



ORIGINAL

Securing Smart Agriculture: Proposed Hybrid Meta-Model and Certificate-based Cyber Security Approaches

Protección de la agricultura inteligente: Propuesta de metamodelo híbrido y enfoques de ciberseguridad basados en certificados

Khaoula Taji¹, Badr Elkhalyly², Yassine Taleb Ahmad³, Ilyas Ghanimi¹, Fadoua Ghanimi¹

¹Electronic Systems, Information Processing, Mechanics and Energy laboratory. Ibn Tofail University, Faculty of Sciences. Kenitra, Morocco

²Department of computer science. Faculty of science, Hassan II University. Casablanca, Morocco

³Engineering science laboratory. Ibn Tofail University, ENSA. Kenitra, Morocco

Cite as: Taji K, Elkhalyly B, Taleb Ahmad Y, Ghanimi I, Ghanimi F. Securing Smart Agriculture: Proposed Hybrid Meta-Model and Certificate-based Cyber Security Approaches. Data and Metadata. 2023; 2:155. <https://doi.org/10.56294/dm2023155>


Submitted: 22-08-2023

Revised: 22-10-2023

Accepted: 29-12-2023

Published: 30-12-2023

Editor: Javier Gonzalez-Argote 

Guest Editor: Yousef Farhaoui 

Note: Paper presented at the International Conference on Artificial Intelligence and Smart Environments (ICAISE'2023).

ABSTRACT

The Internet of Things is a decentralized network of physically connected devices that communicate with other systems and devices over the internet. As the number of IoT-based devices continues to grow at an exponential rate, this technology has the potential to improve nearly every aspect of daily life, from smart networks and transportation to home automation and agriculture. However, the absence of adequate security measures on all levels of the IoT poses a significant security risk, with the potential for cyber-attacks and data theft. While scholars have suggested various security measures, there are still gaps that need to be addressed. In this study, we analyzed previous research and proposed metamodels for security, IoT, and machine learning. We then proposed a new IoT-based smart agriculture model with integrated security measures to mitigate cyber-attacks and increase agricultural output. Our model takes into account the unique features of the smart farming domain and offers a framework for securing IoT devices in this specific application area. Moreover, in order to mitigate a range of cyber security attacks across various layers of IoT, we introduced two certificate-based schemes named CBHA and SCKA for smart agriculture. A comparative analysis of their security with existing literature demonstrates their superior robustness against diverse attacks. Additionally, security testing utilizing scyther affirms the resilience and security of both CBHA and SCKA, establishing them as viable options for ensuring security in smart agriculture.

Keywords: Internet of Things; Smart Agriculture; Smart Farming, Platform-Independent Model; Platform-Specific Models; Security In IoT Architecture; Cyber-Attacks; Certificate Based Cryptography; Multi-Layered Attacks Security; Formal Verification; Scyther.

RESUMEN

La Internet de los objetos es una red descentralizada de dispositivos conectados físicamente que se comunican con otros sistemas y dispositivos a través de Internet. A medida que el número de dispositivos basados en la IoT sigue creciendo a un ritmo exponencial, esta tecnología tiene el potencial de mejorar casi todos los aspectos de la vida cotidiana, desde las redes inteligentes y el transporte hasta la domótica y la agricultura. Sin embargo, la ausencia de medidas de seguridad adecuadas en todos los niveles de la IO plantea un riesgo de seguridad significativo, con el potencial de ciberataques y robo de datos. Aunque los estudiosos han sugerido diversas medidas de seguridad, sigue habiendo lagunas que es necesario abordar. En este estudio, analizamos investigaciones anteriores y propusimos metamodelos de seguridad, IoT y aprendizaje

automático. A continuación, propusimos un nuevo modelo de agricultura inteligente basado en IoT con medidas de seguridad integradas para mitigar los ciberataques y aumentar la producción agrícola. Nuestro modelo tiene en cuenta las características únicas del dominio de la agricultura inteligente y ofrece un marco para asegurar los dispositivos IoT en esta área de aplicación específica. Por otra parte, con el fin de mitigar una serie de ataques de seguridad cibernética a través de diversas capas de la IO, introdujimos dos esquemas basados en certificados llamados CBHA y SCKA para la agricultura inteligente. Un análisis comparativo de su seguridad con la literatura existente demuestra su superior robustez frente a diversos ataques. Además, las pruebas de seguridad realizadas con scyther confirman la resistencia y seguridad tanto de CBHA como de SCKA, estableciéndolas como opciones viables para garantizar la seguridad en la agricultura inteligente.

Palabras clave: Internet de las Cosas; Agricultura Inteligente; Agricultura Inteligente, Modelo Independiente de la Plataforma; Modelos Específicos de la Plataforma; Seguridad en la Arquitectura IoT; Ciberataques; Criptografía Basada en Certificados; Seguridad Contra Ataques Multicapa; Verificación Formal; Scyther.

INTRODUCTION

In recent times, computer science students are particularly interested in the Internet of Things (IoT). Kevin Ashton proposed IoT in 1999, introducing the concept of linking physical objects to the internet using sensors.⁽¹⁾ Ashton also contributed to the development of radio frequency identification (RFID).⁽²⁾ IoT aims to intelligently transform conventional methods.⁽¹⁾ Advanced computing, cloud storage, machine learning, and artificial intelligence have facilitated the evolution of smart devices, depicted in Figure 1 with an exponential increase in linked IoT devices globally.⁽³⁾

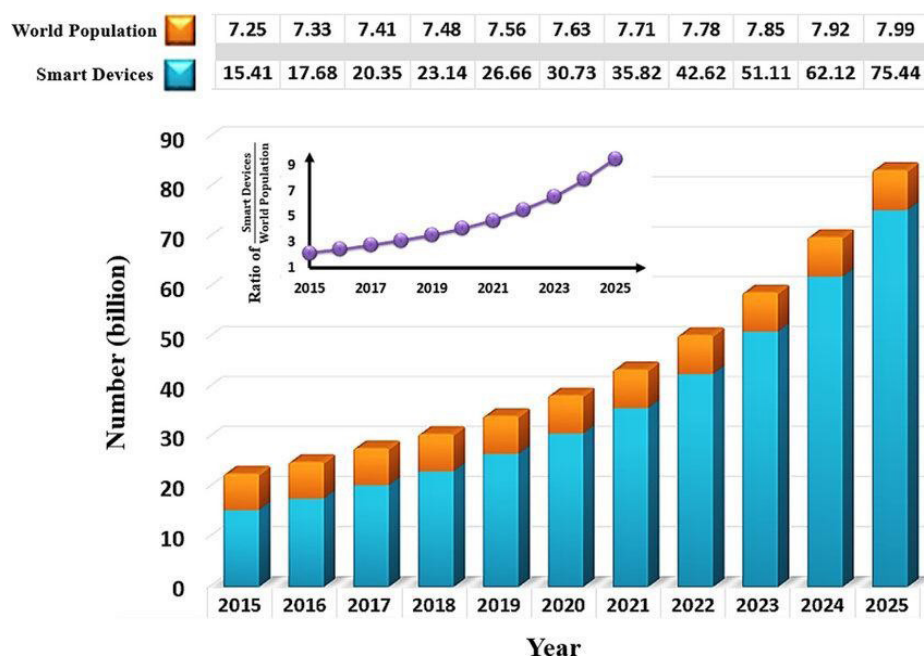


Figure 1. Connected IoT devices vs World population over the years

Through digitalization and smart devices, IoT has revolutionized sectors such as commerce, healthcare, education, agriculture, and economics.⁽⁴⁾ Its integration into daily life is driven by intelligent devices, rapid sensing, and computing capabilities. The transformative potential of IoT is evident in the evolution of smart products, grids, households, and cities across various domains like transport, architecture, retail, and supply, leveraging Big Data and related methodologies,⁽⁵⁾ as illustrated in figure 2.

Ensuring the security of IoT systems is crucial, covering protection for physical components, software, data, and connectivity. The prevalence of flaws in IoT systems necessitates comprehensive security measures, including component hardening, tracking, firmware upgrades, access controls, risk management, and vulnerability mitigation. Given their widespread and vulnerable nature, IoT technologies are susceptible to focused attacks, emphasizing the importance of preventing unauthorized access and data breaches.⁽⁶⁾

Three main tiers make up the IoT architecture:

- the perception/physical layer,
- the network layer, and

- the application layer.

Figure 3 shows these layers in the order in which they appear in the IoT architecture.

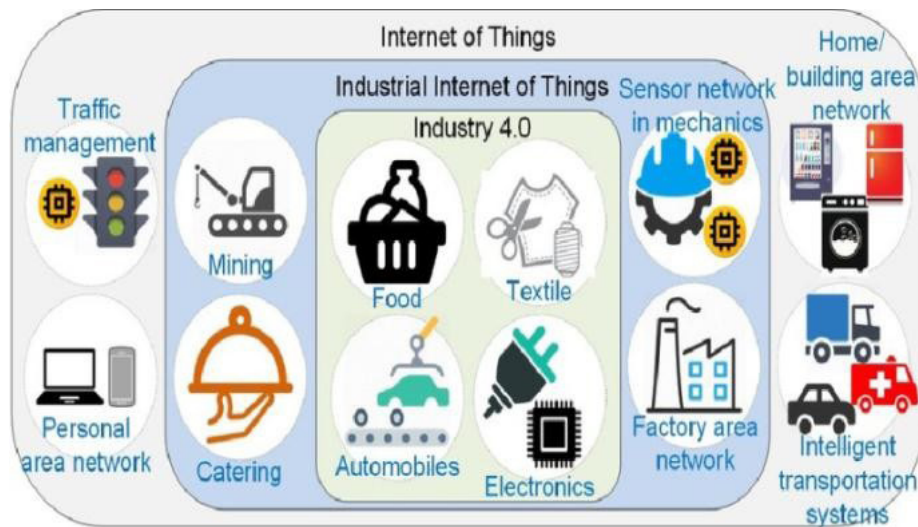


Figure 2. Existence of IoT in different areas

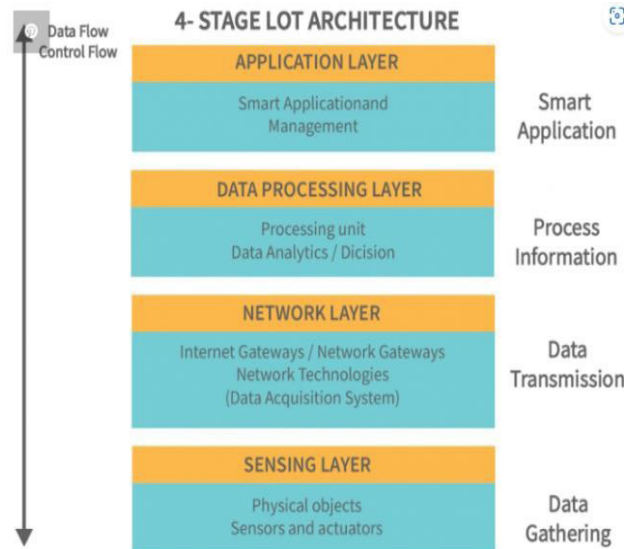


Figure 3. Different Layers in IoT Architecture

In the IoT architecture, some argue for an extra layer enabling cloud and fog computing between the application and network layers. The standard structure comprises three layers: perception, network, and application. The perception layer collects data from sensors and transfers it to the network layer, vital for secure data transfer. The top layer, application, acts as the interface barrier, facilitating user interaction with IoT systems through communication interfaces.

IoT systems, vital for global well-being, face crucial security challenges in data collection and transmission, necessitating strict measures to protect sensitive information. Researchers propose diverse architectures and methodologies to address IoT safety concerns, incorporating security standards at all architecture levels to prevent cyber-attacks.⁽⁷⁾ The comprehensive security of IoT-based systems is vital, considering potential threats to connectivity, accessibility, validity, and privacy. Ensuring the privacy of intelligent machines in smart farming is essential to prevent adverse effects on agriculture, highlighting the significance of security across all IoT sectors.^(6,7)

The contributions of this research paper are as follow:

- Firstly, commencing with an exploration of cyber-attacks on smart farming systems, we delve into the vulnerabilities within this domain.
- Subsequently, we present an exhaustive examination of pertinent research on security in smart farming and various domains. Through a comparative study, we analyze the strengths and limitations of existing

approaches.

- Following this, we introduce metamodels for IoT and security, offering concise descriptions.
- A new global meta-model for IoT and security in agriculture systems is then meticulously presented in this section.
- Furthermore, we present two innovative schemes, CBHA and SCAK, for securing smart agriculture against cyber-attacks across different layers of IoT.
- Afterwards, we conducted a comprehensive security analysis, we compare CBHA and SCAK with existing solutions. Results unequivocally indicate the resilience of both proposed schemes against diverse cyber threats.
- To bolster our claims of security robustness, both schemes (CBHA and SCAK) undergo testing using scyther, with results conclusively demonstrating their efficacy and security.

Review of existing research on security in smart farming and other domains

As the Internet of Things (IoT) continue to evolve, so does the complexity of cyber-attacks targeting various layers of IoT. This section delves into an in-depth examination of current security approaches for IoT, aiming to uncover the strengths and weaknesses of these systems in protecting against a range of potential cyber-attacks.

Aldhyani et al.⁽¹⁾ gave insight of IoT based healthcare systems, spotlighting their complex architecture and security challenges. It underscores the pressing need for robust communication and access control across different scenarios. Critically, existing multi-server solutions fall short in addressing Wireless Body Area Network (WBAN) authentication, rendering them unfit for crucial user-patient and patient-medical server interactions. Afterwards, they proposed an innovative ECC-based multi-factor remote authentication and access control scheme. By incorporating physically un-clonable function and hash mechanism, the proposed scheme achieves security against data theft attack, man in the middle attack and access control attack. However, the proposed scheme lack resistance against sniffing attack, service Interruption attack and DoS attack. Furthermore, it is not performance efficient due to high communication overhead.⁽⁹⁾

Rajalakshmi et al.⁽¹⁰⁾ proposed a certificate-based signature scheme for the Industrial Internet of Things (IIoT) using hyper elliptic curve cryptography (HECC). The proposed scheme employs a unique architecture for the Industrial Internet of Things (IIoT) that employs edge computing, utilizing Bluetooth Low Energy (BLE) to directly retrieve data from IIoT devices. This data is then transmitted to a cloud server via a 5G wireless link. This scheme designed to outperform existing ones in terms of both computational and communication cost, providing better security against various cyber-attacks such as DoS attack, access attack and man in the middle attack. Despite being cost effective, the scheme lack resiliency against data theft attack, access control attack and sniffing attack.

Gondchawar et al.⁽¹¹⁾ proposed an enhancement to the constrained application protocol (CoAP), a widely used protocol in the Internet of Things (IoT) ecosystem, particularly in e-health systems. The proposed mechanism, named authentication and access control scheme for CoAP, in response to the growing security concerns in the expansive IoT landscape, adds resilience to cyber-attacks by modifying CoAP's payload message and employing one-time hashing for communication confidentiality. Their work offer resiliency against range of cyber-attacks such as access control attack, DoS attack and service interruption attack. However, despite their best efforts, their approach lack robustness against data theft attack, MITM attack, and sniffing attack. Moreover, they neglected to utilize performance metrics, such as computational and communication costs, to demonstrate the resilience of their work. Additionally, their security remains untested by any formal security validation tool.

Qureshi et al.⁽¹²⁾ proposed an IoT based smart home authentication scheme designed for remote access, addressing challenges in maintaining data security over the Internet. The proposed scheme employs an authentication device for the home network and a controller device to manage home appliances, preventing various attacks such as data theft attack, man-in-the-middle attacks and DoS attack. The scheme ensures confidentiality and authenticity of users and devices in the network, maintaining network performance in terms of delay, throughput, and energy consumption. The use of asymmetric key cryptography in this authentication technique, along with biometric authentication, enhances security. However, despite their efforts, the proposed approach fails to address sniffing attack, access control attack and access attack. Its communication cost is on the higher side in terms of performance.

Zanella et al.⁽¹³⁾ proposes a security protocol for Internet of Things (IoT) devices, addressing privacy, access control, and authentication challenges. They introduced a mutual authentication and session key establishment protocol for IoT devices, specifically utilizing Silicon PUFs with Arbiter chips. The proposed protocol doesn't store information on the device, avoiding various attacks. Formal verification using VerifPal demonstrates its security and efficiency against attack scenarios. The security assessment reveals that their method defends against data theft, MITM, and DoS attacks, showcasing commendable performance in terms of computational and communication costs. Nevertheless, limitations arise in terms of vulnerability to sniffing attacks, access control attacks, and unauthorized access.

Alavi et al.⁽¹⁴⁾ presents a novel authentication and access control scheme for IoT with aim to address security vulnerabilities and limitations in existing IoT authentication and access control mechanisms. Their proposed approach utilizes the concept of capability, employing lightweight cryptographic operations such as elliptic curve diffie-hellman ephemeral (ECDHE), symmetric key encryption/decryption, message authentication code, and cryptographic hash primitives. The system ensures security against various attack such as data theft attack, MITM attack, and sniffing attack. With a focus on lightweight operations, the protocol demonstrates low CPU and memory usage, making it suitable for resource-constrained IoT environments. Their approach offers scalability, efficiently handling increased device numbers, and ensures interoperability through the gateway node, acting as a protocol bridge for diverse IoT devices. The suggested scheme, however, lacks resilience against access control attacks and access attacks. Additionally, the security of this approach has not undergone testing with any security assessment tools.

Khajenasiri et al.⁽¹⁵⁾ proposes a new device-to-device (D2D) mutual authentication and key agreement (AKA) protocol for IoT environments that use wireless and shared networks. In scenarios where an authentication server is not part of the AKA process, the existing protocols for D2D communication fall short in meeting security and efficiency requirements, being vulnerable to attacks. The proposed protocol addresses these shortcomings by ensuring anonymity, untraceability, and high security without requiring a secure channel for generating paired private and public keys. Security analyses using BAN logic, Real-Or-Random (ROR) model, and the Scyther tool validate the protocol's robustness. The proposed protocol offers security in the form of resistance to data transit attack, resistance to eavesdropping and interference, and resistance to node capture attack. Despite their best work, their work has limitations in the shape of lack of robustness against false data injection attack, side channel attack and sleep deprivation attack. Moreover, their approach suffers from higher computational overhead and high communication overhead.

Li et al.⁽¹⁶⁾ proposes a Certificate less public key signature (CL-PKS) scheme with anonymity to enhance the security of the existing authentication mechanism for the Industrial Internet of Things (IIoT). In response to the key escrow problem inherent in identity-based cryptography (IBC) and the potential compromise of the key generation center (KGC) in existing approaches, the article introduces new scheme that combines the CL-PKS scheme and the ECDHE mechanism, ensuring secure cross-domain authentication and key agreement. Security verification through the formal analysis tool, Tamarin, confirms the robustness of their approach. Furthermore, it offer security against false data injection attack, node capture attack and data transit attack. However the proposed approach has a higher storage overhead and it also lack resiliency against side channel attack, eavesdropping and interference, and sleep Deprivation attack.

Olivier et al.⁽¹⁷⁾ proposes an ECC based authenticated key exchange scheme for securing communication between Industrial Internet of Things (IIoT) devices. Acknowledging the significant security challenges in IIoT, particularly authentication and access control, the author introduces an inter-device authentication scheme utilizing ECC, ensuring good security. Formal security analysis using the random oracle-based ROR model and informal security analysis over the Dolev-Yao channel reinforce the reliability of this approach. Furthermore, it offer resiliency against diverse attacks such as false data injection attack, node capture attack and data transit attack. Additionally, the proposed scheme is implemented using the MQTT protocol, offering a practical solution for various IoT-based industries, such as smart homes, healthcare, transport, security, and surveillance systems, to enhance their security mechanisms with acceptable reliability and efficiency. The approach, however, lacks resilience against sleep deprivation attacks and side-channel attacks, coupled with performance drawbacks stemming from elevated computational cost.

Raj et al.⁽¹⁸⁾ proposes a novel approach called leakage-resilient certificate-based authenticated key exchange for resource constraint environment, aiming to address the vulnerability of existing certificate-based authenticated key exchange scheme to side-channel attacks. Existing systems, known for alleviating certificate management issues and avoiding key escrow problems, have faced security challenges in the form of attackers obtaining secret keys through partial leaks. The protocol proposed by author in several authors aims to handle this vulnerability though generic bilinear group (GBG) model, relying on discrete logarithm (DL) and computational diffie-hellman (CDH) assumptions. The proposed scheme protocol not only withstands side-channel attacks but also eliminates the key escrow problem, along with resistance against node capture attack and data transit attack. However, the proposed mechanism lacks a thorough performance examination to substantiate its efficiency and also lacks resilience against sleep deprivation attack and false data injection attack.

Pradhan et al.⁽¹⁹⁾ proposes a lightweight authentication and session key agreement scheme for the Industrial Internet of Things (IIoT), addressing the security challenges posed by the high autonomy and resource constraints of the IIoT network. The scheme focuses on enabling secure and remote access to resource-constrained intelligent terminal nodes in an open wireless channel. Utilizing a one-way hash function and bitwise XOR operation, the scheme is particularly effective for devices with limited resources. The security of the proposed scheme is rigorously demonstrated under the real-or-random model through formal security analysis. The scheme ensures

robustness against false data injection attack, node capture attack, and eavesdropping and interference the utilization of less time consuming operations ensure that this approach offers less computational cost. The limitation of this work arises from its lack of resiliency against side channel attack, sleep deprivation attack and data transit attack.

Paul et al.⁽²⁰⁾ proposed a two-factor authentication scheme for the Internet of Things (IoT), addressing the challenges posed by resource-constrained IoT devices. The author first critically evaluated existing big data-based authentication schemes, revealing shortcomings in the form of cyber-attacks. In response, the author introduced an authentication approach that provides real two-factor security, along with security against eavesdropping and interference and false detection injection attack.

Security measures in intelligent farming or agricultural systems

The authors of a study conducted a survey on IoT-based intelligent agricultural systems, exploring ways to integrate IoT into the agriculture sector for increased productivity and efficiency.⁽²¹⁾ They assessed various IoT technologies and devices for computing, transmission, and storage. The survey research addresses trends, opportunities, and concerns in agriculture, particularly focusing on creative approaches for precision farming using smart devices, intelligent UAVs, and transportation systems, forming a cyber-physical system. Due to the multitude of devices and technologies involved, such systems are more susceptible to security flaws. Without appropriate security measures and risk mitigation, they can become potentially dangerous. The authors evaluated security concerns and proposed mitigation techniques to address these issues. Quy et al.⁽²²⁾ employed a three-layer architecture for IoT-based precision agriculture, proposing a conceptual architecture with security implementation on each layer. Despite being a positive contribution, it remained limited as it was not implemented in real-time. Kariri et al.⁽²³⁾ showcased IoT-based technology advancements in smart agriculture, highlighting security problems and future projections. They discussed previous breakthroughs and current security challenges posed by IoT devices and emphasized the importance of data analytics in agriculture for future studies. Sinha et al.⁽²⁴⁾ developed an edge-based component for smart farming, incorporating IoT and LoRA with a five-layered design that includes edge computing. They focused on aspects such as efficient energy usage, data collection, minimal transmission delay, improved data quality, and overall system safety. Uman et al.⁽²⁵⁾ presented case studies of blockchain technology and smart contracts in smart farming. They proposed an IoT and blockchain-based system for tracking the life cycle of agricultural products, utilizing smart contracts to eliminate intermediaries, enhance credibility, and build trust. However, the paper contains substantial errors. Another study concentrated on creating a hydroponic farming monitoring system, emphasizing the need for better network security to ensure information security. The authors developed a fully automated system with web-based consumer control and monitoring but overlooked a robust security scheme, which could potentially impair the system's functionality and result in data corruption.⁽²⁶⁾

Quy et al.⁽²⁷⁾ proposes a smart irrigation strategy, optimizing water consumption with mobile application-based remote control and monitoring, yet security gaps leave the system vulnerable to threats such as Forged Measure Injection and Sensor Weakening. Khelifa et al.⁽²⁸⁾ introduces a web-based monitoring system for aquaponics, utilizing WebSocket for secure connections and real-time operation. Jie et al.⁽²⁹⁾ focuses on an intelligent outdoor aquaponics system with automated features, securely storing data on Google Cloud and employing SHA-256 for login security. At the Rajalakshmi et al.⁽¹⁰⁾ study an IoT-based system is developed for crop field and irrigation tracking, featuring web and mobile applications, but lacks security considerations, posing potential risks of unauthorized access and hostile attacks.⁽³⁰⁾

Comparative Study

A comparative analysis of security criteria from reviewed studies (presented in Table 1) reveals both similarities and differences in their approaches. Each study, with unique focuses and methodologies, offers varied conclusions on effective security measures, further detailed in Table 2, providing insights into the multifaceted nature of security and key factors for maintaining a secure environment. Also adding a table for IoT for another domain

PROPOSED METAMODELS

This section aims to offer a comprehensive overview of metamodels related to security, Artificial Intelligence (AI), and the Internet of Things (IoT) by synthesizing existing literature. These metamodels are essential for understanding and constructing complex systems that embody security, intelligence, and interconnectivity.

The IoT metamodel facilitates communication between physical devices and the digital realm, the security metamodel delineates components for a secure IoT system, and the AI metamodel offers a framework for intelligent systems. This comprehensive overview aims to elucidate these metamodels, helping readers grasp underlying principles and apply them to create robust real-world systems.

Table 1. Comparison of Related Work Studies in smart agriculture

References	Layers	Security Levels	Domain of Application	Advantages	Limitations
(15)	Physical, Network and application layers	Physical, communication, information and connectivity.	Crop monitoring and smart irrigation.	Increased productivity while reducing excessive water use. The system is automated.	No threat characterization or mitigation strategy Lack of security consideration.
(22)	Three layers: Physical, network, cloud based processing and application layer.	Physical, communication and information	IoT based agriculture.	Discussed the opportunities and trends of smart agriculture identified security issues.	There is no significant distinction between challenges and security threats.
(23)	Three layers : Perception layer, Network layer and Application layer	Communication and perceptron	Precision Agriculture Based on IoT.	Each layer's security threats have been identified.	No real system implemented
(25)	Five layers including edge computing	Physical, communication, service and information	Smart Farming.	Enhances the system's performance (latency performance and the quality of data)	highly insecure. The lack of security makes systems vulnerable to all attacks
(27)	four layers, including edge computing	Physical, communication and information	Smart Hydroponic System.	A completely automated system.	Improved productivity and simplicity
(28)	Four layers: Physical and Data Link Layers, Network Layer, Transport Layer, Application layer.	Physical, communication, Service and information.	Smart Irrigation Using IoT.	Easy to deploy use and plan irrigation tasks. Minimizes water consumption. HTTPS used for secure communication	Security features are insufficient
(29)	Physical, network and application layers.	Communication and information	Aquaponic Based on Internet of Things	System is Fully automated Security with Web Socket	No information about other security features deployed
(30)	Physical, application layers and network layer is not mentioned	Communication and information	Intelligent Outdoor Smart Aquaponics system.	Security with SHA-256. Encryption. Good security features. Fully-automated	Complex and high-cost architecture. Insufficient security features

- physical devices.
- Domain Asset: This metaclass represents assets that are specific to a particular domain, such as a medical sensor in a healthcare system.
- Vulnerability Domain Asset: This metaclass represents vulnerabilities that are specific to a particular domain, such as a security weakness in a medical sensor.
- Vulnerability Asset: This metaclass represents vulnerabilities that affect assets in general, such as a weakness in a communication protocol.
- Security Objective: This metaclass represents the goals or objectives that the system's security controls are trying to achieve, such as maintaining confidentiality or ensuring availability.
- Threat: This metaclass represents the potential for harm to the system, such as a denial of service attack or a data breach.
- Generic Threat: This metaclass represents a general type of threat, such as a network attack.
- Specific Threat: This metaclass represents a specific instance of a threat, such as a specific malware program.
- Threat Specification: This metaclass represents the details of a specific threat, such as the methods it uses to propagate.
- Security Incident: This metaclass represents an actual occurrence of a security event, such as a successful data breach.
- Security Requirement: This metaclass represents the specific requirements that the system must meet in order to be considered secure, such as compliance with industry standards.
- Authorization: This metaclass represents the process of granting access to resources or actions within the system.
- Audit: This metaclass represents the process of monitoring and reviewing system activity for security purposes.
- Privacy: This metaclass represents the protection of sensitive information and the maintenance of users' privacy.
- Integrity: This metaclass represents the protection of the system's data and resources from unauthorized modification.
- Access Control: This metaclass represents the process of restricting access to resources or actions within the system.
- Non-Repudiation: This metaclass represents the ability to prove the authenticity of a transaction or action.

Figure 5 illustrates the security metamodel, an integral part of the broader IoT metamodel. Key metaclasses within the security metamodel include Assets, representing elements in the IoT ecosystem requiring protection, and Safeguards designed to counter threats like cyber-attacks and physical tampering. Contingency plans are crucial components, encompassing incident response, business continuity, and disaster recovery plans. Security requirements, whether technical or organizational, are specified standards mandated by regulatory bodies, industry standards, or internal policies. The threats metaclass identifies risks from diverse sources, including hackers and natural disasters. The security metamodel ensures comprehensive protection, threat mitigation, and the presence of contingency plans, establishing a robust security framework for the IoT ecosystem and its users.

Hybrid Metamodel for Smart Agriculture

In our pursuit of advancing smart agriculture, we present a novel hybrid meta-model. This combination of Internet of Things (IoT) and security frameworks is carefully intended to improve IoT solutions in agriculture while protecting agricultural data. Smart agriculture relies on the IoT meta-model.³¹ A "Physical Object" class represents virtual entities with unique IDs, services, and physical features. Under the "Domain" meta-class, these "Physical Objects" are essential to the IoT Ecosystem. This ecosystem captures agricultural system dynamics using IoT nodes with microcontrollers, microprocessors, sensors, and actuators, layers, levels, and protocols.

In smart agriculture, our hybrid concept is vital to security. It links "Actor," "Attacker," "Asset," and "Role." The "Asset" class directly connects with the "Physical Object" class, highlighting its importance in protecting agricultural ecosystem components and data streams. This relationship emphasizes the need of protecting agricultural assets and data.

The security meta-models used in several studies can be used to secure critical agricultural components. This connection safeguards the "Physical Objects or IoT-Node" and its data against unauthorized access.^(32,33,34,35) This link protects smart agriculture's data-rich environment, where insights and decisions rely on untampered data streams. Smart agriculture is united by our hybrid meta-model. With this combination, smart farm data is

safe, confidential, and dependable. Our innovative hybrid metamodel for smart agriculture combines IoT and security to boost the agricultural ecosystem. The “Asset” class in the security meta-model and the “Physical Object” class in the IoT meta-model are important to this marriage. By connecting agricultural assets to IoT nodes, valuable components and data streams are protected. This strategy supports both metamodels’ aims to safeguard and improve agricultural operations, laying the framework for data-driven smart agriculture decisions and improvements.

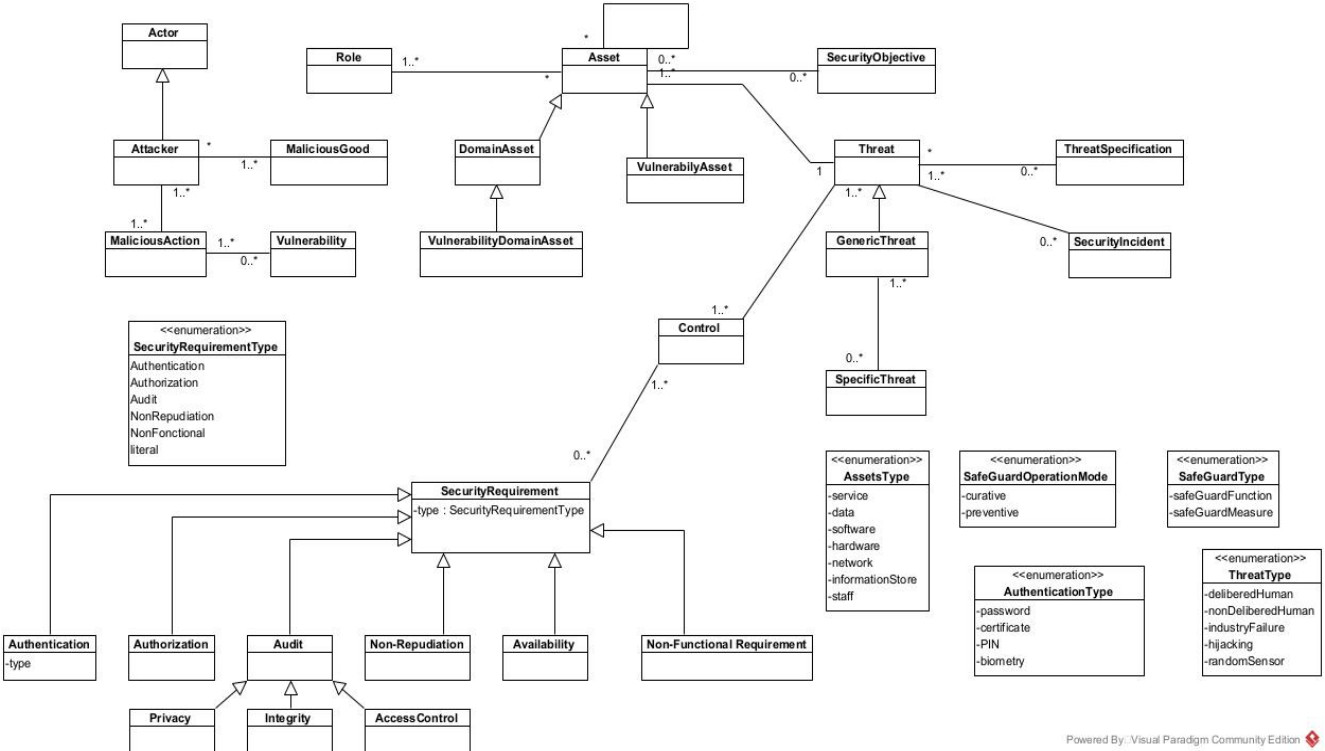


Figure 5. Metamodel of Security.

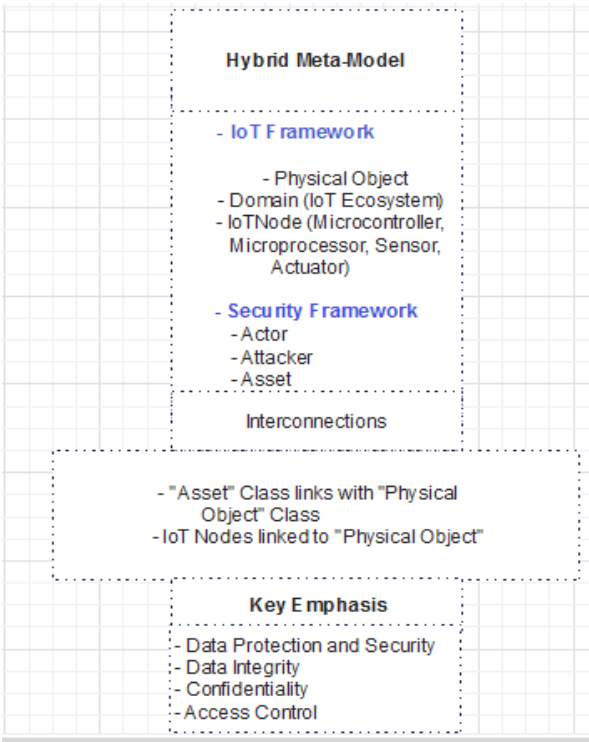


Figure 6. Hybrid Metamodel For Smart Agriculture

IoT Metamodel: In the realm of smart agriculture, the IoT metamodel plays a pivotal role in transforming

<https://doi.org/10.56294/dm20235155>

traditional farming into a data-driven and efficient practice. By incorporating IoT principles, the hybrid metamodel enables the creation of a digital agricultural ecosystem where physical objects, such as crops, livestock, and farming equipment, are equipped with sensors and connected to the internet.

Physical_Object_Class: In smart agriculture, this class represents tangible assets like soil, crops, and livestock. These objects are enriched with attributes such as ID, services, and physical qualities. IoT-enabled sensors on soil can monitor moisture levels, while sensors on plants can gauge growth conditions, allowing farmers to make informed decisions for irrigation and pest control.

IoT Ecosystem Class: Within the context of agriculture, this class embodies the interconnectedness of various IoT nodes, each comprising microcontrollers, sensors, and actuators. For instance, a smart irrigation system can consist of sensors measuring soil moisture, a microcontroller adjusting water flow, and actuators controlling irrigation valves.

Security Metamodel: Securing agricultural operations is crucial in the age of digital farming. The security metamodel addresses the unique challenges of protecting sensitive agricultural data, digital assets, and processes.

Asset_Class: In smart agriculture, assets extend beyond physical objects to include data collected from IoT devices. Crop yield data, weather forecasts, and livestock health information become valuable assets that need protection. This class links agricultural assets to security measures, ensuring data integrity and privacy.

Threat and Security Requirement Classes: These classes are particularly relevant as they connect to potential threats faced by smart agricultural systems. A threat could be a cyberattack on irrigation control systems or data breaches in crop monitoring applications. The security requirement class establishes a link between these threats and the corresponding protective measures, such as encryption and access controls.

In essence, platform-specific models are application packages and interfaces that are predominantly web-based. In this instance, as seen in the graphic beneath, we utilized a platform-specific, cloud-based IoT model for smart farming. Figure 9 presents the PSM model.

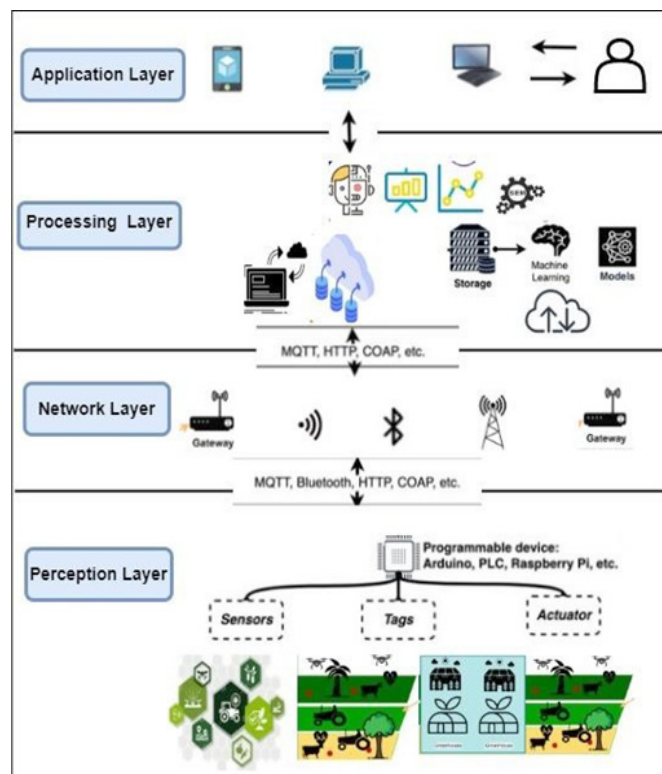


Figure 7. PSM model for Smart Agriculture.

This paragraph outlines a multi-layer design for smart farming ecology, inspired by well-explored multi-layer IoT and Cyber Physical System (CPS) designs. The proposed architecture incorporates the deployment of edge and cloud services, recognizing their potential to leverage data generated by smart devices at the physical layer.⁽³³⁾

Our smart farming design addresses diverse user applications, emphasizing time complexity and edge-cloud scenarios due to substantial data volumes. It comprises four layers: the physical/perception layer, processing layer (edge and cloud), network-communication layer, and application layer. The bottom layer features real physical sensors, including drones, tractors, and animal sensors, facilitating data sensing for various smart

farming use cases. Real-time data on weather, soil moisture, and animal conditions are sent to edge or cloud decision-making systems, enabling automation and recommendations. Edge nodes act as gateways, handling local real-time calculations and decisions, reducing network burden. Prediction services, developed in the central cloud and deployed on the edge, include crop yield predictions, health classifications, fertilizer and water requirements, and soil erosion estimations. Security monitoring and detection technologies handle real-time monitoring, classifying events as malicious or benign. The network layer ensures secure and efficient communication, utilizing wireless sensor networks for continuous monitoring of soil, water, and the environment. The IoT-based system showcases intelligent microcontroller capabilities by making judgments for actions like plant watering based on continuous ecological monitoring.

Proposed Security Schemes for smart agriculture

In this section, we introduce two schemes, CBHA and SCAK, designed to enhance security against a broad spectrum of attacks across various layers of the IoT. Both methodologies integrate certificate-based cryptography and elliptic curve cryptography to ensure robust security. A comprehensive explanation of both schemes follows.

Elliptic Curve

Initially suggested by Neal Koblitz,¹ an elliptic curve represents a mathematical curve that is defined through an equation structured in the form of a cubic equation.^{36,37} The typical expression for an elliptic curve equation within a Cartesian coordinate system is outlined as follows:

$$a^2 = b^3 + ub + v$$

In this context, constants u and v play a role in specifying the particular curve, and the equation is satisfied by points (a,b) on the curve. The equation is established over a field, which constitutes a collection of numbers equipped with operations such as addition and multiplication. In the realm of elliptic curve cryptography, these fields frequently take the form of finite fields.⁽³⁸⁾

Moreover, elliptic curves exhibit interesting geometric and algebraic characteristics that render them valuable in diverse mathematical domains, particularly cryptography. The collection of points (a,b) that fulfill the elliptic curve equation, supplemented by a point at infinity, constitutes an abelian group through a geometrically defined operation known as point addition.⁽³⁸⁾

Elliptic Curve Discrete Logarithm Problem (ECDLP)

Elliptic curve cryptography leverages the complexity of specific mathematical challenges, such as the discrete logarithm problem, to establish robust cryptographic protocols. The incorporation of elliptic curves in cryptography relies on the observation that, despite the ease of performing point addition and multiplication, computationally solving the discrete logarithm problem (given X and Y , finding Z from Equation (1) is challenging.⁽³⁹⁾

$$Z * Y = X \quad \text{Eq (1)}$$

Diffie-Hellman key exchange

The Diffie-Hellman key exchange is a cryptographic protocol designed to facilitate the generation of a shared secret key between two parties over an untrusted communication channel. This exchange enables secure communication by deriving a mutual secret key without directly transmitting it, introducing computational challenges for potential eavesdroppers attempting to discern the shared key.^(40,41,42,43,44)

Shared secret $S = (\text{Received public key})^{\text{private key}} \bmod \text{prime number}$

Access control List

An Access Control List (ACL) serves as a security mechanism that delineates permissions for users or system processes to access designated resources. Comprising rules that articulate permitted or denied actions on objects such as files, directories, or network resources, ACLs are widely utilized in operating systems and network devices to enforce access control policies.^(45,46,47,48,49,50,51)

Certificate-based cryptography

Certificate-based cryptography involves the use of digital certificates, issued by a trusted Certificate Authority (CA), to verify and establish the identity of entities engaged in communication. These certificates associate a public key with an individual, device, or service, facilitating secure and verifiable transactions across unreliable network.⁽⁵²⁾

Scheme 1. Certificate based hybrid approach for security of smart agriculture (CBHA)

The algorithm we propose consists of three primary entities. First is the Certificate Authority (CA), responsible for validating an entity's public key and generating certificates in response. Second is the Controller, strategically positioned near sensors, dedicated to gathering data from sensors and processing information. Lastly, the Farmer, representing the end user who requires continuous agricultural data for making informed decisions, particularly in irrigation. The proposed algorithm combines elliptic curve, certificate based cryptography, access control, signature and authentication mechanism to form a hybrid approach to tackle different layers attacks at smart agriculture. The various stages of our proposed algorithm are outlined below.

Table 2. Symbols used in Proposed Scheme 1

Symbols	Descriptions
F_p	Finite Field
G	Base Point
Pv_{CA}, Pbk_{CA}	Public, private key pair of CA
$Pv_{entity}, Pbk_{entity}$	Public, private key pair of an entity (controller, farmer)
$Cert_{entity}$	Certificate of an entity
ACL	Access control list
S_{Cont}, S_{farmer}	Shared secret of controller and farmer
KDF	Key derivation function
σ_{Cont}	Signature of controller
k	Symmetric key

Initialization Phase

In this phase, parameters are generated by the certificate authority (CA).

- CA first selects an elliptic curve E over a finite field F_p , defined by the equation $y^2 = x^2 + ax + b$.
- Then it selects a base point G on E of larger prime order n .
- Selects a private number Pv_{CA} , randomly from E as its master private key and then uses it to compute master public key $Pbk_{CA} = Pv_{CA} \cdot G$.
- Then it publishes the public parameters $\{Pbk_{CA}, G, E\}$ to the network.

Registration Phase*Key generation*

- When controller and the farmer receives the parameters from CA, they use it to generate their respective public private key pair.
- Controller generates its private key Pv_{Cont} randomly and then uses it to calculate its public key $Pbk_{Cont} = Pv_{Cont} \cdot G$.
- Farmer also generates its private key Pv_{farmer} randomly and then uses it to calculate its public key $Pbk_{farmer} = Pv_{farmer} \cdot G$.
- Afterwards, both controller and farmer generate a timestamp $(t1, t2)$ and send them along with their public keys to the certificate authority.

Certificate Issuance

- When CA receives the information from Controller, it verifies the timestamp $t1$ by matching it with system clock. If it matches, it accepts the public key of controller and sends the certificate $Cert_{Cont}$ to the controller.
- Similarly, CA also verifies the timestamp $t2$ sent by farmer, and matches it with system clock. Upon successful match, it accepts the public key of farmer and sends the certificate $Cert_{farmer}$ to the farmer.

Access control configuration Phase*Access control list setup*

- In this phase, the controller creates ACL for the farmer, specifying permissions.
- Afterwards, controller encrypts the ACL using its public key $Enc_{PbkCont}(ACL)$

Secure Communication Phase*Elliptic Curve Diffie Hellman (ECDH) Key Exchange*

- Controller computes shared secret $S_{Cont} = P_{V_{Cont}} \cdot P_{bk_{farmer}}$
 - Farmer computes shared secret $S_{farmer} = P_{V_{farmer}} \cdot P_{bk_{Cont}}$
 - If $S_{Cont} = S_{farmer}$, generate the symmetric key.
 - Afterwards both parties derive the symmetric key $k = KDF(S)$
- Where KDF is the key derivation function.

Authentication and Encryption and Message Exchange Phase

- In this phase farmer first generates a request M Encrypt it using k $C = Enc_k(M)$
- Afterwards, the farmer sends C and $Cert_{farmer}$ to the controller.
- When the controller receives C and $Cert_{farmer}$, it verifies the $Cert_{farmer}$ using $P_{bk_{CA}}$.
- Afterwards, it decrypts the cipher text $M = Dec_k(C)$

Access Decision Phase

- The phase is controlled by controller, who firstly retrieves the permission to the farmer from Encrypted ACL.
- If the controller has the required permission, controller proceeds to the response phase.

Response Phase

- When controller finds the farmer has required permission, it initiates an approval message M' and signs it. $\sigma_{Cont} = P_{V_{Cont}} \cdot K$
- Afterwards, it encrypts the message using the symmetric key K and transmits the message $\{\sigma_{Cont}, C'\}$ to Farmer. $C' = Enc_k(M')$
- Farmer when receives the message, if first verifies if $\sigma_{Cont'} = \sigma_{Cont}$
- If successful, then it decrypts the C' to obtain M' . $M' = Dec_k(C')$

Correction Proof

- Both shared secrets are equal: $S_{Cont} = S_{farmer}$
 $S_{farmer} = P_{V_{farmer}} \cdot P_{bk_{Cont}} = P_{V_{farmer}} \cdot P_{V_{Cont}} \cdot G$ (1)
 Also $S_{Cont} = P_{V_{Cont}} \cdot P_{bk_{farmer}} = P_{V_{Cont}} \cdot P_{V_{farmer}} \cdot G = P_{V_{farmer}} \cdot P_{V_{Cont}} \cdot G = S_{farmer}$ (from (1)) (Hence Proved)
- Farmer verifies the controller signature as $\sigma_{Cont} \cdot G = \sigma'_{Cont}$
- $\sigma'_{Cont} = P_{V_{Cont}} \cdot K = P_{V_{Cont}} \cdot P_{bk_{Cont}} \cdot G = P_{V_{Cont}} \cdot P_{V_{farmer}} \cdot G = \sigma_{Cont} \cdot G$ (Proved)

Scheme 2. Secure Certificate based authenticated key agreement for smart agriculture (SCAK)

The proposed SCAK scheme comprises three components. Foremost among these is the certificate authority (CA), charged with the validation of entity public variant and the generation of corresponding certificates. The second component, denoted as the controller, assumes the responsibility of acquiring and deciphering data emanating from these sensors. Finally, the Farmer, representing the end party, requires continuous access to agricultural data for informed decision-making, particularly in the context of irrigation management. Presented here with is a comprehensive delineation of the discrete stages comprising our advanced algorithmic framework.

Table 3. Symbols used in Proposed Scheme 2

Symbols	Descriptions
F_p	Finite Field
g	Base Point
ω, β	Public, private key pair of CA
$\varphi_{entity}, \delta_{entity}$	Public, private key pair of an entity (controller, farmer)
H	Collision resistant hash function
$P_{V_{entity}}$	Public variant
N_{entity}	Nonce of an entity
$Cert_{entity}$	Certificate of an entity
$E_{pbk_{farmer}}, E_{pv_{farmer}}$	Ephemeral public, private key
S_{entity}	An entity signature
k	Random number
$Z_{farmer}, Z_{contrller}$	Shared secret of farmer and controller
sk	Session key

Initialization Phase

- In this phase, the Certificate Authority (CA) generates essential parameters. CA begins by choosing an elliptic curve E defined over a finite field F_p , characterized by the equation $y^2 = x^2 + ax + b$.
- Next, CA identifies a base point g on E with a larger prime order denoted as q .
- A private number β is then randomly selected from E to serve as the private key. This key is utilized to compute the public key as $\omega = \beta \cdot g$.
- Afterwards, CA generates a collision resistant hash function from F_p and discloses the public parameters $\{\omega, E, F_p, H\}$ to the network.

Key Generation Phase

- After receiving the public parameters $\{\omega, E, F_p, H\}$, both the entities Controller and Farmer generate their own public, private keys
- Each entity selects a random number directly from F_p of range $[1, q-1]$ as their private key δ_{entity}
- Both entities compute their public key as $\varphi_{\text{entity}} = \delta_{\text{entity}} \cdot g$

Certificate Creation Phase

- After keys generation, both entities requests for certificate and for that they use their identity and public key to generate a public variant $PV_{\text{entity}} = H(\omega || \varphi_{\text{entity}})$ and transmit the message $\{PV_{\text{entity}}, ID_{\text{entity}}, t\}$
- The CA first matches the timestamp t with the onboard system clock and if it matches, then it proceed to verify if $PV_{\text{entity}} = PV'_{\text{entity}}$ and upon successful verification create the certificate as $Cert_{\text{entity}} = \beta (ID_{\text{entity}} + \varphi_{\text{entity}})$ and transmit it to controller and farmer.

Authenticated Key Agreement

- When farmer needs data or information, it aims to create a secure session with controller for communication. It first generates random nonce N_{farmer} and generate a request $R = H(\varphi_{\text{controller}} || \delta_{\text{farmer}})$ and transmit the message $\{N_{\text{farmer}}, R, Cert_{\text{farmer}}\}$ to controller.
- The controller when receives the message, it first verify if $Cert_{\text{farmer}} = \beta \cdot ID_{\text{farmer}} + \beta(\delta_{\text{entity}} \cdot g)$. If verifies, then it proceeds to generate a random nonce N_{Cont} and creates response as $Resp = H(R || \varphi_{\text{farmer}})$ and sends the message $\{N_{\text{Cont}}, Resp, Cert_{\text{Cont}}\}$ to farmer.
- Afterwards, farmer generate its ephemeral private key $Epv_{\text{farmer}} = H(N_{\text{farmer}} || \delta_{\text{farmer}})$ and then uses it to compute its ephemeral public key $Epbk_{\text{farmer}} = Epv_{\text{farmer}} \cdot g$
- Similarly, on the other side, controller generate its ephemeral private key $Epv_{\text{Cont}} = H(N_{\text{Cont}} || \delta_{\text{Cont}})$ and then uses it to compute its ephemeral public key $Epbk_{\text{Cont}} = Epv_{\text{farmer}} \cdot g$
- Farmer then selects a random number k from F_p of range $[1, q-1]$ and then it compute two values which are part of signature S_{farmer} . First it compute $r = (kg)_x \bmod q$, where $(kg)_x$ is the x-coordinate of the point resulting from the scalar multiplication of k and base point g . Then it compute $w = k^{-1} (H(m) + \delta_{\text{farmer}} \cdot r) \bmod q$, the hash of the message signed is $H(m)$ and k^{-1} is the multiplicative inverse of k modulo q . Afterwards, farmer sends the signature $S_{\text{farmer}} = (r, w)$ along with $Epbk_{\text{farmer}}$ to the controller.
- The controller after reception of message, verify the signature S_{farmer} . Firstly it compute $z = w^{-1} \bmod q$ and then it compute $u1 = H(m) \cdot z \bmod q$ and $u2 = r \cdot z \bmod q$. Afterwards, it compute a point $P = u1 \cdot g + u2 \cdot \varphi_{\text{farmer}}$. Then if $(P)_x \bmod q = r$, then the signature is considered valid.
- Afterwards, the controller follow the same step followed by farmer to generate its signature and forwards the signature $S_{\text{Cont}} = (r, w)$ along with $Epbk_{\text{Cont}}$ to the farmer.
- Farmer then accepts the signature if $P = u1 \cdot g + u2 \cdot \varphi_{\text{Cont}}$.
- Afterwards, both parties compute the shared secret as:

$$\begin{aligned} Z_{\text{farmer}} &= Epv_{\text{farmer}} \cdot Epbk_{\text{Cont}} \\ Z_{\text{Cont}} &= Epv_{\text{Cont}} \cdot Epbk_{\text{farmer}} \end{aligned}$$

- Both parties then confirm $Z_{\text{farmer}} = Z_{\text{Cont}}$
- Both parties then derive the session key $sk = H(Z_{\text{entity}} || N_{\text{farmer}} || N_{\text{Cont}})$ and uses it for symmetric encryption for subsequent communication.
- Following a predefined time interval t_2 , the farmer and controller will rotate their ephemeral keys. Subsequently, they will jointly compute the new shared secret and proceed to calculate a new session key for communication.

Correction Proof

1. Upon receiving PV_{entity} , CA validates its authenticity as $PV_{\text{entity}} = PV'_{\text{entity}}$. To verify that, CA calculates PV'_{entity} using the same equation. The integrity of this calculation hinges on the use of a collision-resistant hash function, which ensures deterministic behavior. In simpler terms,

for identical inputs, the hash function consistently generates the same output, and it is practically impossible to find two different inputs producing the same hash value. Thus, under assumption $PV_{\text{entity}} = PV'_{\text{entity}}$ (proved).

2. Each entity verify the certificate as $\text{Cert}_{\text{entity}} = \beta \cdot ID_{\text{entity}} + \beta(\delta_{\text{entity}}) \cdot g$

Using L-H-S

$$\beta \cdot ID_{\text{entity}} + \beta(\delta_{\text{entity}}) \cdot g = \beta \cdot ID_{\text{entity}} + \beta(\delta_{\text{entity}}) \cdot g = \beta \cdot ID_{\text{entity}} + \beta \cdot \varphi_{\text{entity}} = \beta (ID_{\text{entity}} + \varphi_{\text{entity}}) = \text{Cert}_{\text{entity}} \text{ (proved)}$$

3. Each entity accepts the signature if $(P)_x \bmod q = r$

As $P = u_1 \cdot g + u_2 \cdot \varphi_{\text{entity}}$

$$= H(m) \cdot z \cdot g + r \cdot z \cdot \delta_{\text{entity}} \cdot g$$

$$= k \cdot (H(m) + \delta_{\text{entity}} \cdot r^{(-1)}) \cdot H(m) \cdot g + k \cdot (H(m) + \delta_{\text{entity}} \cdot r^{(-1)}) \cdot r \cdot \delta_{\text{entity}} \cdot g$$

$$= k \cdot g \cdot ((H(m) + \delta_{\text{entity}} \cdot r^{(-1)}) \cdot H(m) + (H(m) + \delta_{\text{entity}} \cdot r^{(-1)}) \cdot r \cdot \delta_{\text{entity}})$$

$$= k \cdot g \cdot ((H(m) \cdot (H(m) + \delta_{\text{entity}} \cdot r^{(-1)}) + r \cdot \delta_{\text{entity}} \cdot (H(m) + \delta_{\text{entity}} \cdot r^{(-1)}))$$

$$= k \cdot g \text{ (Since } H(m) + \delta_{\text{entity}} \cdot r \text{ is common factor in parenthesis, it simplifies to 1)}$$

As $P = k \cdot g$ and from signature generation step it is clear that $r = (k \cdot g)_x \bmod q$

Therefore, $(P)_x \bmod q = (k \cdot g)_x \bmod q = r$ (proved)

4. Both entities confirm $Z_{\text{farmer}} = Z_{\text{Cont}}$

Using L-H-S

$$E_{pv_{\text{farmer}}} \cdot$$

$$E_{pbk_{\text{Cont}}} = E_{pv_{\text{farmer}}} \cdot E_{pv_{\text{Cont}}} \cdot g = E_{pv_{\text{farmer}}} \cdot g \cdot E_{pv_{\text{Cont}}} = E_{pv_{\text{Cont}}} \cdot E_{pbk_{\text{farmer}}} = Z_{\text{Cont}} \text{ (Proved)}$$

SECURITY ANALYSIS

Scheme 1 (CBHA) Security Analysis

Security against Data theft attack

Our hybrid strategy utilizes multiple mechanisms to counteract data theft attacks. The implementation of certificates ($\text{Cert}_{\text{entity}}$) guarantees that an unauthorized intruder cannot circumvent authentication and compromise data security. Similarly, the incorporation of Access Control Lists (ACL) ensures that only entities with the appropriate permissions can access the data. Additionally, the utilization of a symmetric key $k = \text{KDF}(S)$ serves to safeguard data from potential intruders. Lastly, the application of a digital signature (σ) contributes to maintaining data integrity, thereby enhancing security against data theft. Collectively, these mechanisms ensure the robust security of our system against data theft attacks.

Security against Access Control Attack

In our approach, the controller creates and encrypts ACL using its public key (Pbk_{Cont}). This encrypted ACL (Encrypted ACL = $\text{Enc}_{\text{PvCont}}(\text{ACL})$) ensures that only authorized parties can access and modify permissions. The decryption of the ACL by the controller using Pv_{Cont} during the access decision phase enables controlled access. It is impossible for adversary to forge ($\text{Pbk}_{\text{Cont}}, \text{Pv}_{\text{Cont}}$) to gain access due to elliptic curve discrete logarithm problem (ECDLP). Thus our approach effectively handle access control attack.

Security against Service Interruption Attack

The access decision phase, controlled by the controller, involves retrieving permissions and making decisions based on the encrypted (ACL). By carefully controlling access and only allowing authorized entities, the algorithm helps prevent unauthorized parties from disrupting services or causing interruptions. Similarly the use of ($\text{Cert}_{\text{entity}}$) and (σ) ensure that parties communicating each other are authentic, hence preventing unauthorized parties from disrupting services or causing interruptions.

Security against Man in the middle attack (MITM)

This is a type of cyber-attack where an unauthorized third party intercepts and possibly alters the communication between two parties without their knowledge. To overcome this attack, our approach employs ECDH key exchange which provides a secure method for the controller and farmer to establish a shared secret (S). Using (S), both parties generate a symmetric key $k = \text{KDF}(S)$ for secure communication. Even if an attacker intercepts the communication, they cannot easily derive the shared secret (S) without the private keys ($\text{Pv}_{\text{Cont}}, \text{Pv}_{\text{farmer}}$) due to ECDLP.

Security against Denial of Service (DoS) Attack

Our approach firstly employs (ACL) to regulate and restrict access, preventing unauthorized entities from overwhelming the system with excessive requests during a Denial of Service (DoS) attack. Secondly, the use of certificate verification ($\text{Cert}_{\text{Cont}}, \text{Cert}_{\text{farmer}}$), ensure that only legitimate entities with valid credentials can interact with the system, mitigating the risk of unauthorized requests causing service disruption. Therefore, the implementation of these robust mechanisms enables our approach to effectively manage and mitigate the impact of a Denial of Service (DoS) attack.

Security against Sniffing Attack

Our devised strategy incorporates a secure communication phase utilizing ECDH key exchange. During this phase, the symmetric key $k = \text{KDF}(S)$, which derived from the shared secret (S) and a Key Derivation Function (KDF), is employed to encrypt information, ensuring the security of the transmitted data. This safeguards against sniffing attacks, as intercepted data would be encrypted and necessitate the symmetric key (k) for decryption. For computing (k), the intruder would need to calculate (S), which is deemed infeasible. Thus, our approach proficiently addresses sniffing attacks.

Access Attack

Our devised strategy effectively mitigates access attacks through multiple mechanisms. The implementation of Access Control Lists (ACL) ensures that access is exclusively granted to authorize entities. Additionally, the use of certificates ($\text{Cert}_{\text{entity}}$) guarantees that only authenticated entities are allowed to participate in the system. Moreover, the deployment of symmetric key $k = \text{KDF}(S)$ prevents unauthorized entities from hijacking sessions to launch access attacks. Collectively, these mechanisms ensure a robust security framework against access attacks.

Scheme 2 (SCAK) Security Analysis

Side channel attack

Side-channel attacks in cyber security exploit unintended information leaked during cryptographic algorithm execution. These attacks aim to extract sensitive data by analyzing its implementations and unintended signals. Our technique employs random nonce (N_{farmer} , N_{Cont}) and ephemeral public private key pair ($\text{Epbk}_{\text{entity}}$, $\text{Epv}_{\text{entity}}$) which handle side channel of the type timing attack by ensuring that each cryptographic operation is unique, reducing the feasibility of timing attacks based on repeated key usage. Similarly, side channel type of the type statistical attack rely on patterns or biases in the data, and the randomness introduced by nonce (N_{farmer} , N_{Cont}) and ephemeral keys ($\text{Epbk}_{\text{entity}}$, $\text{Epv}_{\text{entity}}$) helps disrupt these patterns. Thus, our technique effectively thwart side channel attacks.

Eavesdropping and Interference

The proposed mechanism utilizes ephemeral keys ($\text{Epv}_{\text{entity}}$, $\text{Epbk}_{\text{entity}}$) to generate a shared secret Z between the controller and farmer. A session key, $\text{sk} = H(Z_{\text{entity}} || N_{\text{farmer}} || N_{\text{Cont}})$, is derived for encrypting information during communication, enhancing resistance against eavesdropping. Additionally, the inclusion of the signature $S_{\text{entity}} = (r, w)$, ensures authentication, while nonces (N_{farmer} , N_{Cont}) reduce the impact of replay attempts, collectively strengthening the approach against interference attacks.

Sleep Deprivation Attack

To handle sleep deprivation attack, we have specifically employed an ephemeral key rotation ($\text{Epv}_{\text{entity}}$, $\text{Epbk}_{\text{entity}}$) mechanism after a time interval t_2 . This method limit the exposure of cryptographic material and minimize the window of opportunity for attackers. Furthermore, the session key $\text{sk} = H(Z_{\text{entity}} || N_{\text{farmer}} || N_{\text{Cont}})$ is updated as well after ($\text{Epv}_{\text{entity}}$, $\text{Epbk}_{\text{entity}}$) rotation. Sleep deprivation attacks often rely on the predictability or repetition of cryptographic material. By constantly deriving new sk based on ephemeral keys and nonce N_{entity} , the protocol introduces variability, making it harder for an attacker to predict the cryptographic material used during different communication sessions.

False data injection attack

We have employment several features in our approach which handles false data injection attack. Firstly, the use of signature $S_{\text{entity}} = (r, w)$ verifies that data has not been tampered with during transmission, confirming the legitimacy of the sender. Secondly, the use of certificate $\text{Cert}_{\text{entity}} = \beta (ID_{\text{entity}} + \varphi_{\text{entity}})$ and its verification on receiving side $\beta \cdot ID_{\text{entity}} + \beta (\delta_{\text{entity}} \cdot g)$ mitigates the risk of impersonation, preventing false data injection by verifying the identity of participants. Furthermore, the use of time stamp (t) and nonce (N_{entity}) reduces the risk of reused or outdated information being injected into the communication. Lastly, the use of temper resistant hash function (H) detects any unauthorized changes to the data during transmission, adding a layer of protection against false data injection.

Node capture attack

The security of the system may be jeopardized by an adversary who captures and potentially impersonates one or more entities within the network to execute a node capture attack. However, our approach ensures continuous updates to session keys. Consequently, compromising one node would not impact the other session keys used for communication. This is because $\text{sk} = H(Z_{\text{entity}} || N_{\text{farmer}} || N_{\text{Cont}})$ and attacker would need to calculate $\text{Epv}_{\text{entity}}$ to generate Z_{entity} , subsequently obtaining sk . Nevertheless, the attacker cannot do so, due to elliptic curve discrete logarithm problem.

Data transit attack

In such attacks, adversaries use sophisticated methods to intercept and manipulate communication to compromise data integrity, confidentiality, and availability, exploiting vulnerabilities without the parties' knowledge or consent. In our scheme, the employment of H ensures that any changes to the data is easily detectable thus offering integrity. Similarly the use of certificate ($Cert_{entity}$) and signature ensure continuous authentication thus adding extra layer against data transit layer. Lastly, by incorporating the derived session key, $sk = H(Z_{entity} || N_{farmer} || N_{Cont})$, for encrypted communication, the scheme ensures the confidentiality of the exchanged data. Collectively, the integration of these measures establishes a robust defense against data transit.

Security Attributes Comparison

Scheme 1 (CBHA) Security Attributes Comparison

In this segment, we assess the CBHA scheme in comparison to existing works, focusing on its key security attributes. Our classification of attacks considers the security attributes they endanger. Through a thorough examination of the existing literature, we present the results in Table 4. The findings unequivocally demonstrate that our CBHA scheme provides superior resilience and security compared to the current literature, particularly in managing security against different attacks various layers of the Internet of Things (IoT).

Table 4. CBHA security comparison with existing literature

Schemes	Confidentiality			Authorization		Availability	
	S1	S2	S3	S4	S5	S6	S7
Ref [34]	✓	✓	×	✓	✓	×	×
Ref [35]	×	✓	×	×	✓	✓	✓
Ref [36]	×	×	×	✓	×	✓	✓
Ref [37]	✓	✓	×	×	×	✓	✓
Ref [38]	✓	✓	×	×	×	✓	✓
Ref [39]	✓	✓	✓	×	×	✓	✓
CBHA	✓	✓	✓	✓	✓	✓	✓

Note: S1: Security against Data theft attack; S2: Security against MITM attack; S3: Security against Sniffing Attack; S4: Security against Access Control Attack; S5: Security against Access Attack; S6: Security against Service Interruption Attack; S7: Security against DoS attack

Scheme 2 (SCAK) Security Attributes Comparison

This section concentrates on the primary security attributes of the SCAK scheme and draw comparison with previous research efforts. We categorize attacks according to the security features they undermine. Following a meticulous examination of the present literature, we articulate the results in Table 5. The outcomes distinctly reveal that our SCAK scheme demonstrates resilience against diverse attacks across various layers of the Internet of Things (IoT).

Table 5. SCAK security comparison with existing literature

Schemes	Confidentiality		Availability	Integrity	Authorization, Confidentiality	Integrity, Confidentiality
	F1	F2	F3	F4	F5	F6
Ref [40]	×	✓	×	×	✓	✓
Ref [41]	×	×	×	✓	✓	✓
Ref [42]	×	✓	×	✓	✓	✓
Ref [43]	✓	✓	×	×	✓	✓
Ref [44]	×	✓	×	✓	✓	×
Ref [45]	×	✓	×	✓	×	×
SCAK	✓	✓	✓	✓	✓	✓

Note: F1: Side channel attack; F2: Eavesdropping and Interference; F3: Sleep Deprivation Attack; F4: False data injection attack; F5: Node capture attack; F6: Data transit attack

Scyther,⁽⁴⁶⁾ is a formal verification tool designed for analyzing security protocols, especially those utilized

in cryptographic systems Employing symbolic model checking techniques, it systematically explores the state space of protocols, focusing on critical security features such as secrecy, authentication, and integrity, authorization, availability, non-repudiation. During simulation, Scyther constructs a symbolic representation of the protocol, allowing for the identification of potential attacks or vulnerabilities. It make use of claims to verify that a certain attack jeopardize the specific security property. Each claims is used for specific purpose.

⁽⁴⁷⁾ Secrecy claim verify and ensure the secrecy of information within security protocols. Alive claim Aliveness ensures that certain desirable states or conditions within the protocol can be reached. Nisynch claims addresses issues related to the synchronization of nonces (number used once) in cryptographic protocols. Niagree claim indicates that following the execution of the protocol, both entities acknowledge each other's identities in a reciprocal manner. Weakagree ensure that, under specific conditions, the protocol will consistently progress and achieve agreement over time. This contributes to preventing man-in-the-middle attacks. When these claims are executed, Scyther assesses all potential attacks on the security properties mentioned in the claims. A successful attack results in a label of "False," while the confirmation of a claim's validity is labeled as "True".⁽⁴⁸⁾

We translated both CBHA and SCAK algorithms into the security protocol description language (spdl) and subsequently executed the code in Scyther to assess the robustness of our proposed schemes. The outcomes, illustrated in Figures 11 and 12, unequivocally indicate the absence of attacks on the security properties. This robust performance positions both schemes as robust cyber security defenses, making them viable choice for smart agriculture.

Claim				Status	Comments
CBHA	controller	CBHA,controller1	Secret M	Ok	No attacks within bounds.
		CBHA,controller2	Secret M'	Ok	No attacks within bounds.
		CBHA,controller3	Secret SignatureCont	Ok	No attacks within bounds.
		CBHA,controller4	Alive	Ok	No attacks within bounds.
		CBHA,controller5	Weakagree	Ok	No attacks within bounds.
		CBHA,controller6	Niagree	Ok	No attacks within bounds.
		CBHA,controller7	Nisynch	Ok	No attacks within bounds.
		CBHA,controller8	Secret k(controller, farmer)	Ok	No attacks within bounds.
	farmer	CBHA,farmer1	Secret M	Ok	No attacks within bounds.
		CBHA,farmer2	Secret M'	Ok	No attacks within bounds.
		CBHA,farmer3	Secret SignatureCont	Ok	No attacks within bounds.
		CBHA,farmer4	Alive	Ok	No attacks within bounds.
		CBHA,farmer5	Weakagree	Ok	No attacks within bounds.
		CBHA,farmer6	Niagree	Ok	No attacks within bounds.
		CBHA,farmer7	Nisynch	Ok	No attacks within bounds.
		CBHA,farmer8	Secret k(controller, farmer)	Ok	No attacks within bounds.

Figure 8. CBHA Security Validation through Scyther

Claim				Status	Comments
CBHA	controller	CBHA,controller1	Secret Certfarmer'	Ok	No attacks within bounds.
		CBHA,controller2	Secret SignatureF	Ok	No attacks within bounds.
		CBHA,controller3	Secret eppbkF	Ok	No attacks within bounds.
		CBHA,controller4	Secret Data	Ok	No attacks within bounds.
		CBHA,controller5	Alive	Ok	No attacks within bounds.
		CBHA,controller6	Nisynch	Ok	No attacks within bounds.
		CBHA,controller7	Niagree	Ok	No attacks within bounds.
		CBHA,controller8	Weakagree	Ok	No attacks within bounds.
		CBHA,controller9	Secret k(controller,farmer)	Ok	No attacks within bounds.
	farmer	CBHA,farmer1	Secret Certcontroller'	Ok	No attacks within bounds.
		CBHA,farmer2	Secret SignatureF	Ok	No attacks within bounds.
		CBHA,farmer3	Secret eppbkC	Ok	No attacks within bounds.
		CBHA,farmer4	Secret Data	Ok	No attacks within bounds.
		CBHA,farmer5	Nisynch	Ok	No attacks within bounds.
		CBHA,farmer6	Niagree	Ok	No attacks within bounds.
		CBHA,farmer7	Weakagree	Ok	No attacks within bounds.
		CBHA,farmer8	Secret k(controller,farmer)	Ok	No attacks within bounds.

Figure 9. SCAK Security Validation through Scyther

CONCLUSION

Ensuring security is critical in IoT-based systems to ensure their widespread use without cyber-security concerns. While researchers have primarily focused on developing IoT-based systems, very few have emphasized the importance of security in those systems. This study focused on the IoT-based smart agriculture domain and reviewed several studies related to security in both smart agriculture and other domains. Our work presented a new IoT-based smart agriculture system that incorporates security mechanisms at each layer of IoT, which can enhance productivity and narrow the security gaps in the IoT-based smart agriculture sector. Furthermore, to mitigate a spectrum of cyber security attacks spanning diverse layers of the Internet of Things (IoT), we have introduced two certificate-based schemes, CBHA and SCKA, specifically designed for smart agriculture. A comparative security analysis with existing literature establishes the superior robustness of these schemes against a variety of attacks. Moreover, rigorous security testing employing the scyther tool unequivocally confirms the resilience and security posture of both CBHA and SCKA.

In our forthcoming research endeavors, we intend to conduct a thorough examination and enhancement of the existing system, aiming to identify and address any vulnerabilities and thereby establish an improved iteration. Furthermore, our research will extend to investigating security challenges prevalent in diverse IoT domains, with the objective of formulating a more resilient security framework. The validation of our secure

model for smart agriculture will involve the implementation of specific algorithms, strategies, and advanced security techniques to uphold the system's security at the highest level. Finally, we aspire to incorporate mechanisms capable of mitigating attacks occurring on the cloud side in the context of smart agriculture.

REFERENCES

1. Mingjun W, et al. A research on experimental system for Internet of Things major and application project. In: 2012 3rd International Conference on System Science, Engineering Design and Manufacturing Informatization; 2012. doi: 10.1109/ICSSEM.2012.6340722.
2. Rose K, Eldridge SD, Chapin L. The internet of things: An overview understanding the issues and challenges of a more connected world. *The internet society (ISOC)*. 2015;80:1-50.
3. Lee, Wang X, Nguyen H, Ra I. A hybrid software defined networking architecture for next-generation iots. *KSII Trans Internet Inf Syst*. 2018;12(2):932-945.
4. Sfar R, Chtourou Z, Challal Y. A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. In: 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C); 2017. doi: 10.1109/SM2C.2017.8071828.
5. Singh D, Mishra MK, Lamba AK. Security issues in different layers of iot and their possible mitigation. *Int J Sci Tech Res*. 2020;9(04):2762-2771.
6. Beltran V, Skarmeta AF. Overview of Device Access Control in the IoT and its Challenges. *IEEE Commun Mag*. 2019 Jan;57(1):154-160. doi: 10.1109/mcom.2017.1700433.
7. Khan R, Khan SU, Zaheer R, Khan S. Future internet: The internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology; 2012. doi: 10.1109/FIT.2012.53.
8. Aldhyani THH, Alkahtani H. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics*. 2023 Jan;11(1):233. doi: 10.3390/math11010233.
9. Zanella Rettore de Araujo, Silva E, Albin LCP. Security challenges to smart agriculture: Current state, key issues, and future directions. *Array*. 2020 Dec;8:100048. doi: 10.1016/j.array.2020.100048.
10. Rajalakshmi P, Mahalakshmi SD. IOT based crop-field monitoring and irrigation automation. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO); 2016. doi: 10.1109/ISCO.2016.7726900.
11. Mingjun W, et al. A research on experimental system for Internet of Things major and application project. In: 2012 3rd International Conference on System Science, Engineering Design and Manufacturing Informatization; 2012. doi: 10.1109/ICSSEM.2012.6340722.
12. Rose K, Eldridge SD, Chapin L. The internet of things: An overview understanding the issues and challenges of a more connected world. *The internet society (ISOC)*. 2015;80:1-50.
13. Gonzalez-Argote J. Patterns in Leadership and Management Research: A Bibliometric Review. *Health Leadership and Quality of Life* 2022;1:10-10. <https://doi.org/10.56294/hl202210>.
14. Lee, Wang X, Nguyen H, Ra I. A hybrid software defined networking architecture for next-generation iots. *KSII Trans Internet Inf Syst*. 2018;12(2):932-945.
15. Sfar R, Chtourou Z, Challal Y. A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. In: 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C); 2017. doi: 10.1109/SM2C.2017.8071828.
16. Singh D, Mishra MK, Lamba AK. Security issues in different layers of iot and their possible mitigation. *Int J Sci Tech Res*. 2020;9(04):2762-2771.
17. Gonzalez-Argote J. Analyzing the Trends and Impact of Health Policy Research: A Bibliometric Study.

Health Leadership and Quality of Life 2023;2:28-28. <https://doi.org/10.56294/hl202328>.

18. Beltran V, Skarmeta AF. Overview of Device Access Control in the IoT and its Challenges. *IEEE Commun Mag.* 2019 Jan;57(1):154-160. doi: 10.1109/mcom.2017.1700433.

19. Khan R, Khan SU, Zaheer R, Khan S. Future internet: The internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology; 2012. doi: 10.1109/FIT.2012.53.

20. Aldhyani THH, Alkahtani H. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics.* 2023 Jan;11(1):233. doi: 10.3390/math11010233.

21. Zanella Rettore de Araujo, Silva E, Albini LCP. Security challenges to smart agriculture: Current state, key issues, and future directions. *Array.* 2020 Dec;8:100048. doi: 10.1016/j.array.2020.100048.

22. Rajalakshmi P, Mahalakshmi SD. IOT based crop-field monitoring and irrigation automation. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO); 2016. doi: 10.1109/ISCO.2016.7726900.

23. Auza-Santiv   ez JC, D   az JAC, Cruz OAV, Robles-Nina SM, Escalante CS, Huanca BA. mHealth in health systems: barriers to implementation. *Health Leadership and Quality of Life* 2022;1:7-7. <https://doi.org/10.56294/hl20227>.

24. Mingjun W, et al. A research on experimental system for Internet of Things major and application project. In: 2012 3rd International Conference on System Science, Engineering Design and Manufacturing Informatization; 2012. doi: 10.1109/ICSSEM.2012.6340722.

25. Uman JMM, Arias LVC, Romero-Carazas R. Factores que dificultan la graduaci   n: El caso de la carrera profesional de contabilidad en las universidades peruanas. *Revista Cient   fica Empresarial Debe-Haber* 2023;1:58-74.

26. Rose K, Eldridge SD, Chapin L. The internet of things: An overview understanding the issues and challenges of a more connected world. *The internet society (ISOC).* 2015;80:1-50.

27. Castillo-Gonzalez W. Charting the Field of Human Factors and Ergonomics: A Bibliometric Exploration. *Health Leadership and Quality of Life* 2022;1:6-6. <https://doi.org/10.56294/hl20226>.

28. Lee, Wang X, Nguyen H, Ra I. A hybrid software defined networking architecture for next-generation iots. *KSII Trans Internet Inf Syst.* 2018;12(2):932-945.

29. Sfar R, Chtourou Z, Challal Y. A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. In: 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C); 2017. doi: 10.1109/SM2C.2017.8071828.

30. Singh D, Mishra MK, Lamba AK. Security issues in different layers of iot and their possible mitigation. *Int J Sci Tech Res.* 2020;9(04):2762-2771.

31. Romero-Carazas R. Prompt lawyer: a challenge in the face of the integration of artificial intelligence and law. *Gamification and Augmented Reality* 2023;1:7-7. <https://doi.org/10.56294/gr20237>.

32. Beltran V, Skarmeta AF. Overview of Device Access Control in the IoT and its Challenges. *IEEE Commun Mag.* 2019 Jan;57(1):154-160. doi: 10.1109/mcom.2017.1700433.

33. Khan R, Khan SU, Zaheer R, Khan S. Future internet: The internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology; 2012. doi: 10.1109/FIT.2012.53.

34. Aldhyani THH, Alkahtani H. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics.* 2023 Jan;11(1):233. doi: 10.3390/math11010233.

35. Zanella Rettore de Araujo, Silva E, Albini LCP. Security challenges to smart agriculture: Current state,

key issues, and future directions. *Array*. 2020 Dec;8:100048. doi: 10.1016/j.array.2020.100048.

36. Gonzalez-Argote J. A Bibliometric Analysis of the Studies in Modeling and Simulation: Insights from Scopus. *Gamification and Augmented Reality* 2023;1:5-5. <https://doi.org/10.56294/gr20235>.

37. Rajalakshmi P, Mahalakshmi SD. IOT based crop-field monitoring and irrigation automation. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO); 2016. doi: 10.1109/ISCO.2016.7726900.

38. Mingjun W, et al. A research on experimental system for Internet of Things major and application project. In: 2012 3rd International Conference on System Science, Engineering Design and Manufacturing Informatization; 2012. doi: 10.1109/ICSSEM.2012.6340722.

39. Rose K, Eldridge SD, Chapin L. The internet of things: An overview understanding the issues and challenges of a more connected world. *The internet society (ISOC)*. 2015; 80:1-50.

40. Lee, Wang X, Nguyen H, Ra I. A hybrid software defined networking architecture for next-generation iots. *KSII Trans Internet Inf Syst*. 2018;12(2):932-945.

41. Sfar R, Chtourou Z, Challal Y. A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. In: 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C); 2017. doi: 10.1109/SM2C.2017.8071828.

42. Singh D, Mishra MK, Lamba AK. Security issues in different layers of iot and their possible mitigation. *Int J Sci Tech Res*. 2020;9(04):2762-2771.

43. Beltran V, Skarmeta AF. Overview of Device Access Control in the IoT and its Challenges. *IEEE Commun Mag*. 2019 Jan;57(1):154-160. doi: 10.1109/mcom.2017.1700433.

44. Gonzalez-Argote D, Gonzalez-Argote J, Machuca-Contreras F. Blockchain in the health sector: a systematic literature review of success cases. *Gamification and Augmented Reality* 2023;1:6-6. <https://doi.org/10.56294/gr20236>.

45. Khan R, Khan SU, Zaheer R, Khan S. Future internet: The internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology; 2012. doi: 10.1109/FIT.2012.53.

46. Aldhyani THH, Alkahtani H. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics*. 2023 Jan;11(1):233. doi: 10.3390/math11010233.

47. Zanella Rettore de Araujo, Silva E, Albin LCP. Security challenges to smart agriculture: Current state, key issues, and future directions. *Array*. 2020 Dec;8:100048. doi: 10.1016/j.array.2020.100048.

48. Rajalakshmi P, Mahalakshmi SD. IOT based crop-field monitoring and irrigation automation. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO); 2016. doi: 10.1109/ISCO.2016.7726900.

FINANCING

No financing.

CONFLICT OF INTEREST

None.

AUTHORSHIP CONTRIBUTION

Conceptualization: Khaoula Taji, Badr Elkhalyly, Yassine Taleb Ahmad, Ilyas Ghanimi. Fadoua Ghanimi.

Research: Khaoula Taji, Badr Elkhalyly, Yassine Taleb Ahmad, Ilyas Ghanimi. Fadoua Ghanimi.

Drafting - original draft: Khaoula Taji, Badr Elkhalyly, Yassine Taleb Ahmad, Ilyas Ghanimi. Fadoua Ghanimi.

Writing - proofreading and editing: Khaoula Taji, Badr Elkhalyly, Yassine Taleb Ahmad, Ilyas Ghanimi. Fadoua Ghanimi.