IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 29 April 2023, accepted 15 May 2023, date of publication 5 June 2023, date of current version 13 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3280542

RESEARCH ARTICLE

A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System

SAMIULLA ITOO[1], AKBER ALI KHAN[2], MUSHEER AHMAD[1], AND M. JAVED IDRISI[3]

[1]Department of Applied Sciences and Humanities, Jamia Millia Islamia, New Delhi 110025, India
[2]Department of Applied Sciences and Humanities, IIMT College of Engineering, Greater Noida, Uttar Pradesh 201310, India
[3]Department of Mathematics, College of Natural and Computational Science, Mizan-Tepi University, Tepi Campus, Mizan, Ethiopia

Corresponding author: M. Javed Idrisi (javed@mtu.edu.et)

ABSTRACT Agriculture plays a vital role in the economic life cycle of an agrarian country and considers the backbone of the economy. It supplies not just raw food materials, but also a vast number of job opportunities. Therefore, modern technology is required in agriculture to increase productivity. Wireless Sensor Networks (WSN) could be used to monitor climatic parameters in an agriculture field, such as the acidity level of soil, soil moisture, humidity, light, and so on. Climate variables have a significant impact on crop growth, quality, and productivity. These factors contribute to increased agricultural productivity in terms of both quantity and quality. WSN, on the other hand, has security risks such as impersonation, alteration, interference, and interception all of which have negative effects on crop production and other agricultural activities. The primary issues for agricultural WSN are hence privacy preservation and security enhancement. In this paper, we proposed a privacy-preserving and efficient key agreement framework for smart agriculture monitoring systems by using elliptic curve cryptography and hash function. The proposed framework is secure against various security assaults and provides secure communication in smart agriculture monitoring systems. We demonstrate the accuracy of the proposed protocol for mutual authentication and key exchange using BAN logic, and we also simulate the security correctness of the encrypted proposed framework using the well-known security verification Scyther tool. Using the ROR model, we formalize the security of the proposed system. Further, we provide a comparison based on security features, computation, and communication overheads comparison between the proposed protocol and similar protocols in the same context. Hence, when compared to other similar protocols in the same environment, the proposed protocol provides superior security and efficiency than other existing protocols. For the practical implementation of smart agriculture monitoring systems, the proposed protocol is better than comparable protocols.

INDEX TERMS Agriculture sensors, Elliptic curve cryptography, Gateway, Scyther tool, Wireless sensor networks, Random oracle model, BAN logic.

I. INTRODUCTION

The Internet of Things (IoT) with a wireless sensor network is a standardized mechanism for electronic computers to view and interact with the physical environment through wireless sensor communication. It refers to intelligent WSN gadgets based on IoT that can share and exchange data without the need for human intervention. The devices in this design become more efficient by getting a unique IP address from the internet by utilizing the actuators and sensors, allowing anyone to operate existing technology. The WSN in IoT is a combination of hardware and software technologies. Since its beginnings, it has wide range of applications and is widely utilized in many ranges of fields. Simply said, it works by receiving signals from a variety of sensors through an application that has already been synchronized with the sensors

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

over the internet. IoT involved in WSN has emerged as a game-changing technology with the potential to radically disrupt the existing world. WSN is a technology that consists of a network of connected devices that send and receive data from the environment without physical interaction. After that, the data is analyzed to produce valuable information about the system's existing state. This data can be utilized to create real-time information with the help of software [1]. The components used in such applications can be intangible or tangible, and they must be able to work without the need for human interaction [2], [3]. Preciseness farming is a field of study in which the IoT-based WSN is used to detect various variables using wireless sensor gadgets such as radiation detectors, air humidity measures, light intensity, electrochemical capacitors, air supply, temperature monitoring, and smart cameras, agricultural weather stations, and many more sensors. The information is unprocessed and must be processed before it can be used. Before being turned into useful information, the received sensor data is filtered and optimized. This data is processed to provide an overall overview of the current position of the agrarian field and is sent into a decision-making system that determines the optimum course of action to improve or maintain the field condition [2], [4]. The usage of WSN for harvest monitoring has a number of benefits, which are stated as: crop productivity is constantly monitored, constant surveillance of the agricultural field, reduces the amount of staff required, cost savings in the agriculture sector, and also enables professional agricultural assistance in real-time.

A. SECURITY REQUIREMENTS

Users' privacy must be strictly protected in WSN systems. An authentication mechanism for a WSN environment should meet the following security standards, depending on the situation.

- Session key security and mutual authentication: In order to negotiate a session key that is only known to the authorized entity, the user and the sensor node should authenticate with one another after implementing the authentication method.
- Perfect Forward Secrecy: The session keys are routinely changed to protect the confidentiality of messages sent between the user, gateway, and sensor node. Consider the possibility that the long-term keys have been compromised for some reason; in this case, the authentication protocol must still ensure the privacy of the session keys that were used for earlier communications.
- Resistance to Multiple Attacks: The authentication mechanism should be resilient to the numerous typical attacks that happen in the WSN environment, such as replay attacks, impersonation attacks, man-in-the-middle attacks, attacks involving the theft of smart cards, etc.
- Untraceability and anonymity: User privacy is crucial in the context of WSNs. The authentication process should shield users' real identities from being identified and tracked through the messages they send.

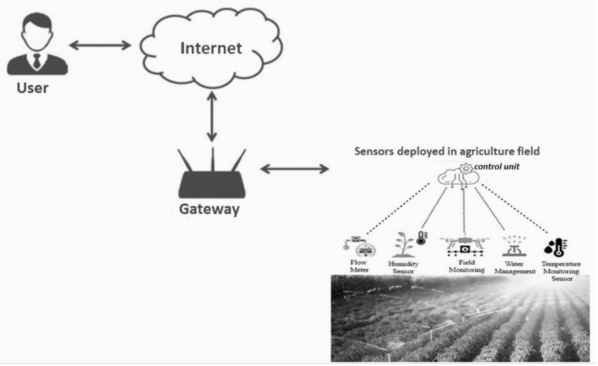


FIGURE 1. Network model of IoT-enabled intelligent precision agriculture using WSN.

- Protective biometrics: Users shouldn't be concerned about the security of their biometric information when using WSN services. Since users are identified using biometric information, the authentication strategy should provide biometric protection.

B. SYSTEM ARCHITECTURE

The Industrial Internet of Things (IIoT) is characterized as a fully integrated, interactive production system that adapts instantaneously to changing demands and conditions in the industry. It is a new phase of the industrial revolution that fully exploits the integration of information and communication technologies to provide a more comprehensive, interconnected, and integrated system. One of the fundamental network infrastructures of IIoT is the WSN. WSN is made up of several physically distributed sensor nodes that monitor and communicate system updates to other users. The basic architecture of the WSN in agriculture IoT is depicted in Figure 1, which is implemented in the proposed design. The communication parties in the WSN in agriculture IoT architecture are the User (U), Gateway (GW), and Sensor Nodes (SN). The capabilities and responsibilities of the communication parties are briefly described below:

- Gateway: In architecture, it serves as a third party. The U and SN, as well as the other communication partners, use their unique public and private key pairs to register with the GW. The GW assists the U and the SN in mutual authentication.
- Sensor Nodes: According to the architecture, there are entities that collect field data. They can come in a variety of shapes and sizes, depending on how they are used and how they work in IIoT. Sensors are used to detect and collect essential data regarding the agricultural field, such as light, humidity, soil pH value, and so on, and then send them to GW.
- User: The user is the most important entity for whom the system is set up. Who will have access to the GW anytime he or she requires agricultural field data for

monitoring and cultivation? In order to get access of data users must register themselves with the GW. During registration, U generates public and private key pairs, which he or she uses to establish a session key with the SN for future data sharing.

The usage of WSN for harvest monitoring has a number of benefits, which are stated as: crop productivity is constantly monitored, constant surveillance of the agricultural field, reduces the amount of staff required, cost savings in the agriculture sector, and also enables professional agricultural assistance in real-time.

C. RELATED WORKS

In this section, we summarise recent research work in WSN on reliable mutual authentication frameworks. Because the SN has limited memory and processing power, a secure key agreement framework that is both lightweight and reliable is required. In 2009, Das [5] proposed a remote user key management framework in WSN, stating that the technique is secure from several security problems. Meanwhile, He et al. [6] asserted that Das suggested the framework was unsafe for impersonation and insider attacks, as well as inefficient password updating. In 2010 Khan et al. [7] confirmed that the Das framework has design flaws. To address this problem, the authors proposed a protocol that is more secure, dependable, and efficient than earlier solutions. Later, in 2012, Vaidya et al [8] cryptanalysis of the He et al. [6] framework and prove that it is vulnerable to impersonation attack on SN. Thus, Vaidya et al. suggested an efficient key agreement approach for WSN. Hsieh et al [9], on the other hand, cryptanalysis the technique suggested by Vaidya et al. and proved it is vulnerable to security flaws such as password guessing attacks. Later, Turkanovic et al. [10] designed an authentication framework for WSN. The approach allowed for dynamic node addition, password modification, password protection, and mutual authentication between members, as well as the ability to survive various forms of security flaws. Chang [11] later demonstrated that the Turkanovics framework has design flaws, especially SN impersonation. WSN has been used in a variety of practical domains in recent years, including IoT [12], coal mines [13], healthcare [14], automotive tracking [15], and cloud computing environments [16]. He et al. [17] designed a key agreement framework for distant users in wireless healthcare sensor networks. He et al. approach improved the quality of healthcare at the hospital, making it important in today's healthcare climate. It can withstand many security concerns and is efficient in terms of computing overheads. Later, Li et al. [18] cryptanalysis of the He et al. framework proved that it has many design flaws such as DoS attack and inappropriate SK agreement. Further, Li et al. [18] designed an enhanced authentication framework that kept anonymity while also overcoming security flaws. In 2017, Liu et al. [19] proposed an enhanced framework for electronic WSN, which capture patients' physiological data continually in a healthcare center. Challa et al. [20], observed that the Liu et al. framework has various design flaws and developed an efficient ECC-based authentication framework for WSN. In 2018, Ali et al. [21] suggested a unique mutual authentication framework for WSN in agriculture monitoring that enabled safe remote user communication. Ali et al. [21] used a 3-factor key agreement approach that included a fuzzy extractor with generative and reproductive functionalities. Ali et al. used a random oracle model to formally assess their method and confirm that it is resistant to various security attacks. In contrast, according to our knowledge, Ali et al. approach are vulnerable to sensor node impersonation as well as failure to maintain perfect forward secrecy. In WSN security and privacy, various mutual authentication frameworks have been recently proposed. After uncovering the design flaws in Jung et al. [22] framework, in 2019 Shin and Kwon [23] designed a lightweight key agreement framework for WSN. In addition, Naresh et al. [24] also designed a new compound elliptic curve-based shared key negotiation protocol for WSN that has a lower key exchange overhead. Soni et al. [25] cryptanalysis the Challa et al. [20] framework and proved that it has security flaws and they proposed an enhanced mutual authentication key agreement framework. In 2020 xu et al. [26] cryptanalysis this approach and proved that their approach fails to maintain perfect forward secrecy. González et al. [27] have established a provably safe, versatile, and competent authentication key agreement approach for WSN. Furthermore, Moghadam et al. [28] suggested that the Alotaibi et al. [29] authentication framework for WSN has various security flaws and suggested an EC-based key agreement framework for WSN. Rangwani et al. [30] recently suggested an efficient and privacy-preserving key agreement for the industry sensor network. In the same context, Vinoth et al. [31] designed an authentication framework for an industrial sensor network. However, they all have higher computating overheads and security flaws, which is a source of concern for agriculture sensor networks. So, they are challenging to deploy in agriculture sensor network nodes with limited resources.

TABLE 1. Existing protocols drawbacks.

Protocol	Drawbacks
Das M.L. [5]	Vulnerable to impersonation and insider attacks, and inefficient password updating
He et al. [6]	Unsafe for impersonation and insider attacks
Vaidya et al. [8]	Vulnerable to impersonation attack on SN
Hsieh et al. [9]	Vulnerable to security flaws such as password guessing attacks
Turkanovic et al. [10]	Design flaws, especially SN impersonation
He et al. [17]	Design flaws such as DoS attack and inappropriate SK agreement
Ali et al. [21]	Vulnerable to sensor node impersonation and failure to maintain perfect forward secrecy
Naresh et al. [24]	Lower key exchange overhead
Soni et al. [25]	Fails to maintain mutual authentication key agreement framework
Xu et al. [26]	Fails to maintain perfect forward secrecy
Moghadam et al. [28]	Design flaws, such as impersonation attack, DoS attack
Rangwani et al. [30]	higher computing and communication overheads
Vinoth et al. [31]	Higher computing overheads and security flaws

D. MOTIVATION AND CONTRIBUTION

Different entities including IoT-enabled smart equipment, U, and GW as controller devices communicate across public channels in an IoT-enabled intelligent smart agriculture system. This allows an adversary to eavesdrop, delete, edit, or inject malicious content into them. The adversary can also breach the WSN system by using various security attacks. In an IoT-enabled smart precision agriculture context, the authentication key establishment framework is a robust cyber security mechanism that enables an external user to safely retrieve factual data remotely from distributed smart equipment. These characteristics motivated us to design a three-factor key agreement framework that is both efficient and secure, with low communication and computation overheads. We made the following contributions to this work, which are listed below:

- In an IoT-enabled intelligent precision agriculture WSN, we proposed a robust authenticated and key exchange framework for a smart agriculture communication system based on ECC. In addition, we use biometrics and the widely established fuzzy extractor for using bio-metric methods to avoid DoS attacks.
- We performed a formal security analysis using the widely established ROR model and also utilize BAN Logic to prove the correctness of mutual authentication. Furthermore, the security of the proposed framework is tested informally, demonstrating that it maintains numerous security features in an IoT-enabled smart agricultural system.
- The suggested framework is also robust against some well-known adversary models Delvo-Yao and Canetti-Krawczyk.
- We determine the security efficiency of our framework by using the Scyther simulation tool. To demonstrate that the suggested framework is robust against so many vulnerabilities and exploits within the bounds.
- The comparative performance analysis is carried out with a related framework in the literature and shows that the proposed scheme generates competitive communication and computation overheads with improved security in the same communication network.

E. ADVERSARIAL MODEL

Higher security standards are required for the agriculture WSN network due to the high level of risk involved. Therefore, it is imperative to consider every conceivable angle from which the system's security may be compromised. The Dolev-Yao threat model [32] is used in this article to analyse the mutual authentication and SK management mechanisms. The following assumptions are taken into consideration in this threat model, which is based on a real-life event:

- An attacker can use the public channel to communicate because the communication parties (SN and U) are not reliable. Since the GW is regarded as a reliable source of information, it is impossible to capture it.

TABLE 2. Symbol and their meaning.

Symbol	Meaning	Symbol	Meaning
ECC	Elliptic curve cryptography	$SK_{\mathcal{U}}$	Session key of $\mathcal{U}$
$E_q(u, v)$	Elliptic curve over finite prime field	$SK_{\mathcal{SN}}$	Session key of $\mathcal{SN}$
q	Prime number	$\mathcal{A}$	An adversary
g	Group generator	$h(.)$	Hash function
$D_{K_{\mathcal{U}}}$	Decryption using secret key $K_{\mathcal{U}}$	$\triangle t_i$	Maximum transmission delay
$\mathcal{ID}_U$	User identity	$\Vert$	Concatenation operation
$\mathcal{PW}_U$	User password	$\oplus$	Bitwise XOR operation
$Z_q^\star$	Multiplicative Group of order $q-1$	$\mathcal{U}$	Agriculture user
$B_{\mathcal{U}}$	Biometrics of $\mathcal{U}$	$\rightarrow$	Public channel
$W_{K_{\mathcal{U}}}$	Encryption using secret key $K_{\mathcal{U}}$	$\Rightarrow$	Secure channel
$\beta_{\mathcal{U}}$	Public reproduction data	$\alpha_{\mathcal{U}}$	Reproduce biometric key
$C_{\mathcal{SN}}$	Registration Counter of $\mathcal{SN}$	$C_{\mathcal{U}}$	Registration Counter of $\mathcal{U}$
s_1, s_2	Random prime number $\in \quad Z_q^\star$	$\mathcal{GW}$	Gateway
G	Elliptic curve group	$\mathcal{SN}$	Senor node

- An attacker can violate any type of security by intercepting, altering, or delaying the message sent across the system.
- An adversary might use a power analysis attack to physically capture SN and get access to the credentials that are stored on it. When a smart device is stolen or lost, the attacker uses power analysis to get access to the passwords that are stored on the device.
- Even a legitimate entity with malicious intent to deceive the system could be the attacker (privileged insider).
- Additionally, the most recent adversary model, Canetti and Krawczyk's adversary model is used [33]. According to this model, the attacker keeps all of its current abilities and may also steal session-specific temporary credentials or any other transitional data, which would reveal the SK established between the communicating devices.

F. PAPER ORGANIZATION

The rest of this work is arranged as follows. Section II, covers the most important mathematical preliminaries. In Section III, we discuss the proposed scheme. In section IV, We used the Scyther tool, BAN Logic, and ROR model to undertake the security verification. In section V, we did a performance analysis of the suggested framework. Finally, we come to a conclusion and future directions.

II. PRELIMINARIES

We discuss the useful mathematical concept and some usable notation in this section, which can be used to describe and analyze the proposed framework.

A. NOTATIONS

We explain the meaning of each useful notation or symbol used in this paper in Table 2.

B. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Let $E_q(u, v)$ be an EC over the prime field $\mathbb{F}_q$, therefore the equation of EC over $\mathbb{F}_q$ is defined

$$y^2 = x^3 + ux + v \; mod \; q \; where \; u, v \in \mathbb{F}_q$$

and

$$4u^3 + 27v^2 \; mod \; q \neq 0$$

where u and v are the curves parameters [34], [35].

ECC is a public key encryption algorithm based on $G(\mathbb{F}_q)$ consists of (x, y) and ∞ points on $E_q(u, v)$.

1) ADDITION ON ECC

If R ans S are two points in $G(\mathbb{F}_q)$ and $R \neq -S$, then $R + S = N \in G(\mathbb{F}_q)$ and N is also a point in elliptic curve. The algebraic calculation is defined as:

$$
\begin{aligned}
Let\ \ R = (x_r, y_r),\ \ S = (x_s, y_s)\ then\ N = (x_n, y_n) \\
where\ x_n = (\lambda^2 - x_r - x_q)\ mod\ q \\
and\ \ y_n = (\lambda(x_r - x_s) - y_r)\ mod\ q
\end{aligned}
$$

$$
\lambda = \begin{cases} (y_r - y_s)/(x_r - x_s)\ mod\ q & \text{if } R = S \\ 3(x_r^2 + c)/2y_r\ mod\ q & \text{if } R \neq S \end{cases}
$$

2) SCALER MULTIPLICATION

Every point on $E_q(c, d)$ is non-singular, so the scaler multiplication based on the addition rule defines as n.Q in $G(\mathbb{F})$ as:

$$Q + Q + Q + \ldots\ldots + Q = n.Q \quad where\ n \in \mathbb{F}_q,\ Q \in G(\mathbb{F})$$

C. ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM (ECDLP)

If R and S are known for a large prime q in polynomial time, it is computationally impossible to determine n for any two points R and S on the elliptic curve$E_q(c, d)$ and for some positive number n such that $S = n.R$. n is the discrete logarithm scalar, and $n.R = R + R + \ldots\ldots + R(n - times)$ is the ECC point or scalar multiplication [36].

D. BIOMETRIC FUZZY EXTRACTOR

A fuzzy extractor is defined as a pair of functions, one of which generates uniform random bits from pre-specified input values and the other of which retrieves a string from an input value that is reasonably near to the original input value while adhering to pre-specified guidelines. The fuzzy extractor is represented mathematically as $(\mathcal{P}, \mathcal{Q}, \mathcal{R})$ where $\mathcal{R}$ is the biometric input of information in the metric space with a finite dimension and $\mathcal{L}$ is the bit length of the output strings. The fuzzy extractor also includes the two approaches which are $Gen(.)$ and $Rep(.)$ [37].

- $Gen(.)$: The $Gen(.)$ is a probabilistic technique that accepts biometric input data $B_i \in \mathcal{R}$ as inputs and outputs hidden key data $\Re_i \in \{0, 1\}^l$ and a public reproduction variable τ_i for the biometric data input $B_i \in \mathcal{R}$. In this case, $Gen(B_i) = \{\Re_i, \tau_i\}$.
- $Rep(.)$: A probabilistic method that uses the biometric data $B_i' \in \mathcal{R}, \mathcal{S}$ and the attribute τ_i to reproduce the biometric key $\Re$ i.e $Rep(\tau_i, B_i') = \Re_i$, such that $d(B_i, B_i') \leq \mathcal{Q}$.

III. THE PROPOSED PROTOCOL

The proposed protocol is based on a bio-metric approach. The three phases of the proposed protocol are explained as follows:

A. INITIALIZATION PHASE

In the suggested protocol, $\mathcal{GW}$ chooses a random integer on the elliptic curve $E_q(c, d)$ mod q and $g \in G$, then uses $h(.)$ as hash function. Additionally, the biometric is carried out using the fuzzy extractor approach [38]. During the login, the $Gen(.)$ and $Rep(.)$ algorithms are run. Additionally, the user computes $PK_{pub} = x_{\mathcal{U}} g$ using a random value generated as the private key, $x_{\mathcal{U}} \in Z_q^\star$. Furthermore, user publish the attributes $\{\alpha_{\mathcal{U}}(.), \beta_{\mathcal{U}}(.), x_{\mathcal{U}}, g, h(.), E_q(c, d)\}$.

B. REGISTRATION PHASE

The suggested scheme comprises two registration phases: the first is user $(\mathcal{U})$ registration, and the second is $(\mathcal{SN})$ registration.

1) USER REGISTRATION PHASE

$\mathcal{U}$ must register his/her identification with the Gateway $(\mathcal{GW})$ in order to receive the data. Using a secure connection, the $\mathcal{GW}$ assists the $\mathcal{U}$ in registering his/her public and private keys. The procedure are given as follows:

- **Step 1:** The $\mathcal{U}_i$ assists $\mathcal{GW}$ for registration. $\mathcal{U}_i$ inputs $\mathcal{ID}_{\mathcal{U}}, \mathcal{PW}_{\mathcal{U}}$ and $B_{\mathcal{U}}$. Then chooses $x_U \in Z_q^\star$. Calculates $(\alpha_{\mathcal{U}}, \beta_{\mathcal{U}}) = Gen(B_{\mathcal{U}})$, $H_1 = h(\mathcal{PW}_{\mathcal{U}} \| \alpha_{\mathcal{U}}) \oplus x_{\mathcal{U}}$ and sends $\{\mathcal{ID}_{\mathcal{U}}, H_1\}$ to $\mathcal{GW}$.
- **Step 2:** The $\mathcal{GW}$ calculates $R_1 = h(\mathcal{ID}_{\mathcal{U}} \| C_{\mathcal{U}} \| y)$ where y is $\mathcal{GW}$ secret key and C_U registration counter number of U provided by GW. $\mathcal{GW}$ computes $R_2 = R_1 \oplus H_1$ stores $\{\mathcal{ID}_{\mathcal{U}}, C_{\mathcal{U}}, R_2\}$ in his/her data base for further communication then sends $\{R_2, C_{\mathcal{U}}\}$ to $\mathcal{U}$.
- **Step 3:** The $\mathcal{U}$ calculates $B_1 = R_2 \oplus \alpha_{\mathcal{U}}$ and $B_2 = h(\mathcal{ID}_{\mathcal{U}} \| \mathcal{PW}_{\mathcal{U}} \| B_1)$. Finally $\mathcal{U}$ stores $\{\beta_{\mathcal{U}}, R_2, B_1, B_2, C_{\mathcal{U}}\}$ in his data base.

2) SENSOR NODE REGISTRATION PHASE

To gain access to the gateway and share information with users, the SN needs to register with it. Sensor nodes must be in user-key agreement. The procedure are as follows:

- **Step 1:** The $\mathcal{SN}$ input his/her $\mathcal{ID}_{\mathcal{SN}}$ and sends it to $\mathcal{GW}$.
- **Step 2:** $\mathcal{GW}$ calculates $R_3 = h(\mathcal{ID}_{\mathcal{SN}} \| y \| C_{\mathcal{SN}})$, where $C_{\mathcal{SN}}$ is registration counter number of $\mathcal{SN}$ provided by $\mathcal{GW}$. $\mathcal{GW}$ stores $\{R_3, C_{\mathcal{SN}}\}$ in data base. The $\mathcal{GW}$ sends $\{R_3, C_{\mathcal{SN}}\}$ to $\mathcal{SN}$ through secure channel.
- **Step 3:** $\mathcal{SN}$ generates $r \in Z_q^\star$. Computes $PK_{\mathcal{SN}} = r.g$ and store $\{R_3, C_{\mathcal{SN}}\}$ in his data base for future communication system.

C. LOGIN, AUTHENTICATION AND KEY-AGREEMENT PHASE

In the authentication phase, $\mathcal{U}$ communicates with $\mathcal{SN}$ and $\mathcal{GW}$ over public channel as shown in Table 3. A detailed illustration of login and authentication is discussed below: As illustrated in Table 3, $\mathcal{U}$ communicating with $\mathcal{SN}$ and $\mathcal{GW}$ over a public channel during the authentication phase.

TABLE 3. Login, authentication and key agreement phase.

$\mathcal{U}$	$\mathcal{GW}$	$\mathcal{SN}$
Login with $\mathcal{ID}^{\star}_{\mathcal{U}}, \mathcal{PW}^{\star}_{\mathcal{U}}$ and $B^{\star}_{\mathcal{U}}$		
And gets $\alpha^{\star}_{\mathcal{U}} = Rep(B^{\star}_{\mathcal{U}}, \beta^{\star}_{\mathcal{U}})$		
Computes $B^{\star}_1 = R_2 \oplus \alpha^{\star}_{\mathcal{U}}$		
Computes $B^{\star}_2 = h(\mathcal{ID}^{\star}_{\mathcal{U}} \Vert \mathcal{PW}^{\star}_{\mathcal{U}} \Vert B^{\star}_1)$		
Verifies $B^{\star}_2 \overset{?}{=} B_2$ if yes then:		
Generates $s_1 \in Z^{\star}_q$		
Computes $A_1 = s_1.g$		
Computes $K_{\mathcal{U}} = h(PK_{\mathcal{SN}} \Vert ID_{\mathcal{SN}}) \oplus t_1$	Verifies $t_2 - t_1 \leq \triangle t$, aborts if not fresh	
Computes $V_1 = h((K_{\mathcal{U}} \Vert C_{\mathcal{U}} \Vert t_1)$	Computes $V^{\star}_2 = h(R_2 \Vert \mathcal{ID}_{\mathcal{U}} \Vert C_{\mathcal{U}})$	
Encrypts $W_1 = W_{K_{\mathcal{U}}}(C_{\mathcal{U}}, A_1, V_1)$	Verifies $V^{\star}_2 \overset{?}{=} V_2$	Verifies $t_4 - t_3 \leq \triangle t$
Computes $V_2 = h(R_2 \Vert \mathcal{ID}_{\mathcal{U}} \Vert C_{\mathcal{U}})$	Computes $V_3 = h(R_3 \Vert \mathcal{ID}_{\mathcal{SN}} \Vert t_3)$	Computes $V^{\star}_3 = h(R_3 \Vert \mathcal{ID}_{\mathcal{SN}} \Vert t_3)$
Sends $M_1 = \{W_1, V_2, t_1\}$	Sends $M_2 = \{W_1, V_3, t_1, t_2\}$	Verifies $V^{\star}_3 \overset{?}{=} V_3$
$\cdots\cdots\cdots\cdots\cdots\cdots \longrightarrow$	$\cdots\cdots\cdots\cdots\cdots\cdots \longrightarrow$	Computes $K_S = h(PK_{\mathcal{SN}} \Vert ID_{\mathcal{SN}}) \oplus t_1$
		Decrypts $(C_{\mathcal{U}}, V_1, A_1) = D_{K_{\mathcal{S}}}(W_1)$
		Computes $V^{\star}_1 = h(K_{\mathcal{SN}} \Vert C_{\mathcal{U}} \Vert t_1)$
		Verifies $V^{\star}_1 \overset{?}{=} V_1$ if yes
		Generates $s_2 \in Z^{\star}_q$
		Computes $A_2 = s_2.g$
		Computes $SK_{\mathcal{SN}} = h(V^{\star}_1 \Vert \mathcal{ID}_{\mathcal{SN}} \Vert C_{\mathcal{U}} \Vert A_1 s_2 \Vert t_5)$
		Computes $V_4 = h(A_1 \Vert A_2 \Vert C_{\mathcal{U}} \Vert C_{\mathcal{SN}} \Vert t_5)$
		Computes $K_{\mathcal{S}_1} = h(C_{\mathcal{U}} \Vert A_1 \Vert V^{\star}_1)$
		Encrypts $W_2 = W_{K_{\mathcal{SN}}}(\mathcal{ID}_{\mathcal{SN}}, A_2, C_{\mathcal{SN}}, t_5, V_4)$
		Computes $V_5 = (V^{\star}_3 \oplus R_3)$
		Sends $M_3 = \{W_2, V_5, t_5\}$
		$\longleftarrow \cdots\cdots\cdots\cdots\cdots\cdots$
	Verifies $t_6 - t_5 \leq \triangle t$	
	Computes $V^{\star}_5 = V_3 \oplus R_3$	
	Verifies $V^{\star}_5 \overset{?}{=} V_5$ if yes	
	Computes $V_6 = (V^{\star}_2 \oplus R_2)$	
	Sends $M_4 = \{W_2, V_6, t_7\}$	
Verifies $t_8 - t_7 \leq \triangle t$	$\longleftarrow \cdots\cdots\cdots\cdots\cdots\cdots$	
Computes $V^{\star}_6 = (V_2 \oplus R_2)$		
Verifies $V^{\star}_6 \overset{?}{=} V_6$ if yes		
Computes $K_{\mathcal{U}_1} = h(C_{\mathcal{U}} \Vert A_1 \Vert V_1)$		
Decrypts $(A_2, t_5, \mathcal{ID}_{\mathcal{SN}}, V_4) = D_{K_{\mathcal{U}}}(W_2)$		
Computes $V^{\star}_4 = h(A_1 \Vert A_2 \Vert C_{\mathcal{U}} \Vert C_{\mathcal{SN}} \Vert t_5)$		
Verifies $V^{\star}_4 \overset{?}{=} V_4$		
Computes $SK_{\mathcal{U}} = h(ID_{\mathcal{SN}} \Vert C_{\mathcal{U}} \Vert s_1.A_2 \Vert V_1 \Vert t_5)$		
Hence $SK_{\mathcal{U}} = SK_{\mathcal{SN}} = SK$		

The complete description of login, authentication and key agreement is discussed below:

- **Step 1:** The $\mathcal{U}$ login with $\mathcal{ID}^{\star}_{\mathcal{U}}$, $\mathcal{PW}^{\star}_{\mathcal{U}}$ and biometric $B^{\star}_{\mathcal{U}}$. The $\mathcal{U}$ get $\alpha^{\star}_{\mathcal{U}} = Rep(B^{\star}_{\mathcal{U}}, \beta^{\star}_{\mathcal{U}})$. Computes $B^{\star}_1 = R_2 \oplus \alpha^{\star}_{\mathcal{U}}$ and $B^{\star}_2 = h(\mathcal{ID}^{\star}_{\mathcal{U}} \| \mathcal{PW}^{\star}_{\mathcal{U}} \| B^{\star}_1)$. User verifies $B^{\star}_2 \overset{?}{=} B_2$ if yes then generates $s_1 \in Z^{\star}_q$ computes $A_1 = s_1.g$, $K_{\mathcal{U}} = h(PK_{\mathcal{SN}} \| ID_{\mathcal{SN}}) \oplus t_1$ and $V_1 = h(K_{\mathcal{U}} \| C_{\mathcal{U}} \| t_1)$. Then, $\mathcal{U}$ encrypts $W_1 = E_{K_{\mathcal{U}}}(C_{\mathcal{U}}, A_1, V_1)$. The user again computes $V_2 = h(R_2 \| \mathcal{ID}_{\mathcal{U}} \| C_{\mathcal{U}})$. Finally, sends $M_1 = \{W_1, V_2, t_1\}$ to $\mathcal{GW}$.
- **Step 2:** The $\mathcal{GW}$ verifies the time span $t_2 - t_1 \leq \Delta t$ aborts if not fresh otherwise computes $V^{\star}_2 = h(R_2 \| \mathcal{ID}_{\mathcal{U}} \| C_{\mathcal{U}})$. $\mathcal{GW}$ verifies $V^{\star}_2 \overset{?}{=} V_2$ if yes, then computes $V_3 = h(R_3 \| \mathcal{ID}_{\mathcal{SN}} \| t_3)$. Finally, sends $M_2 = \{W_1, V_3, t_1, t_3\}$ to sensor node.
- **Step 3:** The $\mathcal{SN}$ verifies $t_4 - t_3 \leq \Delta t$ if yes then computes $V^{\star}_3 = h(R_3 \| \mathcal{ID}_{\mathcal{SN}} \| t_3)$. The $\mathcal{SN}$ verifies $V^{\star}_3 \overset{?}{=} V_3$ if yes then computes $K_S = h(PK_{\mathcal{SN}} \| ID_{\mathcal{SN}}) \oplus t_1$ and decrypts $(C_{\mathcal{U}}, A_1, V_1) = D_{K_{\mathcal{SN}}}(W_1)$ if it is valid then computes $V^{\star}_1 = h(K_{\mathcal{SN}} \| C_{\mathcal{U}} \| t_1)$. The $\mathcal{SN}$ again verifies $V^{\star}_1 \overset{?}{=} V_1$ if yes then generates $s_2 \in Z^{\star}_q$ and computes session key $SK_{\mathcal{SN}} = h(\mathcal{ID}_{\mathcal{SN}} \| C_{\mathcal{U}} \| V^{\star}_1 \| A_1 s_2 \| t_5)$. $\mathcal{SN}$ computes $V_4 = h(A_1 \| A_2 \| C_{\mathcal{U}} \| C_{\mathcal{SN}} \| t_5)$ and $K_{S_1} = h(C_{\mathcal{U}} \| A_1 \| V^{\star}_1)$, then encrypts $W_2 = W_{K_{S_1}}(A_2, C_{\mathcal{SN}}, t_5, \mathcal{ID}_{\mathcal{SN}}, V_4)$ and computes $V_5 = (V^{\star}_3 \oplus R_3)$. The $\mathcal{SN}$ sends back $M_3 = \{W_2, V_5, T_5\}$ to $\mathcal{GW}$ via public channel.
- **Step 4:** The $\mathcal{GW}$ verifies $t_6 - t_5 \leq \Delta t$ if valid then computes $V^{\star}_5 = V_3 \oplus R_3$, again verifies $V^{\star}_5 \overset{?}{=} V_3$ if yes then computes $V_6 = V^{\star}_2 \oplus R_2$. Finally $\mathcal{GW}$ send $M_4 = \{W_2, t_7\}$ to $\mathcal{U}$.
- **Step 5:** The $\mathcal{U}$ verifies $t_8 - t_7 \leq \Delta t$ If valid then computes $V^{\star}_6 = (V_2 \oplus R_2)$. Again verifies $V^{\star}_6 \overset{?}{=} V_6$, if yes then computes $K_{\mathcal{U}_1} = h(C_{\mathcal{U}} \| A_1 \| V_1)$. The $\mathcal{U}$ decrypts $(A_2, t_5, \mathcal{ID}_{\mathcal{SN}}, V_4) = D_{K_{\mathcal{U}}}(W_2)$ and then computes $V^{\star}_4 = h(A_1 \| A_2 \| C_{\mathcal{U}} \| C_{\mathcal{SN}} \| t_5)$. Finally $\mathcal{U}$ verifies $V^{\star}_4 \overset{?}{=} V_4$ if valid then computes his session key $SK_{\mathcal{U}} = h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_1.A_2 \| V_1 \| t_5$. Hence matches his session key $SK = SK_{\mathcal{U}} = SK_{\mathcal{SN}}$

D. UPDATING OF PASSWORD AND BIOMETRIC PHASE

For password and bio-metric updating, U have to do the following analysis that is given below:

- **Step 1:** The $\mathcal{U}$ inputs $\mathcal{ID}^{\star}_{\mathcal{U}}, B^{\star}_{\mathcal{U}}$ and $\mathcal{PW}^{\star}_{\mathcal{U}}$ and gets $\alpha^{\star}_{\mathcal{U}} = Rep(\beta^{\star}_{\mathcal{U}}, B^{\star}_{\mathcal{U}})$ then the user computes $B^{\star}_1 = R_2 \oplus \beta^{\star}_{\mathcal{U}}$ and $B^{\star}_2 = h(\mathcal{ID}^{\star}_{\mathcal{U}} \| \mathcal{PW}^{\star}_{\mathcal{U}} \| B^{\star}_1)$. User verifies $B^{\star}_2 = B_2$, holds or not if not then terminates otherwise $\mathcal{U}$ selects his /her new password and bio-metric as $(B_{\mathcal{U}}^{new}, \mathcal{PW}_{\mathcal{U}}^{new})$. Then $\mathcal{U}$ computes $(\beta_{\mathcal{U}}^{new}, \alpha_{\mathcal{U}}^{new}) = Gen(B_{\mathcal{U}}^{new})$ and encrypts $H_1^{new} = h(\mathcal{PW}_{\mathcal{U}}^{new} \| \alpha_{\mathcal{U}}^{new}) \oplus x_{\mathcal{U}}$ and sends $M_1' = \{\mathcal{ID}_{\mathcal{U}}^{new}, H_1^{new}\}$ to $\mathcal{GW}$.

- **Step 2:** The $\mathcal{GW}$ verifies $\{\mathcal{ID}_{\mathcal{U}}, C_{\mathcal{U}}\}$ in his data base then computes $R_2^{new} = R_1 \oplus H_1^{new}$ and sends $M_2' = \{R_2^{new}, C_{\mathcal{U}}\}$ to $\mathcal{U}$.
- **Step 3:** When $\mathcal{U}$ receives $M_2' = \{R_2^{new}, C_{\mathcal{U}}\}$ then computes $B_1^{new} = R_2^{new} \oplus \alpha_{\mathcal{U}}^{new}$ and $B_2^{new} = h(\mathcal{ID}_{\mathcal{U}} \| \mathcal{PW}_{\mathcal{U}}^{new} \| R_1^{new})$. Then $\mathcal{U}$ replace his old password $\mathcal{PW}_{\mathcal{U}}$ and bio-metric $B_{\mathcal{U}}$ with new password $\mathcal{PW}_{\mathcal{U}}^{new}$ and $B_{\mathcal{U}}^{new}$ and stores $\{\beta_{\mathcal{U}}^{new}, R_2, B_1^{new}, B_2^{new}\}$ in his/her data base.

IV. SECURITY ANALYSIS

In this section, we examine the security of the proposed protocol. We have conducted both official and informal security studies to show that the proposed protocol is completely secure.

A. INFORMAL SECURITY ANALYSIS

We performed an informal security assessment of the suggested protocol and demonstrated that it is secure against a number of security flaws. Additionally, the suggested protocol guarantees the user, gateway, and sensor node's privacy and safe authentication.

1) PRIVATE KEY SECURITY

During the key generation phase, the user selects $x_{\mathcal{U}} \in Z_q^\star$, chooses it as a secret key, and calculates $PK_{pub} = x_{\mathcal{U}}.g$. The entire system can be broken if $\mathcal{A}$ can calculate a private key using public information. Because users compute the private key using the master key, g (elliptic curve number), $\mathcal{A}$ will have a difficult time calculating it. Because the master secret key was used, the attacker will fail, and the crypto-equation $PK_{pub} = x_{\mathcal{U}}.g$ is too difficult to crack due to ECDLP.

2) IMPERSONATION ATTACK

The adversary may pose as a legitimate user in order to get information or advantages. The information provided in the secret key establishment phase of the proposed protocols must be used by the adversary to confirm that the user is legitimate before proceeding.

- *User impersonation attack:* In order to obtain information or gain an advantage, the attacker can take on the role of a U. In order to do so, the adversary must demonstrate that he or she is a legal U by utilising the data in the proposed protocol. The U sends $M_1 = \{W_1, V_2, t_1\}$ to the Gateway via a public channel. The $\mathcal{A}$ computation of W_1 is extremely complex due to the use of secret key encryption. Furthermore, the adversary is unable to locate the secret key due to the ECDLP. As a result, we conclude that the attacker is unable to impersonate an authorised user.
- *Gateway impersonation attack:* The $\mathcal{A}$ attack, like the U impersonation attack, attempts to impersonate an authentic user. During the authentication phase, GWN sends $M_2 = \{W_1, V_3, t_1, t_2\}$ to the sensor node and $M_4 = \{W_2, t_7\}$ to $\mathcal{U}$ via a public channel. Where W_1 and W_2 are both encrypted with the gateway's private key, which is not possible due to ECDLP. The computation of M_2 and M_4 is clearly infeasible due to the parameters, $K_{\mathcal{U}}$ and K_{S1} the secret key of U and SN. Hence, the $\mathcal{A}$ fails to behave as the $\mathcal{GW}$ while communicating with $\mathcal{U}$. As a result, we conclude that the attacker is unable to impersonate an authorised user.
- *Sensor node impersonation attack:* During the authentication phase, the $\mathcal{SN}$ receives $M_2 = \{W_1, V_3, t_1, t_2\}$ from $\mathcal{GW}$ and decrypts W_1 using its own secret key K_{S_1} to validate the received messages. It is difficult for the $\mathcal{A}$ to deliver false information to the $\mathcal{GW}$ through the use of a malicious $\mathcal{SN}$. Because $\mathcal{A}$ does not have access to $\mathcal{SN}$ private key K_{S_1}. Additionally, the $\mathcal{A}$ fails to compute SK, which is critical. As a result, in the proposed protocol, $\mathcal{A}$ cannot impersonate $\mathcal{SN}$.

3) MUTUAL AUTHENTICATION

In the suggested authentication protocol, we primarily considered three entities: $\mathcal{U}$, $\mathcal{GW}$, and $\mathcal{SN}$. Several communications are involved in computing SK. Both the $\mathcal{U}$ and $\mathcal{SN}$ nodes computed a mutual key during the secret key creation phase, but they had to authenticate each other before accepting the session key. In this way, $\mathcal{U}$, $\mathcal{GW}$, and $\mathcal{SN}$ authenticated each other before proceeding to the next step in the authentication phase. Hence, the suggested protocol does have the property of mutual authentication.

4) SESSION KEY DISCLOSURE ATTACK

In the proposed protocol, the $\mathcal{U}$ and $\mathcal{SN}$ have computed a secret key. Following that, this key will be used in the authentication phase. If $\mathcal{A}$ knows the secret key $K_{\mathcal{U}}$ or K_{S_1}, he or she will be unable to determine the session key $SK_{\mathcal{U}} = h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_1.A_2 \| V_1 \| t_5)$. It is noticeable that these keys are difficult to compute without the $s1$ and $s2$,. The secret parameters $s1$ and $s2$, are used on both sides of the $\mathcal{U}$ and the $\mathcal{SN}$ which are generated at random. The adversary needs random information to calculate it, which is impossible to obtain in mean polynomial time. Furthermore, the proposed protocol utilises $SK_{\mathcal{U}} = h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_1.A_2 \| V_1 \| t_5)$ as a secure communication session key. It is obvious that the adversary will not be able to obtain $h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_1.A_2 \| V_1 \| t_5)$ is captured from the protocol description. It's not impossible to obtain all of the information from SK despite the fact that invertible hash functions don't exist. Accordingly, the proposed protocol provides strong defence against SK disclosure attacks, [39].

5) EAVESDROPPING ATTACK

The eavesdropping technique enables the attacker to eavesdrop in on any communications made through an unprotected channel. Consequently, the attacker is able to intercept messages. The suggested approach, however, uses a new random integer for each round of authentication and secures all parameters with a hash function. As a result, neither the identity of $\mathcal{U}$ nor any parameters are obtained by the attacker. Additionally, $\mathcal{A}$ is unable to calculate $SK_{\mathcal{U}} = h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_1.A_2 \| V_1 \| t_5)$. Because of this, $\mathcal{A}$ is unable to acquire $SK_{\mathcal{U}} = h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_1.A_2 \| V_1 \| t_5)$.

6) KEY FRESHNESS

In order to avoid future connectivity from being distorted even if the old keys are compromised, a term called ''key freshness'' is used. Therefore, choose a random number and a time stamp as your principal values whenever you use the freshness of keys in cryptography. The time-stamp and random number used in the suggested protocol were always fresh. Consequently, we keep the key agreements fresh in the suggested framework.

7) PERFECT FORWARD SECRECY

In the unlikely event that $\mathcal{A}$ is aware of the private secret key, the $\mathcal{A}$ will be unable to access the $SK_{\mathcal{U}} = h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_1.A_2 \| V_1 \| t_5)$. Because $SK_{\mathcal{U}}$ is missing from the prior key. The attacker cannot obtain $s_1.A_2$ even if the parameters V_1,and V_2 are compromised because both the $\mathcal{U}$ and $\mathcal{SN}$ selected fresh random number. Which is hard to calculate in mean polynomial time.

8) REPLAY ATTACK

The malicious adversary tries to send a message to launch a counterattack. However, the sent messages contain requirements for message verification, including a new timestamp $t_{i+1} - t_i \leq \Delta t$, a random number, and a secured hash function. This prevents the malicious adversary from launching a reply attack. Hence, the suggested scheme can therefore withstand the reply attack.

9) DENIAL OF SERVICE (DoS) ATTACK

In the suggested scheme we restrict users to a maximum of three logins to $\mathcal{U}$. If $\mathcal{U}$ does not submit his credentials after three tries. For an extended length of time, the login and authentication for the given user/device will be disabled. Hence, the proposed scheme effectively protects against DoS attacks.

10) OFF-LINE USER IDENTITY PREDICTING ATTACK

In the authentication phase, $\mathcal{A}$ tries to guess the user's identity $\mathcal{ID}_{\mathcal{U}}$ by exploiting messages sent over the open channel. $\mathcal{A}$ fails, because, after guessing the users identity $\mathcal{ID}_{\mathcal{U}}$, cannot be generated the users password $\mathcal{PW}_{\mathcal{U}}$ and biometric $B_{\mathcal{U}}$ that cannot be counterfeited. Hence, the suggested framework is resistant to these attacks.

11) USER AND SENSOR NODE TRACEABILITY ATTACK

In order to determine whether two authentication request messages from distinct sessions are similar, an attacker keeps an eye on them. If both messages are similar and same origin, suggest that the $\mathcal{U}$ or $\mathcal{SN}$ for both queries is the same. The $\mathcal{A}$ cannot detect the $\mathcal{U}$ or $\mathcal{SN}$ in our suggested framework yet after stealing the authentication messages $M_1 = \{W_1, V_2, t_1\}$ and $M_3 = \{W_2, V_5, t_5\}$ since these messages include encrypted parameters W_1, V_2, W_2, V_5 with a secret key, one-way hash function, and current timestamp t_1, t_5 that are chosen a fresh timestamp after every new session, for computing new messages M_1 and M_3. Therefore, it is impossible to trace the identity of the $\mathcal{U}$ or $\mathcal{SN}$. Hence, the suggested framework is secured against the $\mathcal{U}$ or $\mathcal{SN}$ untraceable attack [40].

12) INSIDER ATTACK

The message sent by the user and the sensor is still encrypted with private keys. The private key is always kept secret and is only known to authenticated users. The information is hidden by the secret keys, making it impossible for the other entity to access it. Only the user or sensor node with his/her secret key can decrypt the message. As a result, the attacker is unable to leverage his/her identity to gain the password or other user credentials needed to connect to other services. Thus, the proposed protocol is resistant to insider attacks.

13) MAN IN THE MIDDLE ATTACK

An attacker may try to use the previous login messages on the server side. $\mathcal{A}$ replays $M_1 = \{W_1, V_1, t_1\}$ where $W_1 = E_{K_{\mathcal{U}}}(C_{\mathcal{U}}, A_1, V_1)$ is encrypted by secret key $K_{\mathcal{U}}$ of user and $V_1 = h((K_{\mathcal{U}} \| C_{\mathcal{U}} \| t_1)$ is masked by hash function. Similarly the message $M_3 = \{W_2, V_5, T_5\}$ where W_2 is encrypted by private key of $\mathcal{SN}$ and V_5 are masked by hash function. Both the $\mathcal{U}$ and $\mathcal{SN}$ verify the timestamp. Since we employ new random variables and an anonymous identity, the attacker is, therefore, unable to calculate with original entities. Hence, our suggested protocol can resist this assault.

14) ANONYMITY ATTACKS

In agricultural WSN, privacy preservation is a crucial concern. Anonymity attacks aim to uncover the identities of participants in the system, which can lead to the compromise of sensitive information and unauthorized access. The proposed protocol, which utilizes elliptic curve cryptography and hash function, ensures privacy preservation by providing anonymity to the participating entities. It conceals the identities of the communicating parties, making it difficult for attackers to trace or identify them.

15) DESYNCHRONIZATION ATTACKS

Wireless Sensor Networks (WSNs) typically involve numerous sensor nodes that need to synchronize their actions for efficient communication and coordination. Desynchronization attacks exploit vulnerabilities in the synchronization process, leading to disruption or manipulation of network operations. The proposed protocol includes mechanisms to defend against desynchronization attacks by employing efficient key agreement techniques. By ensuring proper synchronization and coordination among the nodes, the protocol prevents malicious actors from disrupting the system's functionality.

16) SESSION KEY SECURITY

Session keys are crucial in securing communications within a network. Attacks targeting session keys can compromise the confidentiality and integrity of data exchanged between nodes. The proposed protocol focuses on providing a privacy-preserving and efficient key agreement framework. By utilizing elliptic curve cryptography and hash functions, it ensures the security and integrity of session keys exchanged between participating entities. This defense mechanism protects against attacks attempting to compromise the confidentiality and integrity of the session keys.

17) EPHEMERAL SECURITY LEAKAGE ATTACKS

Ephemeral keys are temporary keys used during key exchange protocols to establish secure communication channels. Ephemeral security leakage attacks aim to extract or derive information from ephemeral keys, which can lead to the compromise of sensitive data. The proposed protocol employs efficient key exchange techniques using elliptic curve cryptography, ensuring the security and confidentiality of ephemeral keys. It defends against ephemeral security leakage attacks by preventing unauthorized access or extraction of information from these temporary keys.

B. FORMAL SECURITY ANALYSIS

The Random Oracle Model (ROR) is used to conduct a formal security examination (ROR). The ROR is frequently used to systematically check the security of different authentication techniques. It was created by Abdalla et al. [41] and described as a probabilistic polynomial-time turning machine (PPT) where an opponent and challenger engage in gameplay mechanics.

- *Participants:* Let $\mathcal{O}^{t_1}_{\mathcal{U}_i}$, $\mathcal{O}^{t_2}_{\mathcal{SN}_j}$ and$\mathcal{O}^{t_3}_{\mathcal{GW}_k}$ be the t_1, t_2, and t_3 occurrences of $\mathcal{U}$, $\mathcal{SN}$, and $\mathcal{GW}$ that are referred to as oracles, respectively.
- *the Accepted States:* Any instance of $\mathcal{O}^{\sqcup}$ that sets to the accepted phase after obtaining the most recent message from the protocol will be in an acceptable state. Session identification occurs when all of the conveyed messages during the discussion are coordinated in sequence for the current instance.
- *Partnering:* If all three of the following conditions are met at the same time, $\mathcal{O}^{t_1}$ and $\mathcal{O}^{t_2}$ are said to be partnered: (1) Occurrences $\mathcal{O}^{t_1}$ and $\mathcal{O}^{t_2}$ are in an acceptable condition; (2) Both occurrences $\mathcal{O}^{t_1}$ and $\mathcal{O}^{t_2}$ are mutually authenticated and assigned the same session ID. (3) The instances $\mathcal{O}^{t_1}$ and $\mathcal{O}^{t_2}$ are mutually exclusive.
- *Freshness:* $\mathcal{O}^{t_1}$ and $\mathcal{O}^{t_2}$ are regarded fresh if the user-sensor node established session key is currently revealed to $\mathcal{A}$ using reveal query.
- *Adversary:* Since the ROR model utilizes the well-known Dolav Yao model, the attacker has complete control over all communications. Thus, $\mathcal{A}$ can eavesdrop, alter, capture, falsify, replace, and even erase messages sent between the $\mathcal{U}$ and $\mathcal{SN}$ using the queries mentioned below.
  - *Execute ($\mathcal{O}^{t_1}$ and $\mathcal{O}^{t_2}$):* To resemble a passive eavesdropping attack by an adversary. To retrieve any communications exchanged between the two conversing parties, $\mathcal{A}$ uses this query.
  - *Reveal ($\mathcal{O}^{t_1}$):* $\mathcal{A}$ can retrieve the SK negotiated between $\mathcal{O}^{t_1}$ and other participant by launching this query.
  - *Send ($\mathcal{O}^{t_1}$, and message):* To simulate an active attack, $\mathcal{A}$ sends a msg, say Msg, to a participant $\mathcal{O}^{t_1}$ and waits for a response from $\mathcal{O}^{t_1}$.
  - *Test ($\mathcal{O}^{t_1}$):* This query investigates the semantic security of the established SK between $\mathcal{U}$ and $\mathcal{SN}$ using the ROR models interchangeably. To begin, a coin is tossed and the outcome is kept a secret. When the $\mathcal{A}$ executes this query and generates a new SK, the $\mathcal{O}^{t1}$ returns the newly created SK if the $\mathcal{C} = 1$ and a random value if the $\mathcal{C} = 0$. The outcome will be ignored if this is not the case.
- *Semantic Security:* In semantic security, the $\mathcal{A}$ must be able to tell the original SK from the random number. If desired, $\mathcal{A}$ may send a variety of Test queries to any of them, such as $\mathcal{O}^{t1}Ui$, $\mathcal{O}^{t2}SNj$ and $\mathcal{O}^{t3}GWNk$. The Test query output needs to be adaptable in terms of any bit e'. The adversary wins the game and is said to have achieved *Succ* if $\mathcal{A}$ thinks that e' is comparable to the random bit e. The benefit of $\mathcal{A}$ is that it can break semantic security and establish the SK between the $\mathcal{U}$ and $\mathcal{SN}$ in our protocol RMA-SAC in a polynomial time t is denoted by $Adv_{RMA-SAC}(t)$ and defined by $Adv_{RMA-SAC}(t) = |2prob(succ) - 1|$ where $Prob(.)$ denotes probability. RMA-SAC is now safe under the ROR model, if the value of $Adv_{RMA-SAC}(t) < \epsilon$, where $\epsilon > 0$.

Theorem 1: We suppose that the $\mathcal{A}$ executes in polynomial time t against the suggested protocol (RMA-SAC). To undermine the semantically security of RMA-SAC, the $\mathcal{A}$ advantageous function $Adv_{RMA-SAC}(t)$ in polynomial time t is defined as:

$$Adv_{RMA-SAC}(t) \leq \frac{Q_h^2}{|hash|} + \frac{Q_s}{2^{l-1}|d|} + 2Adv_{\mathcal{A}}^{ECDHP}(t)$$

where,Q_h = total number of hash query, Q_s = total number of send queries, $|hash|$ = range space of h(.), l = number of bits in biometric string of the user, $|d|$ = size of password and $Adv_{ECDHP}(t)$ = advantage of $\mathcal{A}$ to break ECDLP.

Proof: In the formal proof, there are five games in order, say G_i, where i = 0,1,2,3,4. The adversary chance of winning the game G_i is represented by *succ*, and the advantage of winning the game is defined as $Adv_{G_i} = Prob[succ_{G_i}]$. All of the games are shown below.

G_0: In this game, adversary $\mathcal{A}$ introduces the first real attack on the proposed protocol RMA-SAC in the ROR model. The semantic security of the session key of the proposed scheme is achieved by guessing e number of bits before beginning the game G_0.

$$Adv_{RMA-SAC}(t) = |2Adv_{G_0} - 1| \tag{1}$$

G_1: In this game, the eavesdropping attack of adversary $\mathcal{A}$ is replicated. At the start of the game G_1, adversary $\mathcal{A}$ Execute ($\mathcal{O}^{t_1}$ and $\mathcal{O}^{t_2}$) query, and once the game is finished, adversary $\mathcal{A}$ executes the Test($\mathcal{O}^{t_1}$) query to determine whether the returned result is the established fresh session key SK or an arbitrary value. The session key SK is computed by both communicating parties as $SK_{\mathcal{U}} = h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_1.A_2 \| V_1 \| t_5)$ in our protocol. Adversary $\mathcal{A}$ requires $s_1.A_2$ and V_1 temporal secrets and permanent secrets, to achieve session key SK. Therefore, the adversary $\mathcal{A}$ chance of winning this game G_1 by eavesdropping are not successful. It indicates that the games G_0 and G_1 are the same. Therefore, it follows:

$$Adv_{G_0} = Adv_{G_1} \tag{2}$$

G_2 Send($\mathcal{O}^{t_1}$ and M_i) and *hash* of a random oracle are implemented in Game G_2. Adversary $\mathcal{A}$ launches active attacks in order to obtain all of the communications exchanged during communication that are $M_1 = \{W_1, V_2, t_1\}$, $M_2 = \{W_1, V_3, t_1, t_2\}$ $M_3 = \{W_2, V_5, t_5\}$ and $M_4 = \{W_2, t_7\}$. Adversary $\mathcal{A}$ can generate as many hash oracles as he likes to search for collisions in the outputs of *hash*. Every message delivered makes use of random numbers as well as other secure credentials like symmetric key encryption. Therefore, adversary $\mathcal{A}$ needs all of these credentials in order to alter the messages. However, each of them is safeguarded by the collision-resistant one-way hash function. The messages additionally contain current time stamps t_1, t_2, t_3, t_4 and an elliptic curve encryption. There are no collisions in the hash oracle as a result of all of the messages becoming inconsistent. With the birthday paradox has been established, we can draw the following conclusion.

$$|Adv_{G_2} - Adv_{G_1}| \leq \frac{Q_h^2}{2|hash|} \tag{3}$$

G_3: This game G_2 simulates the corrupt device ($\mathcal{O}^{t_1}_{\mathcal{U}_1}$) or corrupt-device ($\mathcal{O}^{t_1}_{\mathcal{SN}_1}$) inquiry, in which the attacker can remove all of the data for the user or sensor nodes. Utilizing the thesaurus attack, the adversary can guess the users' password $\mathcal{PW}_{\mathcal{U}}$ and identity $\mathcal{ID}_{\mathcal{U}}$, which is computationally infeasible as unrecognized secret credentials such as biometric $B_{\mathcal{U}}$, when using the Send($\mathcal{O}^{t_1}$ and Msg) query. Moreover, the cost of obtaining a biometric is approximately $1/2^l$. Both G_3 and G_2 are equivalent if the password-guessing approach is not used. The final result is as follows:

$$|Adv_{G_3} - Adv_{G_2}| \leq \frac{Q_s}{2^l|d|} \tag{4}$$

G_4: The final game is modelled for active attack by adversary in order to determine the actual session key $SK_{\mathcal{U}} = h(\mathcal{ID}_{\mathcal{SN}} \| \mathcal{ID}_{\mathcal{U}} \| s_2.A_2 \| V_1 \| t_5)$ created between the user and sensor node. To obtain session key, they needs to compute $s_2.A_2$ and V_i. This is difficult due to the ECDHP problem, which is computationally infeasible. Therefore, the following is the result:

$$|Adv_{G_4} - Adv_{G_3}| \leq Adv^{ECDHP}_{\mathcal{A}}(t) \tag{5}$$

Finally, all of the games are completed, leaving the adversary with only the task of guessing the proper bit of c, resulting in the following outcome.

$$Adv_{G_4} = \frac{1}{2} \tag{6}$$

From equation (1) and (2) we get,

$$\frac{1}{2}Adv_{RMA-SAC}(t) = |Adv_{G_0} - \frac{1}{2}| = |Adv_{G_1} - \frac{1}{2}| \tag{7}$$

From equation (6) and (7) we get,

$$\frac{1}{2}Adv_{RMA-SAC}(t) = |Adv_{G_1} - Adv_{G_4}| \tag{8}$$

By triangular law of inequality, we get

$$|Adv_{G_1} - Adv_{G_4}| \leq |Adv_{G_1} - Adv_{G_2}|$$

$$+ |Adv_{G_2} - Adv_{G_4}| \tag{9}$$

$$|Adv_{G_1} - Adv_{G_2}| + |Adv_{G_2} - Adv_{G_4}| \leq \tag{10}$$

$$|Adv_{G_1} - Adv_{G_2}| + |Adv_{G_2} - Adv_{G_3}| \tag{11}$$

$$+ |Adv_{G_3} - Adv_{G_4}| + |Adv_{G_1} - Adv_{G_4}| \tag{12}$$

$$|Adv_{G_1} - Adv_{G_4}| \leq \frac{Q_h^2}{2|hash|} + \frac{Q_s}{2^l|d|} + Adv^{ECDHF}_{\mathcal{A}}(t) \tag{13}$$

From equations (8) and (11), we get

$$\frac{1}{2}Adv_{RMA-SAC}(t) \leq \frac{Q_h^2}{2|hash|} + \frac{Q_s}{2^l|d|} + Adv^{ECDHP}_{\mathcal{A}}(t) \tag{14}$$

Multiplying equation (14) by 2 on both sides, we get

$$Adv_{RMA-SAC}(t) \leq \frac{Q_h^2}{|hash|} + \frac{Q_s}{2^{l-1}|d|} + 2Adv^{ECDHP}_{\mathcal{A}}(t) \tag{15}$$

C. BAN LOGIC

Using BAN logic, we performed a security analysis to determine that the suggested algorithms have secure mutual authentication. BAN logic notations are shown in table 4. The BAN logic analysis rules, goals, idealized form, and assumptions are also specified. We show that the suggested protocol ensures secure mutual authentication between $\mathcal{U}$, $\mathcal{GW}$, *and* $\mathcal{SN}$.

TABLE 4. BAN logic notation.

Notation	Description
$\mathcal{PP}_1, \mathcal{PP}_2$	Principals
$\mathcal{SM}_1, \mathcal{SM}_2$	Statements
SK	Session key
$\mathcal{PP}_1 \mid\equiv \mathcal{SM}_1$	$\mathcal{PP}_1$ believes $\mathcal{SM}_1$
$\mathcal{PP}_1 \mid\sim \mathcal{SM}_1$	$\mathcal{PP}_1$ once said $\mathcal{SM}_1$
$\mathcal{PP}_1 \Rightarrow \mathcal{SM}_1$	$\mathcal{PP}_1$ has got jurisdiction of $\mathcal{SM}_1$
$\mathcal{PP}_1 \lhd \mathcal{SM}_1$	$\mathcal{PP}_1$ receives $\mathcal{SM}_1$
$\#\mathcal{SM}_1$	$\mathcal{SM}_1$ fresh
$\#\{\mathcal{SM}_1\}_K$	$\mathcal{SM}_1$ is encrypted with key K
$<\mathcal{SM}_1>\mathcal{SM}_2$	$\mathcal{SM}_1$ is combined with $\mathcal{SM}_2$
$\mathcal{PP}_1 \xleftrightarrow{K} X_2$	$\mathcal{PP}_1$ *and* $\mathcal{PP}_2$ have shared key K

1) BAN LOGIC RULES

The following are the main logical postulates of the BAN logic:

- Message Meaning Rule (MMR):

$$\frac{\mathcal{PP}_1 \mid\equiv \mathcal{PP}_1 \xleftrightarrow{K} \mathcal{PP}_2, \mathcal{PP}_1 \lhd \{\mathcal{SM}_1\}_k}{\mathcal{PP}_1 \mid\equiv \mathcal{PP}_2 \mid\sim \mathcal{SM}_1}$$

- Freshness Rule (FR):

$$\frac{\mathcal{PP}_1 \mid\equiv \#(\mathcal{SM}_1)}{\mathcal{PP}_1 \mid\equiv \#(\mathcal{SM}_1, \mathcal{SM}_2)}$$

- Nonce Verification Rule (NVR):

$$\frac{\mathcal{PP}_1 \mid\equiv \#(\mathcal{SM}_1), \mathcal{PP}_1 \mid\equiv \mathcal{PP}_2 \mid\sim \mathcal{SM}_1}{\mathcal{PP}_1 \mid\equiv \mathcal{PP}_2 \mid\equiv \mathcal{SM}_1}$$

- Belief Rule (BR):

$$\frac{\mathcal{PP}_1 \mid\equiv (\mathcal{SM}_1, \mathcal{SM}_2)}{\mathcal{PP}_1 \mid\equiv \mathcal{SM}_1}$$

- Jurisdiction Rule (JR):

$$\frac{\mathcal{PP}_1 \mid\equiv \mathcal{PP}_2 \mid\Rightarrow \mathcal{SM}_1, \mathcal{SM}_1 \mid\equiv \mathcal{PP}_2 \mid\equiv \mathcal{SM}_1}{\mathcal{PP}_1 \mid\equiv \mathcal{SM}_1}$$

2) BAN LOGIC GOALS

- $G_1 : \mathcal{U} \mid\equiv \mathcal{U} \xleftrightarrow{SK} \mathcal{SN}$
- $G_2 : \mathcal{SN} \mid\equiv \mathcal{U} \xleftrightarrow{SK} \mathcal{SN}$
- $G_3 : \mathcal{U} \mid\equiv \mathcal{SN} \mid\equiv \mathcal{U} \xleftrightarrow{SK} \mathcal{SN}$
- $G_4 : \mathcal{SN} \mid\equiv \mathcal{U} \mid\equiv \mathcal{U} \xleftrightarrow{SK} \mathcal{U}$

3) IDEALIZED FORMS

- Message-1 : $\mathcal{U} \rightarrow \mathcal{GW} : M_1 = \{W_1, V_2, t_1\}_{K_{\mathcal{U}}}$
- Message-2 : $\mathcal{GW} \rightarrow \mathcal{SN} : M_2 = \{W_1, V_3, t_3\}_{K_{\mathcal{U}}}$
- Message-3 : $\mathcal{SN} \rightarrow \mathcal{GW} : M_3 = \{W_2, V_5, t_5\}_{K_{\mathcal{SN}}}$
- Message-4 : $\mathcal{GW} \rightarrow \mathcal{U} : M_4 = \{W_2, V_6, t_7\}_{K_{\mathcal{SN}}}$

4) ASSUMPTIONS

- A_1: $\mathcal{U} \mid\equiv (\mathcal{U} \xleftrightarrow{K_{\mathcal{U}}} \mathcal{GW})$
- A_2: $\mathcal{GW} \mid\equiv \#(t_1)$
- A_3: $\mathcal{SN} \mid\equiv (\mathcal{GW} \xleftrightarrow{K_{\mathcal{U}}} \mathcal{SN})$
- A_4: $\mathcal{SN} \mid\equiv \#(t_3)$
- A_5: $\mathcal{GW} \mid\equiv (\mathcal{SN} \xleftrightarrow{K_{\mathcal{SN}}} \mathcal{GW})$
- A_6: $\mathcal{GW} \mid\equiv \#(t_5)$
- A_7: $\mathcal{U} \mid\equiv (\mathcal{GW} \xleftrightarrow{K_{\mathcal{SN}}} \mathcal{U})$
- A_8: $\mathcal{U} \mid\equiv \#(t_7)$
- A_9: $\mathcal{U} \mid\equiv \mathcal{SN} \Rightarrow (\mathcal{U} \xleftrightarrow{SK} \mathcal{SN})$
- A_{10}: $\mathcal{SN} \mid\equiv \mathcal{U} \Rightarrow (\mathcal{U} \xleftrightarrow{SK} \mathcal{SN})$

5) PROOF USING BAN LOGIC

The proof then proceeds as below:

- Step-1: From message-1, we get:

$$S_1 : \mathcal{GW} \lhd (W_1, V_2, t_1)_{K_{\mathcal{U}}}$$

- Step-2: From S_1 and A_1 with MMR, we get.

$$S_2 : \mathcal{GW} \mid\equiv \mathcal{U} \mid\sim (W_1, V_2, t_1)_{K_{\mathcal{U}}}$$

- Step-3: From S_2 and $A_2$with the FR, we obtain

$$S_3 : \mathcal{GW} \mid\equiv \#(W_1, V_2, t_1)_{K_{\mathcal{U}}}$$

- Step-4: From S_2 and S_3 with the NVR, we get

$$S_4 : \mathcal{GW} \mid\equiv \mathcal{U} \mid\equiv (W_1, V_2, t_1)_{K_{\mathcal{U}}}$$

- Step-5: From S_4 with BR, we get

$$S_5 : \mathcal{GW} \mid\equiv \mathcal{U} \mid\equiv (W_1, V_2, t_1)_{K_{\mathcal{U}}}$$

- Step-6: According to message-2, we could get:

$$S_6 : \mathcal{SN} \lhd (W_1, V_3, t_3)_{K_{\mathcal{U}}}$$

- Step-7: From S_6 and A_3 with the MMR, we get.

$$S_7 : \mathcal{SN} \mid\equiv \mathcal{GW} \mid\sim (W_1, V_3, t_3)_{K_{\mathcal{U}}}$$

- Step-8: From S_7 and A_4 with FR, we get

$$S_8 : \mathcal{SN} \mid\equiv \#(W_1, V_3, t_3)_{K_{\mathcal{U}}}$$

- Step-9: From S_7 and S_8 with NVR, we get

$$S_9 : \mathcal{SN} \mid\equiv \mathcal{GW} \mid\equiv (W_1, V_3, t_3)_{K_{\mathcal{U}}}$$

- Step-10: According to message-3, we could get:

$$S_{10} : \mathcal{GW} \lhd (W_2, V_5, t_5)_{K_{\mathcal{SN}}}$$

- Step-11: From S_{10} and A_5 with MMR, we obtain

$$S_{11} : \mathcal{GW} \mid\equiv \mathcal{SN} \mid\sim (W_2, V_5, t_5)_{K_{\mathcal{SN}}}$$

- Step-12: From S_{11} and A_6 with the FR, we get

$$S_{12} : \mathcal{GW} \mid\equiv \#(W_2, V_5, t_5)_{K_{\mathcal{SN}}}$$

- Step-13: From S_{11} and S_{12} with NVR, we get

$$S_{13} : \mathcal{GW} \mid\equiv \mathcal{SN} \mid\equiv (W_2, V_5, t_5)_{K_{\mathcal{SN}}}$$

- Step-14: According to message-4, we could get:

$$S_{14} : \mathcal{GW} \lhd (W_2, V_6, t_7)_{K_{\mathcal{SN}}}$$

- Step-15: From S_{14} and A_7 with MMR, we get.

$$S_{15} : \mathcal{U} \mid\equiv \mathcal{GW} \mid\sim (W_2, V_6, t_7)_{K_{\mathcal{SN}}}$$

- Step-16: From S_{15} and A_8 with FR, we get

$$S_{16} : \mathcal{U}| \equiv \#(W_2, V_6, t_7)_{K_{\mathcal{SN}}}$$

- Step-17:From S_{15} and S_{16} with NVR, we get

$$S_{17} : \mathcal{U}| \equiv \mathcal{GW}| \equiv (W_2, V_6, t_7)_{K_{\mathcal{SN}}}$$

- Step-18: From S_{17} with BR, we get

$$S_{18} : \mathcal{U}| \equiv \mathcal{GW}| \equiv \mathcal{U} \overset{SK}{\longleftrightarrow} \mathcal{GW} \quad (G-3)$$

- Step-19: From S_{18} and A_9 with JR, we get

$$S_{19} : \mathcal{U}| \equiv \mathcal{U} \overset{SK}{\longleftrightarrow} \mathcal{GW} \quad (G-1)$$

- Step-20: From the S_5, S_9, S_{13} and S_{17} we could get

$$S_{20} : \mathcal{GW}| \equiv \mathcal{U}| \equiv \mathcal{U} \overset{SK}{\longleftrightarrow} \mathcal{GW} \quad (G-4)$$

- Step-21: From S_{19} and A_{10} with JR, we get

$$S_{21} : \mathcal{GW}| \equiv \mathcal{U} \overset{SK}{\longleftrightarrow} \mathcal{GW} \quad (G-2)$$

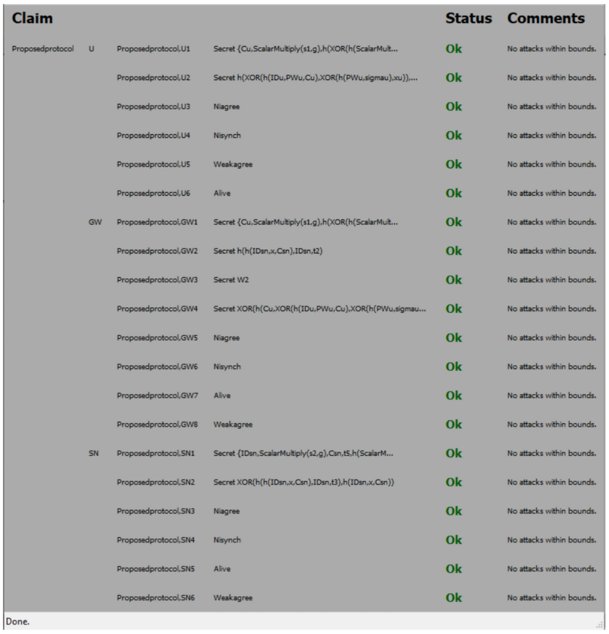
Referring to goals G-1 to G-4, we show that the suggested scheme ensure the robust mutual authentication between $\mathcal{U}$, $\mathcal{GW}$ and $\mathcal{SN}$.

D. SCYTHER TOOL ANALYSIS

Scyther is a tool designed for the formal security evaluation of frameworks based on the assumption of unbreakable cryptography [42]. It can determine the protocol's security requirements as well as its flaws. Scythers systems are capable of performing multi-protocol analysis.

In Figure 2, we show that the authentication process between $\mathcal{U}$, $\mathcal{GW}$ and $\mathcal{SN}$ is secure, with no attacks occurring within the bounds of the proposed protocol. According to the findings, the $\mathcal{U}$, $\mathcal{GW}$ and $\mathcal{SN}$ devices all met the Ni-Agree, Weakagree, Alive, Ni-Synch, commit, and secret key requirements.

- Non-injective synchronisation (Ni-synch): Ni-agree ensures that messages are sent according to protocol specifications. That is, once the protocol has been completed by the initiator and responder, all messages are received in the exact and similar order specified in the framework. This authentication form outperforms Ni-agree, Alive, and Weak-agree in terms of strength.
- Non-injective agreement: When a sender completes a protocol run, presumably with the receiver, the receiver has completed a protocol run with the sender in the past, and they have agreed on all datasets.
- Aliveness (Alive): According to our argument, the protocol guarantees that a sender will always be alive when communicating with a recipient whom has already executed the protocol.
- Weak agreement (weak-agree): Weak agreement is when there is little or no agreement. When the initiator completes a run of the protocol with the responder, we claim that the protocol ensures the initiator's weak agreement with another agent responder.



Claim				Status	Comments
Proposedprotocol	U	Proposedprotocol,U1	Secret {Cu,ScalarMultiply(s1,g),h(XOR(h(ScalarMult...	Ok	No attacks within bounds.
		Proposedprotocol,U2	Secret h(XOR(h(IDu,PWu,Cu),XOR(h(PWu,sigmau),xu)),...	Ok	No attacks within bounds.
		Proposedprotocol,U3	Niagree	Ok	No attacks within bounds.
		Proposedprotocol,U4	Nisynch	Ok	No attacks within bounds.
		Proposedprotocol,U5	Weakagree	Ok	No attacks within bounds.
		Proposedprotocol,U6	Alive	Ok	No attacks within bounds.
	GW	Proposedprotocol,GW1	Secret {Cu,ScalarMultiply(s1,g),h(XOR(h(ScalarMult...	Ok	No attacks within bounds.
		Proposedprotocol,GW2	Secret h(h(IDsn,x,Csn),IDsn,t2)	Ok	No attacks within bounds.
		Proposedprotocol,GW3	Secret W2	Ok	No attacks within bounds.
		Proposedprotocol,GW4	Secret XOR(h(Cu,XOR(h(IDu,PWu,Cu),XOR(h(PWu,sigmau...	Ok	No attacks within bounds.
		Proposedprotocol,GW5	Niagree	Ok	No attacks within bounds.
		Proposedprotocol,GW6	Nisynch	Ok	No attacks within bounds.
		Proposedprotocol,GW7	Alive	Ok	No attacks within bounds.
		Proposedprotocol,GW8	Weakagree	Ok	No attacks within bounds.
	SN	Proposedprotocol,SN1	Secret {IDsn,ScalarMultiply(s2,g),Csn,t5,h(ScalarM...	Ok	No attacks within bounds.
		Proposedprotocol,SN2	Secret XOR(h(h(IDsn,x,Csn),IDsn,t3),h(IDsn,x,Csn))	Ok	No attacks within bounds.
		Proposedprotocol,SN3	Niagree	Ok	No attacks within bounds.
		Proposedprotocol,SN4	Nisynch	Ok	No attacks within bounds.
		Proposedprotocol,SN5	Alive	Ok	No attacks within bounds.
		Proposedprotocol,SN6	Weakagree	Ok	No attacks within bounds.

Done.

FIGURE 2. Scyther test results.

The non-injective synchronization (Ni-Synch) attribute requires the runs noted by the model procedure to implement the appropriate events of sending and receiving parameters in the exact ordering and with identical ranges. The Ni-Agree claims that users consent to the values of transmitted variables, and analytical data validates the accurateness of $\mathcal{U}$. Therefore, $\mathcal{U}$ meets Ni-Synch and Ni-Agree properties of $\mathcal{GW}$. In a similar manner, the $\mathcal{SN}$ fulfills the $\mathcal{GW}$ Ni-Synch and Ni-Agree properties. The private keys between the $\mathcal{U}$ and $\mathcal{GW}$ have been proven to be secret. Also confirmed to be secret between the $\mathcal{GW}$ and $\mathcal{SN}$. In the communication process, random numbers are also kept private and have no vulnerabilities within the bounds.

V. PERFORMANCE ANALYSIS

This section compares the performance of the proposed scheme to existing schemes [12], [19], [20], [21], [25], [28], [30], [31], [43]. The primary goal of the performance evaluation is to demonstrate that our scheme is more capable in terms of extra features with lower overheads than other existing schemes.

A. SECURITY ATTRIBUTES

In this section, we use our simulation metrics to compare the functionality and security characteristics of our authenticated key agreement scheme to those of other schemes, [12], [19], [20], [21], [25], [28], [30], [31], [43]. The usefulness and security of several methods are compared in Table 5. The majority of the schemes do not support password changes, despite being susceptible to a number of security risks. The dynamic connection among the sensors in our system, however, allows users to update their biometrics and passwords.

TABLE 5. Security attributes comparison of the proposed framework with related frameworks.

Features	[12]	[19]	[20]	[21]	[25]	[28]	[30]	[31]	[43]	Proposed
$\mathcal{PKS}$	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{MA}$	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
$\mathcal{SKDA}$	✓	✓	×	✓	×	×	✓	✓	×	✓
$\mathcal{RA}$	✓	✓	✓	✓	×	✓	✓	✓	×	✓
$\mathcal{DA}$	×	×	✓	✓	×	✓	×	×	×	✓
$\mathcal{OIPA}$	×	×	✓	✓	✓	×	×	✓	✓	✓
$\mathcal{EDA}$	✓	✓	×	✓	×	×	×	✓	×	✓
$\mathcal{KF}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{PFC}$	✓	✓	✓	×	×	×	✓	✓	✓	✓
$\mathcal{USTA}$	✓	×	✓	✓	✓	×	✓	✓	✓	✓
$\mathcal{IA}$	✓	×	✓	×	×	✓	×	✓	✓	✓
$\mathcal{INA}$	✓	×	✓	×	✓	×	✓	✓	×	✓
$\mathcal{ROR}$	✓	×	✓	✓	×	×	✓	×	×	✓
$\mathcal{STV}$	×	×	×	×	×	✓	×	✓	×	✓
$\mathcal{BLV}$	×	×	×	✓	✓	×	✓	×	✓	✓

Note : $\mathcal{PKS}$ =Private key security, $\mathcal{MA}$ = Mutual authentication, $\mathcal{SKDA}$ = Session key disclosure attack, $\mathcal{EDA}$ = Eavesdropping attack, $\mathcal{KF}$ =Key Freshness, $\mathcal{PFC}$ = Perfect forward secrecy, $\mathcal{RA}$ = Replay attack, $\mathcal{DA}$ = DoS attack, $\mathcal{OIPA}$ = Off-line user identity predicting attack, $\mathcal{USTA}$ = User and sensor node traceability attack, $\mathcal{IA}$ = Impersonation attack, $\mathcal{INA}$ = Insider attack, $\mathcal{ROR}$ = ROR model, $\mathcal{STV}$ = Scyther Tool verification, $\mathcal{BLV}$ = BAN Logic verification.

TABLE 6. Computation cost of different operators.

Operation	Description	Computation cost (ms)
t_{mod}	Modular exponentiation operation	3.8500
t_{bp}	Bilinear pairing operation	05.811
t_{ecm}	ECC scalar point multiplication	02.226
$t_{as-enc/dec}$	Symmetric encryption /decryption	0.0046
t_{fe}	Fuzzy extraction operation	02.226
t_h	One-way hash function (SHA-1 256)	0.0023
$t_{s-enc/dec}$	Public key encryption/decryption	3.8500
t_{eca}	ECC-based point addition	0.0288

B. COMPUTATION COSTS

Table 6 displays the comparative time execution of required parameters for the execution of the scheme in terms of computing overhead, with the suggested schemes' total duration in milliseconds as the unit of comparison in milliseconds. Only the frequently performed login and mutual authentication phases are used to estimate computing costs. The test is run on a Core-i5 Quad-core 2.20 GHz processor with 4 GB RAM running on windows-10 64-bit operating system [31], [43], [44].

As shown in Table 7, Rangwani et al. [30] used $17t_h$, $7t_{ecm}$ and $10t_{eca}$ in his protocol that will costs 15.9091ms, Vinoth et al. [31] used $12t_h$, $2t_{bp}$, $4t_{a-enc/dec}$, $2t_{ecm}$ and $1t_{mod}$ in his protocol that will costs 19.9700ms, Wu et al. [12] used $17t_h$ and $6t_{s-enc/dec}$ in his protocol that will costs 23.1391ms, Wang et al. [43] used $7t_{mod}$, t_{fe} and $25t_h$ in his protocol that will costs 29.2335ms, Ali et al. [21] used $25t_h$ and $8t_{s-enc/dec}$ in his protocol that will costs 30.8575ms, Liu et al. [19] used $7t_h$, $2t_{ecm}$ and $4t_{bp}$ in his protocol that will costs 27.7121ms, Challa et al. [20] used $12t_h$ and $14t_{ecm}$ in his protocol that will costs 31.1916ms, Soni et al. [25] used $31t_h$, $6t_{ecm}$ and $1t_{fe}$ in his protocol that will costs 15.6533ms, Moghadam et al. [28] used $13t_h$, $3t_{s-enc/dec}$ and $5t_{ecm}$ in his protocol that will costs 22.7099ms. In the proposed protocol we used only $15t_h$, $2t_{ecm}$, $2t_{a-enc/dec}$ and $1t_{fe}$ in his protocol that will costs 6.7217ms. Therefore, the computation cost in our proposed protocol is comparatively low as compared to the existing protocol in the same environment as shown in Figure 3.

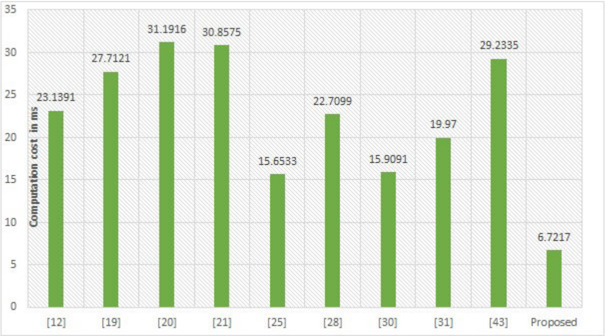


FIGURE 3. Computation cost comparison.

TABLE 7. Computation cost comparison.

Protocols	Operations	Computation cost (milliseconds)
[12]	$17t_h + 6t_{s-enc/dec}$	≈ 23.1391
[19]	$7t_h + 2t_{ecm} + 4t_{bp}$	≈ 27.7121
[20]	$12t_h + 14t_{ecm}$	≈ 31.1916
[21]	$25t_h + 8t_{s-enc/dec}$	≈ 30.8575
[25]	$31t_h + 6t_{ecm} + 1t_{fe}$	≈ 15.6533
[28]	$13t_h + 3t_{s-enc/dec} + 5t_{ecm}$	≈ 22.7099
[30]	$17t_h + 7t_{ecm} + 10t_{eca}$	≈ 15.9091
[31]	$12t_h + 2t_{bp} + 4t_{as-enc/dec} + 2t_{ecm} + 1t_{mod}$	≈19.9700
[43]	$7t_{mod} + t_{fe} + 25t_h$	≈ 29.2335
Proposed	$15t_h + 2t_{ecm} + 2t_{as-enc/dec} + 1t_{fe}$	≈ 6.7217

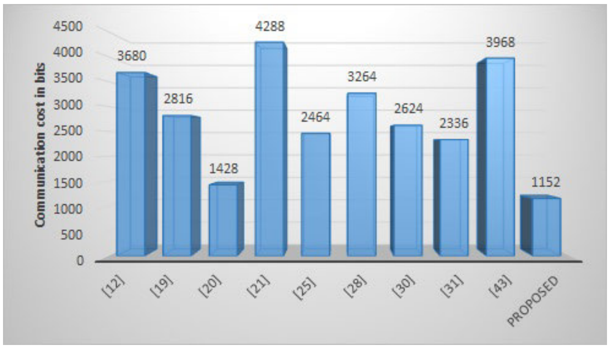


FIGURE 4. Communication cost comparison.

C. COMMUNICATION COSTS

Based on the total lengths of messages sent and received in bits, Table 8 displays the estimated communication expenses for every authority, including gateways, sensor nodes, and remote users. Only the typically completed login and mutual authentication phases are taken into consideration for communication cost estimations. For user, gateway, and sensor node identification, we utilised 64 bits, while for passwords and timestamps, we used 32 bits. This allowed us to determine the communication cost. According to [44], the sizes of symmetric-key encryption and cryptographic hashing are 160 and 128 bits, respectively. Throughout the proposed protocol's login and authentication phase, the user, gateway, and sensor node only use 1152 bits of communication cost to send and receive messages. The proposed protocol consumes less communication cost as compared to the other existing protocols in the same environment as shown in Figure 4.

TABLE 8. Communication cost comparison.

Protocols	Messages	Communication cost (in bits)
[12]	4	3680
[19]	4	2816
[20]	3	1428
[21]	5	4288
[25]	4	2464
[28]	4	3264
[30]	4	2624
[31]	4	2336
[43]	4	3968
Proposed	4	1152

D. LIMITATIONS AND CHALLENGES

The proposed privacy-preserving and efficient key agreement framework for smart agriculture monitoring systems has the following limitations and challenges:

Limited Coverage: While wireless sensor networks have the potential to provide valuable data on a range of climatic parameters in an agricultural field, the coverage area of these networks is limited. This means that it may not be possible to monitor every part of a large agricultural area, which could limit the effectiveness of the proposed protocol.

Reliability: Wireless sensor networks can be prone to interference and other technical issues that could affect the reliability of the data being collected. This could impact the accuracy of the proposed protocol and its ability to provide secure communication in smart agriculture monitoring systems.

Cost: Implementing a wireless sensor network for agricultural monitoring can be costly, especially for small-scale farmers. This could limit the widespread adoption of the proposed protocol and other similar technologies in the agricultural sector.

Privacy Preservation: The proposed protocol aims to ensure privacy preservation in smart agriculture monitoring systems, but it may not be foolproof. There may still be some risks of data breaches or unauthorized access to sensitive data, which could have negative consequences for farmers and other stakeholders in the agriculture industry.

Security Enhancement: While the proposed protocol provides security enhancements, it may not be enough to address all the security risks associated with wireless sensor networks in agriculture. As new threats emerge, it may be necessary to continually update and improve the protocol to ensure that it remains effective.

Scalability: As the number of agricultural monitoring systems grows, the proposed protocol may need to be adapted to handle larger volumes of data. This could require significant changes to the protocol and the underlying technology, which could be a challenge for researchers and developers in the field.

E. STRENGTHS AND ADVANTAGES

The proposed privacy-preserving and efficient key agreement framework for smart agriculture monitoring systems has several strengths and advantages, including:

Improved Agricultural Productivity: The proposed protocol leverages wireless sensor networks to monitor climatic parameters in agriculture fields, such as soil moisture, the acidity level of soil, humidity, and light. This helps to improve crop growth, quality, and productivity, which ultimately leads to an increase in agricultural productivity in terms of both quantity and quality.

Enhanced Security: The proposed framework addresses the security risks associated with wireless sensor networks, such as impersonation, alteration, interference, and an interception. By using elliptic curve cryptography and hash functions, the proposed protocol ensures secure communication in smart agriculture monitoring systems.

Privacy Preservation: Privacy preservation is crucial in smart agriculture monitoring systems to prevent sensitive information from being disclosed to unauthorized parties. The proposed protocol incorporates privacy-preserving mechanisms, which ensure that confidential information is protected.

Efficient Key Agreement: The proposed protocol uses a key agreement framework that facilitates mutual authentication and key exchange using BAN logic. This ensures that communication between devices is secure and efficient.

Formal Security Verification: The proposed protocol's security correctness is verified using the well-known security verification Scyther tool. Additionally, the security of the proposed system is formalized using the ROR model, providing a comprehensive assessment of the protocol's security.

Superiority over Comparable Protocols: The proposed protocol is compared with similar protocols in the same environment based on security features, computation, and communication overheads. The comparison reveals that the proposed protocol provides superior security and efficiency than other existing protocols.

In summary, the proposed privacy-preserving and efficient key agreement framework for smart agriculture monitoring systems provides improved agricultural productivity, enhanced security, privacy preservation, efficient key agreement, formal security verification, and superiority over comparable protocols

VI. CONCLUSION AND FUTURE DIRECTIONS

Agriculture is key to any country's economic development. Therefore, presently IoT based WSN technology used in agriculture can be employed to boost productivity, quality, and growth. However, presently technology has made security and privacy key concerns. For this purpose, we designed a robust mutual authentication and key exchanged framework for an IoT-enabled intelligent precision smart agriculture monitoring system by using wireless sensor networks. The proposed framework makes use of ECC, biometrics, and a commonly utilized fuzzy extractor. The Hamming distance was utilized to examine the fuzzy extractor technique for user biometric verification to avoid erroneous acceptance and rejection mistakes. We performed a formal security evaluation of the suggested framework for secure session key agreement using the well-known ROR model, and mutual authentication is preserved using BAN Logic. The suggested framework allows legitimate users to update or change their biometrics and password. Moreover, the suggested framework is proved to be secure against relevant passive and active threats within the bounds using the well-known Scyther simulation tool. Through informal security analysis and functional requirements, the comparison has been done to show the strength of the proposed key agreement and authentication protocol to other existing protocols. The suggested architecture is also shown to be more effective in terms of computational and communication overheads.

Future directions for this research include exploring the potential of incorporating machine learning and artificial intelligence techniques to further enhance the accuracy and efficiency of the proposed protocol. Additionally, further testing and validation of the protocol in real-world scenarios could be conducted to provide additional evidence of its effectiveness. Overall, the proposed protocol offers significant potential to improve the security and efficiency of smart agriculture monitoring systems, which can ultimately lead to increased agricultural productivity and economic growth.

ACKNOWLEDGMENT

The authors would like to thank the IEEE Access Editor-in-Chief and the anonymous reviewers for their insightful comments and valuable suggestions that have resulted in the improvement of this manuscript and also would like to thank Dr. Vinod Kumar of the Shyam Lal College, University of Delhi, New Delhi, India, for valuable suggestions to improve the proposed manuscript.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.* vol. 54, no. 15, pp. 2787–2805, 2010.

[2] A. Khanna and S. Kaur, "Evolution of Internet of Things (IoT) and its significant impact in the field of precision agriculture," *Comput. Electron. Agricult.*, vol. 157, pp. 218–231, Feb. 2019.

[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[4] X. Shi, X. An, Q. Zhao, H. Liu, L. Xia, X. Sun, and Y. Guo, "State-of-the-art Internet of Things in protected agriculture," *Sensors*, vol. 19, no. 8, p. 1833, Apr. 2019.

[5] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009, doi: 10.1109/TWC.2008.080128.

[6] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks.," *Ad Hoc Sens. Wireless Netw.*, vol. 10, no. 4, pp. 361–371, 2010.

[7] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks,'" *Sensors*, vol. 10, no. 3, pp. 2450–2459, Mar. 2010.

[8] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in *Proc. IEEE 6th Int. Conf. Wireless Mobile Comput., Netw. Commun.*, Oct. 2010, pp. 600–606.

[9] W.-B. Hsieh and J.-S. Leu, "A robust user authentication scheme using dynamic identity in wireless sensor networks," *Wireless Pers. Commun.*, vol. 77, no. 2, pp. 979–989, Jul. 2014.

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

[11] C. Chang and H. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.

[12] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *J. Ambient Intell. Humanized Comput.*, vol. 8, no. 1, pp. 101–116, Feb. 2017.

[13] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Comput. Netw.*, vol. 104, pp. 137–154, Jul. 2016.

[14] J. Srinivas, D. Mishra, and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks," *J. Med. Syst.*, vol. 41, no. 5, pp. 1–19, May 2017.

[15] C. Li, X. Zhang, H. Wang, and D. Li, "An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks," *Sensors*, vol. 18, no. 2, p. 194, Jan. 2018.

[16] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput.*, vol. 74, no. 12, pp. 6428–6453, Dec. 2018.

[17] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Syst.*, vol. 21, no. 1, pp. 49–60, Feb. 2015.

[18] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2643–2655, Oct. 2016.

[19] C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 59, pp. 250–261, Apr. 2017.

[20] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, Jul. 2018.

[21] R. Ali, A. K. Pal, S. Kumari, M. Karuppiah, and M. Conti, "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring," *Future Gener. Comput. Syst.*, vol. 84, pp. 200–215, Jul. 2018.

[22] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, p. 644, Mar. 2017.

[23] S. Shin and T. Kwon, "A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes," *Sensors*, vol. 19, no. 9, p. 2012, Apr. 2019.

[24] V. S. Naresh, S. Reddi, and N. V. E. S. Murthy, "Provable secure lightweight multiple shared key agreement based on hyper elliptic curve Diffie–Hellman for wireless sensor networks," *Inf. Secur. J., A Global Perspective*, vol. 29, no. 1, pp. 1–13, Jan. 2020.

[25] P. Soni, A. K. Pal, and S. H. Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system," *Comput. Methods Programs Biomed.*, vol. 182, Dec. 2019, Art. no. 105054.

[26] G. Xu, F. Wang, M. Zhang, and J. Peng, "Efficient and provably secure anonymous user authentication scheme for patient monitoring using wireless medical sensor networks," *IEEE Access*, vol. 8, pp. 47282–47294, 2020.

[27] I. Santos-González, A. Rivero-García, M. Burmester, J. Munilla, and P. Caballero-Gil, "Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks," *Inf. Syst.*, vol. 88, Feb. 2020, Art. no. 101423.

[28] M. F. Moghadam, M. Nikooghadam, M. A. B. A. Jabban, M. Alishahi, L. Mortazavi, and A. Mohajerzadeh, "An efficient authentication and key agreement scheme based on ECDH for wireless sensor network," *IEEE Access*, vol. 8, pp. 73182–73192, 2020.

[29] M. Alotaibi, "An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN," *IEEE Access*, vol. 6, pp. 70072–70087, 2018.

[30] D. Rangwani, D. Sadhukhan, S. Ray, M. K. Khan, and M. Dasgupta, "A robust provable-secure privacy-preserving authentication protocol for industrial Internet of Things," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 3, pp. 1548–1571, May 2021.

[31] R. Vinoth and L. J. Deborah, "An efficient key agreement and authentication protocol for secure communication in industrial IoT applications," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 3, pp. 1431–1443, Mar. 2023.

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

[33] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 2002, pp. 337–351.

[34] V. Kumar, R. Kumar, A. A. Khan, V. Kumar, Y.-C. Chen, and C.-C. Chang, "RAFI: Robust authentication framework for IoT-based RFID infrastructure," *Sensors*, vol. 22, no. 9, p. 3110, Apr. 2022.

[35] V. Kumar, A. A. Khan, and M. Ahmad, "Design flaws and cryptanalysis of elliptic curve cryptography-based lightweight authentication scheme for smart grid communication," in *Advances in Data Sciences, Security and Applications*. Springer, 2020, pp. 169–179, doi: 10.1007/978-981-15-0372-6_13.

[36] A. A. Khan, V. Kumar, M. Ahmad, and S. Jangirala, "A secure and energy efficient key agreement framework for vehicle-grid system," *J. Inf. Secur. Appl.*, vol. 68, Aug. 2022, Art. no. 103231.

[37] N. Li, F. Guo, Y. Mu, W. Susilo, and S. Nepal, "Fuzzy extractors for biometric identification," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 667–677.

[38] S. A. Chaudhry, H. Naqvi, M. S. Farash, T. Shon, and M. Sher, "An improved and robust biometrics-based three factor authentication scheme for multiserver environments," *J. Supercomput.*, vol. 74, no. 8, pp. 3504–3520, Aug. 2018.

[39] S. A. Chaudhry, "Comments on 'A secure, privacy-preserving, and lightweight authentication scheme for VANET,'" *IEEE Sensors J.*, vol. 22, no. 13, pp. 13763–13766, Jul. 2022, doi: 10.1109/JSEN.2022.3168512.

[40] S. A. Chaudhry, K. Yahya, S. Garg, G. Kaddoum, M. M. Hassan, and Y. B. Zikria, "LAS-SG: An elliptic curve-based lightweight authentication scheme for smart grid environments," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1504–1511, Feb. 2023, doi: 10.1109/TII.2022.3158663.

[41] M. Abdalla, O. Chevassut, P.-A. Fouque, and D. Pointcheval, "A simple threshold authenticated key exchange from short secrets," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Cham, Switzerland: Springer, 2005, pp. 566–584.

[42] C. J. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols," in *Proc. Int. Conf. Comput. Aided Verification*. Cham, Switzerland: Springer, 2008, pp. 414–418.

[43] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, p. 2946, Dec. 2017.

[44] S. Itoo, M. Ahmad, V. Kumar, and A. Alkhayyat, "RKMIS: Robust key management protocol for industrial sensor network system," *J. Supercomput.*, vol. 79, no. 9, pp. 9837–9865, Jun. 2023.

SAMIULLA ITOO received the B.Sc., M.Sc., and M.Phil. (Hons.) degrees in mathematics and the Ph.D. degree in applied mathematics, with a focus on the design and analysis of authentication protocols using cryptographic techniques. He is currently a highly accomplished mathematician with extensive expertise in cryptography. He has published numerous articles in well-respected journals, including SCI, Scopus, and Web of Science. His research interests include centered around cryptography, with a particular focus on the development of innovative and effective encryption protocols. His work has been recognized for its exceptional quality and significance in the field of mathematics. He has been invited to present his research at various conferences and his insights have been incorporated into the design and development of cutting-edge cryptographic techniques. He is an outstanding researcher and a mathematician, who is dedicated to advancing the field of cryptography and improving the security of data systems.

AKBER ALI KHAN received the M.Sc. (Tech.) degree in industrial mathematics with computer application from the Department of Mathematics, Jamia Millia Islamia, New Delhi, India, and the Ph.D. degree in mathematics from Jamia Millia Islamia, in 2021. Currently, he is an Assistant Professor with the Department of Applied Sciences and Humanities, IIMT College of Engineering, Greater Noida, Uttar Pradesh, India. He has qualified Faculty Aptitude Test (FATE-2016) in mathematical science with grade A, conducted by AKTU, Uttar Pradesh, India. He has authored or coauthored dozens of research papers in reputed international journals and conferences, such as Elsevier/Springer/Taylor and Francis. Also, he has coauthored books *Applied Mathematics-I* and *Applied Mathematics-II* (Diploma Engineering Courses). He served as a Reviewer for reputed journals, such as the *Journal of Systems Architecture*, IEEE Access, *Journal of Electrical Power & Energy Systems*, *Cybernetics and Systems*, *Transactions on Emerging Telecommunications Technologies*, *Peer-to-Peer Networking and Applications*, *Scientific Reports*, and *Telecommunication Systems*. His research interests include cryptography, authentication protocols for secure communications, smart grid security and privacy, V2G security and privacy, blockchain, elliptic curve cryptography, optimization, and applied mathematics. He is a Lifetime Member of the MathTech Thinking Foundation (MTTF) in India.

MUSHEER AHMAD received the Ph.D. degree from the Department of Mathematics, Aligarh Muslim University, Aligarh, India. Currently, he is a Professor with the Department of Applied Sciences and Humanities, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi, India. He has authored or coauthored more than 50 research papers in reputed international journals and conferences. His research interests include group theory and its applications, graph theory, information security, support vector machine, fuzzy algebra and its applications, and soft computing. He is a reviewer of many reputed journals.

M. JAVED IDRISI received the M.Sc. degree in mathematics from Jamia Millia Islamia (A Central University of India), New Delhi, India, in 2008, and the Ph.D. degree in mathematics from Maharshi Dayanand University, Rohtak, India, in 2015. He is currently an Associate Professor with the Department of Mathematics, College of Natural and Computational Science, Mizan-Tepi University, Tepi Campus, Ethiopia. He has more than seven years of post-Ph.D. teaching experience at the university level. Till date, he has authored a total of 36 research papers, out of which 16 research papers are published in SCI-listed journals (Springer and Elsevier) and the rest are in Scopus and peer-reviewed journals. He has also authored two books *Applied Mathematics I* and *Applied Mathematics II* (Diploma Engineering Courses). His research interests include mathematical modeling, differential equations, astronomy, astrophysics, cryptography, satellite security and privacy, and network security and privacy. He is a reviewer in several SCI and Scopus-indexed journals and a Lifetime Member of the International Association of Engineers (IAENG), Hong Kong, China, the Centre for Fundamental Research in Space Dynamics and Celestial Mechanics, New Delhi, India, and the MathTech Thinking Foundation, Punjab, India.