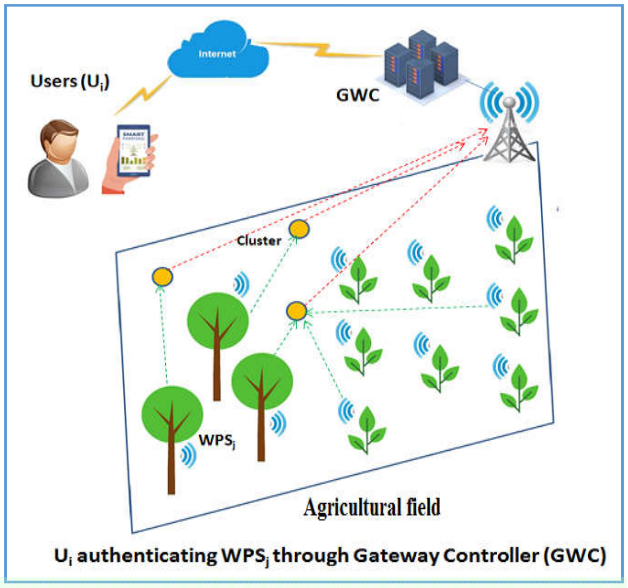
This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2024.3402538

SAWPS: Secure Access control for Wearable Plant Sensors: reinforcing Agriculture 4.0

AZEEM IRSHAD, AMER ALJAEDI, ZAID BASSFAR, SAJJAD SHAUKAT JAMAL, ALI DAUD, SHEHZAD ASHRAF CHAUDHRY*, ASHOK KUMAR DAS

Abstract—The deployment of Agriculture 4.0 depends heavily on the adoption of Internet of Things (IoT) and wireless sensors for increasing productivity and reducing costs of cultivation. Wearable plant sensors (WPS), an IoT variant, can greatly optimize agricultural yields, sense early indications of disease, reduce waste and minimize environmental concerns. Nonetheless, the induction of WPS into the plant fields always remains precarious for its open nature. We can witness many authentication protocols for agriculture setting, yet inefficient or insecure due to their vulnerability to known attacks. Most of these protocols lack privacy and perfect forward secrecy (PFS)-based significant features, and are not suited for agricultural fields due to utilization of complex crypto-primitives. Thus, to realize Agriculture 4.0 objectives, novel security solutions based on ultra-light crypto-primitives are required. We propose an authentication protocol (SAWPS) for wearable plant sensors using Chinese Remainder Theorem (CRT) that is not only lightweight but also ensures privacy and PFS features. Moreoever, SAWPS is resistant to known attacks including Denial of Service (DoS), Ephemeral Secret Leakage, Man-in-The-Middle, impersonation and forgery threats. The theoretical evaluation along with formal analysis based on Real-or-Random (RoR) model is provided for correctness and security. The performance results demonstrate efficiency and effectiveness of SAWPS over the comparative studies.



U_i authenticating WPS_j through Gateway Controller (GWC)

Index Terms— Authentication, smart agriculture, wearable plant sensors, cryptography

*Corresponding author: S. A. Chaudhry (shehzad.ashraf@adu.ac.ae).

A. Irshad is with Department of Computer science and Software Engineering, International Islamic University, Islamabad, Pakistan (email: irshadazeem2@gmail.com)

A. Aljaedi and Z. Bassfar are with Department of Computing and Information Technology, University of Tabuk, Tabuk, Saudi Arabia (emails: aaljaedi@ut.edu.sa and zbassfar@ut.edu.sa)

S. S. Jamal is with Department of mathematics, College of Science, King Khalid University, Abha, Saudi Arabia (email: shussain@kku.edu.sa)

A. Daud is with Faculty of Resilience, Rabdan Academy, Abu Dhabi, UAE (email: alimsdb@gmail.com)

Shehzad Ashraf Chaudhry is with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, UAE, and is also with the Department of Software Engineering, Faculty of Engineering and Architecture, Nisantasi University, Istanbul 34398, Turkey (e-mail: ashraf.shehzad.ch@gmail.com)

A. K. Das is with Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad Gachibowli 500 032, Hyderabad, India (email: iitkgp.akdas@gmail.com)

Digital Object Identifier: 10.1109/LSEN.XXXX.XXXXXXX (inserted by IEEE).

I. INTRODUCTION

The Agriculture 4.0 refers to framework that engages Internet of Things (IoT), artificial intelligence (AI), drones, renewable energy, cyber-physical Systems, robotics, vertical farms in layers, and wireless sensor networks (WSN) for underpinning autonomous operations and mass customization in microenvironment-based agricultural practices. The agriculture inevitably plays a crucial role for the economic development of an agrarian country and is regarded as backbone of the economy. It could supply not only just raw edibles, but also contribue in the form of employment for farmers. Thus, the advanced technology is desperately needed to boost this sector and ultimately the economy. The WSN in IoT module is a blend of software and hardware technologies that works through receiving signals from different sensors based on application which is synchronized with other sensors over the internet [1]-[2]. This is worthy to mention that WSN is game changer for radical disruptions in the existing world. Wearable plant sensors (WPS), one of the emerging technological advancements, are tiny sensor devices that can be fixed with plants to continuously monitor the climatic parameters such as carbon dioxide, humidity, temperature, light, soil PH and moisture, and

nutrients level [3]. This could help monitoring the real time status of plant health and possible diseases through large scale deployments without human intervention. Biological disorders such as pests and pathogens are the main factors for degradation of plant health and the consequent decline of the agricultural yield. To monitor the plant health, a WPS can be simply placed or attached to various sections of plants including roots, leaves or stems. Each of these plant organs constitute a different function and could be separately monitored using WPS sensors. The WPS sensors continuously collect the significant metrics from the plant stem or leaf with direct interaction and greater environmental insight, and send to remote applications through gateway to profile various trait biomarkers [4]. The availability of enriched data could assist the researchers in solving the agricultural yield issues. Moreover, these sensors could predict weather patterns for improving the crop production. The integration of sensors with the agricultural ecosystem might not only assist in plant health monitoring, but also prove cost-effective in the long run by enhanced yields owing to fewer diseases and in-time diagnosis of issues. The precision of prediction metrics can be further improved with the integration of 5G / 6G networks [5]-[6].

The agricultural yield is largely a function of controlled environmental factors. If the reported sensors' data is well protected from unauthorized access or modification and communicated securely to the stakeholders, it may bring forth astonishing economic indicators in the form of productivity for any agrarian economy. This is because, a single unwarranted malicious alteration on the part of adversary could have a catastrophic effect on agricultural growth, for instance the rice productivity may decline 9% for an increase in single degree of Celsius in the average temperature of any geographical region [7]. Likewise, a similar change in temperature may decrease wheat and corn yields by 10% according to Kropff *et al*., 1993 [8]. Likewise, a farmer may communicate with OptRx plant sensor upon sucessful authentication, for the provision of controlled nitrogen to the plants wherever it is needed. Similarly, the fertilizer plays a significant role for the plant growth. However, if its quanity is not controlled that could be devastating for the crops. Thus, initially the crop system authenticates the agricultural user, and then only the latter would be permitted to monitor the plant status or take appropriate actions for balanced growth of the crop. On the other hand, an adversary could authenticate with the weakly desgined system successfully and damage the system by erroneous data injection or manuevering with the data related to fertilizer, water or other mineral provisions [9].

The WSN serves as a vital component of IoT for being the data source linked with the associated applications. In sensor-based architecture there might be three categories of entities such as sensor nodes, mobile user and gateway nodes. The mobile user communicates with the sensor node using wireless channel whenever the former needs the real-time updates of the farm or fields. The WSN carry meagre resources of power, computation and storage in comparison with gateway nodes that are resourceful entities with sufficient power backups, storage and computational capabilities. Thus, the gateway nodes are equipped with sound communication facitilities to interact with remote users and applications. Although, the WSN and wearable sensors has brought convenience for all industries, businesses and life of common man, there are many involved security and privacy concerns about the exchanged data due to open nature of sensors. Primarily, the user node initiates the communication process by submitting authentication request to gateway node. The gateway node processes it and forwards to the particular sensor node. Then, the gateway node, after receiving the response of sensor node, relays the authentication response to the ultimate user [10]. The communication protocol must be secure enough to ensure security requirements for these communication round trips. Hence, the user authentication is crucial for suitable directive to the plant system regarding the supply of balanced nutrients or any appropriate action.

We can witness many WSN-based access control techniques for monitoring the plant and agricultural metrics [11]-[30], however these schemes involve many security issues related to privacy and perfect forward secrecy breach, and lacking resistance to known threats including Denial of Service attacks, Ephemeral Secret Leakage threats, Man-in-the-Middle attack, IoT and sensor node-based physical capture threats, and forgery threats. At the same time, these schemes were not effective in computational and communicational terms for practical deployments in fields. Those schemes were based on public key infrastructure (PKI) cryptosystems [31]. The sensor nodes, WPS in particular, are resource deficient devices with limited energy, computational and storage capabilities. Considering the discussed drawbacks in the previous schemes, we propose a novel access control mechanism SAWPS for wearable plant sensors that is not only secure but also computationally efficient in comparison with previous schemes presented for agriculture. The SAWPS employs lightweight Chinese Remainder Theorem (CRT) instead of computation-intensive crypto-primitives.

A. Contribution

Motivated by the limiting factors of the earlier authentication protocols presented for agricultural crops, we propose a privacy preserving authentication and key agreement mechanism (SAWPS) for wearable plant sensors to monitor the real-time metrics of agricultural plants.The salient points for presenting SAWPS authentication protocol are illustrated below:

- The SAWPS ensures not only anonymity but also offers mutual authenticity, perfect forward secrecy and susceptibility from denial of service attacks, ephemeral secret leakage threats, man-in-the-middle attack, sensor node-based physical capture threats, and forgery threats.
- The SAWPS scheme is analyzed using rigorous Random Oracle model based on Real-or-Random (RoR).
- The comparative findings demonstrate that SAWPS is not only secure against known threats but also efficient in terms of computation and communication.

B. Scheme organization

The organization of scheme is briefly alluded below: Section II presents the related work describing prominent features of comtemporary studies along with limitations. Section III presents system and threat model. The proposed protocol SAWPS is elaborated in section IV. Section V presents informal and RoR-based rigorous formal analysis. Section VI presents the performance

analysis and findings of comparative studies. The last section summarizes the proposed work.

II. RELATED WORK

In WSN architecture, the sensor nodes have scarce computational and storage capacity, thus it is crucial to come up with not only secure but lightweight authentication scheme for sensor-based monitoring system. In 2009, Das *et al.* [8] presented a password and smartcard based remote user Authenticated and Key Agreement (AKA) scheme for WSN, with proclaimations about immunity from security threats. Then, He *et al.* [9] demonstrated that Das *et al.* scheme is vulnerable to impersonation and previliged insider threats. In addition, there was no password modification phase in the protocol. The He *et al.* presented an improved AKA protocol considering those limitations. In 2010, Khan *et al.* [10] exposes the security limitations in [9] as lacking mutual authentication, resistance to previlged insider attack and password updation phase. Later, Chen *et al.* [11] pointed that Khan *et al.* scheme does not ensure mutual authentication, and presented an improved scheme for WSN ensuring mutual authenticity. In 2012, Vaidya *et al.* [12] identified that the schemes [8], [10], [11] were susceptible to sensor node impersonation attack and stolen smart card attack. To counter these threats, Vaidya *et al.* designed an improved scheme for WSNs. The protocol by Vaidya *et al.* was found to be vulnerable by Hsieh *et al.* [13] for many attacks including password guessing attack and malicious insider attack. Also, Hsieh *et al.* presented an improved scheme considering the above mentioned drawbacks. Then, Kim *et al.* [14] cryptanalyzed Vaidya *et al.* scheme with the indication of user impersonation attack and gateway node (GW)-bypasssig attack, and later presented its improved authentication scheme for WSNs.

In 2014, Turkanovic *et al.* [15] presented a new remote user authentictation for WSNs and IoT devices. They claimed that their protocol is protected from all attacks, and provide mutual authentication, password modification facility, password protection, and the node's dynamic addition into the network. Chang [16], in 2015, remarked that Turkanovic *et al.* protocol is vulnerable to sensor node masquerading attack, stolen verifier attack, impersonation attack and stolen smart card attack. To counter these drawbacks, Chang designed two-factor remote user AKA scheme for WSNs. Later, Farash *et al.* [17] also demonstrated that few other attacks such as parameters and session key disclousure attack, man-in-the-middle attack, besides sensor node's traceability and anonymity issues. Farash *et al.* also presented an improved protocol considering the demerits of [15]. Amin *et al.* [18] also cryptanalyzed Turkanovic*et al.* with pointing further attacks including offline-identity and password guessing and forgery threats. Then, Amin *et al.* presented an improved protocol to remedy those drawbacks. Later, Lu *et al.* [19] pointed few security pitfalls in [18] as vulnerable user's identity, offline password guessing attack, user impersonation attack, and known session key temporary information attacks. For addressing these concerns, Lu *et al.* also presented an enhanced scheme for WSN with more security features.

Later, many authentication protocols were presented in diverse fields for WSNs such as coal mines, health care, vehicle tracking, and IoT-cloud ecosystem. In 2015, He *et al.* [20] presented an efficient remote user AKA scheme for patient healthcare employing wireless medical sensor networks (WMSNs). Nonetheless, Li *et al.* [21] discovered many weaknesses in He *et al.* such as incorrect session-key agreement procedure, lacking password verification, and denial of service attack. Later, Li *et al.* presented a privacy-preserving remote user AKA scheme for WMSNs. Wu *et al.* [22] pointed that He *et al.* is vulnerable to offline password guessing attack, sensor node physical capture threat, and user impersonation attack. Also, Wu *et al.* presented an improved protocol by overcoming the flaws in [20]. Kumari *et al.* [23], in 2016 demonstrated a lightweight remote user authentication protocol for WSNs in coal mine monitoring applications, proclaiming security properties and efficiency for increasing the lifetime of the devices. Likewise, Wu *et al.* [24] presented an anonymity-preserving user AKA protocol for WSNs based on IoT technology, proclaiming resistance against known security threats along with efficiency. Next, Amin *et al.* [25] designed an authentication protocol for WSNs based on IoT devices, after cryptanalyzing and improving Farash *et al.* scheme [17] after discovering security pitfalls in [17] such as user impersonation attack, offline password guessing, stolen smart card, and session specific temporary information attacks.

In 2018, Das *et al*. [26] presented a biometrics-based privacy-preserving user authentication protocol for cloud-oriented industrial IoT setting. In 2019, Chen *et al.* [27] designed a three-factor user AKA protocol for wireless medical sensor networks (WMSNs). However, it was found to be vulnerable against sensor node capture attack and offline password guessing attack [25]. In the same year, Sharif *et al.* [28] presented a three-party AKA protocol for data transmission in IoT networks, however, it was not able to support mutual authentication and untraceability, and could not resist many known attacks including DoS attack, key compromise impersonation attack, sensor node impersonation attack, and password guessing attacks [21]. In 2020, Li *et al.* [29] presented a secure three-factor user AKA protocol ensuring forward secrecy for WMSNs. Nonetheless, it is prone to many attacks including password guessing attack, previliged insider attack, sensor node impersonation attack, etc. In 2021, Meshram *et al.* [30] presented a lightweight subtree-based three-factor AKA protocol for large-scale distributed WSNs in random oracle. This scheme was susteptible to anonymity failure, impersonation attack, previliged insider attack and sensor node capture attack [21]. In 2022, Wu *et al.* [31] put forward a novel three-factor AKA scheme for WSN with IoT notion. This scheme was prone to password guessing attack, DoS attack, replay attack and impersonation attack [21]. Then, Li and Tian [32] designed a lightweight, three-factor authentication sccheme for WSNs supporting adpative privacy preserving features for the user. Nonetheless, the scheme [32] was prone to sensor node impersonation attack and also lacks anonymity. Next, Fatima *et al.* [33] demonstrated a 3-factor lightweight authentication protocol using Chinese Remainder Theorem (CRT) for agricultural applications based on WSN. However, this scheme also suffers from many problems including desynchronization threat, previliged insider attack along with many technical defects in the protocol.

III. NETWORK ARCHITECTURE

This section describes system model, threat model and mathematical preliminaries as follows:

Table I. Tabular depiction of wireless sensor networks-based authentication protocols

Scheme	Features	Drawbacks	Year
Kumari et al. [23]	Lightweight key agreement protocol for coal mine environment	Lacks resistance to impernation threats	2016
Amin et al. [25]	Anonymous key agreement scheme for WSN	Lacks resistance to offline password guessing attack, replay and DoS attack	2016
Wu et al. [24]	A privacy-preserving and provable user authentication scheme for wireless sensor networks based on IoT	Lacks resistance to forgery threats	2017
Chen et al. [27]	A three-factor user key agreement protocol for wireless medical sensor networks (WMSNs)	Lacks resistance to sensor node impersonation and offline password guessing attack	2019
Sharif et al. [28]	Three-party secure data transmission in IoT networks through a lightweight key agreement scheme	Lacks resistance to key compromise impersonation attack, sensor node impersonation and DoS attack	2019
Li et al. [29]	A secure three-factor authentication protocol with forward secrecy for WMSN	Lacks resistance to offline password guessing attack, impersonation and DoS attack	2020
Meshram et al. [30]	An efficient subtree-based three-factor authentication technique for large-scale for distributed WSN (DWSN)	Lacks resistance from impersonation attacks and previliged insider threats.	2021
Wu et al. [31]	A three-factor authentication scheme for WSN with IoT notion	Lacks resistance to offline password guessing attack, replay and DoS attack	2021
Li and Tian [32]	A lightweight three-factor key agreement scheme for WSN	Lacks anonymity and resistance to sensor node impersonation attack	2022
Fatima et al. [33]	Privacy-Preserving Three-Factor Authentication Protocol for WSN in agricultural environment	Lacks resistance from desynchronization attacks, previliged insider threats.	2023

A. System model

The SAWPS protocol framework enables monitoring of the real-time status of wearable plant sensors and taking decisions on time to increase the overall productivity along with efficiency. The system model of the SAWPS protocol comprises of user (U_i), gateway controller (GWC) and wearable plant sensor (WPS_j) as depicted in Figure 1. The description of those entities is given below:

1) Users (Ui): Ui may directly approach plant sensors and other devices, in agricultural ecosystem through GWC after logging into the registered smart card.
2) Gateway Controller (GWC): The GWC acts as a trusted third party responsible for enrolling users Ui and plant sensors WPSs.
3) Wearable Plant Sensors (WPSj): These sensors are meant for data collection and report to the high end platforms on real time basis for further computations.

In agricultural setting, the wearable plant sensors scan the real time data such as moisture, temperature. These plant sensors are enrolled by *GWC* through initialization procedure of embedding secret credentials into the memory of WPS_j. For accessing the real-time status of a particular WPS_j, the Ui must be enrolled with *GWC* through implanting secret credentials into the memory of smart device to initiate and strengthen the mutual authentication procedures. The mutual authentication procedure comprises login procedure which is followed by authentication and key establishment procedures. First, the U_i performs login-based challenge. If it is met with success, the authentication request is submitted to *GWC* which, upon due verifications, forwards the request to WPS_j. The WPS_j generates the shared session key by using the same credentials shared with *GWC*. Then the challenge is communicated to *GWC* as well as user for verifying the WPS_j and establishing a mutually agreed session key. In this manner, the Ui may acquire real time warranted status of WPS_j sensors via *GWC*.

B. Threat model

This study assumes the two widely adopted adversary models, i.e. Canetti–Krawczyk (CK) and Dolev–Yao (DY) adversary model [34], [35] for evaluating the resistance of proposed scheme against known attacks. According to the definition of DY model, the attacker may attempt to intercept the communication contents

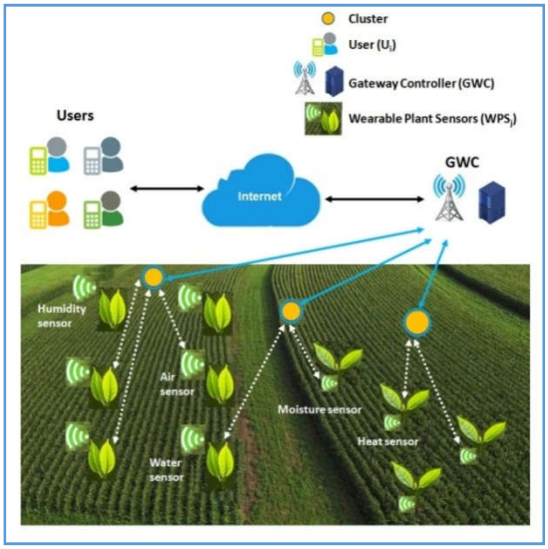


Figure 1. Pictorial depiction of System model

exchanged among the legal entities such as the user U_i, gateway controller *GWC* and wearable plant sensor WPS_j. The attacker can manipulate the communication channel among these entities through modifying, blocking and replaying the contents. The CK model undertakes assumptions of a more capable adversary in which the latter may recover the contents of a stolen smart card or mobile device upon physical examination or employing differential analysis technique. The attacker may act as a privliged insider by intercepting the registration request parameters during registration procedure on secure channel. It may attempt to interact on behalf of other legitimate participants of the system.

C. Chinese Remainder Theorem

The Chinese remainder theorem (CRT) can exclusively solve each pair of congruences bearing relatively prime moduli [33]. While dealing with large moduli, the CRT could be utilized for simplification of the computations through dividing into mutually co-prime factors.

Theorem 1.
Assume that $\theta_1, \theta_2, \ldots, \theta_k$ are pairwise relative primes, for instance GCD $(\theta_i, \theta_j) = 1$, i ≠ j. Next, we assume $\varrho_1, \varrho_2, \ldots, \varrho_k$ be integers. Thus, the congruent equations may be illustrated as:

$x \equiv \varrho_1 \ mod\ \theta_1$
$x \equiv \varrho_2 \ mod\ \theta_2$
… ….
$x \equiv \varrho_k \ mod\ \theta_k$
with exclusive clarification as $x = \sum_{i=1}^{k} \varrho_i V_i' V_i \ (mod V)$
where $V = \prod_{i=1}^{k} \theta_i = \theta_1, \theta_2 = \theta_k$
$V = \frac{V}{\theta_i}$
$V_i' = V_i^{-1} (mod \theta_i)$
$\theta_i = \theta_1, \theta_2 = \theta_k$ are called as CRT moduli, while x characterize the CRT oriented solution.The notations employed in this scheme are given in Table II.

Table II. Notations

Notations	Narrative
U_i, WPS_j:	i^{th} user node, j^{th} Wearable plant sensor
GWC:	Gateway Controller
ID_U, PW_{Ui}, BIO_{Ui}:	Identity, password and biometric secret of U_i
PID_{Ui}:	Pseudo-identity of U_i
K_G	Master secret key of *GWC*
r_{Ui},r_j, r_g:	Random nonces
T_1, T_2, :	Timestamps
Gen(.)/Rep(.):	Generation/Reproduction Fuzzy Extractor functions
K_{WPSj}:	Shared key between *GWC* and *WPSj*
$\mathcal{A}$:	Malicious adversary
SK:	Session key between U_i and WPS_j
⊕, ||, *h(.)*	XOR, Concatenation, A secure one-way hash function

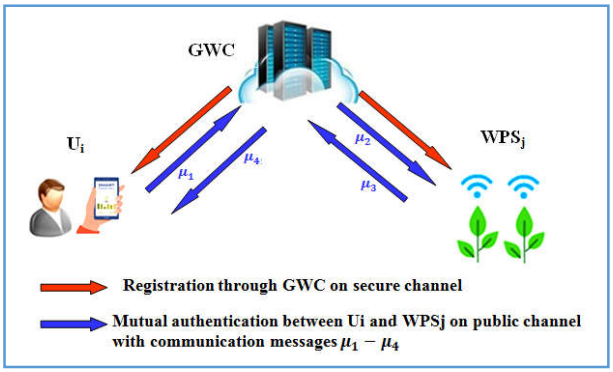


Figure 2. Communication flow in System model

IV. PROPOSED SCHEME

This section proposes a privacy preserving lightweight key agreement technique (SAWPS) for agricultural environment. There are three participating entities in the system, i.e. user U_i, gateway controller *GWC* and wearable plant sensors WPS_j. The SAWPS enables development of a mutually agreed session key between U_i and WPS_j with the supervision of *GWC*. The proposed model comprises system initialization phase, WPS_j enrollment phase, user enrollment phase, and mutual authentication procedure.

A. System initialization phase

In the beginning, the *GWC* chooses its master secret key as K_G. Then, it selects a particular collision resistant hash function $\{h(.): 1, 0^* \rightarrow 1, 0^{\omega}\}$, where the output of *h(.)* is characterized as ω. Then, *GWC* constructs two prime numbers y and z and computes $n = y \,.\, z$. The parameters y and z are well protected secrets by *GWC*, and no other entity is aware of those factors.

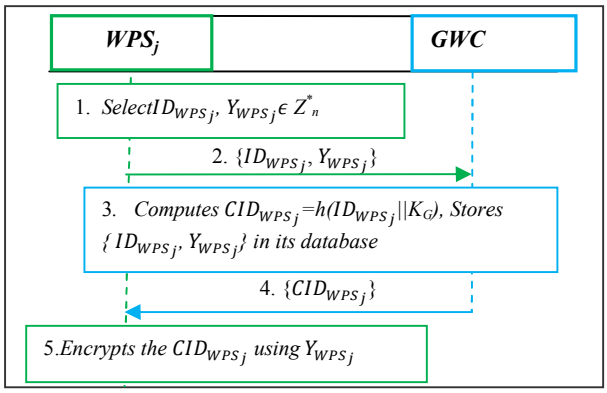


Figure 3. Enrollment of wearable plant sensors (WPS_j)

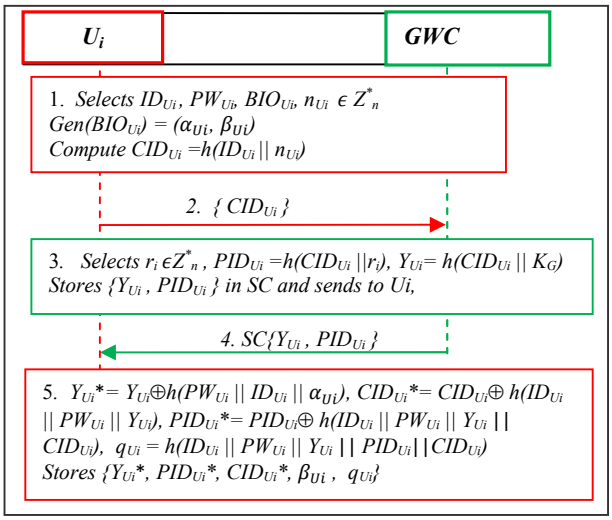


Figure 4. Enrollment of User (Ui)

B. WPS_j enrollment phase

The WPS_j initiates the enrollment process by forwarding the request for registration to *GWC* using the following steps:

1. The WPS_j selects its identity ID_{WPS_j} and generates a random integer Y_{WPS_j}. Then, it submits the authentication request $\{ID_{WPS_j}, Y_{WPS_j}\}$ to *GWC*.
2. The *GWC* computes $CID_{WPS_j} = h(ID_{WPS_j} || K_G)$ and stores $\{ID_{WPS_j}, Y_{WPS_j}\}$ in its database. Then, it submits the message $\{CID_{WPS_j}\}$ to WPS_j.
3. The WPS_j encrypts the CID_{WPS_j} using Y_{WPS_j} and stores in its memory as shown in figure 3.

C. User enrollment phase

This sub-section exhibits the user enrollment phase, in which the *GWC* registers the user U_i by executing the necessary steps on secure communication channel. The necessary steps of the registration are mentioned below:

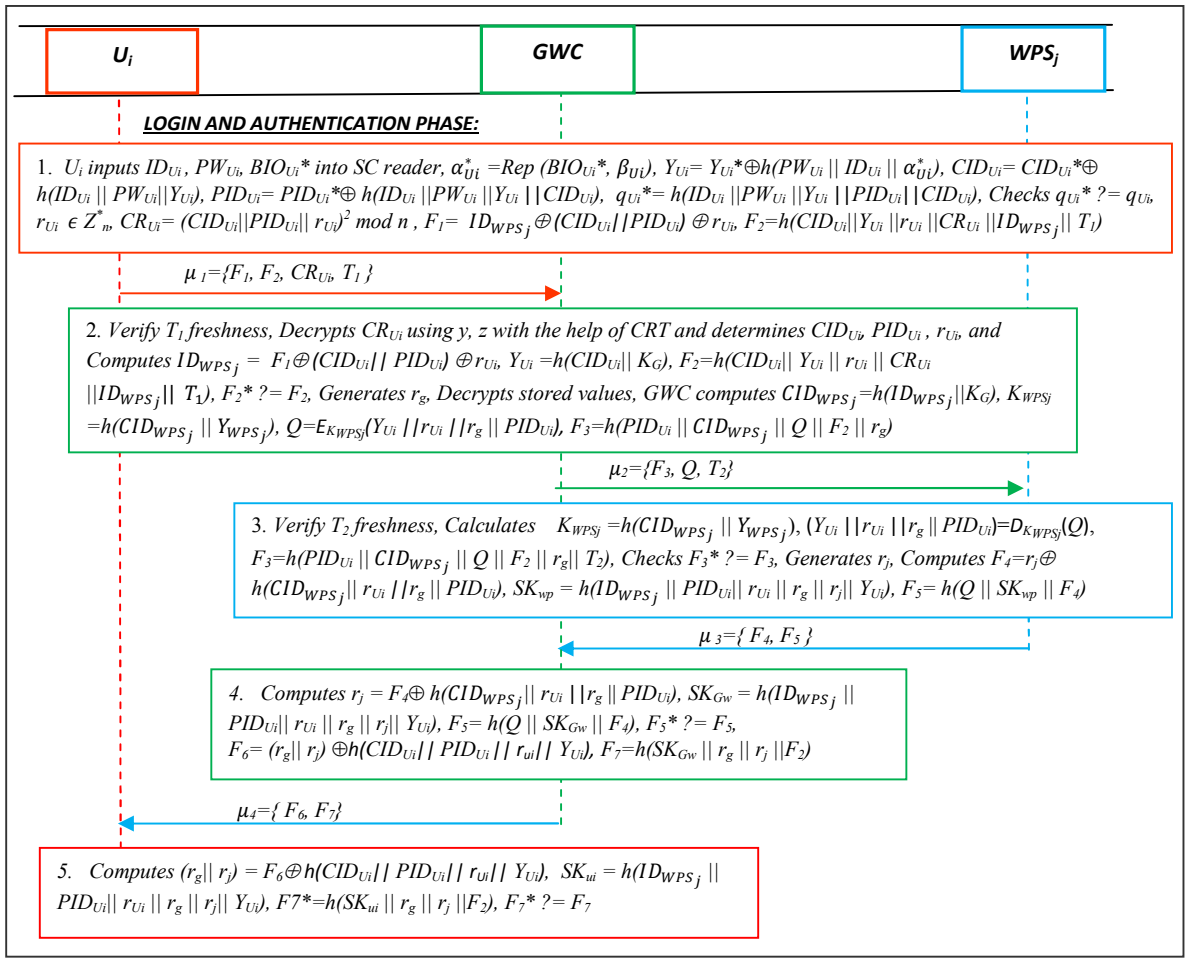


Figure 5. Proposed scheme

1. The U_i selects its identity ID_{Ui} and password PW_{Ui}. Then it inputs its biometric identity BIO_{Ui} into the biometric scanner. Then it chooses a random integer $n_{Ui} \in Z^*_n$. Then it computes $Gen(BIO_{Ui})$ = (α_{Ui}, β_{Ui}) and CID_{Ui} =h(ID_{Ui}|| n_{Ui}). Next it submits the registration request {CID_{Ui}} to *GWC*.
2. The *GWC*, upon receiving the request, chooses a random integer $r_i \in Z^*_n$ and computes pseudo-identity PID_{Ui} =h(CID_{Ui} ||r_i). Then it stores the parameters {Y_{Ui}, PID_{Ui}} in smart card and delivers to Ui on secure channel.
3. Next, the U_i computes Y_{Ui}*= Y_{Ui}⊕h(PW_{Ui} || ID_{Ui} || α_{Ui}), CID_{Ui}*= CID_{Ui}⊕ h(ID_{Ui} || PW_{Ui} || Y_{Ui}), PID_{Ui}*= PID_{Ui}⊕ h(ID_{Ui} || PW_{Ui} || Y_{Ui} || CID_{Ui}), q_{Ui} = h(ID_{Ui} || PW_{Ui} || Y_{Ui} || PID_{Ui}||CID_{Ui}) and stores {Y_{Ui}*, PID_{Ui}*, CID_{Ui}*, β_{Ui} , q_{Ui}} in smart card as shown in figure 4.

D. Mutual authentication phase

The mutual authentication facilitates the construction of an agreed session key between U_i and WPS_j with the help of *GWC* on insecure channel. For this purpose, the user performs few significant steps in mutual authentication phase. The steps involved in this phase are described below:

1. First the user U_i inputs ID_{Ui}, PW_{Ui}, BIO_{Ui}* into *SC* reader and computes α^*_{Ui} =Rep (BIO_{Ui}*, β_{Ui}), Y_{Ui}= Y_{Ui}*⊕h(PW_{Ui} || ID_{Ui} || α^*_{Ui}), CID_{Ui}= CID_{Ui}*⊕ h(ID_{Ui} || PW_{Ui}||Y_{Ui}), PID_{Ui}= PID_{Ui}*⊕ h(ID_{Ui} ||PW_{Ui} ||Y_{Ui} ||CID_{Ui}), q_{Ui}*= h(ID_{Ui} ||PW_{Ui} ||Y_{Ui} ||PID_{Ui}||CID_{Ui}), and checks the equality match for q_{Ui}* ?= q_{Ui}. If it is not true, the smart card aborts the session. Otherwise, it chooses a random integer $r_{Ui} \in Z^*_n$ and computes CR_{Ui}= (CID_{Ui}||PID_{Ui}|| r_{Ui})^2 mod n , F_1= ID_{WPS_j}⊕ (CID_{Ui} ||PID_{Ui}) ⊕r_{Ui}, F_2=h(CID_{Ui}||Y_{Ui} ||r_{Ui} ||CR_{Ui} ||ID_{WPS_j}|| T_1). Then it submits the authentication request μ_1={F_1, F_2, CR_{Ui}, T_1} to *GWC* for verification as shown in Figure 2.
   The *GWC*, upon the receipt of request, checks freshness of $T_1$and decrypts CR_{Ui} using *y*, *z* with the help of *CRT* and determines (CID_{Ui},PID_{Ui} ,r_{Ui}). Then it computes ID_{WPS_j} = F_1⊕ (CID_{Ui} ||PID_{Ui}) ⊕r_{Ui}, Y_{Ui} =h(CID_{Ui}|| K_G), F_2=h(CID_{Ui}||Y_{Ui} || r_{Ui} || CR_{Ui} ||ID_{WPS_j}|| T_1), and compares the equality for F_2* ?= F_2. If it is true, the *GWC* further generates a random integer r_g, and computes CID_{WPS_j}=h(ID_{WPS_j}||K_G), K_{WPSj}=h(CID_{WPS_j}||Y_{WPS_j}), Q=$E_{K_{WPSj}}$(Y_{Ui}||r_{Ui}||r_g||PID_{Ui}) and F_3=h(PID_{Ui} ||CID_{WPS_j} || Q || F_2 || r_g|| T_2). Then, it forwards the message μ_2={ F_3, Q, T_2} to WPS_j.
2. Next, the WPS_j checks freshness of T_2 and computes K_{WPSj} =h(CID_{WPS_j} || Y_{WPS_j}), (Y_{Ui} ||r_{Ui} ||r_g || PID_{Ui})=$D_{K_{WPSj}}$(Q), F_3=h(PID_{Ui} ||CID_{WPS_j} ||Q ||F_2 ||r_g|| T_2) and checks the equality for F_3* ?= F_3. Then it generates a random integer r_j and computes F_4=r_j⊕h(CID_{WPS_j}||r_{Ui} ||r_g || PID_{Ui}), SK_{wp} = h(ID_{WPS_j} || PID_{Ui}|| r_{Ui} || r_g || r_j|| Y_{Ui}) and F_5= h(Q || SK_{wp} || F_4). Next, it forwards the message μ_3={ F_4, F_5 } to *GWC*.

3. Next, *GWC* computes $r_j = F_4 \oplus h(CID_{WPS_j} || r_{Ui} \| r_g \| PID_{Ui})$, $SK_{Gw} = h(ID_{WPS_j} || PID_{Ui} || r_{Ui} || r_g || r_j || Y_{Ui})$, $F_5 = h(Q || SK_{Gw} || F_4)$ and compares the equality $F_5^* ?= F_5$. If it is true, it further computes $F_6 = (r_g || r_j) \oplus h(CID_{Ui} || PID_{Ui} || r_{ui} || Y_{Ui})$, $F_7 = h(SK_{Gw} || r_g || r_j || F_2)$ and submits the message $\mu_4 = \{F_6, F_7\}$ to U_i for final verification as shown in figure 5.
4. In the last step, the U_i computes $(r_g || r_j) = F_6 \oplus h(CID_{Ui} || PID_{Ui} || r_{Ui} || Y_{Ui})$, $SK_{ui} = h(ID_{WPS_j} || PID_{Ui} || r_{Ui} || r_g || r_j || Y_{Ui})$, $F_7^* = h(SK_{ui} || r_g || r_j || F_2)$ and verifies the match for $F_7^* ?= F_7$. If it is true, the session key is deemed to be valid by the user U_i.

V. SECURITY ANALYSIS

This section presents informal and formal security analysis for SAWPS in the following sub-sections:

A. Informal security analysis

The informal security analysis of SAWPS is elaborated below:

i. Mutual Authentication

The SAWPS ensures that all participants verify one another in the same protocol. That is, the *GWC* authenticates U_i on the basis of verification for F_2 parameter after computing it as $F_2 = h(CID_{Ui} || Y_{Ui} || r_{Ui} || CR_{Ui} || ID_{WPS_j} || T_1)$. The *GWC* is acquainted with this fact that no malicious attacker $\mathcal{A}$ could compute F_2 due to lacking access of CID_{Ui}, PID_{Ui} and r_{Ui} parameters. Using same metrics, *GWC* can compute $ID_{WPS_j} = F_1 \oplus (CID_{Ui} || PID_{Ui}) \oplus r_{Ui}$ as well as $Y_{Ui} = h(CID_{Ui} || K_G)$ for seeking help in verification of user by developing a legal F_2 parameter. Likewise, WPS_j verifies the authenticity of *GWC* by computing $F_3^* = h(PID_{Ui} || ID_{WPS_j} || Q || F_2 || r_g || T_2)$ and comparing against the received F_3. The WPS_j knows the fact that no entity other than a legitimate *GWC* can employ the valid r_g and PID_{Ui} parameters to produce F_3. Similarly, GWC verifies WPS_j on the basis of computing $F_5^* = h(Q || SK_{Gw} || F_4)$ and comparing against the received F_5. The *GWC* knows that a valid session key $SK_{Gw} = h(ID_{WPS_j} || PID_{Ui} || r_{Ui} || r_g || r_j || Y_{Ui})$ can only be computed by a valid WPS_j due to priveleged access to Y_{Ui}, r_{Ui}, r_g and PID_{Ui} parameters [35]. Finally, the user authenticates *GWC* as well as WPS_j entities through computing and verification of $F_7^* = h(SK_{ui} || r_g || r_j || F_2)$. The user is acquainted with the fact that none other than a legitimate WPS_j have access to CID_{Ui}, PID_{Ui}, r_{Ui} and Y_{Ui} metrics. Thus, the SAWPS achieves mutual authenticity for the involved participants.

ii. Anonymity and unlinkability

The anonymity feature is integral for the involved participants in any sensor network-based system. This feature can be ensured by circumventing the submission of original identity of participants during communication [36]. The SAWPS supports anonymity as the adversary may not access the user's original identity ID_{Ui} by manipulating eavesdropped contents. This is because, the SAWPS employs pseudo-identity PID_{Ui} in place of real user's identity ID_{Ui}, and is exchanged with *GWC* through CRT-based encryption [36]. The real identity ID_{Ui} is only utilized for verifying the credentials of user while logging into the device for initiating authentication request $\mu_1 = \{F_1, F_2, CR_{Ui}, T_1\}$ towards *GWC*, otherwise it is not needed during session establishment-based exchange of messages. Likewise, SAWPS remains unlinkable on the part of adversary across several sessions among the identical participants. This is because; there is no single parameter that remains constant over multiple sessions. Thus the adversary remains unaided in SAWPS for exploiting the legal participants concerning privacy matters.

iii. Replay attack

In SAWPS, $\mathcal{A}$ remains unaided for initiating any kind of replay attack towards legal participants. The user submits the authentication request by including a timestamp T_1 in F_2 parameter which is checked for its freshness by the *GWC* before processing other messages in its queue. If T_1 in μ_1 is not fresh, the *GWC* aborts the message right away. Likewise, WPS_j checks the freshness of T_2 timestamp in μ_2 before proceeding to further computations, and will only proceed with assurance of fresh timestamp. Thus, our scheme warrants resistance against replay attack.

iv. Offline-password guessing attack

In SAWPS, the adversary may not initiate offline password guessing attack, as it relies on biometric verification using biometric factor BIO_{Ui} besides identity and password [37]. For this purpose, the user U_i inputs ID_{Ui}, PW_{Ui}, BIO_{Ui}* into smart card reader *SC*. Then, *SC* computes $\alpha_{Ui}^* = Rep(BIO_{Ui}^*, \beta_{Ui})$, $Y_{Ui} = Y_{Ui}^* \oplus h(PW_{Ui} || ID_{Ui} || \alpha_{Ui}^*)$, $CID_{Ui} = CID_{Ui}^* \oplus h(ID_{Ui} || PW_{Ui} || Y_{Ui})$, $PID_{Ui} = PID_{Ui}^* \oplus h(ID_{Ui} || PW_{Ui} || Y_{Ui} \| CID_{Ui})$ and $q_{Ui}^* = h(ID_{Ui} || PW_{Ui} || Y_{Ui} \| PID_{Ui} || CID_{Ui})$. Finally, it compares the equality for $q_{Ui}^* ?= q_{Ui}$. It aborts if the equality is not matched. Otherwise, after the successful login it proceeds towards the construction of authentication request.

v. Impersonation attack

In SAWPS, $\mathcal{A}$ may attempt to fabricate the message $\mu_1 = \{F_1, F_2, CR_{Ui}, T_1\}$ on its way to *GWC*, in order to impersonate as a user. However, the *GWC* may counter this attack by computing $F_2^* = h(CID_{Ui} || Y_{Ui} || r_{Ui} || CR_{Ui} || ID_{WPS_j} || T_1)$ and comparing against the received F_2. The *GWC* knows that an adversary cannot construct a valid and fresh F_2 on the part of user without access to legal CID_{Ui} and PID_{Ui} parameters. Similarly, if $\mathcal{A}$ attempts to impersonate as *GWC* towards WPS_j, it will not be a success since $\mathcal{A}$ cannot construct a valid $\mu_2 = \{F_3, Q, T_2\}$ message without acess to r_g and PID_{Ui} parameters to produce F_3. Likewise, to impersonate as a *GWC* the adversary requires access to CID_{Ui}, PID_{Ui}, r_{Ui} and Y_{Ui} metrics. Thus, the SAWPS is immune to user, *GWC* and WPSj impersonation attack.

vi. Session specific ephemeral secrets leakage attack (ESL)

If we assume that an adversary is capable of accessing the short term temporary secrets such as r_{Ui}, r_g and r_j, still the former will not be able to compute the previous session keys constructed among the legitimate participants [38]. This is because, for computing a valid session key $SK = h(ID_{WPS_j} || PID_{Ui} || r_{Ui} || r_g || r_j || Y_{Ui})$, $\mathcal{A}$ requries other parameters as well such as ID_{WPS_j}, PID_{Ui} and Y_{Ui}. However, these parameters can only be computed with the help of y, z and K_G parameters which are only held with the *GWC*.

vii. Perfect forward secrecy

The proposed scheme is compliant to perfect forward secrecy. That is, if an adversary is able to compromise the private secret key K_G of *GWC*, still it may not decrypt CR_{Ui} using CRT theorem without y and z critical parameters which are only held with the *GWC* other than K_G secret key [39]. Without decryption of CR_{Ui}, the adversary may not produce CID_{Ui}, PID_{Ui}, r_{Ui} parameters and ultimately it may not compute ID_{WPS_j} which is crucial for the construction of session

key $SK = h(ID_{WPS_j} || PID_{Ui}|| r_{Ui} || r_g || r_j|| Y_{Ui})$. Thus, the SAWPS supports perfect forward secrecy.

B. Formal security analysis

In this section, we demonstrate the formal security analysis of the contributed scheme SAWPS employing Real-or-Random (RoR)-based model. This analysis model was presented by Canetti *et al*. [34]. The RoR model analyzes the scheme's security through computing probability for the successful guessing of session key SK using the modeled games played by the adversary.

Assume the proposed model engages three entities such as U_i, *GWC* and WPS_j to establish mutual authentication among these entities, within the same protocol SAWPS. The $\prod_{U_i}^{p}$, $\prod_{WPS_j}^{q}$ and $\prod_{GWC}^{r}$ describe the p^{th}, q^{th} and r^{th} instance oracles of U_i, WPS_j and *GWC*, respectively. Besides, the malicious intruder $\mathcal{A}$ is assumed to be capable of launching these queries: Q^*= $\{\prod_{U_i}^{p}, \prod_{WPS_j}^{q}, \prod_{GWC}^{r}\}$.

- *Execute* (Q^*): Using the output of Execute query, the attacker may eavesdrop passively by intercepting the transcripts of coomunicated messages among the entities U_i, WPS_j and *GWC*.
- *Send*($\prod_{U_i}^{p}$, *Start*): By using this query, the authentication protocol is initialized by the user U_i.
- *Send*(Q^*,$M_{\mathcal{A}}$): The malicious user $U_{\mathcal{A}}$ may generate fabricated messages $M_{\mathcal{A}}$ with the help of intercepted messages, and send to the instance Q^* in order to elicit response from it.
- *Hash_*Q^* *(string):* By employing *Hash* query, the attacker may insert any string as input and get its hash value in response.
- *Corrupt* (Q^*, *CF*): It is assumed that the adversary may compromise at most two out of three factors such as password, smart card and biometric parameters. The adversary may perform this query under three scenarios:
  - In case *CF*=1 and Q^*=$\prod_{U_i}^{p}$, the adversary may recover the password as well as smart card credentials of $\prod_{U_i}^{p}$.
  - In case *CF*=2 and Q^*=$\prod_{U_i}^{p}$, the adversary may recover biometric factor as well as smart card credentials of $\prod_{U_i}^{p}$.
  - In case *CF*=3 and Q^*=$\prod_{U_i}^{p}$, the adversary recovers biometric value as well the password of $\prod_{U_i}^{p}$.
  - In case *CF*=1 and Q^*=$\prod_{GWC}^{r}$, the adversary recovers long term secret credentials of $\prod_{GWC}^{r}$.
- *Test* (Q^*)*:* By using this query, the adversary flips an unbiased coin with possible output C_b. If C_b =0, the attacker gets the output of random key with an equivalent size of session key. If C_b =1, it recovers the accurate session key SK.

Proof. Theorem 1. Using the RoR model, an adversary may execute *Send*, *Test*, *Corrupt*, *Hash* and *Execute* queries. Thus, the advantage of $\mathcal{A}$ in breaking the *SK* security and privacy of demonstrated protocol SAWPS in polynomial time can be referred to

$$Adv_{\mathcal{A}}^{SAWPS} \leq \frac{q_{S_{nd}}}{2^{b_l-2}} + \frac{3q_{h_{sh}}^2}{2^{b_l}} + \frac{\left(q_{S_{nd}}+q_{exe}\right)^2}{n} + 2max\{C_b{}'.q_{S_{nd}}^{s'}, \frac{q_{S_{nd}}}{2^{b_l}}\} \quad (1)$$

Where $q_{S_{nd}}$ exhibits the number of send queries; $q_{h_{sh}}$shows number of times the hash query is executed; b_l shows the bitwise length of biological string. Here, $C_b{}'$ and s' be the constant factors.

Proof. The proof utilizes seven rounds of security games, from WG_0 to WG_6 in order to prove theorem. The $Succ_{\mathcal{A}}^{WG_i}$shows adversary's probability to win the contest for all game sequences $\{WG_i \mid 0 \leq i \leq 6\}$.

WG₀: In RoR model, the simulation for game WG_0 is identical with the real attack, and is initiated with the flipping of a coin C_b without using any query. Hence, the probability to crack SAWPS by the adversary is calculated as:

$$Adv_{\mathcal{A}}^{SAWPS}(\rho) = |\, 2\Pr[Succ_{\mathcal{A}}^{WG_0}] - 1\,| \quad (2)$$

WG₁: The game WG_1 is similar to WG_0, however with an additional *Execute* (Q^*) query. In this game, the adversary eavesdrop the exchanged messages $\{\mu_1 - \mu_4\}$ on open channel, i.e., μ_1={ F_1, F_2, CR_{Ui}, T_1} , μ_2={ F_3, Q, T_2}, μ_3={ F_4, F_5 }, μ_4={ F_6, F_7} . An adversary may attempt to compute session key *SK* using *Test* (Q^*) query, however these message parameters are constructed out of ephemeral random credentials such as r_{Ui}, r_g are r_j which are not accessible to the former. Thus the probability of WG_1 is similar to WG_0, i.e.,

$$\Pr\left[Succ_{\mathcal{A}}^{WG_1}\right] = \Pr\left[Succ_{\mathcal{A}}^{WG_0}\right] \quad (3)$$

WG₂: This game stands identical to WG_1 with the exception that the game WG_2 fails if there happens to be collision in the *Hash_*Q^*query. This is because the probability of hash based collision is at most $q_{h_{sh}}^2/2^{b_l+1}$, and the maximum probability for hash-based collision in transcripts can be computed as $\left(q_{S_{nd}} + q_{exe}\right)^2/2n$. In view of birthday paradox [40]-[41], we can compute the associated probability for this game as $|\Pr\left[Succ_{\mathcal{A}}^{WG_2}\right] - \Pr\left[Succ_{\mathcal{A}}^{WG_1}\right]| \leq \frac{q_{h_{sh}}^2}{2^{b_l+1}} + \frac{\left(q_{S_{nd}}+q_{exe}\right)^2}{2n}$ (4)

WG₃: This game is similar to WG_2 with the exception that the attacker can make an accurate guess of the number of verifiers foregoing the hash query oracle, and comes to an end, ultimately. Hence, the probability fof WG_3 can be calculated as

$$|\Pr\left[Succ_{\mathcal{A}}^{WG_3}\right] - \Pr\left[Succ_{\mathcal{A}}^{WG_2}\right]| \leq \frac{q_{S_{nd}}}{2^{b_l}} \quad (5)$$

WG₄: This round of game explores the security of session key SK in two perspectives. That is, in the first perspective, the attacker is assumed to have compromised with the *GWC*'s long term secret key K_G in order to check the perfect forward secrecy. In the second perspective, the adversary may be exposed with the ephemeral random secrets to check the resistance of the scheme against Session Specific Temporary Information attack (SSTI) [42]. The adversary may attempt to compromise with the session key SK upon execution of *Corrupt* (Q^*, *CF*) in order to break the long term secret K_G of instance $\prod_{GWC}^{r}$. Consequently, in case the *CF* =1, the attacker may not be able to recover the ephemeral secrets r_{Ui}, r_g and r_j for computing session key $SK_{ui} = h(CID_{WPS_j} || PID_{Ui}|| r_{Ui} || r_g || r_j|| Y_{Ui})$. Nonetheless, the attacker is not capable of computing any two of the three values using the third number, and thus the former is unable to calculate SK_{Ui}. Thus, the attacker could only compromise the session key by using *Hash* as well as *Send* queries in both perspectives, as discussed above. The probability of WG_4 may be computed as

$$|\Pr\left[Succ_{\mathcal{A}}^{WG_4}\right] - \Pr\left[Succ_{\mathcal{A}}^{WG_3}\right]| \leq \frac{q_{S_{nd}}}{2^{b_l}} + \frac{q_{h_{sh}}^2}{2^{b_l+1}} \quad (6)$$

WG₅: The difference between game WG_5 and WG_4 is that the adversary tries to initiate a password guessing as well as stolen smart card attack using the *Corrupt* query. In case, the query *Corrupt* ($U_{\mathcal{A}}$, *2*) is called, the other queries such as *Corrupt* ($U_{\mathcal{A}}$, *1*) and *Corrupt*

$(U_{\mathcal{A}}, 3)$ may not be queried [43]. Upon the submission of $q_{S_{nd}}$ times *Send* queries in order to guess the password online, the chances of computing the password is evaluated at most as $C'.\ q_{s_{nd}}^{s'}$, where C' and s' define the constants corresponding to the length of password [44]. Thus, the probability for game WG_5 is depicted as

$$|\Pr[Succ_{\mathcal{A}}^{WG_5}] - \Pr[Succ_{\mathcal{A}}^{WG_4}]| \leq C'.q_{s_{nd}}^{s'} \quad (7)$$

***WG*$_7$**: Similarly, the game WG_7 is different from WG_6 in a manner that the game WG_6 halts upon the initiation of queries for guessing the session key $SK_{Gw} = h(CID_{WPS_j} || PID_{Ui} || r_{Ui} || r_g || r_j || Y_{Ui})$. The objective of WG_7 is to determine the resistance of SAWPS against impersonation threats.

$$|\Pr[SucP_{\mathcal{A}}^{WG_7}] - \Pr[SucP_{\mathcal{A}}^{WG_6}]| \leq \frac{q_{h_{sh}}^2}{2^{b_l+1}} \quad (8)$$

In view of games from WG_0 till WG_7, the winning probability to guess the SK may be evaluated as

$$Adv_{\mathcal{A}}^{SAWPS}(t) = 2\Pr[SucP_{\mathcal{A}}^{WG_0}] - 1 \quad (9)$$

Using equations (1)-(9), we have

$$= 2\Pr[SucP_{\mathcal{A}}^{WG_7}] - 1 + 2(\Pr[SucP_{\mathcal{A}}^{WG_0}] - \Pr[SucP_{\mathcal{A}}^{WG_7}])$$

$$\leq 2 \times \frac{1}{2} - 1 + 2\sum_{n=0}^{7}(\Pr[SucP_{\mathcal{A}}^{WG_{(n+1)}}] - \Pr[SucP_{\mathcal{A}}^{WG_n}])$$

$$Adv_{\mathcal{A}}^{SAWPS} \leq 2 \times [\frac{q_{h_{sh}}^2}{2^{b_l+1}} + \frac{(q_{S_{nd}}+q_{exe})^2}{2n} + \frac{q_{S_{nd}}}{2^{b_l}} + \frac{q_{S_{nd}}}{2^{b_l}} + \frac{q_{h_{sh}}^2}{2^{b_l+1}} + C'.q_{s_{nd}}^{s'} + \frac{q_{h_{sh}}^2}{2^{b_l+1}}] \quad (10)$$

$$= \frac{3q_{h_{sh}}^2}{2^{b_l}} + \frac{(q_{S_{nd}}+q_{exe})^2}{n} + \frac{q_{S_{nd}}}{2^{b_l-2}} + 2\,C'.q_{s_{nd}}^{s'}$$

VI. PERFORMANCE EVALUATION

This section evaluates the performance of the proposed scheme SAWPS against the comparative studies [23], [25] - [33] regarding computational cost, communication cost and accomplishment of security functions. To compute the computational overhead of schemes employing various crypto-primitives, an experiment was conducted on Lenovo Desktop with Windows 10, Intel(R) Core i5-9500 CPU @ 8 GHz having 8GB for Gateway-based simulation, Redmi note 9 with Android 4.4.2 OS, Qualcomm Snapdragon 750 processor and 8 GB of memory to simulate users, while the experiment was performed on Raspberry PI 3, 64-b processor, and 1 GB RAM to simulate sensor node [45]. The reported execution timings for the performed experiments are shown in Table III for various crypto-primitives including hash function, fuzzy extractor, sqalar point multiplication, symmetric key operation, and CRT operation as T_h, T_{fe}, T_m, T_S, T_C, respectively. The exclusive-OR operation is not accomodated in computational cost of comparative schemes, as it takes negligible cost on computation [31].

The Table IV exhibits the comparison of computational overheads and delay for the proposed scheme and other studies [23], [25] - [33] as 30.59ms, 20.82ms, 27.24ms, 38.39ms, 33.51ms, 30.07ms, 101.58ms, 41.05ms, 29.33ms, 31.93ms and 22.55ms, respectively. It is evident that the schemes [23]-[25], [28], [31] and [33] bear less computational overheads and delay than proposed scheme SAWPS,

Figure 7. Computational cost

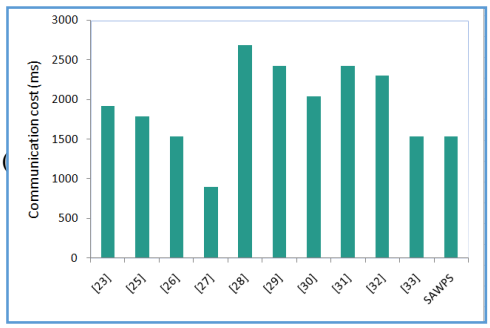
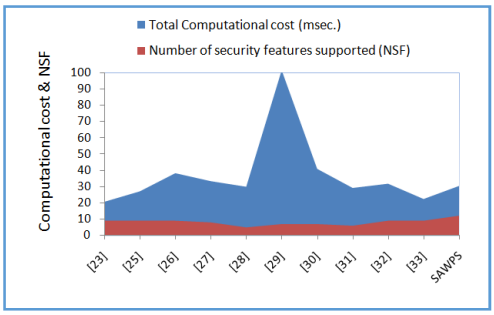


Figure 6. Communication latency



while the schemes [26]-[27], [29]-[30], [32] incur more computational overheads and delay than our scheme. The Table V summarizes the comparative analysis of security attributes of proposed scheme and other studies [23], [25] - [33]. It is obvious that the scheme [23] is vulnerable to previliged insider attack. The scheme [25] is prone to impersonation attack and does not provide mutual authentication to its participants. The scheme [26] does not resist against offline password guessing threat, and is unable to confer perfect forward secrecy to the subscribers. The scheme [27] does not ensure anonymity to the user and cannot resist offline-password guessing attack. The scheme [28] does not ensure mutual authentication to its entities. In addition, it is prone to sensor node capture attack, stolen smart card attack, desynchronizatin attack, previliged insider attack and DoS threat. The scheme [29] is susceptible to sensor node capture attack, previliged insider attack and offline password guessing threat. The scheme [30] does not fully support anonymity and mutual authentication, and is also prone to impersonation threat and sensor node capture threats. Likewise, the scheme [31] does not support mutual authentication and perfect forward secrecy, and is also vulnerable to impersonation threat, DoS threat, replay attack and offline password guessing attack. The scheme [32] is prone to de-synchronization attack. Similarly, the scheme [33] is prone to previleged insider attack and desynchronization attack. For computing the communicational costs of compared protocols, we assume that the communication messages such as user's identity

Table III: Experimental cost of primitives

Operations	U_i	*GWC*	SN_j
T_h	0.92	0.12	2.34
T_S	1.61	0.19	4.05
T_m	6.218	0.997	22.80
T_C	0.15	0.02	0.09
$T_{fe} \approx T_m$	6.218	0.997	22.80

Table IV: Computational costs

	U_i	GWC	SN_j	Total Computational cost (msec.)
[23]	$9T_h$	$7T_h$	$5T_h$	$21T_h \approx_{20.82}$
[25]	$12T_h$	$18T_h$	$6T_h$	$36T_h \approx_{27.24}$
[26]	$T_{fe}+ 16T_h$	$9T_h$	$7T_h$	$T_{fe}+ 32T_h \approx_{38.39}$
[27]	$T_{fe}+ 10T_h+ T_S$	$3T_h+ 2T_S$	$5T_h+ T_S$	$T_{fe}+ 18T_h+4T_s \approx_{33.51}$
[28]	$T_{fe}+ 11T_h$	$17T_h$	$5T_h$	$T_{fe}+ 33T_h \approx_{30.07}$
[29]	$T_{fe}+ 8T_h+ 3T_m$	$8T_h+ T_m$	$4T_h+ 2T_m$	$T_{fe}+20T_h+ 6T_m \approx_{101.58}$
[30]	$11T_h +T_{fe}$	$11T_h$	$10\ T_h$	$T_{fe} +32T_h \approx_{41.05}$
[31]	$13T_h +T_{fe}$	$15T_h$	$4T_h$	$T_{fe} +32T_h \approx_{29.33}$
[32]	$11T_h +T_{fe}$	$13T_h$	$6T_h$	$T_{fe} +30T_h \approx_{31.93}$
[33]	$4T_h +T_{fe}$	$8T_h$	$5T_h$	$17T_h +T_{fe} \approx_{22.55}$
SAWPS	$8T_h +T_{fe}$	$9T_h+ T_S$	$5T_h+ T_S$	$T_{fe}+22T_h+ 2T_S \approx_{30.59}$

Table V: Security Attributes and Comparison

Schemes	[23]	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	SAWPS
Comm. Cost	1920	1792	1536	896	2688	2432	2048	2432	2304	1536	1536

Table VI: Security Attributes and Comparison

	[23]	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	SAWPS
ST_a	*S*	*S*	*S*	*w*	*w*	*w*	*w*	*S*	*S*	*S*	*S*
ST_b	*S*	*w*	*S*	*S*	*S*	*S*	*w*	*w*	*w*	*w*	*S*
ST_c	*S*	*w*	*S*	*S*	*S*	*S*	*w*	*w*	*S*	*S*	*S*
ST_d	*S*	*S*	*S*	*w*	*w*	*w*	*w*	*S*	*S*	*S*	*S*
ST_e	*S*	*S*	*S*	*S*	*S*	*S*	*S*	*S*	*S*	*S*	*S*
ST_f	*w*	*S*	*S*	*S*	*w*	*w*	*w*	*S*	*S*	*w*	*S*
ST_g	*S*	*S*	*S*	*S*	*w*	*S*	*S*	*w*	*S*	*S*	*S*
ST_h	*S*	*S*	*w*	*S*	*S*	*S*	*S*	*w*	*S*	*S*	*S*
ST_i	*S*	*S*	*S*	*S*	*w*	*S*	*S*	*S*	*w*	*w*	*S*
ST_j	*S*	*S*	*S*	*S*	*S*	*S*	*S*	*w*	*S*	*S*	*S*
ST_k	*S*	*S*	*S*	*S*	*w*	*S*	*S*	*S*	*S*	*S*	*S*
ST_l	*S*	*S*	*w*	*w*	*w*	*w*	*S*	*w*	*S*	*S*	*S*

ST_a: Anonymity and Unlinkability, ST_b: Mutual authentication, ST_c: Safe against impersonation threat, ST_d: Safe against sensor node capture attack, ST_e: Safe against Man-In-The-Middle attack, ST_f: Safe against privileged insider attack, ST_g: Safe against DoS threat, ST_h: perfect forward secrecy, ST_i: Safe against desynchronization attack, ST_j: Safe against replay attack, ST_k: Safe against stolen smart card attack, ST_l: Safe against online/offline password guessing attack, *S*: Security Trait is strong, *w*: Security Trait is weak

ID_{Ui}, hash function $h(.)$, random nonce generation, symmetric encryption/decryption, ECC point, and timestamp take 160-bits, 256-bits, 160-bits, 128-bits, 320-bits (160+160) and 32-bits, respectively. The communication cost for SAWPS and the compared schemes [23], [25] - [33] are shown in Table V as well as depicted in Fig. 6. The cost of communication for SAWPS is 1536 bits which is less than the cost of [23]-[25], [28]-[32] as 1920, 1792, 2688, 2432, 2048, 2432, respectively. Although, this cost for SAWPS is equivalent to [26] and [33], and more than [27], yet the SAWPS is more secure than those schemes as shown in Table VI and Fig. 7.

VII. CONCLUSION

The deployment of smart agriculture attributes to the increasing use of wireless sensor devices for helping the farmers improve their agricultural yields and reduce costs. However, adopting wireless technology variants such as wearable plant sensors and devices might have security concerns for its inherent limitations of the technology. In the wake of escalating occurences of security breaches, a novel authenticated key exchange technique (SAWPS) has been proposed to verify the authenticity of stakeholders associated with an agricultural ecosystem. The proposed scheme is resistant against known threats such as ESL and other forgery threats besides supporting anonymity. The informal theoretical analysis along with formal rigorous analysis based on Real-or-Random (RoR) model is demonstrated for verifying the security properties of SAWPS. It can be witnessed from the the presented findings that performance results demonstrate the efficiency and effectiveness of SAWPS over other contemporary studies. In future, the proposed system can be extended to monitor the wearable plant sensors by enabling ecosystems using other wireless communication channels such as WiFi, Bluetooth, and ZigBee, etc.

Acknowledgement

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University, for funding this work through large group Research Project under grant number RGP2/238/44.

REFERENCES

[1] Ojha, T., Misra, S., & Raghuwanshi, N. S. (2015). Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. *Comp. and electr. in agriculture*, *118*, 66-84

[2] Zhou, Y., Fang, Y., & Zhang, Y. (2008). Securing wireless sensor networks: a survey. *IEEE Comm. Surveys & Tutorials*, *10*(3), 6-28.

[3] Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks, 36, 152-176

[4] Gope, P., Das, A. K., Kumar, N., & Cheng, Y. (2019). Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE trans. on industrial inform., 15(9), 4957-4968.

[5] Shabaz, M., & Soni, M. (2024). Adaptive enhancement of spatial information in adverse weather. Spatial Information Research, 1-12.

[6] Abbasinezhad-Mood, D., Mazinani, S. M., Nikooghadam, M., & Ostad-Sharif, A. (2020). Efficient provably-secure dynamic ID-based authenticated key agreement scheme with enhanced security provision. *IEEE Trans. on Dep. and Secure Comp.*, *19*(2), 1227-1238

[7] Abdi Nasib Far, H., Bayat, M., Kumar Das, A., Fotouhi, M., Pournaghi, S. M., &Doostari, M. A. (2021). LAPTAS: lightweight anonymous privacy-

preserving three-factor authentication scheme for WSN-based IIoT. *Wireless Networks*, *27*, 1389-1412.

[8] M.L. Das, Two-factor user authentication in wireless sensor networks, IEEE Trans. Wirel. Commun. 8 (3) (2009) 1086–1090.

[9] D. He, Y. Gao, S. Chan, C. Chen, J. Bu, An enhanced two-factor user authentication scheme in wireless sensor networks., Ad Hoc Sensor Wirel. Netw. 10 (4)(2010) 361–371.

[10] M.K. Khan, K. Alghathbar, Cryptanalysis and security improvements of two factor user authentication in wireless sensor networks, Sensors 10 (3) (2010) 2450–2459.

[11] T.-H. Chen, W.-K. Shih, A robust mutual authentication protocol for wireless sensor networks, ETRI J. 32 (5) (2010) 704–712

[12] B. Vaidya, D. Makrakis, H. Mouftah, Two-factor mutual authentication with key agreement in wireless sensor networks, Secur. Commun. Netw. 9 (2) (2016) 171–183.

[13] W.B. Hsieh, J.S. Leu, A robust user authentication scheme using dynamic identity in wireless sensor networks, Wirel. Pers. Comm. 77 (2) (2014) 979–989.

[14] J. Kim, D. Lee, W. Jeon, Y. Lee, D. Won, Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks, Sensors 14 (4) (2014) 6443–6462.

[15] M. Turkanović, B. Brumen, M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Netw. 20 (2014) 96–112.

[16] C.-C. Chang, H.-D. Le, A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks, IEEE Trans. Wirel. Commun. 15 (1) (2016) 357–366.

[17] M.S. Farash, M. Turkanović, S. Kumari, M. Hölbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, Ad Hoc Netw. 36 (2016) 152–176.

[18] R. Amin, G. Biswas, A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, Ad Hoc Netw. 36 (2016) 58–80.

[19] Y. Lu, L. Li, H. Peng, Y. Yang, An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks, Sensors 16 (6) (2016) 837

[20] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, S.-S. Yeo, Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks, Multimedia Syst. 21 (1) (2015) 49–60.

[21] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, M.K. Khan, A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity, Secur. Commun. Netw. 9 (15) (2015) 2643–2655.

[22] F. Wu, L. Xu, S. Kumari, X. Li, An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks, Multimedia Syst. 23 (2) (2017) 195–205.

[23] S. Kumari, H. Om, Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines, *Comput. Netw*. 104 (2016) 137–154

[24] F. Wu, L. Xu, S. Kumari, X. Li, A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security, J. Ambient Intell. Humanized Comput. 8 (1) (2017) 101–116

[25] R. Amin, S.H. Islam, G. Biswas, M.K. Khan, L. Leng, N. Kumar, Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks, Comput. Netw. 101 (2016) 42–62

[26] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloudbased industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[27] Y. Chen, Y. Ge, Y. Wang, and Z. Zeng, "An improved three-factor user authentication and key agreement scheme for wireless medical sensor networks," *IEEE Access*, vol. 7, pp. 85440–85451, 2019.

[28] A. O. Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Fut. Gen. Comp. Syst.*, vol. 100, pp. 882–892, 2019.

[29] X. Li, J. Peng, M. S. Obaidat, F. Wu, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Syst. J.*, vol. 14, no. 1, pp. 39–50, 2020.

[30] C. Meshram, M. S. Obaidat, C. C. Lee, and S. G. Meshram, "An efficient, robust, and lightweight subtree-based three-factor authentication procedure for large-scale DWSN in random oracle," *IEEE Syst. J.*, vol. 15, no. 4, pp. 4927–4938, Dec. 2021.

[31] F. Wu, X. Li, L. Xu, P. Vijayakumar, and N. Kumar, "A novel three-factor authentication protocol for wireless sensor networks with IoT notion," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1120–1129, Mar. 2021.

[32] Li, Y., & Tian, Y. (2022). A lightweight and secure three-factor authentication protocol with adaptive privacy-preserving property for wireless sensor networks. *IEEE Systems Journal*, 16(4), 6197-6208

[33] Fatima, M. N., Obaidat, M. S., Mahmood, K., Shamshad, S., Saleem, M. A., & Ayub, M. F. (2023). Privacy-Preserving Three-Factor Authentication Protocol for Wireless Sensor Networks Deployed in Agricultural Field. ACM Trans. on Sensor Networks.

[34] Canetti, R.; Goldreich, O.; Halevi, S. The random oracle methodology, revisited. J. ACM (JACM) 2004, 51, 557–594.

[35] D. Dolev and A. Yao, ''On the security of public key protocols,'' IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198–208, Mar. 1983

[36] Ahmad, T., Li, X. J., & Seet, B. C. (2016, June). A self-calibrated centroid localization algorithm for indoor ZigBee WSNs. In 2016 8th IEEE Int. Conf. on Comm. Soft. and Netw. (ICCSN) (pp. 455-461).

[37] Shahidinejad, A. and Abawajy, J., 2024. An All-Inclusive Taxonomy and Critical Review of Blockchain-Assisted Authentication and Session Key Generation Protocols for IoT. ACM Computing Surveys.

[38] Chen, C. M., Miao, Q., Khan, F., Srivastava, G., & Kumari, S. (2023). Sustainable Secure Communication in Consumer-Centric Electric Vehicle Charging in Industry 5.0 Environments. IEEE Transactions on Consumer Electronics.

[39] Ali, Z., Ghani, A., Khan, I., Chaudhry, S. A., Islam, S. H., & Giri, D. (2020). A robust authentication and access control protocol for securing wireless healthcare sensor networks. J. of Inf. Sec. and Apps., 52, 102502.

[40] Ghani, A., Naqvi, H., Sher, M., Khan, M. A., Khan, I., & Irshad, A. (2016). Spread spectrum based energy efficient collaborative communication in wireless sensor networks. PloS one, 11(7), e0159069.

[41] Ahmad, T., Usman, M., Murtaza, M., Benitez, I. B., Anwar, A., Vassiliou, V., & Al-Ammar, E. A. (2024). A Novel Self-Calibrated UWB Based Indoor Localization Systems for Context-Aware Applications. IEEE Transactions on Consumer Electronics.

[42] Irshad, A., Alzahrani, B. A., Albeshri, A., Alsubhi, K., Nayyar, A., & Chaudhry, S. A. (2023). SPAKE-DC: A Secure PUF Enabled Authenticated Key Exchange for 5G-based Drone Communications. IEEE Transactions on Vehicular Technology

[43] Chaudhry, S. A., Irshad, A., Yahya, K., Kumar, N., Alazab, M., & Zikria, Y. B. (2021). Rotating behind privacy: An improved lightweight authentication scheme for cloud-based IoT environment. ACM Transactions on Internet Technology (TOIT), 21(3), 1-19

[44] Mehmood, A., Nadeem, A., Ashraf, M., Siddiqui, M. S., Rizwan, K., & Ahsan, K. (2020). A fall risk assessment mechanism for elderly people through muscle fatigue analysis on data from body area sensor network. IEEE Sensors Journal, 21(5), 6679-6690.

[45] Zia, M., Obaidat, M. S., Mahmood, K., Shamshad, S., Saleem, M. A., & Chaudhry, S. A. (2022). A provably secure lightweight key agreement protocol for wireless body area networks in healthcare system. IEEE Transactions on Industrial Informatics, 19(2), 1683-1690