Hindawi
Security and Communication Networks
Volume 2024, Article ID 9753659, 1 page
https://doi.org/10.1155/2024/9753659

Retraction

Retracted: FHAAPS: Efficient Anonymous Authentication with Privacy Preservation Scheme for Farm-to-Home Communication

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] A. S. Rajasekaran, M. Azees, and K. Yahya, "FHAAPS: Efficient Anonymous Authentication with Privacy Preservation Scheme for Farm-to-Home Communication," *Security and Communication Networks*, vol. 2023, Article ID 1225675, 12 pages, 2023.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 1225675, 12 pages
https://doi.org/10.1155/2023/1225675

Research Article

FHAAPS: Efficient Anonymous Authentication with Privacy Preservation Scheme for Farm-to-Home Communication

Arun Sekar Rajasekaran,[1] M. Azees ,[2] and Khalid Yahya[3]

[1]*Department of ECE, KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India*
[2]*School of Computer Science and Engineering, VIT-AP University, Inavolu, Beside AP Secretariat, Amaravathi 522237, India*
[3]*Department of Electrical and Electronics Engineering, Nisantasi University, Istanbul 34398, Turkey*

Correspondence should be addressed to M. Azees; azeesmm@gmail.com

Received 25 June 2022; Revised 29 August 2022; Accepted 2 February 2023; Published 21 February 2023

Academic Editor: Muhammad Shafiq

With the advancement in information and communication technology (ICT), secure farm-to-home communication has become an emerging concept. Food is the most basic essential commodity for the survival of human beings which is produced by farmers. However, because of the presence of intermediaries, farmers/producers do not make a sufficient profit and also the consumers have to pay more money to buy food items from these mediators. As a result, in this work, we proposed an efficient farm-to-home anonymous authentication privacy-preserving scheme in which the storehouse will buy goods from farmers and sell them to the consumers at the base rate. Moreover, in our scheme, an unprofitable trusted delivery agent assists in the transfer of food commodities between end users and storehouses to provide maximum profit for the farmers and consumers. Further, essential security parameters are provided to the end users and it provides conditional privacy to the delivery agent; i.e., if any mishap occurs, then the malicious delivery agent's privacy is revoked to avoid further damage to the system. The performance analysis section shows that our scheme supports the transfer of food commodities with minimum computational and communication costs.

1. Introduction

Food cultivation becomes essential for the survival of human beings around the globe. Farmers are the primary cultivators of food crops. They play an important role in society, as they provide food to human beings through agriculture. However, the presence of the mediators has an impact on their agricultural income. Moreover, the agreement restrictions prevent the majority of the farmers from benefiting from it. If the trade prices fall just below the minimum support price (MSP), farmers will receive cost shortfall payouts under the agreement system. The profiting intermediaries are the main impediment to boosting the farmer's revenue. Market intermediaries, merchants, and distributors take a large portion of the earnings from farmer production. Moreover, the intermediaries act like an in-charge of the market, which will affect both the customer and the farmer. As a result, farmers will not receive adequate profit for their subsequent crops, resulting in debt. Even some farmers commit suicide because of their indebtedness and reduced revenue.

So, we introduced the concept of eliminating the intermediaries and establishing communication between the farmers and the consumer known as a Farm-to-Home Anonymous Authentication with Privacy Preservation Scheme (FHAAPS). It is a web-based customer service platform. It has become a convincing and widely accepted commercial standard for buyers and sellers to communicate and engage in the purchasing process. As a result, the main organisation is housed in server space, whereas the sub-branches are housed in distinct places. The information from the sub-branches will be transferred to the authenticated users of the specific location. Online communication of information for any online service may be vulnerable to malicious attacks. Unless adequate security practices [1] are

to be implemented, the users could be subject to a variety of assaults, namely, replication attacks and bogus information attacks. The most important security factor to prevent these attacks and perform secure data transactions is authentication. If users are not provided with authentication, a malicious user could mislead the data in the trusted farm-to-home (TFH) platform. Here, TFH may not act as a profitable middleman, but act as a link between the farmer and the consumer.

To ensure secure communication [2], an unprofitable centralized main branch generates a fully authenticated TFH in different locations offline. Initially, authenticated TFH provides authentication parameters to the end entities (farmers/consumers) through offline registration. These authentication parameters [3] increase the trust between the entities and the TFH. The keys generated by TFH are used to verify the data communication authenticity. Only verified users can get access to message their requirements through the specific application provided by the TFH. Moreover, the scheme will be a popular way for purchasers to purchase goods and a handy platform for the farmers to improve their revenues. In addition, it transforms into a two-way profitable platform by which both the consumer and farmer get benefitted. In the existing system, even though user authentication is provided [4, 5], there may be a chance of identity theft of the user, resulting in a loss of privacy and protection for entities. Some malevolent users can gain access to the network of authenticated users by stealing information from authorised users. There are some protection solutions that prohibit fraudulent individuals from gaining access to the network. But they require a significant amount of computing time, and there is a risk that the user's real identity would be revealed using these approaches [6, 7]. So in this proposed scheme, we provide anonymous authentication by using dummy identities of entities to provide service for the end users, which takes less computational and verification cost.

Data integrity is a critical security component [8–10]. The farm-to-home (FH) main branch is a trusted element that preserves data and monitors the TFH, which in turn monitors the end entities. Moreover, the basic security criteria such as privacy, confidentiality, integrity, and availability are met in our scheme. To achieve long-term trading communications between end users and TFH, a straightforward privacy revocation mechanism and reliable anonymous authentication with little complexity are proposed to sustain end-user entity communication. The scheme is developed in order to meet the following critical security standards:

(i) End users obtain anonymous authentication keys at the time of initial offline registration, which is stored separately in the TFH database to protect their privacy

(ii) If any attack happens, the TFH will trace the fraudulent person's identity and broadcast it to all the authenticated users and also revoke them from the network

(iii) It provides end users with robust data protection and privacy

1.1. Our Research Contributions. The suggested approach's main contributions to enhance the aforementioned security standards are as follows:

(i) To reduce the risk of data loss when transferring information from TFH to end users (either farmers or customers) or vice versa

(ii) To design an authentication scheme for the end users with less computation complexity which provides anonymity and conditional privacy

(iii) To provide the user's data integrity with minimum signature and certificate verification cost

(iv) -To provide conditional privacy to all entities in the system by using conditional tracking to trace the real identities of all compromised entities

The following is a summary of the rest of the article: In the next section, related works are explained. The overview of the system is explained in Section 3. In Section 4 the proposed methodology of our approach is discussed. The proposed approach to security and performance analysis is addressed in Sections 5 and 6. Finally, Section 7 concludes the work.

2. Related Works

In recent years, online trading has attracted several end users due to the massive development of ICT. The existing trading is affected by a number of security issues because of the presence of mediators. Several works related to security issues are discussed in this section. León et al. [11] proposed anonymous communication in e-government services. The authors focussed on anonymous communication with the application called delta. Its function is to enable the offers and lay the groundwork for future e-government service procedures. When information is exchanged, anonymous communication is implemented through the delta application. The message integrity is not maintained in this work. Moreover, a separate communication channel is required for the transfer of information. Fouladfar [12] proposed a work that is based on the following two types of securities: soft securities and hard securities. Hard securities are related to information hiding and cryptography, whereas soft security deals with trust issues. In this work, a security graph is used for exchanging information from one to another. But, this approach is unable to detect the real identity of the malevolent users. Almuzairai et al. [13] proposed a privacy protection scheme for users of e-commerce systems. In this work, the importance of digitalized services is focussed. Through these online services, the user shares their personal data in e-commerce trading. Since it is open source, it is easy for an attacker to interrupt the user's data.

Liu et al. [14] proposed a blockchain-based autonomous transaction settlement system for IoT-basede-commerce. The system proposed a normal chain with three layered blockchain networks which can improve the efficiency of the transaction and the stability of the system. Though this work has provided security in an advanced way, the

computational cost of this approach is high and the system is to be upgraded frequently with respect to technology. Aitzhan et al. [15] proposed a decentralized energy trading model through multisignatures, blockchain, and anonymous messaging streams. In this work, the current financial infrastructures are centralised, implying that a trusted third party is involved which handles the payments and security. Though peer-to-peer communication can be done through data replication methods, there are scalability issues in this work. Wang et al. [16] work on the evaluation method for e-commerce transaction systems with unobservable transactions. This work can be used in the analysis and design of the system for online transaction processes. However, some e-commerce systems are incompatible with this approach because they ignore data information.

Zhang et al. [17] proposed a hybrid trust evaluation framework for e-commerce in online social networks. This work is based on improving trust managing mechanisms. Though it can give an accurate trustworthy view, it is not much accurate in the complex social network trading platforms. Jiang et al. [18] proposed a privacy-preserving business protocol by using private smart contracts to ensure privacy in e-commerce. This approach allows both seller and buyer to make deals without revealing their real identities such as name, address, and phone numbers. In this work, the user's privacy is preserved, but there is no conditional tracking mechanism to revoke the privacy of a compromised entity in the system. Niu et al. [19], proposed a TPDM system to enhance the truthfulness and privacy preservation in data markets. This system is internally built in an encrypt-then-sign fashion by using homographic encryption and identity-based signature which ensures the privacy of the user's data. Though the proposed work allows batch verification, data processing, and outcome verification. But an external attacker can forge the signature of the authorised users and they can send fake messages into the system. Moreover, this system uses profile-matching techniques which may give false results, if we compare authorised profiles with a fake profile which is created by a malicious user.

In [20], Fan et al. proposed a secure mutual authentication protocol using an asymmetric cryptosystem and universal second factor (U2F) technique to ensure security in mobile payments in e-commerce platforms. This system enhances the security and privacy of user account information in the mobile payment transaction process. But, when the servers and clients are mutually authenticating each other, they will use their real identities which may lead to identity theft by malicious or compromised users. Tsobdjou et al. [21] proposed a mutual authentication protocol based on elliptical curve cryptography for communication between the server and mobile client to avoid additional hardware and to withstand impersonation attacks. Moreover, the authors have focussed on session key security, perfect forward secrecy, resistance to replay, and insider attacks. But the system cannot withstand a denial of service attack, and it may have more communication and computation overheads because of more complexity.

Trade Map as an integrated architecture is proposed in [22], to enable privacy in online end-to-end marketplace transactions. Here, the authors used the FINMA-KYC platform to register and authenticate entities. Moreover, blockchain-based transactions are used to store the data by employing Ethereum smart contracts. In addition, the user data is only visible to KYC platforms in registration the phase, thereby providing anonymity to the user's data. But, because of other KYC platform involvement, there may be a lot of communication and computation overheads in the system while identifying the legitimacy of the users. In [23], Li et al. proposed a cross-realm authentication scheme of Kerberos protocol in-home delivery services. This Kerberos protocol is applied in online ordering and offline delivery businesses to establish authenticity for all entities in the system. Though physical security is ensured, authentication of delivery men is crucial and there may be a chance of privacy leakage because of the usage of real identities. In [24], Yuniati et al. proposed a credit card payment method using visual cryptography to withstand attacks like phishing and identity theft. The authors applied visual cryptography to the captcha which is generated by the merchant during the registration phase. Though it enhances the e-payment security in terms of authorisation and confidentiality, there is a possibility for an intruder to modify the visual image, so that it cannot be decrypted appropriately at the receiver side. Further, it cannot withstand a man-in-the-middle attack.

3. System Overview

The system model, pairing parameters, and attack models are described in this section.

3.1. System Model. Trusted farm-to-home (TFH) branches, delivery agents (DA), and end users are the major components of the proposed system. Figure 1 shows the system model of the farm-to-home platform. An end user can be a farmer or a consumer. The delivery agent delivers/gathers goods at the consumer/farmer location and RFID tags are incorporated in the dummy identity of the delivery agent to trace the location of him by the end user/TFH at any time. Initially, the trusted main branch installs TFH in the required areas in an offline manner.

3.1.1. Trusted Farm-to-Home (TFH) Platform. TFH is the main component of our proposed system. It is a trusted authority, and it is extremely impossible for an attacker to compromise the farm-to-home platform. When an end-user registers in the TFH, he will receive specific certified keys that will allow him to communicate with the TFH using a one-time password (OTP). Initially, the end users (farmers/consumers) register at TFH by submitting their credentials in the offline mode. Here, the entire communication between the TFH and the end users will be done in a safe manner. If a user requests his requirements to the TFH, the TFH will send him an OTP, to check his authenticity. Similarly, if a farmer is willing to sell the goods, he will inform TFH about the details of the goods. Then, the

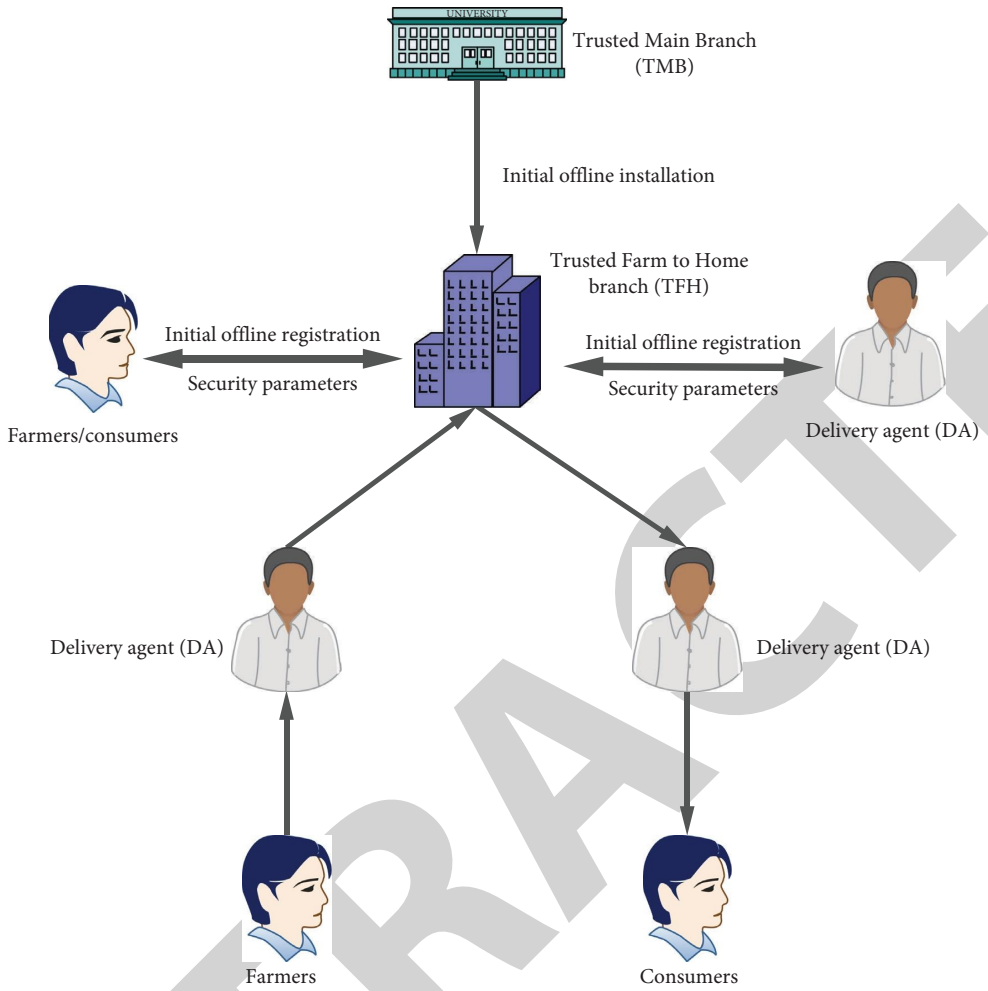

Figure 1: System model of the farm-to-home platform.

TFH will issue him an OTP to confirm whether he is a legitimate user or not. So, once the authenticity of the consumer/farmer is verified, only then transfer of goods takes place between the end user and TFH or vice versa.

3.1.2. End Users. An end user can be a farmer or a buyer who is willing to sell or buy goods at TFH. The user's (farmer/consumer) registration can be done in an offline manner at TFH. The end user can communicate with TFH to get service at any time. After successful offline registration, the farmer/user will be provided with definite credentials. Once the farmer logs into the producer portal with his credentials, he will be initially verified by the OTP. After successful validation, he will send the details of the commodities to a specific TFH. Similarly, consumers also login into the portal and will be initially verified by OTP. After successful verification, he sends his demand message to TFH. Based on the requirements, TFH provides the service to the end user.

3.1.3. Delivering Agents (DA_i). Delivery agents are the essential entity in our proposed scheme, who provide service to the end users. Initially, the registration of the delivery agents can be done in an offline mode to their nearest TFH. When the end user contacted the TFH about his requirements, then the TFH will message to the DA_i, who are working under the TFH to contact them. Then, after the arrival of DA_i, TFH will check his identity and provide him with the details of the particular end user like location and dummy identity. A dummy identity is used to provide privacy to the user's real identity thereby ensuring anonymity. Here, there may be a chance for the DA_i being compromised. Hence, at the time of the registration, an RFID tag will be attached to the DA_i and it will be activated at the time of delivering or carrying the products to/from the end users. After reaching the end user's location, the user will authenticate the DA_i. Only, if the DA_i is an authorised agent, then the farmer will provide his goods or the consumer will receive his requested goods. The usage of RFID tags which are provided to DA_i will allow TFH to monitor the progress of the delivery of the goods. Notations used in this work are shown in Table 1.

3.2. Security Attack Models. The attackers are divided into two categories in the suggested strategy. One type of attacker is an internal one, while the other is an external one.

Table 1: List of notations.

Notations	Description
TFH	Trusted farm-to-home
DA	Delivery agent
OTP	One time password
j, k	Master secret keys of TFH
K_1, J_1	Public keys of TFH
e	Bilinear pairing
DRI_I	Delivery agent's real identity
$DADI_i$	Delivery agent dummy identity
M_i^k, N_i^k	Elements of tracking list
Dk	Delivery agent key
P_m	Short-time private keys
R_m	Short-time public keys
DCK	Delivery agent contender key
$cert_j$	Delivery agent anonymous certificate
sig	Delivery agent short time signature

Both external and internal attackers pose a threat, but there will be a more threat from the external attacker. Internal attackers can attack the proposed system by using the keys which are given to the end users at the time of registration. If the end users are compromised, then the privacy of the compromised entity will be revoked by the TFH. But, there may be a possibility of external attackers gaining access to the valid user's personal information and trying to change their data. So, the proposed approach is planned to avoid the influence of the following attacks from external attackers:

(i) Impersonation attack: an attack in which the attacker gets access to the authorised users and manipulates the end user's required data.

(ii) Certificate and key duplication attack: without the assistance of the authenticated user, the malicious user can construct similar credentials of the authenticated user and access the valid end user site for their benefit.

(iii) Identity revealing attack: the focus of this attack is on the user's privacy. Here, the intruders illegally gather the confidential information of the end users.

(iv) Fake message attack: by changing the information of the end entities, an attacker can deliver fake information to the TFH.

3.3. Bilinear Pairing. Let G_a, G_b, and G_T be the three multiplicative cyclic groups of order n. Here, n represents the large prime number. Let g_a and g_b belongs to the generators G_a and G_b, respectively. Moreover, δ be an isomorphism from G_b to G_a such that $\delta(g_b) = g_a$. The bilinear mapping function is represented as e: $G_a \times G_b \longrightarrow G_T$ and it should obey the following properties:

(i) Bilinear: $e(g_a^p, g_b^q) = e(g_a, g_b)^{pq}$ for all $g_a \in G_a$, $g_b \in G_b$, and $p, q \in Z_n^*$

(ii) Nondegeneracy: $e(g_a, g_b) \neq 1G_T$

(iii) Computability: there exists an efficient algorithm to compute the bilinear map e: $G_a \times G_b \longrightarrow G_T$.

4. Proposed FHAAPS

In this section, the system initialization and delivery agent's authentication processes are described. Initially, end users and delivery agents should register in the TFH platform with their credentials through offline mode. After successful registration, the TFH provides the required credentials to the end user and delivery agent. If the end user (farmers/consumers) wishes to sell or buy a commodity, he must send his sale/demand message to TFH through the specific application. Once the username and password are successfully entered into the application, the end users receive an OTP (one-time password). Once the OTP is entered, the end users are allowed to send their sale/demand message to TFH. After receiving the message information, the TFH assigns this task (buying/delivering farm goods) to the nearby authenticated delivery agent. Once the message is received, the delivery agent performs the specific task assigned to them. Here, the delivery agent should be authenticated by the end user. Once the delivery agent is authenticated, the end user (farmer/consumer) may send/receive the agricultural goods to/from the TFH through the delivery agent. Here, the message integrity and legitimacy are performed by bilinear pairing.

4.1. System Initialization. The TFH issues system parameters by using the bilinear parameters (G_a, G_b, p, e) as follows: Initially, the TFH selects the random numbers $j, k \in Z_p^*$ as the master secret keys and computes $K_1 = g_a^k$ and $J_1 = g_a^j$. Then, TFH selects the secure cryptographic hash function H: $\{0,1\}^* \longrightarrow Z_p^*$. Finally, the TFH issues the FH parameters and broadcasts in the open network platform as $FH_{param} = (G_a, G_b, p, g_a, g_b, K_1, J_1, H, e)$.

4.2. Delivery Agent (DA_i) Authentication by End Users. In our proposed scheme, the delivery agent authentication process consists of DA_i registration, required keys generation, generation of anonymous certificate and signature, verification of both certificate and signature, and conditional tracking.

4.2.1. DA_i Registration. Initially, DA_i should register in TFH through offline mode. During initial offline registration, the Delivery agent (DA_i) have to submit the necessary information such as user name, address, mail ID, and phone number to the TFH. Once the registration process is successfully completed, the TFH provides credentials to the DA_i.

4.2.2. Key Generation. After DA_i registration, the TFH generates the necessary secret keys for the DA_i by using a key generation scheme. Initially, the TFH generates the delivery agent's (DA_i) real identity (DRI_I) and also dummy identity ($DADI_i$). This $DADI_i$ is in-build with an RFID tag. To generate a dummy identity $DADI_i$, the TFH uses two random numbers $f_i, h_i \in Z_p^*$ and then computes $DADI_i = g_a^{j+k+f_i}$. Then, the TFH maps the original identity with a dummy identity. Moreover, the TFH creates dummy

identities for all delivery agents to check the legitimacy and integrity of the source of information and to track the movement of DA_i. Then, the TFH selects random numbers h_i and f_i such that $h_i, f_i \in Z_p^*$ and computes $M_i = g_a^{1/(h_i+k+f_i)}$ and $N_i = g_a^{k+j+h_i}$ for tracking the identity of DA_i. Then, TFH places these values $(DARI_i, DADI_i, M_i^k, N_i^k)$ in the tracking list and issues the delivery agent key (Dk) to DA_i as $Dk = (DADI_i, M_i^k, N_i^k, P_i, Q_i)$ and this Dk will be kept securely by the delivery agent, where $P_i = g_a^{-(j+f_i)}$ and $Q_i = g_a^{-(h_i+k)}$. Once the registration and key distribution process is completed, the delivery agent DA_i become the authenticated agent for delivering/getting the commodities to/from the end users (farmers/consumers).

4.2.3. Anonymous Certificate Generation. The delivery agent DA_i perform the following steps to generate the required anonymous certificates.

Step 1. Initially the DA_i choose random numbers $P_1, P_2, P_3, \ldots, P_r \in Z_p^*$, where $r \leq p$ as short time temporary private keys and computes the short time public keys $R_m = g_b^{P_m}$ for $m = 1, 2..r$.

Step 2. Then, the DA_i generate the anonymous one-time certificate $cert_j$ by using their short-time public keys R_m as follows:

Initially, the DA_i randomly selects $t_1, t_2, t_3, t_4 \in Z_p^*$ and calculates $\mu_1, \mu_2, \mu_3, \varnothing_1, \varnothing_2, \varnothing_3$, where

$$\mu_1 = K_1^{(t_1+t_2)}, \mu_2 = M_i J_1^{(t_1+t_2)}, \mu_3 = N_i K_1^{(t_1+t_2)}, \varnothing_1 = \mu_1^{(t_1+t_2)} + \mu_2^{(t_3+t_4)}, \varnothing_2 = \mu_2^{(t_1+t_2)} - \mu_3^{(t_3+t_4)}, \varnothing_3 = \frac{\mu_1^{t_1+t_2} \cdot \mu_2^{t_3+t_4}}{\mu_3^{t_1+t_4}}. \quad (1)$$

After computing $\mu_1, \mu_2, \mu_3, \varnothing_1, \varnothing_2, \varnothing_3$, the DA_i calculates the delivery agent contender key $DCK = H(DDI_i \parallel J_1 \parallel K_1 \parallel P_i \parallel \mu_1 \parallel \mu_2 \parallel \mu_3 \parallel \varnothing_1 \parallel \varnothing_2 \parallel \varnothing_3 \parallel R_m)$ and then compute the values of $\theta_1, \theta_2, \theta_3$ and θ_4 as below $\theta_1 = t_1 - P_m$, $\theta_2 = t_2 + P_m$, $\theta_3 = t_3 - P_m$, $\theta_4 = t_4 + P_m$

Finally, the DA_i will generate the anonymous certificate as
$cert_j = (DADI_i \parallel R_m \parallel P_i \parallel Q_i \parallel DCK \parallel \mu_1 \parallel \mu_2 \parallel \mu_3 \parallel N_i \parallel \theta_1 \parallel \theta_2 \parallel \theta_3 \parallel \theta_4)$.

(i) Signature generation: the DA_i generate the short-time signature as $\text{sig} = g_a^{(1/P_m+H(CM))}$ to maintain the integrity of the message. Then, the DA_i broadcasts the message as message = $(CM \parallel sig \parallel cert_j \parallel R_m)$ by appending the certificate, signature, and short-time public key. From the received message, the end user extracts the values of $DADI_i, P_i, Q_i, N_i$. Moreover, the end-user computes $H_i = DADI_i \times P_i$, $D_i = N_i \times Q_i$, and check whether $H_i = K_1$ and$D_i = J_1$. If they are equal, then the end user accepts the DA_i as an authorised DA_i. Initially, the delivery agent sends this message to the end user while communicating with them. The end user authenticates the delivery agent and verifies the integrity of the message. Once the verification is completed, the end user allows the delivery agent to perform their specific function; i.e., the delivery agent (DA_i) authentication by the end user. Here, the end user (farmer/consumer) will authenticate the delivery agent by using DA_i's certificate (Cer_j) and signature (sig) by following the verification process.

(ii) Verification process: after receiving the Message = $(CM \parallel \text{sig} \parallel \text{cert}_j \parallel R_m)$ from the delivery agent, the end user (farmer/consumer) will perform the following steps to authenticate the delivery agent.

Step 1: To check the authenticity of the source message, the receiver will calculate $H_i, I_i, \beta_1', \beta_2', \beta_3'$ parameters, where

$$H_i = DADI_i \times P_i, D_i = N_i \times Q_i, \varnothing_1' = \mu_1^{(\theta_1+\theta_2)} + \mu_2^{(\theta_3+\theta_4)}, \varnothing_2' = \mu_2^{(\theta_1+\theta_2)} - \mu_3^{(\theta_3+\theta_4)}, \varnothing_3' = \left(\frac{\mu_1}{\mu_3}\right)^{\theta_1} \left(\frac{\mu_2}{\mu_3}\right)^{\theta_4} \cdot \mu_1^{\theta_2} \cdot \mu_2^{\theta_3}. \quad (2)$$

Step 2: By using the above parameters the end user computes
$DCK' = H(DDI_i \parallel H_i \parallel D_i \parallel P_i \parallel R_m \parallel \mu_1 \parallel \mu_2 \parallel \mu_3 \parallel \varnothing_1' \parallel \varnothing_2' \parallel \varnothing_3')$ and it verifies whether $DCK = DCK'$. If it holds, the end user accepts the delivery agent message otherwise it will be discarded. Moreover, the end user also checks the dummy identity (incorporated RFID tag) of the delivery agent by calculating H_i and D_i.

Proof of Correctness

$$\begin{aligned}
H_i &= DADI_i \times P_i \\
&= g_a^{j+k+f_i} \times g_a^{-(j+f_i)} \\
&= g_a^k \\
&= K_1, \\
D_i &= N_i \times Q_i \\
&= g_a^{k+j+h_i} \times g_a^{-(h_i+k)} \\
&= g_a^j \\
&= J_1, \\
\varnothing_1' &= \mu_1^{(\theta_1+\theta_2)} + \mu_2^{(\theta_3+\theta_4)} \\
&= \mu_1^{(t_1-P_m+t_2+P_m)} + \mu_2^{(t_3-P_m+t_4+P_m)} \\
&= \mu_1^{(t_1+t_2)} + \mu_2^{(t_3+t_4)} \\
&= \varnothing_1, \\
\varnothing_2' &= \mu_2^{(\theta_1+\theta_2)} - \mu_3^{(\theta_3+\theta_4)} \\
&= \mu_2^{(t_1-P_m+t_2+P_m)} - \mu_3^{(t_3-P_m+t_4+P_m)} \\
&= \mu_2^{(t_1+t_2)} - \mu_3^{(t_3+t_4)} \\
&= \varnothing_2, \\
\varnothing_3' &= \left(\frac{\mu_1}{\mu_3}\right)^{\theta_1} \left(\frac{\mu_2}{\mu_3}\right)^{\theta_4} .\mu_1^{\theta_2}.\mu_2^{\theta_3} \\
&= \left(\frac{\mu_1}{\mu_3}\right)^{t_1-P_m} \left(\frac{\mu_2}{\mu_3}\right)^{t_4+P_m} .\mu_1^{t_2+P_m}.\mu_2^{t_3-P_m} \\
&= \frac{\mu_1^{t_1+t_2}\mu_2^{t_3+t_4}}{\mu_3^{t_1+t_4}} \\
&= \varnothing_3,
\end{aligned} \tag{3}$$

Step 3: once the verification of the delivery agent contender key is performed, the end user checks the integrity of the message as follows:

$$e\left(sig, R_{m.} g_b^{H(CM)}\right) = e\left(g_a, g_b\right), \tag{4}$$

if it holds, then the end user accepts the message otherwise the message will be rejected.

Proof of Correctness

$$\begin{aligned}
e\left(sig, R_{m.} g_b^{H(CM)}\right) &= e\left(\frac{1}{g_a^{P_m + H(CM)}}, g_b^{p_m}.g_b^{H(CM)}\right) \\
&= e\left(\frac{1}{g_a^{p_m + H(CM)}}, g_y^{p_m+H(CM)}\right) \\
&= e\left(g_a, g_b\right) \text{(by using the bilinear property).}
\end{aligned} \tag{5}$$

(iii) Conditional tracking: if any conflict occurs or any delivery agent is compromised, then the end user can easily detect the real identity of that delivery agent by using the tracking parameter M_i^k. The end user calculates μ_2^k/μ_1^j to get M_i^k with the help of the $\text{cert}_j = (DADI_i \parallel R_m \parallel P_i \parallel Q_i \parallel DCK \parallel \mu_1 \parallel \mu_2 \parallel \mu_3 \parallel N_i \parallel \theta_1 \parallel \theta_2 \parallel \theta_3 \parallel \theta_4)$.

$$\begin{aligned}
\frac{\mu_2^k}{\mu_1^j} &= \frac{\left(M_i J_1^{(t_1+t_2)}\right)^k}{\left(K_1^{(t_1+t_2)}\right)^j} \\
&= \frac{M_i^k.J_1^{(t_1+t_2)k}}{K_1^{(t_1+t_2)j}} \\
&= \frac{M_i^k.g_a^{(t_1+t_2)jk}}{g_a^{(t_1+t_2)jk}} \\
&= M_i^k.
\end{aligned} \tag{6}$$

Once M_i^k is calculated, the end user maps these parameters to the real identity of the delivery agent by using the tracking list. Moreover, the end user revokes the privacy of the delivery agent and removes the compromised DA_i from the network to avoid further damage.

5. Security Analysis

This section discusses the security analysis of our proposed approach. The constraints that are analysed in this section are user privacy, data integrity, and authentication. In this scheme, the signature and certificate generation of the delivery agent are the essential parameters to provide defence against the security attacks such as impersonation, key duplication, and masquerade attacks. In this approach, it is not possible for an outside attacker to generate the valid signatures and certificates of an authorised user. The registration of both the end user entities i.e., registration of both farmer and consumer will be done in the offline mode at the trusted farm-to-home (TFH) platform. The end users will login into the "farm-to-home" application by using the credentials which

are given by the TFH at the time of offline registration. So, in our proposed system it is impossible for an attacker to create duplicate keys and inject fake messages into the network. Moreover, in our scheme impersonation attack can't be performed by the external attacker, because the attacker must acquire the short-term private key of the delivery agent which will be issued by the TFH in the offline mode. In addition, these private keys are only known to the delivery agent. As a result, it is difficult for the attacker to acquire the delivery agent's information without compromising the offline registration process. The protection against various attacks is described in the following subsection:

5.1. Protection against Impersonation Attack. To perform an impersonation attack, an intruder needs to find the confidential parameters of the authenticated user such as, M_i and N_i. For finding the values of M_i and N_i, the attacker has to detect the values of the μ_2 and μ_3 in the delivery agent's certificate $cert_j$. Moreover, the values of the μ_2 and μ_3 are calculated as $\mu_2 = M_i J_1^{(t_1+t_2)}$ and $\mu_3 = N_i K_1^{(t_1+t_2)}$. In this μ_2 and μ_3 equations, t_1 and t_2 values are the random numbers that are chosen by the users. So, it is difficult for the attacker to find the values of μ_2 and μ_3 because of Elliptic Curve Discrete Logarithm Problem (ECDLP). It is extremely difficult to find the t_1 and t_2 in μ_2 and μ_3 because it involves ECDLP complexity which is represented as $[p^{(1/2)+o(1)} \log(\log \varnothing)]$, where the '$\varnothing$' represents the number of delivery agents. As a result, breaking an anonymous delivery agent certificate and carrying out an impersonation attack is extremely difficult.

5.2. Protection against Fake Message Attack. If an attacker wants to send fake messages to the end users, he/she must find the values of the dummy identity DDI_i, P_i, Q_i, and N_i. Here, $H_i = DADI_i \times P_i = K_1$ and $D_i = N_i \times Q_i = J_1$. Here, the internal parameters like $DADI_i, P_i, Q_i$ are generated by the TFH and given to the delivery agent during the offline registration. So, the external attacker is unable to find the values of h_i, f_i, K_1, and J_1 that are present in the $DADI_i, P_i, Q_i$, and N_i because of the ECDLP. Moreover, the values of h_i and f_i are selected randomly and the values of the J_1 and K_1 (master secret keys) are only known to TFH. In addition, the complexity of finding these values based on ECDLP is $O[p^{(1/2)+o(1)} \log \Theta]$ where 'Θ' represents the number of delivery agents. There is a complexity of $O[2^{\Theta} - 1]$ while finding the h_i and f_i values. So, it is extremely difficult to find the values of h_i, f_i, K_1, and J_1 and to find the values of H_i and D_i , as there will be a complexity of $O([p^{(1/2)+o(1)} m \log \Theta].[2^{\Theta} - 1]^2)$ and $O([p^{(1/2)+o(1)} \log \Theta]^2.[2^{\Theta} - 1])$. So, it is hard to carry out a bogus message attack for an attacker. Therefore, our proposed approach can withstand against this attack.

5.3. Conditional Privacy Preserving. In our proposed approach, the delivery agent (DA_i) generates an anonymous certificate and signature to conceal his true identity. The end user knows only the dummy identity ($DADI_i$) of the DA_i. So, the real identity of DA_i is hidden. If any miscellaneous activities are observed from the DA_i side, then the TFH reveals the real identity of the DA_i. Moreover, if the DA_i is compromised, then TFH computes the value of (μ_2^k/μ_1^j) to get M_i^k from the tracking list and revoke the privacy of the particular DA_i.

5.4. Protection from Nonrepudiation Attack. Our proposed scheme is resistant to nonrepudiation attacks. While receiving the information from the DA_i, the authorised end user checks the authenticity of the DA_i using an anonymous certificate and signature verification. As a result, the DA_i cannot repudiate after getting the information from the end user. End-user repudiation is also not possible, because the end user logs into his account using the valid credentials provided by TFH during initial offline registration. Moreover, login is validated by the OTP sent by TFH at the time of logging in.

5.5. Unlinkability. During the information exchange between the delivery agent and end users, our proposed approach provides unlinkability of security parameters such as anonymous certificates and signatures. In our scheme, the DA_i uses temporary short time private and public keys to create anonymous certificates and signatures. The lifetime of the keys is noticeably short and is known as short-term keys. The lifetime of these keys will expire after the successful exchange of information by validating the signature and certificate. For further information exchange, new random keys will be generated. Once the generation is completed, these keys get expire and new keys are to be generated for the next information exchange. Thus, short-time keys and unlinkability are interlinked. As a result of this unlinkability, the intruder cannot perform any attacks by detecting DA_i s true identity during the information exchange.

5.6. Anonymity and Privacy Preservation. In our proposed scheme, the delivery agents attach a signature and certificate to their confirmation message. So, it is extremely hard to trace the real identity of the delivery agent who signed the message. Moreover, the certificate and signature are generated using short-term private keys that will be changed by DA_i after a certain period of time. As a result, attackers will have zero knowledge of the real identity of DA_i who signed the messages with their dummy identities. Even if the dummy identities of the DA_i are revealed, they are not useful for the external attacker to seek information about the true identity of the particular DA_i.

5.7. Protecting Against Message Modification Attack. In the message modification attack, an external attacker modifies the message or changes the content of the message before it is received by the end user. In our proposed approach, DA_i transfer the message as Message = $(CM \parallel sig \parallel \text{cert}_j \parallel R_m)$. Here, a signature is appended to the message. Moreover, a signature is calculated as $g_a^{(1/P_m + H(CM))}$, where P_m is the short-term private key. Its value is only known to DA_i, and it is randomly changeable for every exchange of information.

Table 2: Computational cost of various schemes.

Schemes	For single signature and certificate verification	For 'n' signature and certificate verification
Wazid et al.	$3T_m + 2T_p + T_e + 5T_h$	$3nT_m + 2nT_p + nT_e + 5nT_h$
Odelu et al.	$3T_m + T_e + 6T_h$	$3nT_m + nT_e + 6nT_h$
Kaur et al.	$4T_h + 2T_m$	$4nT_h + 2nT_m$
Gong et al.	$5T_p + 2nT_h$	$(1 + 4n)T_p + 2nT_h$
Proposed scheme	$2T_p + 5T_{ex}$	$(1 + n)T_p + 5nT_{ex}$

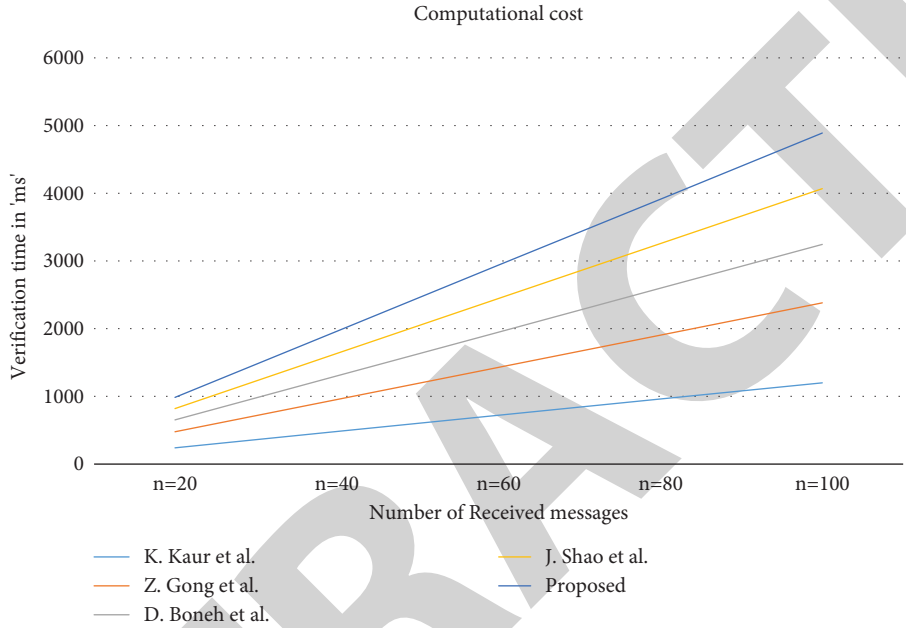

Figure 2: Signature and verification cost of different schemes.

So, it is not possible to create duplicate values of the same signature for message modification. Thus, our proposed approach strongly withstands against the message modification attack.

5.8. Protecting against the Sybil Attack. This attack is performed by the intruder by sending fake messages to the users. Moreover, the intruder makes the user to believe that the message is from the origin branch. However, in our proposed approach, if an intruder wishes to send a false message, he must know the dummy identity of the delivery agent where $DADI_i = g_a^{j+k+f_i}$. Here, j and k are the secret keys that are only known to TFH and f_i value is randomly generated for every information transaction. To create multiple identities, the values of these parameters must be known to an external attacker, otherwise, it is impossible for him to create multiple identities for sending fake messages.

6. Performance Analysis

In this section, the proposed scheme's performance is evaluated in terms of computation and communication costs. The total cost incurred for the verification of the signature and certificate is known as computational costs. Communication costs are the number of bits needed for information to be communicated.

6.1. Computational Complexity. Computational cost refers to the total verification time required for single/n certificates and single/n signatures. This is primarily calculated to verify the authenticity of the delivery agents arriving at the end user and also to check the integrity of the information. The proposed scheme's total verification time is compared to existing works such as Wazid et al. [25], Odelu et al. [26], Kaur et al. [27], and Gong et al. [28]. Let T_p, T_h, T_m, and T_e represents the time taken to perform the pairing operation, hashing operation, one point multiplication operation and exponential operation, respectively. The Type-Acurve-basedpairing-based cryptography (PBC) library is used to perform all of the above operations. Moreover, for our executions, we used a 2 GHz PC with 8 GB RAM and Cygwin version 1.7.35–15 [29]. T_p, T_h, T_m, and T_e have time values of 1.6 ms, 2.7 ms, 0.6 ms, and 0.7 ms, respectively. Here, "ms" represents time in milliseconds. The time taken for pairing and hashing operations is more in the calculation of computational cost based on the timing parameters. When compared to the existing schemes, Table 2 clearly shows that our proposed scheme consumes less computational cost.

Table 3: Communication cost of various schemes.

Scheme	Communication cost for a single message (bits)	Communication cost for n messages (bits)
Odelu et al.	2912	$2912n$
Wazid et al.	1408	$1408n$
Jo et al.	1920	$1920n$
Kaur et al.	1120	$1120n$
Proposed scheme	800	$800n$

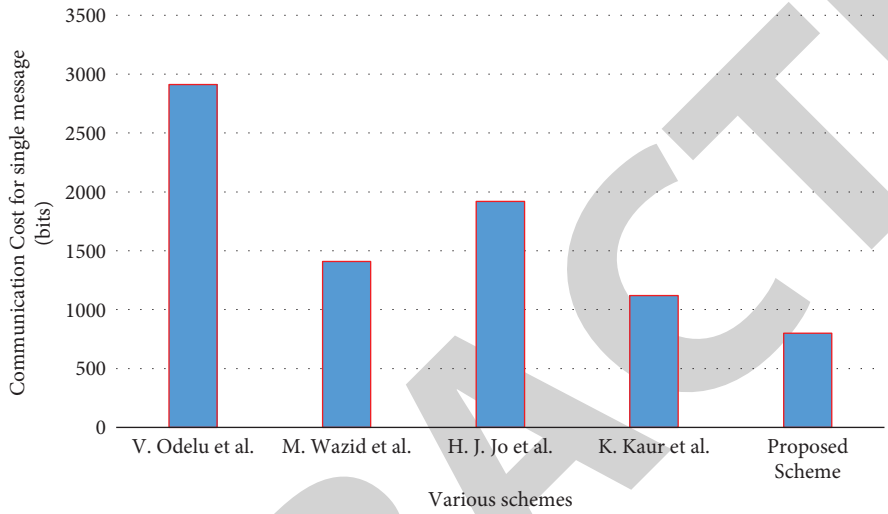

Figure 3: Communication cost of different schemes.

Moreover, in our proposed scheme, there are no single-point multiplicative or additive operations. Further, in our scheme, verifying a single certificate and signature takes only 6.2 ms. Figure 2 clearly shows that our proposed scheme requires less computational time for both signature and certificate verification.

6.2. Communication Cost. The proposed scheme communication overhead is examined and compared to other comparable schemes such as Odelu et al. [26], Wazid et al. [25], Jo et al. [30], and Kaur et al. [27]. The data size of the information exchanged between the delivery agent and the end user is considered to analyse the communication overhead. The proposed scheme considers the size of the confirmation message to be 160 bits, the size of an anonymous signature to be 160 bits, the size of the certificate to be 160 bits, and the length of security parameters such as a public key to be 320 bits. So, the entire message consumes Message = $(CM \parallel sig \parallel \text{cert}_j \parallel R_m) = 800$ bits. Table 3 summarises the communication overhead of the proposed scheme and other existing related schemes. The communication cost for different schemes is depicted in Figure 3. As a result, when compared to existing schemes, our proposed scheme evidenced to be notable in terms of communication cost.

7. Conclusion

In this work, a new FHAAPS is proposed to provide secure and efficient anonymous authentication with privacy preservation in the farm-to-home management system. In the FHAAPS, the delivery agent is anonymously authenticated by the end user to check the legitimacy of the DA_i. Moreover, this scheme allows the end users to trade with a lot of trusts by providing conditional privacy and security to them. In addition, the privacy of the genuine delivery agent is preserved and the privacy of the compromised delivery agent is revoked from the farm-to-home platform. The security analysis section ensures that the proposed scheme provides the essential security features, and the performance analysis section shows that the proposed scheme performs better than the other existing schemes in terms of computational overhead and communication overhead. Hence, our scheme outperforms

the existing scheme and provides an efficient transfer of commodities between the end users and TFH. The future work of this scheme is to create a tracking system for all carrier bags by attaching RFID tags to them, thereby allowing the tracking of goods more efficiently in case of any dispute.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors thank KPR Institute Engineering and Technology, Tamil Nadu, VIT University, Andhra Pradesh, and Nisantasi University, Istanbul, Turkey.

References

[1] M. M. Hamdi, Y. A. Yussen, and A. S. Mustafa, "Integrity and authentications for service security in vehicular ad hoc networks (vanets): a review," in *Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization And Robotic Applications (HORA)*, pp. 1–7, Ankara, Turkey, June 2021.

[2] J. Subramani, A. Maria, R. B. Neelakandan, and A. S. Rajasekaran, "Efficient anonymous authentication scheme for automatic dependent surveillance-broadcast system with batch verification," *IET Communications*, vol. 15, no. 9, pp. 1187–1197, 2021.

[3] A. Iqbal, A. S. Rajasekaran, G. S. Nikhil, and M. Azees, "A secure and decentralized Blockchain based EV energy trading model using smart contract in V2G network," *IEEE Access*, vol. 9, pp. 75761–75777, 2021.

[4] P. Kumar and M. Liyanage, "Efficient and anonymous mutual authentication protocol in multi-access edge computing (mec) environments," *IoT Security*, vol. 6, pp. 119–131, 2019.

[5] Y. Jiang, K. Zhang, Y. Qian, and L. Zhou, "Anonymous and efficient authentication scheme for privacy-preserving distributed learning," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2227–2240, 2022.

[6] A. Arasan, R. Sadaiyandi, F. Al-Turjman, A. S. Rajasekaran, and K. Selvi Karuppuswamy, "Computationally efficient and secure anonymous authentication scheme for cloud users," *Personal and Ubiquitous Computing*, vol. 25, 2021.

[7] T.-F. Lee, X. Ye, and S.-H. Lin, "Anonymous dynamic group authenticated key agreements using physical unclonable functions for internet of medical things," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 15336–15348, 2022.

[8] S. Aghapour, M. Kaveh, D. Martín, and M. R. Mosavi, "An ultra-lightweight and provably secure broadcast authentication protocol for smart grid communications," *IEEE Access*, vol. 8, pp. 125477–125487, 2020.

[9] N. V. Abhishek, M. N. Aman, T. J. Lim, and B. Sikdar, "DRiVe: detecting malicious roadside units in the internet of vehicles with low latency data integrity," *IEEE Internet of Things Journal*, vol. 9, 2021.

[10] F. Zhu, X. Yi, A. Abuadbba et al., "Certificate-based anonymous authentication with efficient aggregation for wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12209–12218, 2022.

[11] D. Leon, F. Mayorga, J. Vargas, R. Toasa, and D. Guevara, "Using of an anonymous communication in e-government services: in the prevention of passive attacks on a network," in *Proceedings of the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, Caceres, Spain, June 2018.

[12] F. Fouladfar, "Proposing a distributed algorithm to finding malevolent entities and improving security in e-commerce environments," in *Proceedings of the 2016 10th International Conference on E-Commerce in Developing Countries: With Focus on E-Tourism (ECDC)*, Isfahan, Iran, April 2016.

[13] S. Almuzairai, S. Alaradi, and N. Innab, "Ensuring privacy protection of the users of e-commerce systems," in *Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, Saudi Arabia, April 2018.

[14] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: a blockchain-based normalized autonomous transaction settlement system for IoT-basedE-commerce," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4680–4693, 2019.

[15] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, Blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[16] M. Wang, Z. Ding, and P. Zhao, "Vulnerability evaluation method for E-commerce transaction systems with unobservable transitions," *IEEE Access*, vol. 8, pp. 101035–101048, 2020.

[17] B. Zhang, R. Yong, M. Li, J. Pan, and J. Huang, "A hybrid trust evaluation framework for E-commerce in online social network: a factor enrichment perspective," *IEEE Access*, vol. 5, pp. 7080–7096, 2017.

[18] Y. Jiang, C. Wang, Y. Wang, and L. Gao, "A privacy-preservingE-commerce system based on the Blockchain technology," in *Proceedings of the 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, Hangzhou, China, March 2019.

[19] C. Niu, Z. Zheng, F. Wu, X. Gao, and G. Chen, "Trading data in good faith: integrating truthfulness and privacy preservation in data markets," in *Proceedings of the 2017 IEEE 33rd International Conference on Data Engineering (ICDE)*, San Diego, CA, USA, May 2017.

[20] K. Fan, H. Li, W. Jiang, C. Xiao, and Y. Yang, "Secure authentication protocol for mobile payment," *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 610–620, 2018.

[21] L. D. Tsobdjou, S. Pierre, and A. Quintero, "A new mutual authentication and key agreement protocol for mobile client—server environment," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1275–1286, 2021.

[22] S. R. Niya, S. Allemann, A. Gabay, and B. Stiller, "Trademap: a finma-compliant anonymous management of an end-2-end trading market place," in *Proceedings of the 2019 15th International Conference On Network And Service Management*, Halifax, NS, Canada, February 2019.

[23] H. Li, Y. Niu, J. Yi, and H. Li, "Securing offline delivery services by using Kerberos authentication," *IEEE Access*, vol. 6, pp. 40735–40746, 2018.

[24] T. Yuniati and R. Munir, "Secure e-payment method based on visual cryptography," in *Proceedings of the 2018 3rd International Conference On Information Technology,*

Information System And Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, November 2018.

[25] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three factor user authentication scheme for renewable energy based smart grid environment," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3144–3153, 2017.

[26] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, p. 1, 2016.

[27] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, S. H. Ahmed, and M. Guizani, "A secure, lightweight, and privacy-preserving authentication scheme for V2G connections in smart grid," in *Proceedings of the IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Paris, France, September 2019.

[28] Z. Gong, Y. Long, X. Hong, and K. Chen, "Two certificateless aggregate signatures from bilinear maps," in *Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, Qingdao, China, July 2007.

[29] Cygwin, "Linux environment emulator for windows," 2020, http://www.cygwin.com/.

[30] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and privacy-preserving metering protocols for smart grid systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1732–1742, 2016.