming, including irrigation management, yield estimation, disease monitoring, and quality assessment. By leveraging these technologies, smart rice farming practices transition into a new era of precision agriculture, characterized by data driven decision-making and resource optimization [6].

Reference	**Method Used**	**Findings**	**Results**	**Limitations**
[1]	Smart contract-based blockchain-envisioned authenticated key agreement mechanism in smart farming	Designed a new smart contract-based blockchain-envisioned authenticated key agreement mechanism for smart farming.	Superior security and functionality features compared to existing authentication protocols. Blockchain-based simulation conducted for computational time measurement.	Limited exploration of scalability issues and real-world implementation challenges.
[2]	Overview of smart agriculture development modes, technologies, applications, and security challenges	Presented three development modes and key technologies and applications of smart agriculture. Analyzed security challenges and impact of agricultural	Identified future research directions in smart agriculture technologies.	Lack of in-depth analysis on specific security solutions for smart agriculture.

		equipment on security.		
[3]	Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural IoT networks	Proposed an efficient blockchain-enabled authenticated key agreement scheme for precision agricultural IoT networks. Conducted formal and informal security analysis and verification.	Demonstrated robustness against various potential attacks. Real-time testbed experiments showcased practical usefulness.	Potential challenges in large-scale deployment and interoperability with existing systems not fully addressed.
[4]	IoT-based network framework and control strategies for greenhouse farming	Proposed an IoT-based network framework for greenhouse farming and discussed control strategies for resource management. Reviewed IoT-based greenhouse sensors/devices and communication protocols.	Provided insights into challenges and security issues in smart greenhouse farming.	Lack of detailed discussion on security solutions and their effectiveness.
[5]	Enhanced Black Widow Optimization with Hybrid Deep Learning Enabled Intrusion Detection for IoT-based Smart Farming	Designed an intrusion detection technique using enhanced black widow optimization and hybrid deep learning for IoT-based smart farming. Utilized DL algorithms for anomaly detection.	Demonstrated satisfactory performance on benchmark datasets.	Limited discussion on scalability and real-world deployment challenges.
[6]	Survey of intelligent data processing technology in rice production	Reviewed the application of big data, machine learning, and IoT in rice smart farming. Analyzed various scenarios and applications of	Provided insights into the transformative potential of BD, ML, and IoT in rice precision agriculture.	Lack of detailed discussion on security implications and challenges in adopting these technologies.

		machine learning in rice production processes.		
[7]	Analysis of phase-locked loop-synchronized wind farms under grid faults	Analyzed coupling effects and stability assessment method for phase-locked loop-synchronized wind farms under grid faults. Proposed a current distribution method to minimize instability risk.	Validated theoretical analysis and proposed method through simulations.	Limited discussion on broader implications and applicability beyond wind farm scenarios.
[8]	Authentication and key establishment scheme based on the Rabin cryptosystem for resource-asymmetric smart environments	Proposed a practical authentication and key establishment scheme based on the Rabin cryptosystem for resource-asymmetric smart environments.	Proved anonymity and security features using Proverif and BAN logic. Demonstrated effectiveness through comparative analysis.	Lack of discussion on potential vulnerabilities and practical deployment challenges.
[9]	Literature review and proposed blockchain-based security architecture for smart agriculture	Conducted a comprehensive literature review on blockchain-based security schemes for smart agriculture. Proposed a generalized blockchain-based security architecture.	Identified security goals and challenges in smart agriculture. Conducted cost analysis and comparative study.	Limited empirical validation and discussion on scalability issues in blockchain implementation for smart agriculture.
[10]	Redactable blockchain-based secure data aggregation method with source authentication for fog-enabled IoFT	Introduced a secure data aggregation method using redactable blockchain for fog-enabled IoFT. Supported resistance to collusion and malicious data mining threats.	Demonstrated perfect data confidentiality and integrity against various attacks.	Limited exploration of real-world deployment challenges and scalability issues.

[11]	Review of privacy preservation utilizing Blockchain and Smart Contracts, with focus on smart agriculture	Outlined the state of privacy preservation using Blockchain and Smart Contracts in various domains, including smart agriculture. Proposed a privacy-preserving framework (PPSAF) for smart agriculture.	Identified challenges and potential applications of privacy-preserving blockchain in smart agriculture.	Lack of detailed discussion on implementation challenges and real-world adoption barriers.
[12]	Privacy-preserving data aggregation scheme with ElGamal Cryptosystem for smart agriculture	Proposed a privacy-preserving data aggregation scheme using the ElGamal Cryptosystem for smart agriculture.	Demonstrated security, privacy, and flexibility through analysis and simulations.	Limited discussion on practical deployment challenges and scalability issues.
[13]	Frequency security constrained scheduling approach considering wind farms providing frequency support and reserve	Proposed a scheduling approach considering wind farms for frequency support and reserve. Introduced dynamic frequency indices and a wind power reserve model.	Validated effectiveness through case studies showing cost reduction and VRE curtailment.	Limited discussion on broader implications beyond wind farm scenarios.
[14]	Review of sensor-based AI applications for poultry farming and smart farming advancements	Reviewed sensor-based AI applications for poultry farming and discussed smart farming advancements. Identified gaps in literature regarding poultry well-being assessment.	Provided insights into potential for intelligent automation in poultry farming.	Lack of detailed analysis on security challenges and solutions in poultry farming.
[15]	Blockchain-based service platform for efficient agricultural service operations	Proposed a blockchain-based service platform for efficient agricultural service operations, with a focus on drone plant protection	Demonstrated effectiveness through numerical experiments and functional tests.	Limited discussion on scalability challenges and interoperability with existing systems.

		services. Developed optimization models and smart contract terms.		
[16]	Implementation framework for agriculture 4.0 in Nigeria's food security	Conducted a systematic literature review on Nigeria's agriculture, food security, and agriculture 4.0. Developed an implementation framework integrating precision agriculture and digital technologies.	Provided insights into addressing Nigeria's food insecurity challenges using agriculture 4.0.	Lack of empirical validation and discussion on scalability issues in implementing the proposed framework.

Table 1. Empirical Review of Existing Smart Farming Security Methods

As per table 2, the agricultural sector has witnessed a significant transformation due to the integration of advanced technologies, particularly in the realm of smart agriculture. This literature review synthesizes and analyzes the current state-of-the-art solutions and research efforts in various domains of smart agriculture, including the adoption of emerging technologies like LoRa, Blockchain, Internet of Things (IoT), deep learning-enabled computer vision, and cyber-physical systems. The following sections delve into the key findings and insights garnered from the literature. The adoption of Low Power Wide Area Network (LPWAN) technologies, such as LoRa, has garnered considerable attention in the agricultural domain [17]. This technology offers a scalable and energy-efficient solution for diverse infield applications, including irrigation systems, plantation and crop monitoring, tree monitoring, and livestock monitoring. The review conducted by [17] highlights the potential of LoRa-based solutions in addressing the heterogeneous requirements of these scenarios, encompassing network bandwidth, sensor complexity, energy demand, and decision latency.

Blockchain technology has emerged as a promising enabler for enhancing data aggregation and security in smart agriculture systems [18]. By leveraging Blockchain and innovative data aggregation techniques, [18] proposed a cluster head sleep schedule method to optimize data collection and management processes in large-scale agricultural settings. This approach not only reduces data redundancy but also enhances energy efficiency, thereby promoting sustainable and cost-effective agricultural operations. The Internet of Things (IoT) has revolutionized various sectors, including agriculture, by offering smart solutions for precision farming, greenhouse management, and livestock monitoring [19]. The comprehensive survey conducted by [19] categorizes and synthesizes existing research work in the domain of IoT-based livestock management, focusing on network infrastructure, topologies, platforms, communication protocols, security issues, and monitoring applications. Moreover, the study identifies and analyzes open research challenges, paving the way for future advancements in IoT-enabled livestock management.

Similarly, IoT-based solutions have been instrumental in automating greenhouse farming parameters, thereby mitigating challenges associated with food security and environmental sustainability [20]. By integrating IoT technologies, such as cloud/edge computing, data analytics, and sensors, [20] presents a hierarchical overview of IoT-based greenhouse farming components and applications. The review underscores the significance of addressing open issues and research challenges to further optimize and standardize IoT-enabled greenhouse farming practices. Deep learning and computer vision techniques have played a pivotal role in revolutionizing agricultural practices, particularly in greenhouse environments [25]. By providing real-time insights and enabling data-driven decision-making, these technologies facilitate growth monitoring, disease detection, yield estimation, and other critical tasks. The literature review conducted by [25] comprehensively analyzes recent advancements in deep learning-enabled computer vision techniques tailored for greenhouse farming, highlighting key challenges, performance results, and future trends. The integration of cyber-physical systems (CPS) in agriculture has introduced new challenges related to security and threat detection [26]. [26] proposes a physics-data-based detection method to identify and mitigate cyber-attacks in photovoltaic (PV) farms using power electronics-enabled harmonic state space (HSS) models. This innovative approach enhances the accuracy and robustness of attack detection at both device and system levels, thereby ensuring the security and reliability of PV farm operations.

Reference	**Method Used**	**Findings**	**Results**	**Limitations**
[17]	Survey	Analyzed adoption of LoRa in agriculture and reviewed state-of-the-art solutions for smart agriculture. Explored LoRa's potential in various agricultural scenarios.	Identified four reference scenarios: irrigation systems, plantation and crop monitoring, tree monitoring, and livestock monitoring. Discussed scalability, interoperability, network architecture, and energy efficiency of LoRa-based solutions.	Limited discussion on implementation challenges and real-world case studies.
[18]	Data Aggregation Technique, Blockchain, Cluster Head Sleep Schedule	Introduced efficient data aggregation technique leveraging Blockchain and cluster head sleep schedule for smart agriculture.	Reduced data redundancy, enhanced energy utilization, and facilitated immediate pest attack control in agriculture.	May require further validation in real-world agricultural settings.
[19]	Survey	Presented a comprehensive survey on IoT's role	Identified IoT applications in livestock monitoring,	Limited discussion on implementation challenges and

		in livestock management, including network infrastructure, platforms, communication protocols, applications, and security issues.	controlling, and tracking. Developed a collaborative security model to detect and minimize security risks.	future research directions.
[20]	Survey	Explored IoT-based greenhouse farming, including technologies, applications, success stories, and research challenges.	Discussed IoT applications for plant monitoring, atmosphere control, irrigation, and success stories from agricultural countries. Presented open issues and research challenges.	Lacks detailed analysis of specific IoT implementations and case studies.
[21]	Detection Methodology	Proposed a physics-data-based detection method for cyber-attacks in PV farms using harmonic state space models.	Developed HSS-based detection at device and system levels for PV farms. Tested comprehensive attack models with real-time data acquisition.	Limited discussion on practical implementation challenges and scalability.
[22]	Security Scheme	Presented a secure multifactor authenticated key agreement scheme for IIoT environments.	Developed a secure and efficient scheme using symmetric cryptography and hash functions. Analyzed the performance and security of the proposed scheme.	May require further validation in real-world IIoT environments.
[23]	Survey	Conducted a comprehensive survey on blockchain-based IoT payments and marketplaces.	Explored challenges and solutions in realizing IoT payments and marketplaces using blockchain. Discussed blockchain-based smart applications and integration challenges.	Limited discussion on real-world implementation challenges and case studies.

[24]	Model and Assessment Method	Established a simplified model and assessment method for synchronization stability of multi-paralleled wind farms during asymmetrical grid faults.	Studied the effects of coupling characteristics on synchronization stability. Proposed a current control strategy to maximize stability margin.	Theoretical analysis needs validation through real-world experiments.
[25]	Review	Provided a review of deep learning-enabled computer vision techniques for greenhouse environments in agriculture.	Reviewed over 100 studies on deep learning applications for growth monitoring, disease detection, and yield estimation. Identified key challenges and future trends.	Limited discussion on specific methodologies and comparative analysis.
[26]	Security Measures	Discussed cyber–physical security challenges in PV systems and proposed solutions using firmware, network, and grid security measures.	Described vulnerabilities of PV systems and introduced blockchain technology for cyber-attack prevention. Presented simulation and experimental results.	Limited discussion on practical implementation challenges and scalability.
[27]	Service Provisioning Platform	Presented PenChain, a platform for SLA-minded service provisioning using blockchain technology.	Developed penalty-aware SLAs for general services and algorithms for ranking services based on SLAs. Evaluated PenChain in precision agriculture and automotive manufacturing scenarios.	Requires validation and scalability testing in diverse service ecosystems.
[28]	UAV-based Intrusion Detection	Proposed a UAV-assisted intrusion detection system for AIoT in agriculture	Developed algorithms for UAV deployment optimization and intrusion detection using CNN and LSTM.	Limited discussion on real-world deployment challenges and scalability.

		using machine learning algorithms.	Conducted simulation experiments to evaluate system performance.	
[29]	NFV-based Orchestrated UAV System	Proposed a decentralized UAV-aided MEC system for smart agriculture and formulated it as a decentralized partially observable Markov decision process.	Developed a federated learning-based solution for efficient NFV orchestration. Simulated the proposed approach to minimize energy consumption and AoI.	May require further validation in real-world agricultural environments.
[30]	Cyber-attack Detection for PV Farms	Presented a study on cyber-attack detection and diagnosis for PEC-enabled PV farms using single waveform sensor.	Proposed frequency-domain and time-domain-based features for threat detection. Validated the effectiveness using an online HIL testbed.	Limited discussion on scalability and real-world implementation challenges.
[31]	Yellow Rust Disease Monitoring	Explored aerial visual perception for yellow rust disease monitoring using UAV sensing and deep learning techniques.	Developed a framework integrating multispectral imaging, vegetation segmentation, and CNN-based classification for disease detection. Conducted field experiments to evaluate system performance.	Requires further validation in diverse agricultural settings and under different environmental conditions.
[32]	Threat Model and Analysis	Introduced a novel threat model for cyber-physical systems that combines cyber, physical, and human aspects.	Proposed a threat analysis method and implemented it into an automatic tool called TAMELESS. Demonstrated the use of the model and analysis through three case studies.	May require refinement and validation in various cyber-physical system domains.

[33]	Disease Classification in PA	Presented MMF-Net, a CNN-based architecture for plant leaf disease classification in precision agriculture.	Integrated multi-contextual features using RL-block and PL-blocks for disease classification. Achieved high accuracy in classifying corn leaf diseases through experiments.	Limited discussion on real-world deployment challenges and scalability.

Table 2. Review of Existing Applications in Secure Smart Farming

Furthermore, as per table 3, the Internet of Things (IoT) has emerged as a transformative technology, promising enhanced connectivity and decision-making capabilities [37]. However, the proliferation of IoT devices has also introduced new security challenges, particularly in group communication scenarios. To address this, a lightweight NTRU and Secret Sharing Based Secure Group Communication Scheme was proposed, offering enhanced security for IoT applications such as IoMT, VANET, and Precision Agriculture [37]. Moreover, the vulnerability of power systems, especially those relying entirely on inverter-based resources (IBRs), poses significant operational challenges [39]. To mitigate this, an operator support system (OSS) was introduced, integrating dynamic security assessment and optimization techniques. Through advanced simulation models, it was demonstrated that stable operation with 100% IBR generation is achievable, particularly with the utilization of grid-forming inverters [39] & circuit sets. In the context of Mobile-edge computing (MEC), security and privacy concerns have gained prominence due to its distributed nature and reliance on diverse technologies [40]. Researchers have explored the application of artificial intelligence (AI) algorithms to address security challenges, leveraging frameworks such as the European Telecommunications Standards Institute (ETSI) MEC reference architecture [40]. By identifying new security issues and proposing AI-driven solutions, the study offers insights into mitigating risks associated with MEC deployments. Furthermore, the healthcare sector faces unique challenges in ensuring data integrity and privacy within IoT ecosystems [42]. Redactable signature schemes (RSS) have emerged as a viable solution, allowing for flexible data sharing while preserving privacy. However, existing RSS implementations face scalability and security concerns. To address this, researchers proposed lightweight identity-based RSS tailored for healthcare IoT applications, offering enhanced security and efficiency [42]. In the realm of Vehicular ad hoc networks (VANETs), ensuring secure communication is essential for traffic safety and management [43]. Traditional conditional privacy-preserving authentication (CPPA) schemes face limitations in terms of communication overhead and key management. To overcome these challenges, researchers proposed innovative CPPA schemes based on elliptic curve cryptography and fog computing models, offering improved efficiency and security for VANET applications [43][46].

Reference	**Method Used**	**Findings**	**Results**	**Limitations**
[34]	Green synthesis of metal-based nanoparticles	Green synthesis methods utilizing biological resources	Green synthesized MNPs showed potential for various	Lack of detailed discussion on specific green

	(MNPs) for agriculture and food security	to produce MNPs for agricultural applications were reviewed.	agricultural applications, including plant growth promotion, disease and pest management, food packaging, and shelf life extension.	synthesis methods and their efficacy in different agricultural scenarios.
[35]	Machine learning for cyber-attack detection in PV farms	Proposed a Convolutional Neural Network (CNN) using micro-phase measurement units (μ PMU) for cyber-attack detection in PV farms.	The CNN-based method demonstrated effective detection of cyber-attacks with adequate accuracy and robustness under various scenarios.	Limited discussion on the scalability and practical implementation challenges of the proposed method in real-world PV farm settings.
[36]	Design principles for IoT systems inspired by financial technology ecosystem	Identified principles derived from the financial technology ecosystem for designing technically sound and economically efficient IoT systems, focusing on smart agriculture.	The proposed design principles offer a comprehensive basis for assessing IoT systems, beyond traditional technology readiness levels, to evaluate market potential.	Lack of empirical validation or case studies to demonstrate the practical applicability and effectiveness of the proposed design principles.
[37]	Lightweight secure group communication scheme for IoT applications	Proposed a lightweight NTRU and Secret Sharing Based Secure Group Communication Scheme for low bandwidth communication in IoMT, VANET, and precision agriculture.	The proposed scheme offers enhanced security for group communication in IoT applications while maintaining computational efficiency and low bandwidth requirements.	Limited discussion on potential scalability challenges and performance trade-offs in large-scale IoT deployments.
[38]	Deep sequence learning for data integrity attacks on PV systems	Introduced a deep sequence learning-based diagnosis solution for	The proposed method demonstrated superior	Lack of discussion on potential real-world implementation

		detecting data integrity attacks on PV systems, leveraging time-series electric waveform data samples.	performance in detecting and diagnosing various data integrity attacks on PV systems compared to classic data-driven methods.	challenges and scalability of the proposed solution in large-scale PV systems.
[39]	Operator support system for stable operation of power systems with IBR generation	Presented an operator support system (OSS) to enable stable operation of power systems with up to 100% IBR generation, utilizing dynamic security assessment and optimization techniques.	The OSS effectively improves system stability by optimizing control parameters of generators and inverters, particularly using grid-forming inverters, as demonstrated in high-fidelity simulations.	Limited discussion on practical deployment challenges and scalability considerations, especially in transitioning from simulations to real-world power systems.
[40]	Security and privacy in mobile-edge computing (MEC)	Provided a comprehensive survey of security and privacy issues in MEC from the perspective of AI, based on the ETSI MEC reference architecture.	Identified new security and privacy challenges in MEC and discussed potential AI-based solutions, highlighting opportunities and challenges for future research.	Limited empirical validation or case studies to demonstrate the effectiveness of AI-based security solutions in real-world MEC deployments.
[41]	Best practices for IoT privacy and security	Identified and discussed best practices for ensuring privacy and security in IoT systems, applied them to real IoT use cases, and evaluated their impact using risk assessment.	Following the proposed best practices resulted in significantly lower risk scores for implemented IoT systems, indicating improved privacy and security.	Lack of discussion on the generalizability of the identified best practices across diverse IoT applications and ecosystems.
[42]	Identity-based redactable	Proposed an identity-based	The proposed scheme offers	Limited discussion on potential

	signature scheme for healthcare data sharing in IoT	redactable signature scheme for healthcare data sharing in IoT, addressing integrity, source authentication, and privacy concerns without relying on PKI systems.	efficient and secure data sharing in resource-limited IoT environments while providing selective disclosure control and practical performance.	vulnerabilities or attack vectors specific to the proposed identity-based redactable signature scheme in healthcare IoT scenarios.
[43]	Conditional privacy-preserving authentication scheme for VANETs	Proposed a CPPA scheme based on elliptic curve cryptography for VANETs, addressing ultra-low transmission delay and secure system secret key (SSK) updating.	The proposed scheme achieves secure and efficient authentication in VANETs with formal security proof, reduced storage size, and low transmission delay compared to related schemes.	Limited discussion on potential implementation challenges and scalability considerations in large-scale VANET deployments.
[44]	Security solutions for IoT using blockchain technology	Reviewed security and privacy issues in IoT systems and proposed security solutions based on blockchain technology, with a case study implemented using Ethereum-based blockchain in a smart IoT system.	Blockchain-based security solutions offer improved data integrity and privacy protection in IoT systems, as demonstrated in the case study implementation.	Limited discussion on scalability challenges and potential trade-offs between blockchain-based security solutions and resource-constrained IoT devices.
[45]	Dual blockchain-assisted authentication framework for VANETs	Proposed a dual blockchain-assisted conditional privacy-preserving authentication framework for VANETs, enabling decentralized identity	The proposed framework offers efficient and scalable authentication in VANETs without relying on centralized trusted third parties, with decentralized	Limited discussion on potential vulnerabilities or attack vectors specific to the proposed dual blockchain-assisted authentication

		authentication, privacy preservation, and dynamic revocation of illegal vehicles.	dynamic revocation of illegal vehicles through smart contracts.	framework in VANET scenarios.
[46]	Lightweight CPPA scheme based on elliptic curve cryptography for VANETs	Proposed a lightweight CPPA scheme for VANETs based on elliptic curve cryptography, addressing key escrow issues and supporting mobility, low latency, and location awareness using a fog computing model.	The proposed scheme achieves efficient and secure authentication in VANETs with reduced computation and communication overheads, ensuring security requirements and scalability.	Limited discussion on potential performance variations or limitations in dynamic VANET environments with varying network conditions and mobility patterns.
[47]	Privacy-preserving scheme based on homomorphic encryption for IoT	Proposed a lightweight privacy-preserving scheme based on homomorphic encryption for IoT, addressing privacy concerns between data owners, untrustworthy third-party cloud servers, and data users.	The proposed scheme effectively prevents privacy breaches in IoT systems, offering privacy protection with computationally efficient homomorphic algorithms and practical applicability.	Limited discussion on potential compatibility issues or performance trade-offs when integrating the proposed homomorphic encryption-based scheme with existing IoT infrastructures and protocols.
[48]	Certificateless redactable signature scheme for healthcare IoT	Introduced a certificateless redactable signature scheme for healthcare IoT, addressing public key management and secret key escrow issues while supporting batch verification and redaction control.	The proposed scheme offers efficient and secure data sharing in healthcare IoT environments, ensuring data integrity, source authentication, and privacy preservation with reduced computational and	Limited discussion on potential vulnerabilities or attack vectors specific to the proposed certificateless redactable signature scheme in healthcare IoT scenarios.

			communication overheads.	
[49]	Privacy methods for intelligent infrastructure services in IoT	Surveyed privacy methods and use cases for intelligent infrastructure services in IoT, focusing on post-quantum cryptography techniques and their applications in real-world scenarios.	Identified post-quantum cryptographic primitives suitable for IoT applications and discussed practical deployment challenges and future research scopes.	Limited empirical validation operations

Table 3. Review of Existing Methods used for General Purpose Security Deployments

Overall, the literature highlights the importance of adopting advanced techniques such as machine learning, lightweight cryptography, and distributed architectures to address cybersecurity challenges across diverse domains, from renewable energy systems to healthcare IoT and vehicular networks. These advancements pave the way for more resilient and secure cyber-physical systems in the face of evolving threats. Next, we discuss the results of these methods, and compare them for different use case scenarios.

3. Result & Analysis

This section aims to compare various methods proposed in different research papers focusing on smart agriculture. The comparison is based on different performance metrics, including security, efficiency, scalability, and practicality. The analysis compares methods proposed in different texts focusing on smart agriculture. It evaluates these methods based on performance metrics such as security, efficiency, scalability, and practicality. Table 4 compared the methods, advantages, and disadvantages are summarized to provide a comprehensive comparison.

Paper	**Methods Proposed**	**Performance Metrics**	**Advantages**	**Disadvantages**
[1]	Blockchain-based smart farming technology, smart contract-based blockchain-envisioned authenticated key agreement mechanism	Security, transparency, efficiency, scalability	Provides reliability, transparency, and scalability. Offers superior security compared to existing protocols.	May have high computational overhead.
[2]	Key technologies and applications in smart agriculture, security and	Security, privacy, efficiency	Addresses security challenges in various modes of smart agriculture.	May lack specific implementation details.

	privacy countermeasures			
[3]	AgroMobiBlock authenticated key agreement scheme, blockchain-based simulation	Security, efficiency	Offers robust security against various attacks. Demonstrates practical usefulness through simulations and real-time experiments.	Computational time for large-scale simulations may be high.
[4]	IoT-based network framework for greenhouse farming, review of IoT-based greenhouse sensors and communication protocols	Efficiency, practicality	Provides comprehensive insights into IoT-based greenhouse farming. Identifies challenges and future research directions.	May lack detailed security analysis.
[5]	Enhanced Black Widow Optimization with Hybrid Deep Learning Enabled Intrusion Detection (EBWO-HDLID) technique	Security, reliability	Detects intrusions effectively using deep learning. Validates performance on benchmark datasets.	May require extensive parameter tuning.
[6]	Use of Big Data, Machine Learning, and IoT in rice smart farming, survey of research on intelligent data processing	Efficiency, scalability	Utilizes emerging technologies to improve rice production processes. Presents a framework for rice smart farming.	May require advanced technical expertise for implementation.
[7]	Phase-locked loop (PLL)-synchronized wind farms, transient stability assessment method	Stability, reliability	Identifies coupling effects in wind farms. Proposes methods to improve stability during grid faults.	Simulation results may need verification in real-world scenarios.
[8]	Authentication and key establishment scheme based on Rabin cryptosystem for resource-asymmetric smart environments	Security, anonymity, efficiency	Provides lightweight authentication for resource-asymmetric environments. Offers user anonymity and efficiency.	Security proofs may need validation in diverse scenarios.
[9]	Generalized blockchain-based security architecture for	Security, cost-effectiveness	Proposes a comprehensive security architecture. Conducts detailed cost	May require further empirical validation of cost analysis.

	smart agriculture, cost analysis		analysis of existing schemes.	
[10]	Redactable blockchain-based secure data aggregation method with source authentication for fog-enabled IoFT	Security, privacy	Ensures data confidentiality and integrity in IoT-enabled smart agriculture. Resists collusion and malicious attacks.	Practical implementation may face challenges in real-world deployments.
[11]	Privacy-preserving framework (PPSAF) for smart agriculture, future research scopes	Privacy, scalability	Addresses privacy concerns in various domains including smart agriculture. Proposes a framework for privacy preservation.	Practical implementation may require integration with existing systems.
[12]	Privacy-preserving data aggregation scheme with flexibility property using ElGamal Cryptosystem	Privacy, flexibility	Ensures data privacy while balancing data publishing needs. Provides theoretical security analysis and performance simulations.	Real-world deployment may face compatibility issues with existing systems.
[13]	Frequency security constrained scheduling approach considering wind farms, simulation results	Stability, efficiency	Quantifies wind farm contributions to frequency support and reserve. Reduces operation cost and VRE curtailment.	Simulation results may need validation in diverse grid scenarios.
[14]	Sensor-based AI applications for poultry farming, review of IoT systems with AI capabilities	Efficiency, practicality	Provides insights into AI-enabled poultry farming. Identifies benefits and challenges of AI and IoT integration.	Implementation may require integration with existing farm infrastructure.
[15]	Blockchain-based service platform for agricultural service operations, numerical experiments	Efficiency, reliability	Proposes a secure and efficient platform for agricultural services. Validates performance through numerical experiments.	Real-world deployment may require integration with existing service frameworks.

[16]	Implementation framework for agriculture 4.0 in Nigeria, systematic literature review	Security, scalability, practicality	Addresses food insecurity challenges in Nigeria using agriculture 4.0. Provides a comprehensive framework based on literature review.	Real-world implementation may face socio-economic challenges in Nigeria.

Table 4. Empirical Comparison of Different Security Methods

The analysis provides valuable insights into the state-of-the-art methods in smart agriculture. It highlights the strengths and weaknesses of each approach, helping researchers and practitioners make informed decisions when designing and implementing smart agriculture solutions. Additionally, the comparison underscores the importance of considering various factors such as security, efficiency, and scalability in the development of smart agriculture technologies. Further research and validation are recommended to address the identified limitations and enhance the effectiveness of smart agriculture solutions. Table 5 summarizes the performance of methodologies discussed in papers [17] to [34] across different metrics relevant to smart agriculture. Each methodology is evaluated based on criteria such as scalability, energy efficiency, security, and practical applicability.

Paper	**Methodology**	**Scalability**	**Energy Efficiency**	**Security**	**Practical Applicability**
[17]	LoRa Adoption	High	High	Moderate	Widely Applicable
[18]	Blockchain Data Aggregation	Moderate	High	High	Field Monitoring
[19]	IoT in Livestock Management	High	Moderate	High	Livestock Monitoring
[20]	IoT-based Greenhouse Farming	High	High	Moderate	Greenhouse Control
[21]	Cyber-Attack Detection in PV Farms	Moderate	High	High	PV Farm Security
[22]	Secure Authentication in IIoT	High	High	High	IIoT Security
[23]	Blockchain-based IoT Payments	High	High	High	IoT Payments
[24]	Stability Assessment of Wind Farms	Moderate	High	High	Wind Farm Stability
[25]	Deep Learning in Greenhouses	High	Moderate	High	Crop Monitoring
[26]	Cyber-Physical Security of PV Systems	Moderate	High	High	PV System Security

[27]	SLA-based Service Provisioning	High	High	High	Service Ecosystems
[28]	UAV-based Agricultural Monitoring	High	High	Moderate	Farmland Information
[29]	IoT-enabled Precision Agriculture	High	High	High	Precision Farming
[30]	Cyber-Attack Detection in PEC-enabled PV Farms	Moderate	High	High	PV Farm Security
[31]	Computer Vision for Disease Monitoring	High	High	High	Disease Detection
[32]	Threat Analysis for Cyber-Physical Systems	High	High	High	System Security
[33]	CNN-based Disease Classification	High	High	High	Disease Identification
[34]	Green Synthesized MNPs in Agriculture	High	High	High	Agricultural Applications

Table 5. Comparison of Existing Methods

Table 5 illustrates the diverse methodologies employed in smart agriculture, highlighting their respective strengths and weaknesses across various metrics. It is evident that most methodologies exhibit high scalability and energy efficiency, with a significant emphasis on security and practical applicability. Blockchain-based solutions and IoT applications are particularly prominent, offering robustness in data aggregation, payment systems, and livestock management. Additionally, advancements in cybersecurity, such as cyber-attack detection in PV farms and PEC-enabled PV farms, underscore the growing importance of securing agricultural infrastructures. Moreover, the integration of deep learning and computer vision techniques facilitates precise crop monitoring and disease detection in greenhouse environments, enhancing overall agricultural productivity. Overall, these methodologies collectively contribute to the advancement of smart agriculture, addressing critical challenges and fostering sustainable agricultural practices.

Table 6 compares various methods proposed in terms of different performance metrics related to security, privacy, efficiency, and practicality. Each paper introduces novel techniques or frameworks to address specific challenges in the domains of cyber-physical systems, Internet of Things (IoT), vehicular ad hoc networks (VANETs), and healthcare IoT, among others. The metrics considered for comparison include detection accuracy, robustness, computational overhead, communication overhead, security guarantees, privacy preservation, and practical feasibility. The table below provides a comprehensive overview of how each method performs across these metrics, offering insights into their strengths and limitations. The analysis table below offers a comparative evaluation of the methods proposed in the work, focusing on key performance metrics such as detection accuracy, robustness, computational overhead, communication overhead, security guarantees, privacy preservation, and practical feasibility. Each method is assessed based on its effectiveness in addressing the challenges within its respective domain, highlighting its strengths and potential drawbacks. This comparative

analysis serves to guide researchers and practitioners in selecting suitable techniques for specific application scenarios, considering factors such as security requirements, resource constraints, and scalability.

Paper	**Methodology**	**Detection Accuracy**	**Robustness**	**Computational Overhead**	**Communication Overhead**	**Security Guarantees**	**Privacy Preservation**	**Practical Feasibility**
[35]	CNN using μ PMU and figures of merit	High	Adequate	Moderate	Low	Strong	Limited	High
[36]	IoT system design principles from financial technology ecosystem	Low	Low	Low	Low	Low	Low	High
[37]	Lightweight NTRU and Secret Sharing Based Secure Group Communication	High	Strong	Low	Low	Moderate	Strong	Moderate
[38]	Deep sequence learning for data integrity attacks on PV systems	High	Strong	High	Moderate	Strong	Limited	Moderate
[39]	Operator support system for stable operation of power	High	Strong	Moderate	Low	Strong	Low	Moderate

	systems with IBRs							
[40]	Survey of security and privacy in MEC from the perspective of AI	Low	Low	Low	Low	Low	Low	High
[41]	Best practices for IoT privacy and security implementation	Low	Low	Low	Low	Low	High	High
[42]	Identity-based redactable signature scheme for healthcare data sharing in IoT	High	Strong	Moderate	Low	Strong	High	Moderate
[43]	Conditional privacy-preserving authentication scheme for VANETs	High	Strong	Low	Low	Strong	High	High
[44]	Security solutions for IoT using blockchain technology	Low	Low	Low	Low	Low	Low	High
[45]	Dual blockchain	High	Strong	Moderate	Low	Strong	High	High

	-assisted conditional privacy-preserving authentication for VANETs							
[46]	Lightweight CPPA scheme based on elliptic curve cryptography for VANETs	High	Strong	Low	Low	Strong	High	High
[47]	Lightweight privacy-preserving scheme based on homomorphic encryption for IoT	Low	Low	Low	Low	Low	High	High
[48]	Certificateless RSS for secure and efficient data sharing in healthcare IoT	High	Strong	Moderate	Moderate	Strong	High	Moderate
[49]	Privacy methods for II services with focus on post-quantum	Low	Low	Low	Low	Low	High	High

	cryptography							
[50]	Optional privacy-preserving data aggregation scheme based on BGN homomorphic encryption for IoT	Low	Low	Low	Low	Low	High	High

Table 6. Analytical Comparison of Existing Methods

This analysis highlights the diversity of approaches in addressing security and privacy challenges across different domains, ranging from machine learning-based intrusion detection to cryptographic techniques for data sharing and privacy preservation. While each method exhibits strengths in certain areas, such as detection accuracy or privacy preservation, trade-offs exist in terms of computational complexity, communication overhead, and practical feasibility. Researchers and practitioners can leverage this comparative analysis to identify suitable methodologies based on the specific requirements and constraints of their applications.

This analysis encompasses a diverse array of methodologies proposed with a focus on security and privacy applications in various domains such as smart farming, IoT, healthcare, and cyber-physical systems. Across these papers, a multitude of methods are proposed, each tailored to address specific challenges while prioritizing different performance metrics. For instance, blockchain-based technologies, as explored in papers [1], [3], [9], [10], [15], and [18], offer promising solutions for ensuring security, transparency, and reliability in smart agriculture and IoT environments. These methods leverage the inherent properties of blockchain, such as immutability and decentralized consensus, to provide robust security guarantees. However, they may incur high computational overheads, particularly during transaction verification and consensus mechanisms.

On the other hand, lightweight cryptographic schemes, as exemplified in papers [37], [42], [43], [46], [47], and [48], prioritize efficiency and practical feasibility while maintaining strong security and privacy assurances. These schemes, such as lightweight NTRU encryption and elliptic curve cryptography-based authentication, are well-suited for resource-constrained environments like IoT devices and VANETs. They offer high detection accuracy and robustness against various attacks while minimizing computational and communication overheads. Moreover, privacy-preserving techniques, including homomorphic encryption and redactable signature schemes, play a crucial role in safeguarding sensitive data in healthcare IoT applications, as evidenced in papers [42], [47], and [48].

In terms of scalability and applicability, methods such as LoRa adoption, discussed in paper [17], and IoT-enabled precision agriculture, presented in paper [29], stand out for their high scalability and wide-ranging applicability in diverse environments. These methods leverage existing infrastructure and standards to deliver efficient and reliable solutions for field monitoring, livestock management, and precision farming. Additionally, machine learning and AI-based approaches, as explored in papers [5], [14], [25], and [33], offer advanced capabilities for intrusion detection, disease monitoring, and crop management, demonstrating high detection accuracy and practical feasibility in real-world scenarios.

Overall, the optimal methods for different security and privacy applications depend on specific requirements, constraints, and contextual factors. While blockchain-based technologies provide robust security and transparency, lightweight cryptographic schemes offer efficiency and practicality for resource-constrained environments. Privacy-preserving techniques play a crucial role in protecting sensitive data, particularly in healthcare and IoT applications. Scalability and applicability are key considerations, with methods leveraging existing infrastructure and standards demonstrating wider adoption potential. Machine learning and AI-based approaches offer advanced capabilities for intrusion detection, disease monitoring, and crop management, enhancing security and efficiency in diverse domains.

4. Conclusion & Future Scopes

In conclusion, the analysis highlights the diverse array of methodologies proposed in the field of security and privacy applications across various domains, including smart farming, IoT, healthcare, and cyber-physical systems. The studies reviewed showcase a wide range of approaches, each tailored to address specific challenges while prioritizing different performance metrics such as security, scalability, efficiency, and practical feasibility. The findings underscore the importance of adopting a holistic approach to security and privacy, considering the unique requirements and constraints of each application domain. Blockchain-based technologies offer robust solutions for ensuring security, transparency, and reliability, albeit with potential computational overheads. Meanwhile, lightweight cryptographic schemes provide efficient and practical solutions, particularly for resource-constrained environments like IoT devices and smart farming scenarios. Privacy-preserving techniques emerge as crucial for safeguarding sensitive data, especially in healthcare and IoT applications, emphasizing the need for ongoing research and development in this area.

Looking ahead, the future scope lies in advancing methodologies that strike a balance between security, efficiency, and scalability while addressing emerging challenges in evolving application domains. This includes further exploration of machine learning and AI-based approaches for enhancing intrusion detection, disease monitoring, and crop management, as well as continued efforts to develop privacy-preserving techniques for protecting sensitive data samples. Additionally, there is a need for interdisciplinary collaboration to integrate security and privacy considerations seamlessly into the design and implementation of emerging technologies, ensuring that advancements are not only technically sound but also ethically and socially responsible in different scenarios. Overall, the research presented in this paper provides valuable insights into the state-of-the-art methodologies and lays the groundwork for future endeavors aimed at fortifying security and privacy in an increasingly

interconnected and data-driven world. Through continued innovation and collaboration, the field can forge ahead towards realizing the full potential of emerging technologies while safeguarding individual privacy and security.

5. References

[1] A. Vangala, A. K. Sutrala, A. K. Das and M. Jo, "Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10792-10806, 1 July1, 2021, doi: 10.1109/JIOT.2021.3050676.

keywords: {Authentication;Blockchain;Servers;Logic gates;Agriculture;Security;Internet of Things;Authentication;blockchain;Internet of Things (IoT);key agreement;security;smart farming},

[2] X. Yang et al., "A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges," in IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 2, pp. 273-302, February 2021, doi: 10.1109/JAS.2020.1003536.

keywords: {Agriculture;Security;Production;Information technology;Privacy;Internet of Things;Loss measurement;Agricultural artificial intelligence;agricultural automation;agricultural Internet of Things;security;smart agriculture},

[3] A. Vangala, A. K. Das, A. Mitra, S. K. Das and Y. Park, "Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 904-919, 2023, doi: 10.1109/TIFS.2022.3231121.

keywords: {Blockchains;Authentication;Security;Farming;Smart agriculture;Remote monitoring;Costs;Intelligent precision agriculture;Internet of Things (IoT);mobile vehicles;blockchain;authentication and key agreement;security;simulation},

[4] M. S. Farooq, R. Javid, S. Riaz and Z. Atal, "IoT Based Smart Greenhouse Framework and Control Strategies for Sustainable Agriculture," in IEEE Access, vol. 10, pp. 99394-99420, 2022, doi: 10.1109/ACCESS.2022.3204066.

keywords: {Farming;Green products;Sensors;Monitoring;Wireless sensor networks;Taxonomy;Protocols;Security;Internet of Things;Communication protocols;Big Data;Data analysis;Cloud computing;Internet of Things (IoT);greenhouse;applications;sensors;communication protocols;cloud computing;big data analytics;security attacks},

[5] R. Y. Aburasain, "Enhanced Black Widow Optimization With Hybrid Deep Learning Enabled Intrusion Detection in Internet of Things-Based Smart Farming," in IEEE Access, vol. 12, pp. 16621-16631, 2024, doi: 10.1109/ACCESS.2024.3359043.

keywords: {Smart agriculture;Intrusion detection;Internet of Things;Artificial neural networks;Feature extraction;Mathematical models;Farming;Deep learning;Cyberattack;Smart farming;Internet of Things;deep learning;intrusion detection;cyberattacks;feature selection},

[6] R. Alfred, J. H. Obit, C. P. -Y. Chin, H. Haviluddin and Y. Lim, "Towards Paddy Rice Smart Farming: A Review on Big Data, Machine Learning, and Rice Production Tasks," in IEEE Access, vol. 9, pp. 50358-50380, 2021, doi: 10.1109/ACCESS.2021.3069449.

keywords: {Agriculture;Digital agriculture;Machine learning;Machine learning algorithms;Market research;Big Data;Internet of Things;Rice production;big data analytics;Internet of Things;machine learning;smart farming;precision agriculture;agriculture supply chain},

[7] S. Chen, J. Yao, Y. Liu, J. Pei, S. Huang and Z. Chen, "Coupling Mechanism Analysis and Transient Stability Assessment for Multiparalleled Wind Farms During LVRT," in IEEE Transactions on Sustainable Energy, vol. 12, no. 4, pp. 2132-2145, Oct. 2021, doi: 10.1109/TSTE.2021.3083830.

keywords: {Wind farms;Transient analysis;Power system stability;Phase locked loops;Stability criteria;Multiparalleled wind farms;transient stability;low voltage ride-through (LVRT);equilibrium points;transient stability assessment method},

[8] L. Bai, C. Hsu, L. Harn, J. Cui and Z. Zhao, "A Practical Lightweight Anonymous Authentication and Key Establishment Scheme for Resource-Asymmetric Smart Environments," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 4, pp. 3535-3545, 1 July-Aug. 2023, doi: 10.1109/TDSC.2022.3203874.

keywords: {Security;Logic gates;Authentication;Encryption;Protocols;Smart homes;Smart devices;Anonymity;key establishment;lightweight;mutual authentication;rabin cryptosystem;resource-asymmetry},

[9] A. Vangala, A. K. Das, N. Kumar and M. Alazab, "Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective," in IEEE Sensors Journal, vol. 21, no. 16, pp. 17591-17607, 15 Aug.15, 2021, doi: 10.1109/JSEN.2020.3012294.

keywords: {Agriculture;Sensors;Monitoring;Internet of Things;Temperature measurement;Smart agriculture;Internet of Things (IoT);blockchain technology;authentication;security},

[10] R. Mishra, D. Ramesh, P. Bellavista and D. R. Edla, "Redactable Blockchain-Assisted Secure Data Aggregation Scheme for Fog-Enabled Internet-of-Farming-Things," in IEEE Transactions on Network and Service Management, vol. 20, no. 4, pp. 4652-4667, Dec. 2023, doi: 10.1109/TNSM.2023.3322442.

keywords: {Data models;Data aggregation;Computational modeling;Blockchains;Security;Servers;Data privacy;Internet-of-Farming-Things (IoFT);fog computing;data aggregation;redactable blockchain},

[11] Q. N. Tran, B. P. Turnbull, H. -T. Wu, A. J. S. de Silva, K. Kormusheva and J. Hu, "A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture," in IEEE Open Journal of the Computer Society, vol. 2, pp. 72-84, 2021, doi: 10.1109/OJCS.2021.3053032.

keywords: {Blockchains;Privacy;Bitcoin;Smart contracts;Peer-to-peer computing;Data privacy;Consensus algorithm;Biometrics;Digital agriculture;Smart grids;Internet of things;Biometrics;blockchain;consensus protocol;internet of things;privacy;privacy-preservation;smart agriculture;smart energy},

[12] J. Song, Q. Zhong, W. Wang, C. Su, Z. Tan and Y. Liu, "FPDP: Flexible Privacy-Preserving Data Publishing Scheme for Smart Agriculture," in IEEE Sensors Journal, vol. 21, no. 16, pp. 17430-17438, 15 Aug.15, 2021, doi: 10.1109/JSEN.2020.3017695.

keywords: {Agriculture;Cloud computing;Data privacy;Data aggregation;Privacy;Sensors;Security;Smart agriculture;data aggregation;data privacy;flexibility;data publishing},

[13] Z. Zhang, M. Zhou, Z. Wu, S. Liu, Z. Guo and G. Li, "A Frequency Security Constrained Scheduling Approach Considering Wind Farm Providing Frequency Support and Reserve," in IEEE Transactions on Sustainable Energy, vol. 13, no. 2, pp. 1086-1100, April 2022, doi: 10.1109/TSTE.2022.3150965.

keywords: {Wind farms;Wind power generation;Wind turbines;Frequency control;Security;Frequency synchronization;Wind forecasting;Frequency support;wind power reserve;wind farms;low-carbon operation;robust optimization scheduling},

[14] M. R. Bhuiyan and P. Wree, "Animal Behavior for Chicken Identification and Monitoring the Health Condition Using Computer Vision: A Systematic Review," in IEEE Access, vol. 11, pp. 126601-126610, 2023, doi: 10.1109/ACCESS.2023.3331092.

keywords: {Animals;Monitoring;Behavioral sciences;Farming;Diseases;Productivity;Deep learning;Smart agriculture;Computer vision;Deep learning;Machine learning;Smart farming;computer vision;deep learning;machine learning;chicken detection and monitoring},

[15] Q. Zheng et al., "Smart-Contract-Based Agricultural Service Platform for Drone Plant Protection Operation Optimization," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 21363-21376, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3288870.

keywords: {Drones;Smart contracts;Crops;Blockchains;Optimization;Internet of Things;Plants (biology);Smart agriculture;Farming;Agricultural service platform;blockchain;drone plant protection;service optimization;smart contract},

[16] S. O. Oruma, S. Misra and L. Fernandez-Sanz, "Agriculture 4.0: An Implementation Framework for Food Security Attainment in Nigeria's Post-Covid-19 Era," in IEEE Access, vol. 9, pp. 83592-83627, 2021, doi: 10.1109/ACCESS.2021.3086453.

keywords: {Agriculture;Security;Supply chains;Systematics;Production;Government policies;Climate change;Agriculture 4.0;agri-food 4.0;food security;sustainability;SDG goal 2;implementation framework;supply chain},

[17] A. Pagano, D. Croce, I. Tinnirello and G. Vitale, "A Survey on LoRa for Smart Agriculture: Current Trends and Future Perspectives," in IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3664-3679, 15 Feb.15, 2023, doi: 10.1109/JIOT.2022.3230505.

keywords: {Smart agriculture;Monitoring;Internet of Things;Wireless sensor networks;Temperature sensors;Sensors;Power demand;Internet of Things (IoT);LoRa;LoRaWAN;low-power wide-area network (LPWAN);precision agriculture;smart agriculture;smart farming;wireless sensor networks (WSNs)},

[18] A. Ahmed, I. Parveen, S. Abdullah, I. Ahmad, N. Alturki and L. Jamel, "Optimized Data Fusion With Scheduled Rest Periods for Enhanced Smart Agriculture via Blockchain Integration," in IEEE Access, vol. 12, pp. 15171-15193, 2024, doi: 10.1109/ACCESS.2024.3357538.

keywords: {Blockchains;Smart agriculture;Internet of Things;Crops;Monitoring;Sensors;Data aggregation;Wireless networks;Smart agriculture;blockchain technology;sleep field monitoring;Internet of Things;wireless network},

[19] M. S. Farooq, O. O. Sohail, A. Abid and S. Rasheed, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Livestock Environment," in IEEE Access, vol. 10, pp. 9483-9505, 2022, doi: 10.1109/ACCESS.2022.3142848.

keywords: {Agriculture;Monitoring;Animals;Protocols;Internet of Things;Sensors;Logic gates;IoT;livestock;animal monitoring;cattle monitoring;cloud computing;animal tracking;feeding;poultry management},

[20] M. S. Farooq, S. Riaz, M. A. Helou, F. S. Khan, A. Abid and A. Alvi, "Internet of Things in Greenhouse Agriculture: A Survey on Enabling Technologies, Applications, and Protocols," in IEEE Access, vol. 10, pp. 53374-53397, 2022, doi: 10.1109/ACCESS.2022.3166634.

keywords: {Green products;Air pollution;Crops;Internet of Things;Monitoring;Soil measurements;Protocols;Climate change;IoT;smart greenhouse;hydroponics;vertical farm;security issues;network technologies;communication protocols;IoT sensors;mobile apps},

[21] J. Zhang, L. Guo and J. Ye, "Cyber-Attack Detection for Photovoltaic Farms Based on Power-Electronics-Enabled Harmonic State Space Modeling," in IEEE Transactions on Smart Grid, vol. 13, no. 5, pp. 3929-3942, Sept. 2022, doi: 10.1109/TSG.2021.3121009.

keywords: {Voltage control;Power harmonic filters;Harmonic analysis;Microgrids;Inverters;Stability analysis;Smart grids;Cyber security;harmonics state space;physical-based detection;clustering;PV farm},

[22] F. Rafique, M. S. Obaidat, K. Mahmood, M. F. Ayub, J. Ferzund and S. A. Chaudhry, "An Efficient and Provably Secure Certificateless Protocol for Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8039-8046, Nov. 2022, doi: 10.1109/TII.2022.3156629.

keywords: {Industrial Internet of Things;Security;Sensors;Authentication;Protocols;Informatics;Cloud computing;Authentication protocol;industrial Internet of Things (IIoT);key agreement;smart card},

[23] A. Saputhanthri, C. De Alwis and M. Liyanage, "Survey on Blockchain-Based IoT Payment and Marketplaces," in IEEE Access, vol. 10, pp. 103411-103437, 2022, doi: 10.1109/ACCESS.2022.3208688.

keywords: {Internet of Things;Blockchains;Sensors;Intelligent sensors;Ecosystems;Cloud computing;Distributed ledger;Security;Privacy;Interoperability;Electronic commerce;Online banking;Internet of Things;IoT payment;IoT marketplace;blockchain;smart contracts;decentralization},

[24] Q. Zhong, J. Yao, Y. Luo, S. Huang and S. Chen, "Dual-Sequence Synchronization Stability Analysis and Control of Multi-Paralleled Wind Farms During Asymmetrical Grid Faults," in IEEE Transactions on Sustainable Energy, vol. 15, no. 1, pp. 381-397, Jan. 2024, doi: 10.1109/TSTE.2023.3289079.

keywords: {Wind farms;Phase locked loops;Power system stability;Synchronization;Stability criteria;Couplings;Impedance;Asymmetrical grid faults;multi-paralleled wind farms;synchronization stability;equilibrium points;low voltage ride-through (LVRT);synchronization stability assessment method},

[25] J. U. M. Akbar, S. F. Kamarulzaman, A. J. M. Muzahid, M. A. Rahman and M. Uddin, "A Comprehensive Review on Deep Learning Assisted Computer Vision Techniques for Smart Greenhouse Agriculture," in IEEE Access, vol. 12, pp. 4485-4522, 2024, doi: 10.1109/ACCESS.2024.3349418.

keywords: {Green products;Computer vision;Farming;Agriculture;Crops;Deep learning;Air pollution;Agriculture;Convolutional neural networks;Image segmentation;Precision agriculture;Object detection;Agricultural automation;computer vision;deep learning;convolutional neural networks(CNN);controlled-environment agriculture (CEA);greenhouse farming;smart farming;smart agriculture;precision agriculture;image classification;image segmentation;object detection},

[26] J. Ye et al., "A Review of Cyber–Physical Security for Photovoltaic Systems," in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 4, pp. 4879-4901, Aug. 2022, doi: 10.1109/JESTPE.2021.3111728.

keywords: {Inverters;Power electronics;Smart grids;Microgrids;Computer security;Monitoring;Reliability;Cybersecurity assessment;cyber–physical security;detection and mitigation;firmware and network security;photovoltaic (PV) converter},

[27] T. -V. Nguyen, L. -S. Lê, S. A. Shah, S. Hameed and D. Draheim, "PenChain: A Blockchain-Based Platform for Penalty-Aware Service Provisioning," in IEEE Access, vol. 12, pp. 1005-1030, 2024, doi: 10.1109/ACCESS.2023.3344038.

keywords: {Blockchains;Service level agreements;Monitoring;Cloud computing;Ecosystems;Smart contracts;Internet of Things;Smart agriculture;Blockchain;manufacturing industry;penalty-aware services;precision smart agriculture;service-level agreements;service provisioning;smart contracts},

[28] R. Fu, X. Ren, Y. Li, Y. Wu, H. Sun and M. A. Al-Absi, "Machine-Learning-Based UAV-Assisted Agricultural Information Security Architecture and Intrusion Detection," in IEEE Internet of Things Journal, vol. 10, no. 21, pp. 18589-18598, 1 Nov.1, 2023, doi: 10.1109/JIOT.2023.3236322.

keywords: {Autonomous aerial vehicles;Monitoring;Machine learning algorithms;Intrusion detection;Internet of Things;Sensors;Machine learning;Agricultural information security;convolutional neural network (CNN);geographic position information (GPI);intrusion detection;machine learning;unmanned aerial vehicles (UAVs)},

[29] M. Akbari, A. Syed, W. S. Kennedy and M. Erol-Kantarci, "AoI-Aware Energy-Efficient SFC in UAV-Aided Smart Agriculture Using Asynchronous Federated Learning," in IEEE Open Journal of the Communications Society, vol. 5, pp. 1222-1242, 2024, doi: 10.1109/OJCOMS.2024.3363132.

keywords: {Internet of Things;Smart agriculture;Servers;Real-time systems;Network function virtualization;Information age;Farming;Internet of Things;UAV-aided mobile edge computing (UAV-aided MEC);age of information;network function virtualization;federated reinforcement learning},

[30] L. Guo, J. Zhang, J. Ye, S. J. Coshatt and W. Song, "Data-Driven Cyber-Attack Detection for PV Farms via Time-Frequency Domain Features," in IEEE Transactions on Smart Grid, vol. 13, no. 2, pp. 1582-1597, March 2022, doi: 10.1109/TSG.2021.3136559.

keywords: {Phase locked loops;Voltage control;Training;Phasor measurement units;Power electronics;Computer security;Time-frequency analysis;Grid-connected power electronics converters;photovoltaic farms;cyber-physical security;time and frequency domain features;mean current vector},

[31] J. Su et al., "Aerial Visual Perception in Smart Farming: Field Study of Wheat Yellow Rust Monitoring," in IEEE Transactions on Industrial Informatics, vol. 17, no. 3, pp. 2242-2249, March 2021, doi: 10.1109/TII.2020.2979237.

keywords: {Diseases;Monitoring;Cameras;Agriculture;Stress;Informatics;Sensors;Deep learning;multispectral image;precision agriculture;semantic segmentation;U-Net;unmanned aerial vehicle (UAV)},

[32] F. Valenza, E. Karafili, R. V. Steiner and E. C. Lupu, "A Hybrid Threat Model for Smart Systems," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 4403-4417, 1 Sept.-Oct. 2023, doi: 10.1109/TDSC.2022.3213577.

keywords: {Smart buildings;Passwords;Cyber-physical systems;Phishing;Object recognition;Internet of Things;Wind farms;Threat analysis;cybersecurity modelling;threat model;cyber-physical systems},

[33] R. Rashid, W. Aslam, R. Aziz and G. Aldehim, "An Early and Smart Detection of Corn Plant Leaf Diseases Using IoT and Deep Learning Multi-Models," in IEEE Access, vol. 12, pp. 23149-23162, 2024, doi: 10.1109/ACCESS.2024.3357099.

keywords: {Diseases;Feature extraction;Crops;Data models;Visualization;Internet of Things;Deep learning;Precision agriculture;Smart agriculture;Plants (biology);Pest control;Heterogeneous networks;Precision agriculture;corn disease;sensors;pest control;CNN;decision level fusion;multi-model;MULTI-context;AlexNet;VGG-16;ResNeXt;heterogeneous data},

[34] S. Shende et al., "Metal-Based Green Synthesized Nanoparticles: Boon for Sustainable Agriculture and Food Security," in IEEE Transactions on NanoBioscience, vol. 21, no. 1, pp. 44-54, Jan. 2022, doi: 10.1109/TNB.2021.3089773.

keywords: {Agriculture;Green products;Security;Biology;Plants (biology);Nanoparticles;Production;Food protection;microorganisms;MNPs;nanobiosensor;smart nanopackaging;sustainable agriculture},

[35] J. Zhang et al., "Machine Learning-Based Cyber-Attack Detection in Photovoltaic Farms," in IEEE Open Journal of Power Electronics, vol. 4, pp. 658-673, 2023, doi: 10.1109/OJPEL.2023.3309897.

keywords: {Cyberattack;Inverters;Phasor measurement units;Power electronics;Capacitors;Sensors;Security;Grid-tied power electronics converters;photovoltaic farms;cyber-attack detection;waveform;micro-phasor measurement units},

[36] S. Polymeni, D. N. Skoutas, G. Kormentzas and C. Skianis, "FINDEAS: A FinTech-Based Approach on Designing and Assessing IoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 24, pp. 25196-25206, 15 Dec.15, 2022, doi: 10.1109/JIOT.2022.3195770.

keywords: {Internet of Things;Financial services;Sensors;Smart agriculture;Technological innovation;System analysis and design;Financial technology (FinTech);FINDEAS;Internet of Things (IoT);smart agricultural systems;system design and assessment;technology readiness level (TRL)},

[37] S. Saha, A. Hota, B. Choudhury, A. Nag and S. Nandi, "NTRU and Secret Sharing Based Secure Group Communication for IoT Applications," in IEEE Access, vol. 11, pp. 117341-117350, 2023, doi: 10.1109/ACCESS.2023.3325305.

keywords: {Internet of Things;Security;Cryptography;Sensors;Quantum computing;Protocols;Encryption;Collaborative software;Group technology;Internet of Things;NTRU;secret sharing;group communication},

[38] F. Li et al., "Detection and Diagnosis of Data Integrity Attacks in Solar Farms Based on Multilayer Long Short-Term Memory Network," in IEEE Transactions on Power Electronics, vol. 36, no. 3, pp. 2495-2498, March 2021, doi: 10.1109/TPEL.2020.3017935.

keywords: {Smart grids;Sensors;Data models;Cyberattack;Data integrity;Training;Analytical models;Data integrity attack (DIA);deep learning;machine learning;smart grids;solar inverter},

[39] N. Xue et al., "Dynamic Security Optimization for N-1 Secure Operation of Hawai‘i Island System With 100% Inverter-Based Resources," in IEEE Transactions on Smart Grid, vol. 13, no. 5, pp. 4009-4021, Sept. 2022, doi: 10.1109/TSG.2021.3135232.

keywords: {Power system stability;Security;Power system dynamics;Inverters;Optimization;Generators;Renewable energy sources;Grid-forming inverter;low-inertia system;controller parameter optimization;EMT simulation},

[40] C. Wang, Z. Yuan, P. Zhou, Z. Xu, R. Li and D. O. Wu, "The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 22008-22032, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3304318.

keywords: {Security;Privacy;Artificial intelligence;Internet of Things;Cloud computing;Data privacy;Computer architecture;Artificial intelligence (AI);fifth generation (5G);Internet of Things (IoT);machine learning (ML);mobile-edge computing (MEC);security and privacy;software-defined network (SDN) security;virtual machine security},

[41] M. Anedda et al., "Privacy and Security Best Practices for IoT Solutions," in IEEE Access, vol. 11, pp. 129156-129172, 2023, doi: 10.1109/ACCESS.2023.3331820.

keywords: {Internet of Things;Security;Best practices;Privacy;Data privacy;Guidelines;Regulation;Risk management;Internet of Things;IoT security;best practices;non-personal data;privacy by design;risk assessment},

[42] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, S. Nepal and X. Huang, "Cost-Effective Authenticated Data Redaction With Privacy Protection in IoT," in IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11678-11689, 15 July15, 2021, doi: 10.1109/JIOT.2021.3059570.

keywords: {Internet of Things;Security;Medical services;Authentication;Data privacy;Heart beat;Digital signatures;Authentication;healthcare data sharing;Internet of Things (IoT);privacy;redactable signature},

[43] L. Wei, J. Cui, Y. Xu, J. Cheng and H. Zhong, "Secure and Lightweight Conditional Privacy-Preserving Authentication for Securing Traffic Emergency Messages in VANETs," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1681-1695, 2021, doi: 10.1109/TIFS.2020.3040876.

keywords: {Security;Privacy;Delays;Authentication;Safety;Protocols;Vehicular ad hoc networks;Security;VANETs;conditional privacy-preserving;elliptic curve;message recovery;key updating},

[44] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand and A. H. Gandomi, "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 881-888, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3008906.

keywords: {Internet of Things;Security;Privacy;Smart devices;Blockchain;Intelligent sensors;Blockchain;cryptography;distributed;Internet of Things (IoT);privacy;security},

[45] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina and H. Zhong, "DBCPA: Dual Blockchain-Assisted Conditional Privacy-Preserving Authentication Framework and Protocol for Vehicular Ad Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 23, no. 2, pp. 1127-1141, Feb. 2024, doi: 10.1109/TMC.2022.3230853.

keywords: {Blockchains;Security;Authentication;Privacy;Vehicular ad hoc networks;Smart contracts;Vehicle dynamics;Authentication;dual blockchain;smart contract;vehicular ad hoc networks},

[46] H. Zhong, L. Chen, J. Cui, J. Zhang, I. Bolodurina and L. Liu, "Secure and Lightweight Conditional Privacy-Preserving Authentication for Fog-Based Vehicular Ad Hoc Networks," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8485-8497, 1 June1, 2022, doi: 10.1109/JIOT.2021.3116039.

keywords: {Security;Authentication;Privacy;Safety;Message authentication;Computational modeling;Resists;Authentication;conditional privacy preserving;fog computing;vehicular ad hoc networks (VANETs)},

[47] S. Li, S. Zhao, G. Min, L. Qi and G. Liu, "Lightweight Privacy-Preserving Scheme Using Homomorphic Encryption in Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14542-14550, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3066427.

keywords: {Industrial Internet of Things;Data privacy;Security;Industries;Encryption;Servers;Privacy;Industrial Internet of Things (IIoT);IoT security;lightweight privacy;provenance;security},

[48] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, S. Nepal and X. Huang, "Authenticated Data Sharing With Privacy Protection and Batch Verification for Healthcare IoT," in IEEE Transactions on Sustainable Computing, vol. 8, no. 1, pp. 32-42, 1 Jan.-March 2023, doi: 10.1109/TSUSC.2022.3211298.

keywords: {Internet of Things;Medical services;Data privacy;Servers;Bandwidth;Privacy;Medical diagnostic imaging;Authentication;healthcare IoT;redactable signature;certificateless;data privacy},

[49] L. Malina et al., "Post-Quantum Era Privacy Protection for Intelligent Infrastructures," in IEEE Access, vol. 9, pp. 36038-36077, 2021, doi: 10.1109/ACCESS.2021.3062201.

keywords: {Privacy;Data privacy;Security;Internet of Things;Sensors;Encryption;General Data Protection Regulation;Authentication;cryptography;Internet of Things;intelligent infrastructures;post-quantum cryptography;privacy;privacy-enhancing technologies;security;threats},

[50] Z. Zeng, Y. Liu and L. Chang, "A Robust and Optional Privacy Data Aggregation Scheme for Fog-Enhanced IoT Network," in IEEE Systems Journal, vol. 17, no. 1, pp. 1110-1120, March 2023, doi: 10.1109/JSYST.2022.3177418.

keywords: {Data aggregation;Data privacy;Smart devices;Encryption;Privacy;Security;Internet of Things;Boneh–Goh–Nissim (BGN) homomorphic encryption;data aggregation;fog computing;Internet of Things (IoT);privacy protection},