IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 June 2024, accepted 7 August 2024, date of publication 12 August 2024, date of current version 26 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3442619

RESEARCH ARTICLE

Trust-Enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management

VINCENT OMOLLO NYANGARESI[1,2], EESA ALSOLAMI[3], AND MUSHEER AHMAD[4]

[1]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya
[2]Department of Applied Electronics, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, India
[3]Department of Information Security, University of Jeddah, Jeddah 21493, Saudi Arabia
[4]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India

Corresponding author: Musheer Ahmad (mahmad9@jmi.ac.in)

ABSTRACT Trust and energy efficiency are key requirements in remote sensing devices, which are frequently deployed in electronic commerce supply chain management. This remote sensing is facilitated by wireless sensor networks (WSNs) which have been integrated into the e-commerce landscape. These WSNs provide various services, including product tracking, monitoring, optimization and design evolution. This integration is evident in Logistics 4.0, whose aim is to enhance adaptability, intelligence and resilience in supply chain management and logistics. However, due to the limited energy, memory, communication and computing power of the sensors deployed in WSNs, numerous energy consumption reduction approaches have been proposed. Nevertheless, these techniques often overlook security and privacy aspects, which are crucial for fostering trust in an e-commerce ecosystem. Consequently, various schemes have been developed to bridge this gap. Unfortunately, these protocols often exhibit vulnerabilities and privacy loopholes that can compromise trust among e-commerce stakeholders. In this paper, we propose a trust-enabled energy efficient protocol for secure remote sensing in supply chain management. Performance evaluation demonstrates that our protocol incurs the lowest energy, computation and communication complexities compared to existing solutions. Additionally, it provides essential security features, including session key agreement, mutual authentication, key secrecy, untraceability and anonymity. These features are critical for trust preservation in e-commerce. Our semantic security analysis confirms the protocol's resilience against various attacks. In addition, its formal security analysis using the Real-Or-Random (ROR) model validates the security of the negotiated session key.

INDEX TERMS E-commerce, supply chain management, trust, wireless sensor networks, energy-efficiency, security.

I. INTRODUCTION

Electronic commerce (e-commerce) encompasses the buying and selling of goods and services over the internet [1]. This paradigm integrates information processing technologies, computing devices, and electronic communication platforms into commercial activities [2]. For example, WSNs have been employed to facilitate digital management and effective monitoring of cold chain logistics transportation [3]. Additionally, the Internet of Things (IoT) has been deployed in value chains to enable real-time monitoring of resource inventory [4]. This remote monitoring, data collection and information exchange within diverse business environments streamline decision-making and optimization of business processes. In the context of cold chain logistics, WSNs gather compartment environment data during transportation and transmit it to the logistics monitoring center [5]. However, in-depth research on WSN-based cold chain temperature monitoring remains limited, particularly from the perspective of low power consumption [6]. Moreover, secure transmission of the sensed data poses challenges due to the utilization of open public channels [7]. Furthermore, privacy and security preservation face challenges in the face of botnet attacks [8].

To enhance security and privacy, various authentication and key agreement protocols have been developed. However, most of these protocols deploy complex algorithms which require extensive resources. WSNs are constrained in terms of power, memory, computation, communication, and battery life. Therefore, employing highly complex security

The associate editor coordinating the review of this manuscript and approving it for publication was Guangjie Han.

algorithms can easily drain the sensor battery due to excessive energy consumptions.

A. MOTIVATION

WSNs hold immense promise for the establishment of Logistics 4.0. This paradigm seeks to enhance adaptability, intelligence, as well as resilience in supply chain management and logistics within the e-commerce landscape. Furthermore, by integrating WSNs with technologies like blockchains, transparency, trust, and traceability can be elevated for all stakeholders involved in supply chain management. However, WSNs remain susceptible to a variety of attacks. This necessitates the development of robust security mechanisms. Unfortunately, most of the existing security solutions rely on energy-intensive technologies like blockchains. Consequently, there is an urgent need for a truly energy-efficient protocol that can bolster trust, security, and privacy in WSN-enabled e-commerce environments.

B. MATHEMATICAL PRELIMINARIES

In this paper, we deploy fuzzy extraction in which $Gen(.)$ is taken as a probabilistic fuzzy biometric generator function while $Rep(.)$ is regarded as a deterministic fuzzy biometric reproduction function. Basically, a fuzzy extractor is deployed to solve noise problems that frequently occur in biometric inputs. Here, β_i denotes user biometric data, which serves as the input to the Gen (.) algorithm. This algorithm generates two outputs; the private biometric secret key ε_i, and the public reproduction token μ_i associated with β_i. Therefore, $Gen(.)$ $(\beta_i) = (\varepsilon_i, \mu_i)$, where μ_i is utilized to recover the key values through noise elimination. On the other hand, the Rep agorithm restores ε_i^* from helper string μ_i and the entered biometric data β_i^*. As such, Rep $(\beta_i^*, \mu_i) = \varepsilon_i^*$. To ensure accurate recovery of ε_i^*, the metric spacial distance between β_i and β_i^* should be within some defined tolerance level for the fuzzy extractor.

C. RESEARCH CONTRIBUTIONS

The primary contributions of this paper are as follows:

- Energy-Efficient Protocol Design: We introduce a novel protocol that utilizes fuzzy extraction and a collision-resistant one-way hashing function to achieve energy efficiency. This renders this protocol well-suited for WSN-enabled e-commerce applications.
- Rigorous Formal Security Analysis: We conduct a comprehensive formal security analysis using the Real-Or-Random (ROR) model to demonstrate that the negotiated session key is provably secure against various cryptographic attacks.
- Semantic Security Analysis: We perform an in-depth semantic security analysis to demonstrate that our protocol fosters trust in e-commerce applications by providing key agreement, mutual authentication, anonymity, untraceability, and key secrecy. Additionally, we show its resilience against various attacks.
- Comparative Performance Evaluation: We conduct a comparative performance analysis to showcase that our proposed protocol outperforms existing solutions in terms of computation and communication complexities.

The remainder of this paper is structured as follows: Section II delves into related works, while Section III meticulously describes the system model of the proposed protocol. Section IV presents a rigorous security analysis, while Section V comprehensively discusses the performance evaluation. Finally, Section VI concludes the paper and outlines potential avenues for future research.

II. RELATED WORKS

Various techniques have been developed in recent years to enhance energy efficiency, security, privacy, and trust in WSNs. For instance, energy-aware routing techniques are proposed in [9] and [10], while network lifetime maximization schemes are presented in [11] and [12]. Similarly, efficient, low-latency, and energy-consumption minimization techniques are developed in [13] and [14]. However, these algorithms fail to address trust-related issues such as security and privacy. In response to this gap, a scheme is proposed in [15] to establish trust in an e-commerce environment. However, this model lacks evaluation against other attacks and its performance evaluation is missing.

Several protocols have been developed to address these challenges. For example, two-factor authentication protocols are presented in [16] and [17]. While the protocol in [17] offers mutual authentication and preserves both privacy and user anonymity, it remains vulnerable to session key exposure and impersonation attacks. The scheme in [18] addresses the shortcomings of [17] by providing resilience against impersonation attacks. However, it fails to preserve sensor anonymity [19].

In an effort to further bolster trust in e-commerce systems, three-factor authentication schemes have been introduced in [20], [21], [22], and [23]. While the protocol in [20] safeguards user anonymity and shields against replay attacks, it remains susceptible to Man-in-the-Middle (MitM) attacks [19]. On the other hand, the scheme in [21] provides mutual authentication but falls short in protecting against offline password guessing attacks [18]. Similarly, the protocol in [22] offers perfect forward secrecy but is vulnerable to sensor node spoofing attacks [24]. Lastly, the scheme in [23] lacks resilience against offline guessing attacks [25].

It is evident that most of the current energy consumption reduction techniques for e-commerce do not consider security and privacy which can help boost trust in business transactions. It is also clear that although numerous schemes have been developed to offer both privacy and security, most of them have many shortcomings which need to be addressed. The proposed protocol is demonstrated to be both energy efficient and provably secure and hence solves some of these problems.

III. SYSTEM MODEL

The proposed protocol facilitates e-commerce product tracking and monitoring using WSNs. During the tracking process, sensors gather product information, including identity, unique

composition, and location. This data is then relayed to the gateway node. Additionally, the sensors continuously monitor the product's real-time conditions and environment. This enables the generation of notifications and alerts to relevant stakeholders. Through this comprehensive tracking and monitoring, operations control and optimization can be streamlined. Furthermore, it can inform design evolution by leveraging product lifecycle feedback data. Table 1 summarizes the notations employed throughout this paper.

TABLE 1. List of deployed notations.

Symbol	Description
SN_j	Sensor node j
U_i	User i
MD_i	Mobile device for user i
BID_k	Unique identity of the k^{th} branch
R_i	Random nonce i
SID_j	Unique identity of the j^{th} sensor node
h (.)	Collision-resistant one-way hash function
β_i	User biometric data
ID_{GWN}	Unique identity of the GWN
ε_i	Private biometric secret key
μ_i	Public reproduction token associated with β_i
GSK_j	Long term secret key for the GWN
Gen(.)	Fuzzy biometric generator function
T_i	Timestamp i
ΔT	Permissible transmission delay
Rep (.)	Fuzzy biometric reproduction function
SSK_j	Long term secret key for the SN_j
K_{SN}	Session key derived at SN_j
$SK_{G\text{-}S}$	Shared key between GWN and SN_j
UID_i	Unique identity of user i
K_{SM}	Session key derived at MD_i
PW_i	Password for user i
$\|\|$	Concatenation operation
$\oplus$	XOR operation

Our protocol's network model comprises of sensor nodes (SNs), a gateway node (GWN), and users. Sensor nodes perform tasks like tracking and monitoring. This facilitates activities such as optimization and design evolution in e-commerce. Figure 1 depicts the proposed network model. As illustrated in Figure 1, users employ mobile devices (MDs) to interact with sensor nodes through the GWN. During trust establishment, system setup, registration, login, mutual authentication, and key negotiation are performed. After each successful authentication session, security token updates must occur. These phases are described in detail in the following subsections.

A. SYSTEM SETUP PHASE

Consider an organization with n branches, each equipped with a network of sensors. During the system initialization phase, the GWN generates its identity ID_{GWN} and BID_k as the unique identity for the k^{th} branch as shown in Figure 2.

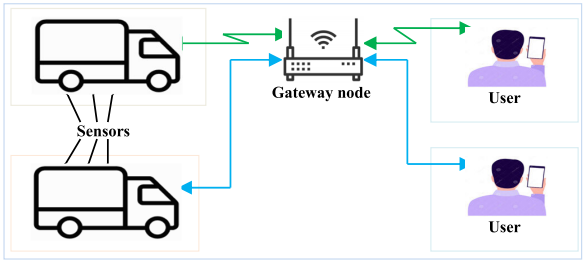

FIGURE 1. Proposed network model.

Next, it inializes m as the number of sensors to be deployed within a given branch.

B. SENSOR REGISTRATION

The following three steps are followed to register sensor node j to the GWN.

Step 1: The GWN generates unique identity SID_j for each sensor deployed in the k^{th} branch. Next, it generates GSK_j and SSK_j as the long term secret keys for the GWN and sensor node SN_j respectively.

Step 2: The GWN selects some one-way hashing function $h(.)$ and computes $SK_{G-S} = h\ (BID_k||SID_j||GSK_j||SSK_j)$ as the shared key between the GWN and SN_j. This is followed by the construction of registration message $Rg_1 = \{ID_{GWN}, BID_k, SID_j, SK_{G-S}, h(.)\}$. Finally, Rg_1 is forwarded to SN_j over secured channels as shown in Figure 2.

Step 3: GWN stores parameter set $\{ID_{GWN}, \{BID_k | 1 \leq k \leq n\}, \{(SID_j, SK_{G-S}) | 1 \leq j \leq m\}, GSK_j, h(.)\}$ in its repository.

C. USER REGISTRATION

In order to access the data from a particular sensor deployed in a given branch, user U_i needs to register at the GWN. This is accomplished using his/her mobile device MD_i that is equipped with biometric sensor. The following 4 steps are executed to accomplish this process.

Step 1: User U_i chooses UID_i and PW_i as his/her unique identity and password respectively. Next, random nonce R_1 is generated by MD_i before parameters $A_1 = h\ (UID_i||R_1)$ and $A_2 = h\ (PW_i||R_1)$ are derived. It then constructs registration message $Rg_2 = \{A_1, h(.)\}$ that is transmitted to the GWN over secure channels as shown in Figure 2.

Step 2: Upon receiving message Rg_2, the GWN computes $A_3 = h\ (A_1||GSK_j)$, transient parameter $A_4 = h\ (BID_k||A_3||ID_{GWN})$ and $A_5 = BID_k \oplus h\ (A_1||A_3)$. Next, it composes registration message $Rg_3 = \{A_3, A_4, A_5, BID_k, ID_{GWN}, h\}$ that it sends to U_i over trustworthy channels.

Step 3: On getting message Rg_3, user U_i imprints biometric data β_i onto the sensor of MD_i. This is followed by the computation of $Gen\ (\beta_i) = (\varepsilon_i, \mu_i)$, where ε_i is the private biometric key and μ_i is the public reproduction token associated with β_i.

Step 4: The MD_i computes parameters $B_1 = R_1 \oplus h\ (\varepsilon_i||UID_i||PW_i)$, $B_2 = h\ (A_3||A_4||R_1||\varepsilon_i)$ and $B_3 = A_3 \oplus h\ (R_1||A_1||A_2||\varepsilon_i)$. Finally, the MD_i stores parameter set

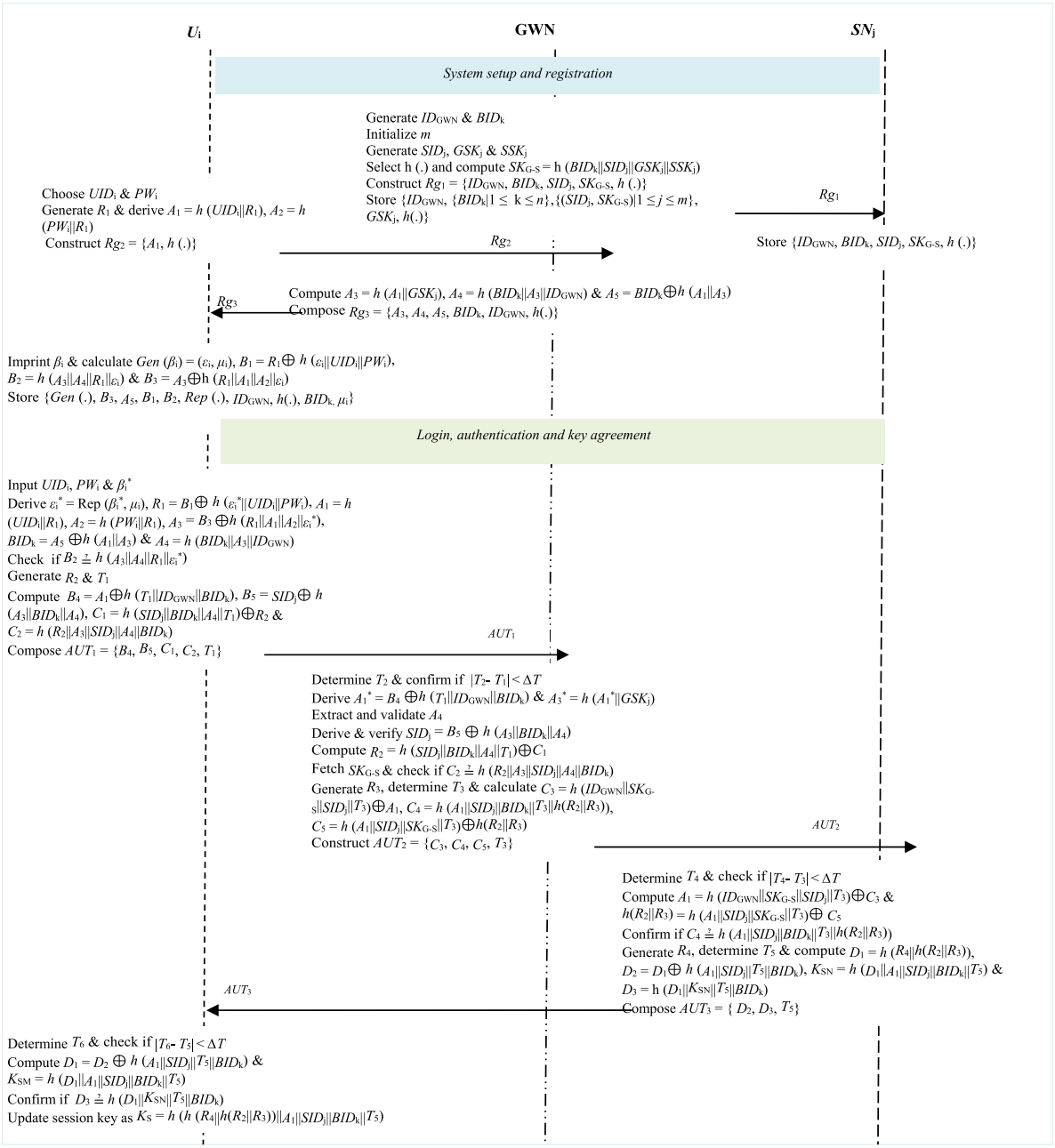

FIGURE 2. System setup, registration, login, authentication and key agreement phases.

{Gen(.), B_3, A_5, B_1, B_2, Rep(.), ID_{GWN}, h(.), BID_k, μ_i} in its memory.

D. LOGIN, AUTHENTICATION AND AGREEMENT

In this phase, user U_i is validated via the tokens that were input during the login phase as well as the security parameters stored in the MD_i. These procedures are executed over public channels using the challenge-response interaction mode. Here, U_i sends login request which has to be verified by both the GWN and SN_j located in a given branch. Basicaly, a particular user has access to real-time data from some specific sensors located in various branches. The following steps are executed during this phase.

Step 1: The U_i inputs UID_i, PW_i and β_i^* onto the MD_i. This is followed by the derivation of $\varepsilon_i^* = Rep\ (\beta_i^*, \mu_i)$, $R_1 = B_1 \oplus h\ (\varepsilon_i^*||UID_i||PW_i)$, $A_1 = h\ (UID_i||R_1)$, $A_2 = h\ (PW_i||R_1)$, $A_3 = B_3 \oplus h\ (R_1||A_1||A_2||\varepsilon_i^*)$, $BID_k = A_5 \oplus h\ (A_1||A_3)$ and $A_4 = h\ (BID_k||A_3||ID_{GWN})$.

Step 2: The MD_i then checks if $B_2 \stackrel{?}{=} h\ (A_3||A_4||R_1||\varepsilon_i^*)$ such that the session is aborted when this verification flops. Otherwise, the MD_i generates random nonce R_2 and establishes the current timestamp T_1. Next, it derives $B_4 = A_1 \oplus h\ (T_1||ID_{GWN}||BID_k)$, $B_5 = SID_j \oplus h\ (A_3||BID_k||A_4)$, $C_1 = h\ (SID_j||BID_k||A_4||T_1) \oplus R_2$ and $C_2 = h\ (R_2||A_3||SID_j||A_4||BID_k)$. Finally, it constructs message $AUT_1 = \{B_4, B_5, C_1, C_2, T_1\}$ that is

forwarded to the GWN over public channels as shown in Figure 2.

Step 3: After getting message AUT_1 at timestamp T_2, the GWN determines if $|T_2\text{-}\ T_1| < \Delta T$. If this condition does not hold, the message is flagged as a replay and the session is terminated. Otherwise, it computes $A_1^* = B_4 \oplus h\ (T_1||ID_{\text{GWN}}||BID_{\text{k}})$ and $A_3^* = h\ (A_1^*||GSK_{\text{j}})$.

Step 4: The GWN extracts A_4 and confirms the existence of A_3^* in its repository. If this verification is unsuccessful, the session is aborted. Otherwise, the GWN derives $SID_{\text{j}} = B_5 \oplus h\ (A_3||BID_{\text{k}}||A_4)$ and determines its existence in its repository. Here, the session is terminated if SID_{j} cannot be found in GWN's database. Otherwise, it derives $R_2 = h\ (SID_{\text{j}}||BID_{\text{k}}||A_4||T_1) \oplus C_1$.

Step 5: GWN fetches $SK_{\text{G-S}}$ corresponding to this particular SID_{j} and confirms whether $C_2 \stackrel{?}{=} h\ (R_2||A_3||SID_{\text{j}}||A_4||BID_{\text{k}})$. Basically, the session is aborted if this verification flops. Otherwise, GWN generates random nonce R_3 and establishes the current timestamp T_3.

Step 6: The GWN computes $C_3 = h\ (ID_{\text{GWN}}||SK_{\text{G-S}}||SID_{\text{j}}||T_3) \oplus A_1$, $C_4 = h\ (A_1||SID_{\text{j}}||BID_{\text{k}}||T_3||h(R_2||R_3))$ and $C_5 = h\ (A_1||SID_{\text{j}}||SK_{\text{G-S}}||T_3) \oplus h(R_2||R_3)$. Next, it composes message $AUT_2 = \{C_3, C_4, C_5, T_3\}$ that is transmitted to SN_{j} over public channels.

Step 7: Upon receiving message AUT_2 at timestamp T_4, the SN_{j} confirms if $|T_4\text{-}\ T_3| < \Delta T$. Here, the request is marked as a replay and the session is terminated upon verification failure. Otherwise, it computes $A_1 = h\ (ID_{\text{GWN}}||SK_{\text{G-S}}||SID_{\text{j}}||T_3) \oplus C_3$ and $h(R_2||R_3) = h\ (A_1||SID_{\text{j}}||SK_{\text{G-S}}||T_3) \oplus C_5$. Next, it establishes whether $C_4 \stackrel{?}{=} h\ (A_1||SID_{\text{j}}||BID_{\text{k}}||T_3||h(R_2||R_3))$ such that message AUT_2 is rejected on validation failure. Otherwise, it generates random nonce R_4 and determines the current timestamp T_5.

Step 8: The SN_{j} computes parameters $D_1 = h\ (R_4||h(R_2||R_3))$, $D_2 = D_1 \oplus h\ (A_1||SID_{\text{j}}||T_5||BID_{\text{k}})$, session key $\text{K}_{\text{SN}} = h\ (D_1||A_1||SID_{\text{j}}||BID_{\text{k}}||T_5)$ and $D_3 = \text{h}\ (D_1||\text{K}_{\text{SN}}||T_5||BID_{\text{k}})$. It then constructs message $AUT_3 = \{D_2, D_3, T_5\}$ which is forwarded to the MD_{i} over public channels.

Step 9: On receiving message AUT_3 at timestamp T_6, the MD_{i} checks if $|T_6\text{-}\ T_5| < \Delta T$. Essentially, this message is flagged as a replay and the session is aborted upon verification failure. Otherwise, it derives $D_1 = D_2 \oplus h\ (A_1||SID_{\text{j}}||T_5||BID_{\text{k}})$ and session key $\text{K}_{\text{SM}} = h\ (D_1||A_1||SID_{\text{j}}||BID_{\text{k}}||T_5)$.

Step 10: The MD_{i} confirms whether $D_3 \stackrel{?}{=} h\ (D_1||\text{K}_{\text{SN}}||T_5||BID_{\text{k}})$, terminating the session if this condition does not hold. Otherwise, the MD_{i} has successfully authenticated the SN_{j}. At the end of the current communication session, both the MD_{i} and SN_{j} update the session key as $\text{K}_{\text{S}} = h(h(R_4||h(R_2||R_3))||A_1||SID_{\text{j}}||BID_{\text{k}}||T_5)$.

E. SECURITY TOKENS UPDATE PHASE

The goal of this phase is to refresh the user biometrics and password used to log into the MD_{i}, and by extension the SN_{j}. This may be occassioned by the compromise of these security tokens, or when there is need for frequent refreshments to enhance security. The following 4 steps are executed during this process.

Step 1: The user U_{i} inputs UID_{i}, PW_{i} and β_{i}^* onto the MD_{i}. This is followed by the derivation of parameters $\varepsilon_{\text{i}}^* = Rep\ (\beta_{\text{i}}^*, \mu_{\text{i}})$, $R_1 = B_1 \oplus h\ (\varepsilon_{\text{i}}^*||UID_{\text{i}}||PW_{\text{i}})$, $A_1 = h\ (UID_{\text{i}}||R_1)$, $A_2 = h\ (PW_{\text{i}}||R_1)$, $A_3 = B_3 \oplus h\ (R_1||A_1||A_2||\varepsilon_{\text{i}}^*)$, $BID_{\text{k}} = A_5 \oplus h\ (A_1||A_3)$ and $A_4 = h\ (BID_{\text{k}}||A_3||ID_{\text{GWN}})$.

Step 2: The MD_{i} confirms if $B_2 \stackrel{?}{=} h\ (A_3||A_4||R_1||\varepsilon_{\text{i}}^*)$ such that the tokens change request is rejected upon verification failure. Otherwise, the MD_{i} prompts the user to input new password and biometrics $PW_{\text{i}}^{\text{New}}$ and $\beta_{\text{i}}^{\text{New}}$ respectively.

Step 3: User U_{i} enters $PW_{\text{i}}^{\text{New}}$ and $\beta_{\text{i}}^{\text{New}}$ to the MD_{i} after which parameters $A_1 = h\ (UID_{\text{i}}||R_1)$, $A_2^{\text{New}} = h\ (PW_{\text{i}}^{\text{New}}||R_1)$, $(\varepsilon_{\text{i}}^{\text{New}}, \mu_{\text{i}}^{\text{New}}) = \text{Gen}\ (\beta_{\text{i}}^{\text{New}})$, $B_1^{\text{New}} = R_1 \oplus h\ (\varepsilon_{\text{i}}^{\text{New}}||UID_{\text{i}}||PW_{\text{i}}^{\text{New}})$, $B_2^{\text{New}} = h\ (A_3||A_4||R_1||\varepsilon_{\text{i}}^{\text{New}})$ and $B_3^{\text{New}} = A_3 \oplus \text{h}\ (R_1||A_1||A_2^{\text{New}}||\varepsilon_{\text{i}}^{\text{New}})$ are computed.

Step 4: The MD_{i} substitutes B_1, B_2 and B_3 with their updated versions B_1^{New}, B_2^{New} and B_3^{New} respectively in its memory.

IV. SECURITY ANALYSIS

To demonstrate that our scheme can boost trust in e-commerce applications, this section presents the analysis of its privacy and security features.

A. FORMAL SECURITY ANALYSIS

In this section, the widely used Real-Or-Random (ROR) model is deployed to show that the proposed protocol offers session key security. Here, the polynomial time adversary $\mathring{A}$ interacts with the q^{th} instance of each executing party, denoted as K^{q}. As such, we model $K_{U_i}^{q_1}$, $K_{GWN}^{q_2}$ and $K_{SN_j}^{q_3}$ as the q_1^{th}, q_2^{th} and q_3^{th} of the U_{i}, GWN and SN_{j} respectively. In addition, we model different queries such as *Reveal*(.), *Send*(.), *Corrupt*(.), *Execute*(.) and *Test*(.) that simulate real attacks.

In addition, all the parties (including $\mathring{A}$) have access to the one-way hash function h(.), which is collision-resistant and modeled as random oracle *Hash*(.). The detailed description of these queries is given in Table 2.

In *Hypothesis 1*, the security of the session key derived in our protocol under the ROR model is proved. This is faciliated by the five queries in Table 2.

Hypothesis 1: Let α and ρ denote the number of *Hash*(.) and *Send*(.) queries respectively. In addition, let φ and $|Hash|$ represent the number of bits in ε_{i} and the range space of the hashing function respectively. Moreover, we take τ and σ as the Zipf's parameters. Suppose that adversary $\mathring{A}$ runs in polynomial time t against our scheme. The advantage that $\mathring{A}$ has in breaking the semantic security of our protocol so as to access the session key K_{SM} negotiated between U_{i} and SN_{j} is approximated as,

$$Adv^{\mathring{A}}(t) \leq \frac{\alpha^2}{|Hash|} + 2\max\{\tau.\rho^{\sigma}, \frac{\rho}{2^{\varphi}}\} \quad (1)$$

TABLE 2. Adversarial queries.

Query	Description
Reveal (K^q)	Allows $\AA$ to access the current session key shared between K^q and its associate
Send (K^q, m)	Is an active attack where $\AA$ sends message m to instance K^q upon which K^q institutes an appropriate response
Test (K^q)	Permits $\AA$ to request K^q for the session key after which K^q probabilistically responds with the outcome of flipped fair coin Φ.
Execute ($K_{U_i}{}^{q_1}$, $K_{GWN}{}^{q_2}$, $K_{SN_i}{}^{q_3}$)	Facilitates the adversarial eavesdropping of messages exchanged among the U_i, GWN and SN_j
Corrupt ($K_{U_i}{}^{q_1}$)	Allows $\AA$ to obtain user ε_i and PW_i stored in lost or stolen MD_i

Proof: We let the polynomial time adversary $\AA$ execute four games, denoted as G_k, $k \in [0, 3]$. Here, $Succ_k$ represents an event that $\AA$ has accurately guessed random bit ϕ in G_k. We also let the probability of event ψ be denoted by $Pr[\psi]$. As such, the advantage that $\AA$ has in winning game G_k is represented as,

$$Adv^{\AA,G_k}(t) = \Pr[Succ_k] \tag{2}$$

G_0: This is the actual game played by $\AA$ against our protocol under the ROR model. It basically involves $\AA$ randomly selecting bit ϕ and hence,

$$Adv^{\AA}(t) = |2\left(Adv^{\AA,G_0}(t)\right) - 1| \tag{3}$$

G_1: In this game, adversary $\AA$ attempts eavesdropping all the messages exchanged during the login, authentication and key negotiation phase. These messages include $AUT_1 = \{B_4, B_5, C_1, C_2, T_1\}$, $AUT_2 = \{C_3, C_4, C_5, T_3\}$ and $AUT_3 = \{D_2, D_3, T_5\}$. This is facilitated by the launch of the *Execute* ($K_{U_i}^{q_1}$, $K_{GWN}^{q_2}$, $K_{SN_j}^{q_3}$) query. The goal is to obtain the session key negotiated during this phase. Therefore, the *Execute* (.) query is followed by the *Reveal* (K^q) and *Test* (K^q) queries whose aim is to ascertain whether the captured session key $K_S = h(h(R_4||h(R_2||R_3))||A_1||SID_j||BID_k||T_5)$ is real or is just an arbitrary key. Evidently, the derivation of K_S requires short term secrets (such as T_5, R_2, R_3 and R_4) and long term secrets (such as A_1, SID_j and BID_k). However, adversary $\AA$ does not have access to all these secrets. Therefore, eavesdropping messages AUT_1, AUT_2 and AUT_3 does not increase the chance of $\AA$ winning game G_1. As such, both G_0 and G_1 are indistinguishable and hence,

$$Adv^{\AA,G_1}(t) = Adv^{\AA,G_0}(t) \tag{4}$$

G_2: This is an active attack modeled by both *Send* (K^q, m) and *Hash* queries. This attack is launched during the login, authentication and key agreement phase. This is achieved by targettting the exchanged messages $AUT_1 = \{B_4, B_5, C_1, C_2, T_1\}$, $AUT_2 = \{C_3, C_4, C_5, T_3\}$ and $AUT_3 = \{D_2, D_3, T_5\}$. Here, $B_4 = A_1 \oplus h(T_1||ID_{GWN}||BID_k)$, $B_5 = SID_j \oplus h(A_3||BID_k||A_4)$, $C_1 = h(SID_j||BID_k||A_4||T_1) \oplus R_2$, $C_2 = h(R_2||A_3||SID_j||A_4||BID_k)$, $C_3 = h(ID_{GWN}||SK_{G-S}||SID_j||T_3) \oplus A_1$, $C_4 = h(A_1||SID_j||BID_k||T_3||h(R_2||R_3))$, $C_5 = h(A_1||SID_j||SK_{G-S}||T_3) \oplus h(R_2||R_3)$, $D_1 = h(R_4||h(R_2||R_3))$, $D_2 = D_1 \oplus h(A_1||SID_j||T_5||BID_k)$ and $D_3 = h(D_1||K_{SN}||T_5||BID_k)$.

It is clear that these ephemerals are protected by the collision-resistant one-way hashing function $h(.)$. In addition, random nonces (R_i), timestamps (T_i), identities (such as BID_k, SID_j, ID_{GWN}) and secret values (such as SK_{G-S}) are incorporated in the derivation of these ephemerals. As such, the *Send*(.) and *Hash*(.) queries executed by $\AA$ cannot result in any collision. Therefore, G_2 and G_1 are indistinguishable in spite of the simulation of the *Hash*(.) and *Send* (.) queries in G_2. By the birthday paradox, we have the following:

$$Adv^{\AA,G_1}(t) - Adv^{\AA,G_2}(t) \leq \frac{\alpha^2}{2(|Hash|)} \tag{5}$$

G_3: In this game, the adversary $\AA$ executes the *Corrupt* ($K_{U_i}^{q_1}$) query to facilitate the acquisition of parameter set $\{Gen(.), B_3, A_5, B_1, B_2, Rep(.), ID_{GWN}, h(.), BID_k, \mu_i\}$ stored in MD_i memory. Suppose that $\AA$ uses Zipf's law on passwords to verify some guessed passwords based on the extracted information $B_1 = R_1 \oplus h(\varepsilon_i||UID_i||PW_i)$ and $B_3 = A_3 \oplus h(R_1||A_1||A_2||\varepsilon_i)$. Here, $A_1 = h(UID_i||R_1)$ and $A_2 = h(PW_i||R_1)$. Considering only the guessing attacks, the advantage of $\AA$ will be more than 0.5 for $\rho = 10^7$ or 10^8 [26]. However, using the victim's personal information in targetted guessing attacks, $\AA$'s advantage will be more than 0.5 for $\rho \leq 10^6$ [27]. The fuzzy extractor deployed in the proposed protocol retrieves at most φ arbitrary bits. As such, the probability of $\AA$ guessing $\varepsilon_i \in \{0, 1\}^{\varphi}$ is approximately $(2^{\varphi})^{-1}$ [28]. In spite of the simulation of the *Corrupt* ($K_{U_i}^{q_1}$) query against our protocol in G_3, the two games G_3 and G_2 are indistinguishable. Given that limited number of wrong password inputs are admissible in the system, the application of Zipf's law [26] yields,

$$Adv^{\AA,G_2}(t) - Adv^{\AA,G_3}(t) \leq \max\{\tau.\rho^{\sigma}, \frac{\rho}{2^{\varphi}}\} \tag{6}$$

It is evident that all queries simulated by $\AA$ have failed to assist $\AA$ win any game. The only winning option left for $\AA$ is to predict bit ϕ. This is facilited by executing the *Test* query and hence,

$$Adv^{\AA,G_3}(t) = \frac{1}{2} \tag{7}$$

Using the triangular inequality, equations (3) to (6) are simplified to obtain the following:

$$\begin{aligned}\frac{1}{2}.Adv^{\AA}(t) &= |Adv^{\AA,G_0}(t) - \frac{1}{2}| \\ &= |Adv^{\AA,G_1}(t) - Adv^{\AA,G_3}(t)| \\ &\leq |Adv^{\AA,G_1}(t) - Adv^{\AA,G_2}(t)| \\ &\quad + |Adv^{\AA,G_2}(t) - Adv^{\AA,G_3}(t)| \\ &\leq \frac{\alpha^2}{2(|Hash|)} + \max\{\tau.\rho^{\sigma}, \frac{\rho}{2^{\varphi}}\}\end{aligned} \tag{8}$$

Mutiplying both side of equation (8) by factor 2 yields the following:

$$Adv^{\mathring{A}}(t) \leq \frac{\alpha^2}{|Hash|} + 2\max\{\tau.\rho^{\sigma}, \frac{\rho}{2^{\varphi}}\} \quad (9)$$

Equation (9) completes the proof and hence the derived session key is provably secure.

B. INFORMAL SECURITY ANALYSIS

In this sub-section, we analyze our protocol against conventional WSNs attacks. In addition, the salient features supported by our protocol are demonstrated.

1) PHYSICAL CAPTURE

Suppose that adversary $\mathring{A}$ has physically captured SN_j deployed in a given business premise. The next goal is to extract all the information stored in this sensor. During the registration phase, parameter set $\{ID_{GWN}, BID_k, SID_j, SK_{G-S}, h(.)\}$ is stored in the memory of SN_j. Here, $SK_{G-S} = h(BID_k||SID_j||GSK_j||SSK_j)$. Due to the incorporation of unique identity and long term secret key of the j^{th} sensor node SID_j and SSK_j respectively, all the shared keys between GWN and sensor nodes are distinct. As such, the compromise of SK_{G-S} belonging to a particular SN_j does not lead to the compromise of other shared keys within the network.

2) DENIAL OF SERVICE AND DE-SYNCHRONIZATION

The assumption made here is that adversary $\mathring{A}$ has used side-channeling attacks to extract secrets $\{ID_{GWN}, BID_k, SID_j, SK_{G-S}, h(.)\}$ stored in SN_j. This is followed by an attempt to derive the session key $K_{SN} = h(D_1||A_1||SID_j||BID_k||T_5)$ negotiated between SN_j and GWN. Here, $D_1 = h(R_4||h(R_2||R_3))$ and $A_1 = h(ID_{GWN}||SK_{G-S}||SID_j||T_3) \oplus C_3, h(R_2||R_3)$. Although $\mathring{A}$ has captured keying parameters such as ID_{GWN}, BID_k, SID_j and SK_{G-S}, access to random nonces R_2, R_3 and R_4 as well as timestamp T_3 is still required. Therefore, $\mathring{A}$ cannot establish any communication session with GWN. Similarly, $\mathring{A}$ cannot derive session key $K_{SM} = h(D_1||A_1||SID_j||BID_k||T_5)$ negotiated between the MD_i and SN_j. Consequently, denial of service and de-synchronization attacks against the SN_j and MD_i will not succeed.

3) IDENTITY GUESSING

During the registration phase, messages $Rg_1 = \{ID_{GWN}, BID_k, SID_j, SK_{G-S}, h(.)\}$, $Rg_2 = \{A_1, h(.)\}$ and $Rg_3 = \{A_3, A_4, A_5, BID_k, ID_{GWN}, h(.)\}$ are exchanged. Here, $SK_{G-S} = h(BID_k||SID_j||GSK_j||SSK_j)$, $A_1 = h(UID_i||R_1)$, $A_3 = h(A_1||GSK_j)$, $A_4 = h(BID_k||A_3||ID_{GWN})$ and $A_5 = BID_k \oplus h(A_1||A_3)$. Although messages Rg_1 and Rg_3 contain plaintext GWN unique identity ID_{GWN} and SN_j identity SID_j, these messages are exchanged over secure channels. It is clear that A_1 carries the unique identity of user i, UID_i. However, this identity is encapsulated in random nonce R_1 before being hashed. Therefore, it cannot be easily obtained by the attckers due to the difficulty of reversing the one-way hash function. During the login, mutual authentication and session key negotiation phase, messages AUT_1, AUT_2 and AUT_3 are exchanged. Although login, authentication and session key agreement take place over the public channels, none of the transmitted messages contain clear text identities ID_{GWN}, UID_i and SID_j. In all the intermediary parameters, identities ID_{GWN} and SID_j are encapsulated in other values before being hashed. As such, it is difficulty for the attacker to guess these identities.

4) STOLEN MOBILE DEVICE AND PASSWORD GUESSING

Suppose that the user has lost MD_i after which adversary $\mathring{A}$ is able to extract all parameter set $\{Gen(.), B_3, A_5, B_1, B_2, Rep(.), ID_{GWN}, h(.), BID_k, \mu_i\}$ stored in it. Here, $B_3 = A_3 \oplus h(R_1||A_1||A_2||\varepsilon_i)$, $A_5 = BID_k \oplus h(A_1||A_3)$, $B_1 = R_1 \oplus h(\varepsilon_i||UID_i||PW_i)$ and $B_2 = h(A_3||A_4||R_1||\varepsilon_i)$. Next, $\mathring{A}$ tries to obtain the unique identity UID_i and password PW_i for user U_i. Among all the extracted parameters, it is only B_1 that can facilitate this attack. However, UID_i and PW_i are concatenated with parameter ε_i before being hashed. Since $\mathring{A}$ does not have access to ε_i, user identity and password cannot be recovered. In addition, it is cumbersome to reverse the one-way hashing function to extract user password and identity.

5) SESSION HIJACKING

The assumption made in this attack is that adversary $\mathring{A}$ has stolen the user mobile device MD_i and wants to establish a communication session with both GWN and SN_j. It is also assumed that value set $\{Gen(.), B_3, A_5, B_1, B_2, Rep(.), ID_{GWN}, h(.), BID_k, \mu_i\}$ can be extracted via power analysis. To hijack MD_i session, $\mathring{A}$ selects some bogus PW_i^b, R_1^b and β_i^b then attempts to derive $A_1 = h(UID_i||R_1^b)$, $A_2^b = h(PW_i^b||R_1^b)$, $Gen(\beta_i^b) = (\varepsilon_i^b, \mu_i^{New})$, $B_1^b = R_1^b \oplus h(\varepsilon_i^b||UID_i||PW_i^b)$, $B_2^b = h(A_3||A_4||R_1||\varepsilon_i^b)$ and $B_3^b = A_3 \oplus h(R_1||A_1||A_2^b||\varepsilon_i^b)$. However, it has already been shown that identity UID_i cannot be otained by $\mathring{A}$. In addition, we have already detailed the difficulty of obtaining both UID_i and PW_i. Without valid private biometric key ε_i and public reproduction token μ_i associated with β_i, this attack flops. This is because of the subsequent failure of authentications such as $B_2 \stackrel{?}{=} h(A_3||A_4||R_1||\varepsilon_i^*)$, $C_2 \stackrel{?}{=} h(R_2||A_3||SID_j||A_4||BID_k)$ and $D_3 \stackrel{?}{=} h(D_1||K_{SN}||T_5||BID_k)$.

6) UNTRACEABILITY AND ANONYMITY

During the login, authentication and key agreement phase, $AUT_1 = \{B_4, B_5, C_1, C_2, T_1\}$, $AUT_2 = \{C_3, C_4, C_5, T_3\}$ and $AUT_3 = \{D_2, D_3, T_5\}$ are exchanged. It is clear that user, sensor and gateway identities UID_i, SID_j and ID_{GWN} are never exchanged in clear text in all these three messages. Although SID_j and ID_{GWN} are componets of the exchanged parameters, they are encapsulated in other values. Therefore, user, sensor and gateway anonymities are upheld. To preserve untraceability, random nonces such as R_2, R_3 and R_4 as

well as timestamps T_1, T_3 and T_5 are incorporated in the exchanged messages. As such, it is difficult for the attackers to trace user activities during the various communication sessions.

7) MITM AND FABRICATION

The goal of this attack is to modify messages AUT_1, AUT_2 and $AUT_3 = \{D_2, D_3, T_5\}$ exchanged over public channels. These altered messages are then forwarded to unsuspecting receivers. To fabricate message AUT_1, adversary needs access to identities such as ID_{GWN}, BID_k, SID_j, intermediary values such as A_1, A_3, A_4, random nonces such as R_2, as well as timestamps T_1. Similary, the fabrication of messages AUT_2 and AUT_3 requires timestamps T_3 and T_5, nonces R_2, R_3 and R_4, shared key SK_{G-S}, ephemeral value A_1 as well as identities ID_{GWN}, SID_j and BID_k. However, it has already been shown that these identities cannot be easily obtained by $\AA$ and hence these attacks flop.

8) EPHEMERAL LEAKAGE

The aim of this attack is to obtain transient keying parameters and attempt session key derivation. After successful mutual authentication, session keys $K_{SN} = h\,(D_1||A_1||SID_j||BID_k||T_5)$ and $K_{SM} = h\,(D_1||A_1||SID_j||BID_k||T_5)$ are derived at the SN_j and MD_i respectively. Here, $D_1 = h\,(R_4||h(R_2||R_3))$ and $A_1 = h\,(ID_{GWN}||SK_{G-S}||SID_j||T_3) \oplus C_3$. Suppose that short term secrets such as nonces R_2, R_3 and R_4 have been captured by adversary $\AA$. An attempt is thereafter made to derive these session keys. However, this calls for long term secrets such as A_1, SID_j, BID_k, ID_{GWN} and SK_{G-S}, as well as short terms secrets such as timestamp T_5. Since all these parameters are never sent in plain text in messages AUT_1, AUT_2 and AUT_3, they cannot be intercepted by $\AA$. Let us assume that the attacker has captured long terms secrets and wants to derive these session keys. Since $\AA$ still needs short term keys, this attack flops.

9) KEY SECRECY

Suppose that attacker has captured the current session keys K_{SN}, K_{SM} and K_S. It has already been shown that both long terms and short term secrets keys are deployed in these session keys. As such, these keys are disparate for each communication session. Since these session keys incorporate timestamps T_3 and T_5 as well as random nonces R_2, R_3 and R_4, they are stochastic. As such, $\AA$ cannot use the short term secrets for the current session to derive keys for the previous and subsequent session.

10) IMPERSONATION AND PRIVILEGED INSIDER

The aim of this attack is for some privileged insider to masquerade as legitimate user, SN_j and GWN. To achieve this, attempts are made to construct valid messages AUT_1, AUT_2 and AUT_3. The case studies below describe these attacks in detail.

***Case 1*:** To impersonate the user U_i, attacker $\AA$ must compose valid message $AUT_1 = \{B_4, B_5, C_1, C_2, T_1\}$ sent from U_i towards GWN. To prevent this impersonation, the GWN must check if $C_2 \stackrel{?}{=} h\,(R_2||A_3||SID_j||A_4||BID_k)$. Here, $A_4 = h\,(BID_k||A_3||ID_{GWN})$, $A_3 = B_3 \oplus h\,(R_1||A_1||A_2||\varepsilon_i^*)$, $B_3 = A_3 \oplus h\,(R_1||A_1||A_2||\varepsilon_i)$ and $A_2 = h\,(PW_i||R_1)$. Therefore, for message AUT_1 fabricated by $\AA$ to pass this check, valid parameters such as BID_k, ID_{GWN}, ε_i^*, PW_i, SK_{G-S}, T_1, R_1 and ID_{GWN} are required. As such, user impersonation flops.

***Case 2*:** To masquerade as GWN, adversary $\AA$ needs to compose valid message $AUT_2 = \{C_3, C_4, C_5, T_3\}$ sent from the GWN towards the SN_j. In addition, $\AA$ must pass the $C_4 \stackrel{?}{=} h\,(A_1||SID_j||BID_k||T_3||h(R_2||R_3))$ check. To pass this test, valid parameters such as BID_k, ID_{GWN}, SID_j, T_3, R_2 and R_3 are needed, and hence GWN impersonation will fail.

***Case 3*:** To impersonate SN_j, privileged insider needs to compose legitimate message $AUT_3 = \{D_2, D_3, T_5\}$ transmitted from SN_j towards the MD_i. In addition, test $D_3 \stackrel{?}{=} h\,(D_1||K_{SN}||T_5||BID_k)$ must be passed. Here, $D_1 = h\,(R_4||h(R_2||R_3))$ and $D_3 = h\,(D_1||K_{SN}||T_5||BID_k)$. The unavailability of valid parameters K_{SN}, BID_k, R_2, R_3, R_4 and T_5 to the adversary means that this attack has failed.

11) MUTUAL AUTHENTICATION

Proof: In our protocol, all the three communicating entities validate each other before exchanging the sensed data. The following three case studies elaborate the procedures involved in these verifications.

Case 1: $U_i \rightarrow$ GWN

To execute mutual authentication between U_i and GWN, the MD_i composes message $AUT_1 = \{B_4, B_5, C_1, C_2, T_1\}$ that is sent to the GWN. To authenticate this request, GWN establishes if $|T_2 - T_1| < \Delta T$ and $C_2 \stackrel{?}{=} h\,(R_2||A_3||SID_j||A_4||BID_k)$. On condition that these two tests are successful, the user is verified.

Case 2: GWN $\rightarrow SN_j$

For this authentication, the GWN constructs message $AUT_2 = \{C_3, C_4, C_5, T_3\}$ that is forwarded to SN_j. On receiving this request, the SN_j confirms if $|T_4 - T_3| < \Delta T$ and $C_4 \stackrel{?}{=} h\,(A_1||SID_j||BID_k||T_3||h(R_2||R_3))$. The GWN is considered validated when these two tests are positive. Here, $h(R_2||R_3)$ directly verifies the GWN while $A_1 = h\,(UID_i||R_1)$ indirectly authenticates user U_i.

Case 3: $SN_j \rightarrow MD_i$

To verify the authenticity of SN_j, the sensor node composes message $AUT_3 = \{D_2, D_3, T_5\}$ that is transmitted to the MD_i. Here, the MD_i confirms whether $|T_6 - T_5| < \Delta T$ and $D_3 \stackrel{?}{=} h\,(D_1||K_{SN}||T_5||BID_k)$. Provided that these two tests are positive, the MD_i has successfully verified SN_j.

12) PACKET REPLAY

During the login, authentication and key negotiation phase, three messages are exchanged among the GWN, SN_j and MD_i. These messages include $AUT_1 = \{B_4, B_5, C_1, C_2, T_1\}$, $AUT_2 = \{C_3, C_4, C_5, T_3\}$ and $AUT_3 = \{D_2, D_3, T_5\}$. Evidently, all these messages incorporate timestamps. Suppose that attacker $\AA$ has captured any of these messages. Thereafter, modifications are carried out before being forwarded

to unsuspecting receivers. However, all these timestamps are verified at the receiver end before these messages are accepted.

13) SESSION KEY NEGOTIATION

In the proposed protocol, all the three entities negotiate session keys that are used to encipher the messages exchanged among them. The case studies below describe these procedures in detail.

Case 1: GWN $\leftrightarrow SN_j$

Upon receiving message AUT_2 from the GWN, the sensor node SN_j validates its timestamp T_3. Provided that this verification succeeds, SN_j computes parameter $A_1 = h(ID_{GWN}||SK_{G-S}||SID_j||T_3) \oplus C_3$. Next, it generates nonce R_4 and establishes the current timestamp T_5 before computing value $D_1 = h(R_4||h(R_2||R_3))$. Finally, the session key is derived as $K_{SN} = h(D_1||A_1||SID_j||BID_k||T_5)$.

Case 2: $SN_j \leftrightarrow MD_i$

After receiving message AUT_3 from the SN_j, the mobile device MD_i validates its timestamp T_5. On condition that this verification is successful, MD_i derives $D_1 = D_2 \oplus h(A_1||SID_j||T_5||BID_k)$ that is used to compute the session key as $K_{SM} = h(D_1||A_1||SID_j||BID_k||T_5)$. At the end of the current communication session, this shared key between the MD_i and SN_j is updated as $K_S = h(h(R_4||h(R_2||R_3))||A_1||SID_j||BID_k||T_5)$.

V. PERFORMANCE EVALUATION

This section assesses the efficacy and efficiency of the proposed protocol. The evaluation considers computational, communication, energy overheads,and supported security as detailed in the subsequent subsections.

A. COMPUTATIONAL OVERHEAD

During the login, authentication and key agreement phase, the user U_i through his/her MD_i execute 14 one-way hashing operations and a single fuzzy extraction. On the other hand, the GWN and SN_j executes 9 and 7 one-way hashing operations respectively. As such, the total computation overhead of our protocol is 30 one-way hashing and one fuzzy extraction operations. Table 3 details the implementation parameters deployed in this protocol.

TABLE 3. Implementation parameters.

Feature	Description
Processor	Intel Pentium Dual CPU E2200
Operating system	Ubuntu 22.04.2 LTS
RAM	2GB
Clock speed	2.20 GHz
Cryptographic library	PBC library (built in GMP)
Symmetric encryption/decryption	AES

In the environment described in Table 3, the execution time for the one-way hashing (T_H), fuzzy extraction (T_{FE}), elliptic curve point multiplication (T_{EM}), and symmetric encryption/decryption (T_{ED}) were determined as 0.213 ms, 2.675 ms, 2.215 ms and 3.841 ms respectively. Based on these values, the computation overheads of our protocol as well as other related schemes are presented in Table 4.

TABLE 4. Computation overheads.

Scheme	Derivation	Total (ms)
[17]	$17T_H + 3T_{EM}$	10.266
[18]	$25T_H + 6T_{EM}$	18.615
[19]	$16T_H + 5T_{EM}$	14.483
[20]	$21T_H + 3T_{EM}$	11.118
[21]	$18T_H + 3T_{EM}$	10.479
[23]	$16T_H + 4T_{ED}$	18.772
Proposed	$30T_H + T_{FE}$	9.065

As shown in Figure 3, the scheme in [23] incurs the highest computation overhead of 18.772 ms. This is followed by the protocols in [17], [18], [19], [20], and [21] with computation costs of 18.615 ms, 14.483ms, 11.118 ms, 10.479 ms, 10.479 ms and 10.266 ms respectively. In contrast, the proposed protocol incurs the lowest computational overhead of only 9.065 ms. Compared to the scheme in [17], our protocol reduces computational overheads by 13.49%. Given the limited computational power of sensor nodes in WSNs, our protocol is the most suitable choice for deployment in these environments.

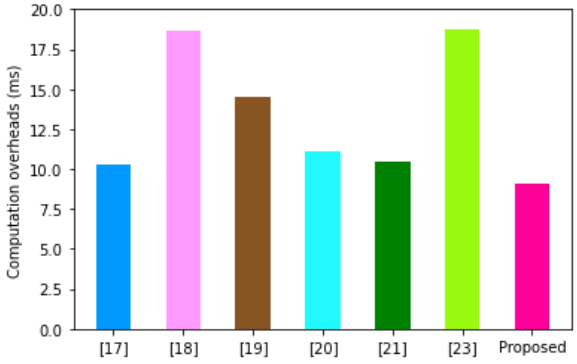

FIGURE 3. Computation overheads.

TABLE 5. Communication complexities.

Scheme	No. of exchanged messages	Total (bits)
[17]	4	3712
[18]	4	2432
[19]	4	1600
[20]	4	2112
[21]	4	6656
[23]	3	3072
Proposed	3	1536

B. COMMUNICATION OVERHEAD

In this section, the computation overhead of our protocol is derived from the size of the messages exchanged during

the login, authentication, and key agreement phases. These messages include $AUT_1 = \{B_4, B_5, C_1, C_2, T_1\}$, $AUT_2 = \{C_3, C_4, C_5, T_3\}$ and $AUT_3 = \{D_2, D_3, T_5\}$. Here, the length of ECC is 320 bits and that of timestamp is 32 bits. On the other hand, the lengths of hash, identity, random nonce and symmetric encryption are 160 bits each. Using these values, the communication overhead of the proposed protocol is derived as follows: $AUT_1 = \{160+160+160+160+32 = 672$ bits$\}$; $AUT_2 = \{160+160+160+32 = 512$ bits$\}$; and $AUT_3 = \{160+160+32 = 352$ bits$\}$. As such, the total communication overhead of our protocol is 1536 bits. Table 5 presents the communication overhead comparison of our protocol with other related schemes.

As depicted in Figure 4, the protocol in [21] exhibits the highest communication overhead of 6656 bits, followed by the schemes in [17], [18], [19], [20], and [23] with overheads of 3712 bits, 3072 bits, 2432 bits, 2112 bits, and 1600 bits, respectively. Conversely, our proposed scheme incurs a communication overhead of only 1536 bits.

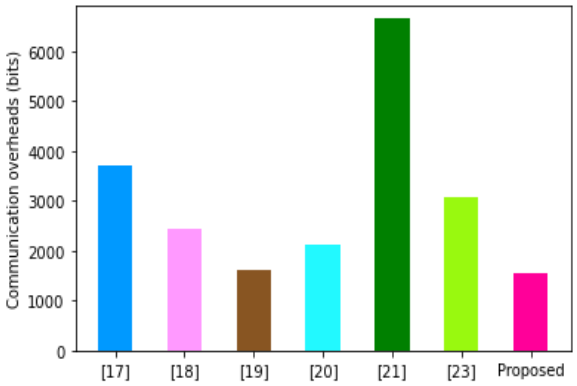

FIGURE 4. Communication complexities.

Building upon the protocol in [19], our protocol achieves a 4% reduction in communication overhead. As sensor nodes in WSNs have limited communication capabilities, our scheme emerges as the most suitable choice for this scenario.

C. ENERGY CONSUMPTION

In this section, we present the energy efficiency of our scheme. In addition, we compare the energy consumption in our protocol with other peer schemes. Taking E, I, V and C_C as energy consumption, current, voltage and computation overhead respectively, then $E = I \times V \times C_C$. We use the values in [29], where $V = 3.0$ volts and $I = 8 \times 10^{-3}$ amperes at active mode. Consequently, our scheme's total energy consumption is 0.217560 mJ. In contrast, the schemes in [17], [18], [19], [20], [21], and [23] have energy consumptions of 0.246384 mJ, 0.44676 mJ, 0.347592 mJ, 0.266832 mJ, 0.251496 mJ, and 0.450528 mJ, respectively. As evidenced from Figure 5, the protocol in [23] has the highest energy consumption, followed by the schemes in [17], [18], [19], [20], and [21], respectively. Notably, our protocol stands out with the lowest energy consumption of 0.217560 mJ. Given the difficulties in replacing batteries for sensor nodes located in hard-to-reach or impassable areas, our scheme's reduced energy consumption is a significant advantage.

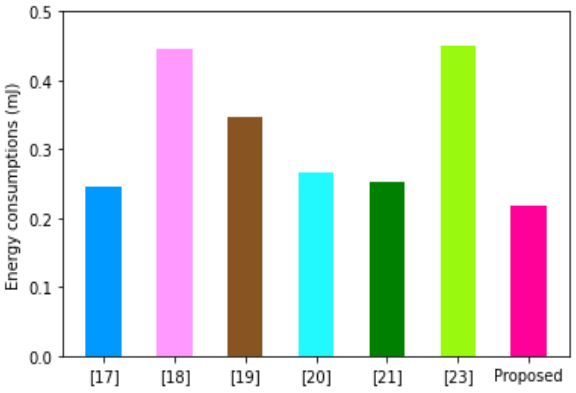

FIGURE 5. Energy efficiencies.

TABLE 6. Supported security features.

	[23]	[21]	[17]	[18]	[20]	[19]	**Proposed**
Security features							
F1	√	√	√	√	√	√	√
F2	√	√	√	√	√	√	√
F3	√	×	×	√	√	√	√
F4	√	×	×	√	√	√	√
F5	×	√	√	√	√	×	√
F6	×	√	√	√	√	√	√
F7	√	√	√	√	√	√	√
Robust against							
F8	√	×	×	×	×	√	√
F9	√	×	√	√	×	×	√
F10	√	×	√	√	√	√	√
F11	×	×	×	×	×	×	√
F12	×	×	×	×	×	×	√
F13	√	√	√	√	√	√	√
F14	×	×	×	×	√	×	√
F15	×	√	√	√	×	√	√
F16	√	×	√	√	√	√	√
F17	√	√	√	√	×	×	√
F18	√	×	×	×	×	×	√
F19	√	×	×	√	√	√	√
F20	√	×	×	√	√	√	√

F1: Key agreement; F2: Mutual authentication, F3: Key secrecy, F4: Anonymity, F5: Untraceability, F6: Formal verification, F7: No password verification tables, F8: Ephemeral secret leakage, F9: Password guessing, F10: Stolen mobile device, F11: Session hijacking, F12: Identity guessing, F13: Replays, F14: Fabrication, F15: MitM, F16: Privileged insider, F17: De-synchronization, F18: DoS, F19: Physical capture, F20: Impersonation, √ Supported; × Not supported or not considered.

Building upon the technique in [17], our protocol achieves an 11.69% reduction in energy consumption. As our scheme exhibits the lowest energy consumption, it aligns perfectly with the requirements of electronic commerce WSN-based sensing application environment.

D. SUPPORTED FEATURES

Trust is paramount in WSN-based e-commerce environments, and robust security and privacy features that safeguard the network from attacks are essential for achieving it. Table 6 provides a comparative analysis of the supported features and attack resilience of our protocol against other related schemes.

As illustrated in Table 6, the scheme in [21] supports the fewest features (8), making it the most vulnerable. The protocol in [17] offers 11 features, followed by the protocols in [19] and [20] with 3 features each. On the other hand, the schemes in [18] and [23] support 14 features each. Notably, our protocol supports all 20 features, making it the most secure. This comprehensive security can foster trust among stakeholders engaged in e-commerce activities.

E. COMPARISON WITH EXISTING PROTOCOLS

The proposed work proposes a trust-enabled energy-efficient sensing protocol that is specifically designed for e-commerce supply chain management. It is designed to address the security and privacy vulnerabilities of existing protocols, while also being energy efficient. The key differences are the following:

1- The proposed work focuses on the development of a new sensing protocol, while the previous works focus on different aspects of security and privacy, such as authentication, decision-making, and DDoS mitigation.

2- The new work considers the energy constraints of sensor nodes, while most of the other works do not explicitly consider energy efficiency.

VI. CONCLUSION

WSNs offer personalization, contextualization, monitoring, tracking and optimization among other services in an e-commerce environment. However, trust and energy efficiency during sensing and data transmissions are critical concepts that must be taken into consideration, owing to the sensitive nature of the e-commerce transactions and the resource-constrained nature of sensor nodes. To this end, numerous energy-aware routing techniques have been presented in literature. However, security and privacy is not considered in many of these techniques. As such, a myriad of privacy and security preserving schemes have been developed. Nevertheless, it has been shown that the attainment of ideal trust at optimum energy consumption still remains a mirage. In this paper, an energy efficient sensing protocol is developed, which is demonstrated to be provably secure. In addition, its semantic analysis has demonstrated its resilience against numerous security and privacy attacks. It has been shown to reduce energy, computation and communication overheads by 11.69%, 13.49% and 4% respectively. It is therefore ideal for resource constrained sensor nodes.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] H. Treiblmaier and C. Sillaber, "The impact of blockchain on e-commerce: A framework for salient research topics," *Electron. Commerce Res. Appl.*, vol. 48, Jul. 2021, Art. no. 101054.

[2] S. Shorman, M. Allaymoun, and O. Hamid, "Developing the e-commerce model a consumer to consumer using blockchain network technique," *Int. J. Manag. Inf. Technol.*, vol. 11, no. 2, pp. 55–64, May 2019.

[3] M. Javaid, A. Haleem, R. P. Singh, S. Rab, and R. Suman, "Significance of sensors for Industry 4.0: Roles, capabilities, and applications," *Sensors Int.*, vol. 2, Mar. 2021, Art. no. 100110.

[4] H. D. Mohammadian, "IoE—A solution for energy management challenges," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Apr. 2019, pp. 1455–1461.

[5] Z. Wang, Y. Wu, W. Jiang, Q. Liu, X. Wang, J. Zhang, Z. Zhou, H. Zheng, Z. Wang, and Z. L. Wang, "A universal power management strategy based on novel sound-driven triboelectric nanogenerator and its fully self-powered wireless system applications," *Adv. Funct. Mater.*, vol. 31, no. 34, Aug. 2021, Art. no. 2103081.

[6] J. Ren, H. Li, M. Zhang, C. Wu, and X. Yu, "A self-powered sensor network data acquisition, modeling and analysis method for cold chain logistics quality perception," *IEEE Sensors J.*, vol. 23, no. 18, pp. 20729–20736, Feb. 2023.

[7] V. O. Nyangaresi, "Privacy preserving three-factor authentication protocol for secure message forwarding in wireless body area networks," *Ad Hoc Netw.*, vol. 142, Apr. 2023, Art. no. 103117.

[8] M. Roy and A. Roy, "Nexus of Internet of Things (IoT) and big data: Roadmap for smart management systems (SMgS)," *IEEE Eng. Manag. Rev.*, vol. 47, no. 2, pp. 53–65, 2nd Quart., 2019.

[9] X. Zhao, W. Zhong, and Y. D. Navaei, "A novel energy-aware routing in wireless sensor network using clustering based on combination of multiobjective genetic and cuckoo search algorithm," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–14, Apr. 2022.

[10] Z. Peng, M. S. Jabloo, Y. D. Navaei, M. Hosseini, R. J. Oskouei, P. Pirozmand, and S. Mirkamali, "An improved energy-aware routing protocol using multiobjective particular swarm optimization algorithm," *Wireless Commun. Mobile Comput.*, vol. 2021, no. 1, pp. 1–16, Jan. 2021.

[11] M. K. Shahzad, S. M. R. Islam, M. Hossain, M. Abdullah-Al-Wadud, A. Alamri, and M. Hussain, "GAFOR: Genetic algorithm based fuzzy optimized re-clustering in wireless sensor networks," *Mathematics*, vol. 9, no. 1, Dec. 2020, Art. no. 43.

[12] M. Radhika and P. Sivakumar, "Energy optimized micro genetic algorithm based LEACH protocol for WSN," *Wireless Netw.*, vol. 27, no. 1, pp. 27–40, Jan. 2021.

[13] L. Chen, R. Zhao, K. He, Z. Zhao, and L. Fan, "Intelligent ubiquitous computing for future UAV-enabled MEC network systems," *Cluster Comput.*, vol. 25, no. 4, pp. 2417–2427, Aug. 2022.

[14] L. Chen and J. Xia, "Physical-layer security on mobile edge computing for emerging cyber physical systems," *Comput. Commun.*, vol. 99, pp. 1–12, Oct. 2022.

[15] D. Huang and S. Xu, "A transaction frequency based trust for e-commerce," *Comput., Mater. Continua*, vol. 74, no. 3, pp. 5319–5329, 2023.

[16] S. U. Jan, S. Ali, I. A. Abbasi, M. A. A. Mosleh, A. Alsanad, and H. Khattak, "Secure patient authentication framework in the healthcare system using wireless medical sensor networks," *J. Healthcare Eng.*, vol. 2021, pp. 1–20, Jul. 2021.

[17] D. Kaur and D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102787.

[18] X. Wang, Y. Teng, Y. Chi, and H. Hu, "A robust and anonymous three-factor authentication scheme based ECC for smart home environments," *Symmetry*, vol. 14, no. 11, p. 2394, Nov. 2022.

[19] S. S. Sahoo, S. Mohanty, K. S. Sahoo, M. Daneshmand, and A. H. Gandomi, "A three factor based authentication scheme of 5G wireless sensor networks for IoT system," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 15087–15099, May 2023.

[20] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K.-R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018.

[21] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S. M. Pournaghi, and M. A. Doostari, "LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT," *Wireless Netw.*, vol. 27, no. 2, pp. 1389–1412, Feb. 2021.
[22] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, 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, Mar. 2020.
[23] 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.
[24] M. A. Saleem, S. Shamshad, S. S. Ahmed, Z. Ghaffar, and K. Mahmood, "Security analysis on 'a secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems,'" *IEEE Syst. J.*, vol. 15, pp. 5557–5559, 2021.
[25] G. Gao, Z. Feng, and Z. Xia, "Energy efficient three-factor authentication in wireless sensor networks with resisting insider attacks," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 3, pp. 1297–1308, Mar. 2023.
[26] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
[27] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted online password guessing: An underestimated threat," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Vienna, Austria, Oct. 2016, pp. 1242–1254.
[28] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.
[29] S. Gupta, F. Alharbi, R. Alshahrani, P. K. Arya, S. Vyas, D. H. Elkamchouchi, and B. O. Soufiene, "Secure and lightweight authentication protocol for privacy preserving communications in smart city applications," *Sustainability*, vol. 15, no. 6, p. 5346, Mar. 2023.

VINCENT OMOLLO NYANGARESI received the B.Sc. degree in telecommunications and information technology, the M.Sc. degree in information technology security and audit, and the Ph.D. degree in information technology security and audit. He is an experienced researcher in areas of computer science and information technology, having published over 120 research articles in peer reviewed journals and conferences covering areas, such as communication systems, secure network communications, D2D, smart homes, the Internet of Drones, smart grids, WSNs, cellular network security, VANETs, information systems acceptance modeling, TCP architecture and design, radio wave propagation, virtualization, and cloud computing. He is a renowned reviewer for numerous IEEE, Taylor and Francis, MDPI, *PLOS One*, Elsevier, and Springer journals. In addition, he has served as a Technical Committee Member (TPC) for numerous international conferences and symposia, such as the International Conference on IoT as a Service (IoTaaS), Congress on Intelligent Systems (CIS), the International Conference on Smart Grid and Energy Engineering (SGEE), and the International Conference on Cloud, Big Data and IoT (CBIoT). Moreover, he serves as an Editor to some top journals, such as *PLOS One*, *International Journal of Business Data Communications and Networking*, *Security and Communication Networks*, *Discover Data*, *Computers, Materials and Continua*, and *OBM Neurobiology*.

EESA ALSOLAMI received the bachelor's degree in computer science from King Abdulaziz University, Saudi Arabia, in 2002, and the master's degree in information technology and the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2008 and 2012, respectively. He is currently with the Department of Information Security, University of Jeddah, Saudi Arabia, as an Assistant Professor. His research interests include information security and biometric technology.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he was with the Department of Computer Engineering, Aligarh Muslim University, Aligarh. Since 2011, he has been an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia. He has published over 125 research papers in internationally reputed refereed journals and conference proceedings of IEEE/Springer/Elsevier. He has more than 4300 citations of his research works with an H-index of 39, i-10 index of 95, and cumulative impact factor of more than 300. His research interests include multimedia security, chaos-based cryptography, cyber security, machine learning and deep learning, and optimization techniques. He has been consecutively listed three times among World's Top 2% Researchers in studies conducted by Elsevier and Stanford University, in 2021, 2022 and 2023. Recently, he is felicitated with Jamia Achievers Award by Jamia Millia Islamia. He has served as a reviewer and a technical program committee member of many international conferences. He is serving as an Associate Editor for *International Journal of Information Security and Privacy* and *International Journal of Artificial Intelligence in Scientific Disciplines* from IGI. He is an Editorial Board Member of *Discover Computing* (Springer), *International Journal of Chaos, Control, Modeing and Simulation*, and *Journal of Theoretical Physics and Cryptography*. He has also served as a Referee of some renowned journals, such as *Information Sciences*, *Signal Processing*, *Journal of Information Security and Applications*, *Expert Systems with Applications*, *Knowledge-Based Systems*, *Applied Soft Computing*, *Engineering Applications of Artificial Intelligence*, *Chaos Solitons and Fractals*, *Physica A: Statistical Mechanics and its Applications*, *Signal Processing: Image Communication*, *Neurocomputing*, IEEE Internet of Things Journal, IEEE Journal on Selected Areas in Communications, IEEE Journal of Biomedical and Health Informatics, IEEE Transactions on Cybernetics, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transactions on Industrial Informatics, IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Systems, Man, and Cybernetics, IEEE Transactions on Consumer Electronics, IEEE Transactions on Cognitive and Developmental Systems, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Nanobioscience, IEEE Transactions on Circuits and Systems—I: Regular Papers, IEEE Transactions on Big Data, IEEE Transactions on Reliability, IEEE Multimedia, IEEE Access, *Wireless Personal Communications*, *Neural Computing and Applications*, *Multimedia Tools and Applications*, *International Journal of Bifurcation and Chaos*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Optik*, *Complexity*, *Computers in Biology and Medicine*, and *Computational and Applied Mathematics*, and *Concurrency and Computation*.