Journal of Ambient Intelligence and Humanized Computing (2023) 14:16081–16098
https://doi.org/10.1007/s12652-022-03834-9

ORIGINAL RESEARCH

Two factor authentication protocol for IoT based healthcare monitoring system

Abhay Kumar Agrahari[1] · **Shirshu Varma**[1] · **S. Venkatesan**[1]

Received: 1 March 2021 / Accepted: 28 March 2022 / Published online: 18 April 2022

Abstract
In the last few years, technological advancement has led to the use of wearable body sensors for gathering patient information. Wireless body area networks played an essential role in the modern medical era. Through wearable body sensors, patient data are sent to medical professionals in real-time without any hindrance. This information moves through the public channel, and thus proper security and protection are needed because of its sensitiveness. Many authentication protocols proposed for solving these issues were neither secure nor cost-effective. This paper proposed an authentication protocol using certificateless cryptography for wireless body area networks to resolve the associated security concerns. A formal security analysis is done using the Burrows–Abadi–Needham logic shows that the proposed protocol is resilient against prevailing attacks. Additionally, we employ the Real-or-Random model for mathematical proof and Automated Verification Security Protocol and Analysis simulation tool for security analysis. A detailed comprehensive comparison with the existing protocols indicates that the proposed protocol is cost-effective with improved functionality.

Keywords Certificateless cryptography · Security and privacy · Wearable body sensors · Mutual Authentication

1 Introduction

With the progression in the Internet of Things (IoT), many remote innovation have been implemented for instance in smart homes, innovative medical services, smart grid technology, for a more brilliant life. They utilized this innovation to beat the issues of this present reality climate. In this innovation region, the wearable medical services observing framework is a piece of the shrewd medical services framework. Wireless body area network (WBAN) is also part of the intelligent health care system where the sensors can be use for the network to obtain the patient information to screen their health. These sensors are portable and small in size and an intercommunicating device can be used as a wearable or is implanted in the patient body to observe the vitals symptoms of the patient. These wearable sensors observed various physiological data, including electromyography, electrocardiogram, oxygen saturation (SPO2) level, blood pressure, blood glucose, temperature, heartbeat level, etc. (Koya and Deepthi 2018). The advancement in the technology has solved the issue of sending real-time medical data to the concerned authority. These wearable sensors will be beneficial for more older people and sick individuals who cannot get to the clinic routinely for medication (Omala et al. 2018; Suriyakrishnaan and Sridharan 2018).

In WBAN, patients' information are collected via multiple wearable sensors and is forwarded to a regulator, such as a Personal Digital Assistant (PDA). The PDA then sends received information to the medical server using a public channel. Finally, this collective information is delivered to a specialist who prescribes the medication accordingly. Since health data is classified; therefore only authorized users should be able to access this information. Thus, trustworthiness and security is the fundamental aspect of this proposed system.

As indicated by the hypothesis of Gartner (https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends), more than 14 billion IoT gadgets have been utilized till 2020, which is a lot higher than the earlier years. Gartner

✉ Abhay Kumar Agrahari
abhayagrahari92@gmail.com

Shirshu Varma
shirshu@iiita.ac.in

[1] Indian Institute of Information Technology, Allahabad, Uttar Pradesh 211012, India

conjectures that 25 billion associated gadgets will be put to use in 2021, delivering massive volumes of non-structured or semi-organized information (Assunção et al. 2015).

In this paper, will discuss about specific uses of wearable sensors. In our day-to-day tasks, wearable gadgets are used to monitor carbohydrate levels, step count, etc. We make use of smart wearable sensors for constantly observing the patients' information to identify the patient's crisis in medical care. Table 1 defines the important abbreviations used in this paper.

1.1 Motivation

As observed in the COVID-19 crisis, with a multitude of positive patients, the lack of hospitals and limited medical infrastructure restricted patients from availing needed treatment. Non-critical patients were provided healthcare supervision from their homes. Thus, remotely accessing patient data must become an essential part of healthcare monitoring systems. Remote sensly data collected using wearable sensors are sensitive thus require a secure communication channel. Hence, we propose an authentication protocol that utilizes Certificateless encryption and satisfies all necessary security boundaries.

1.2 Research contribution

The fundamental commitment of this work is as follows:-

- A new two-factor authentication scheme is designed for Wireless Body Area Network (WBAN), where the doctor will remotely access the patient data.
- Self-authentication of the user (doctor) is done using the user's smart card that stores the essential credentials. It means that in the login phase, the server will authenticate the user from their smart card and credentials.
- The proposed scheme will mainly focus to secure against prevailing attack and key escrow problem.
- A secure Mutual Authenticate and Key Agreement (MAKA) scheme is established between the PDA and the hospital server.
- The proposed authentication scheme is semantic secure, and proved by the ROR model. We also show that our proposed authentication protocol is secure against different notable attacks in the informal security analysis.
- To support our claims, a formal security analysis is conducted using the BAN logic and a formal verification using the AVISPA simulation tool.
- Finally, we present a detailed comparative analysis between the proposed scheme and the existing schemes. This analysis shows that our proposed scheme is more effective and efficient compared to the other schemes, and is also secure against the prevailing attacks.

1.3 Road map of the paper

The paper's road map is as follows: We have review the current research work in the Sect. 2. Section 3 defines the system framework and threat model. Section 4 discusses the mathematical preliminaries and some complex concept used in the proposed protocol. The proposed scheme is introduced in Sect. 5, divided into the four phases, i.e., the setup phase,

Table 1 Used abbreviations and their meaning

Abbreviation	Description
WBAN	Wireless body area network
IOT	Internet of Things
PDA	Personal digital assistant
TA	Trusted authority
MAKA	Mutual authentication and key agreement protocols
BAN logic	Burrows–Abadi–Needham logic
AVISPA	Automated verification security protocol and analysis simulation
ROR	Real-or-Random (ROR)
SPO2	oxygen saturation
$\boldsymbol{A}$	Adversary
k-mBIDH	Modified Bilinear inverse Diffie–Hellman with k values
CDH problem	Computational Deffie–Hellman problem
DY adversary model	Dolev–Yao adversary model
CK adversary model	Canetti and Krawczyk's adversary model
$Adv_A^{\mathcal{P}}(t)$	the advantage of $\boldsymbol{A}$ to break the semantic security of our proposed protocol $\mathcal{P}$ in the polynomial time t
$\Pr[Succ_i]$	$Succ_i$ denotes the probability of $\boldsymbol{A}$ winning the game G_i

registration phase, login phase, and authentication and key agreement phase. Section 6 give a detailed formal, informal, and mathematical security analysis of the proposed scheme. In Sect. 7, we have compared our proposed protocol based on computational cost and security requirements, and conclude our work in Sect. 8.

2 Related work

Currently, there are numerous mutual authentication and key agreement protocols (MAKA). In 2009, Yang and Chang (2009) published the Id-based scheme utilizing the elliptic curve cryptography. However, Yoon and Yoo (2009) showed that Yang's scheme didn't exhibit the perfect forward secrecy. Like Yang, Cao et al. (2010) published the authentication protocol based on identity-based encryption, however, it couldn't represent user obscurity and unlinkability. In 2012, Debiao et al. (2012) proposed a validation protocol utilizing the elliptic curve idea. However, Wang and Ma (2013) demonstrated that (Debiao et al. 2012) did not give the mutual authentication and wasn't sure against the reflection attack.

Wang and Zhang (2015) proposed the new anonymous authentication protocol with bilinear pairing, which has the key escrow problem. Zhao (2014) also proposed an authentication protocol for WBAN, but it was not cost effective. Wu et al. (2016) highlighted that Wang and Zhang (2015) couldn't withstand to impersonation attack. The two schemes based on wireless body area network proposed by Liu et al. (2013), and Xiong and Qin (2015) could not resist impersonation attack. Likewise, in 2015 Tsai and Lo (2015) proposed the identity-based authentication protocol. In this protocol, mobile users and service providers register for the third party, who produce the long-term secret key for every client and service provider and furthermore guarantees that this protocol is secure against some notable attacks. But Jiang et al. (2016) illustrated that Tsai and Lo (2015) was not secure against the impersonation attack and also failed accomplish the mutual authentication. Nonetheless, potential solutions for the aforementioned issues were introduced in Irshad et al. (2016); Amin et al. (2016); He et al. (2016). Karati et al. (2018a) have tended to the key escrow issue in their certificate-less signature scheme, which is secure against the active attacker. Similarly, Karati et al. (2018b) also address the key escrow issue in their industrial IoT authentication protocol. Nonetheless, both schemes do not accomplish full authentication, i.e., client's public key is not verified by the focal authority.

Recently, Jia et al. (2019) proposed an identity-based authentication and key arrangement protocol that fulfills client secrecy but not safe from the key escrow problem. In 2020 Sowjanya et al. (2020) established that Li et al. (2017) authentication protocol is not good for end-to-end communication for the medical services framework. In the same year, Zhang et al. (2020) proposed the authentication protocol utilizing the bilinear pairing, however, they couldn't safeguard their protocol from the key escrow issue. We have also reviewed some more papers which is related to our work (Abualigah et al. 2021a, b; Abualigah and Diabat 2021; Abualigah 2019; Singh and Chaurasiya 2021).

A detailed analysis of related work is done in Table 2.

3 System framework and threat model

3.1 System framework

The system framework has four entities, namely, Trusted Authority (TA), user, server, and PDA. The user initially sends the registration request to the TA. At that point, the TA issues the smart card for the user. The server and the PDA also send the registration requests to the TA. TA creates the long-term secrets and fractional secret keys and send to the server and PDA qfter getting the keys, the server and the PDA produce their secret keys. After the registration phase, the login phase is enabled, and in this phase, the server checks the user's authenticity. In the last phase, the server and the PDA mutually authenticate each other and create a session key for future communication. The system framework is depicted in Fig.1.

3.2 Threat model

For authentication, there are two widely accepted adversary models, i.e., the Dolev-Yao adversary model (Dolev and Yao 1983) and the CK-adversary model (Canetti and Krawczyk 2001). These models are applicable when two parties communicate with each other through the public (insecure) channel. According to the DY model, an adversary $\boldsymbol{A}$ can intercept the messages which are sent between the parties and also reposition, control, manipulate, eavesdrop, or delete the messages. In the proposed framework, in addition to the DY model, we will also use the CK-adversary model, which is currently de facto for authentication and key exchange protocol. In the CK-adversary model, the adversary $\boldsymbol{A}$ not only controls, manipulates, eavesdrops, or deletes the message but also compromises the secret key and the session key. The adversary $\boldsymbol{A}$ captures the wearable body sensors physically and can get the stored credentials of those devices. This information is used for unauthorized activities like session key computation, impersonation attack, node capture attack, and privileged-insider attack. However, the TA is treated as a trusted authority in our proposed protocol and it is not physically captured by adversary $\boldsymbol{A}$.

Table 2 Issues in previous authentication schemes

Schemes	Methodology	Drawbacks	Formal analysis	Mathematical analysis	Simulation analysis
Yang and Chang (2009)	Elliptic curve cryptography	Not achieve perfect forward secrecy	No	No	No
Yoon and Yoo (2009)	Elliptic curve cryptography	Existence of Key escrow problem	No	No	No
Cao et al. (2010)	Identity based cryptography	Existence of Key escrow problem and could not achieve user anonymity	No	No	Yes
Debiao et al. (2012)	Elliptic curve cryptography	Parallel key session attack and Reflection attack	No	Yes	No
Wang and Zhang (2015)	Identity based cryptography	Existence of Key escrow problem and Impersonation attack	No	No	No
Wu et al. (2016)	Identity based cryptography	Existence of Key escrow problem	No	Yes	No
Tsai and Lo (2015)	Identity based cryptography	Existence of Key escrow problem and impersonation attack	No	Yes	Yes
Karati et al. (2018a)	Certificate-less signature scheme	Do not accomplish full authentication and not secure against Type-I adversary and	No	No	Yes
Karati et al. (2018b)	Certificate-less signature scheme	Do not accomplish full authentication and existentially forgeable against the key replacement attack	No	No	No
Jia et al. (2019)	Identity based cryptography	Existence of Key escrow problem	No	Yes	Yes
Li et al. (2017)	Elliptic curve cryptography	No key control and also perfect forward secrecy not exist	Yes	No	No
Zhang et al. (2020)	Identity based cryptography	Existence of Key escrow problem	No	Yes	Yes

4 Mathematical preliminaries

This section will discuss the fundamental concepts and some predefined hard problems that were used in our proposed protocol to ensure wearable sensors' security.

4.1 Ony way cryptographic hash function

A one-way cryptographic hash function takes an input string X$\in\{0,1\}^*$ of an arbitrary length and outputs a fixed length string Y$\in\{0,1\}^n$ called the hash value. The main property of the hash function is as follows:

- *Collision resistance* It is hard to find the pair of two inputs like $(X, X') \in \{0,1\}^*$, where $X \neq X'$, but $H(X) = H(X')$.
- *Pre-image resistance* From the given hash value Y , it is hard to find the value of $X \in \{0,1\}^*$, Where $Y = H(X) \in \{0,1\}^n$.

4.2 Bilinear pairing

Let G_1 and G_2 are two cyclic groups. Where, G_1 is the additive group and G_2 is the multiplicative group. The order of both the group is q. The bilinear pairing function can be defined as $e : G_1 \times G_1 \rightarrow G_2$ and P is the generator point of G_1 and g is the generator point of G_2.

The condition of bilinear pairing function exist when the pairing is able to meet the following conditions:

1. *Bilinear* Given two points $P, Q \in G_1$ and two numbers $a, b \in Z_q^*$, The bilinear property states that equation $e(a.P, b.Q) = e(P, Q)^{a.b}$ holds.
2. *Non-degeneracy* Given two points $P, Q \in G_1$ and let 1 is the identity element of G_2. Then non-degeneracy property states that $e(P, Q) \neq 1$.
3. *Computability* It is efficient to find the value of $e(P, Q)$, for all points of G_1.

4.3 Complexity assumption

This subsection discusses some hard problems which are difficult to solve in polynomial time. These hard problems have been used in our proposed scheme:

- *Computational Deffie–Hellman (CDH) problem* He et al. (2016) Given two points $g^a, g^b \in G_2$, it is hard to compute the value of $g^{a.b} \in G_2$, where the value of $a, b \in Z_q^*$ is unknown.
- *Modified Bilinear inverse Diffie-Hellman with k values (k-mBIDH) problem* Given the values of $\{Q, a.Q, b.Q\} \in G_1$, $\{\alpha_1, \alpha_2, \cdots \alpha_k\} \in Z_q^*$ and $\frac{1}{s+\alpha_1}.Q, \frac{1}{s+\alpha_2}.Q$

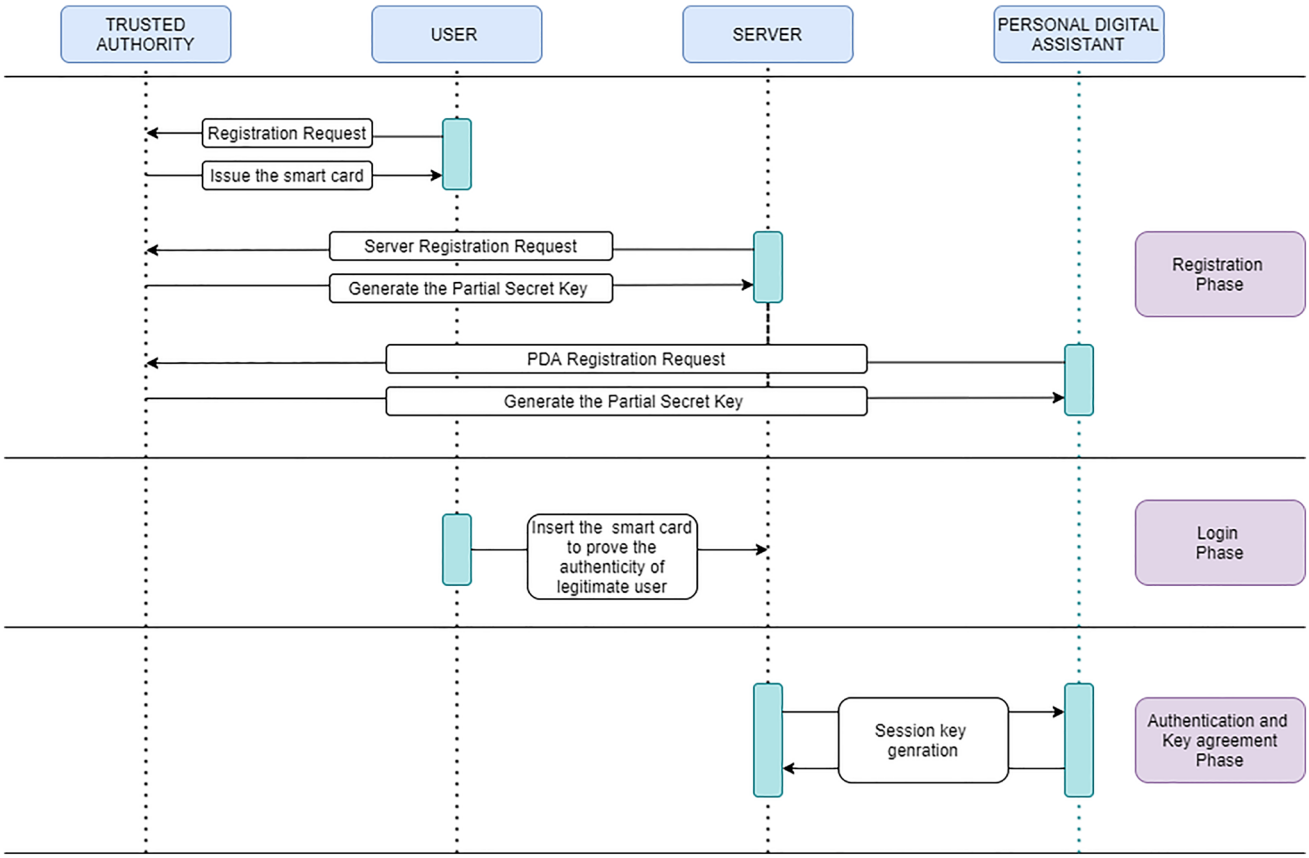

Fig. 1 System framework

$\ldots\frac{1}{s+\alpha_k}.Q$. It is hard to compute the value of $e(Q,Q)^{\frac{1}{s+\alpha}.t}$ where the value of α is unknown.

- *Elliptic curve discrete logarithm problem* Agrahari and Varma (2020) Given the two points $P, Q \in G_1$, it is computationally hard to find the value of $\{a\}$ from $Q = a.P$ in polynomial time. Where $a \in Z_q^*$.

5 Proposed scheme

In this section, we elaborate our proposed certificateless cryptography scheme for mutual authentication and key establishment.

Our scheme is divided into 4 phases, i.e., "setup phase", "registration phase", "login phase", and "authentication and key establishment phase". The notations used in our proposed protocol are mentioned in Table 3. The description of all the phases is as follows:

Table 3 Notation used in our proposed protocol

Notations	Detail description
λ	Security parameter
TA	Trust authority
G_1	Cyclic additive group
G_2	Cyclic multiplicative group
q	order of the Cyclic groups $G_1$and G_2
P	Generator point of the group G_1
g	Generator point of the group G_2
e	Bilinear map function i.e. $e : G_1 \times G_1 \rightarrow G_2$
$H_i(.)$	Hash function where i= 1,2,3$\cdots$
s	TA secret key
P_{pu}	TA public key
Id_u	Identity of the user
Id_s	Identity of the server
Id_p	Identity of the PDA (personal digital assistant)
HID	Mask identity of the user
HPW, H_1PW	Mask password of the user
S_s	Secret key of the server
S_{pd}	Secret key of the PDA

5.1 Setup phase

In the setup phase, the TA generates the system parameter as well as their private and public keys. The TA also selects the cyclic groups used in the proposed protocol.

- At first, the TA chooses the security parameter λ and then generates the system parameters.
- TA appoints two cyclic groups of order q where G_1 is the additive group and G_2 is the multiplicative group. The tate pairing map is used where mapping is $e : G_1 \times G_1 \rightarrow G_2$, P is the generator point of G_1 whereas g is the generator point of G_2, and $g = e(P, P)$.
- TA picks $s \in Z_q^*$ which is the TA's private key, following which, the TA calculates its public key, $P_{pu} = s.P$
- TA selects the secure hash function. TA then stores the private key and publishes the system parameter, i.e., $\{G_1, G_2, P, P_{pu}, e, H_i(.)\}$

5.2 Registration phase

The user, server and PDA register in this phase. The process is as follows:

5.2.1 User registration

To access patient data from the server, the users needs to register themselves securely. The whole process is summarized in Table 4.

- Firstly, the user generates $ID_u, PW \in Z_q^*$, and after that, it creates two long term secrets $r, \alpha \in Z_q^*$. After producing ID_u and PW, the user calculates the value of mask identity, i.e., $HID = H_1(ID_u||r)$, mask password, i.e., $HPW = H_1(PW||r)$, $H_1PW = HPW \oplus \alpha$, and sends this information to the TA.
- After getting the user's value, the TA generates the random number $t \in Z_q^*$, calculates $T = t.P$, uses this value to generate $R = H_2(T||HID||H_1PW)$ and $C_i = T \oplus HID$, $B_i = H_3(H_1PW||R||C_i)$, and finally sends $\{C_i\}$ to the user. TA uses $\{C_i\}$ in the server registration process and also stores the value of B_i into the server's memory for user verification.
- After obtaining the value from TA, the user computes $W_i = H_1(ID_u||PW) \oplus r$, $V_i = C_i \oplus r$, and $Z_i = \alpha \oplus H_1(HID||HPW)$, and stores these values in the smart card for further verification.

Table 4 User registration phase

User	TA
Generate $ID_u, PW \in Z_q^*$	
$r, \alpha \in Z_q^*$	
$HID = H_1(ID_u\|\|r)$	
$HPW = H_1(PW\|\|r)$	
$H_1PW = HPW \oplus \alpha$	
$\xrightarrow{\{HID, H_1PW\}}$	
	Genaerate $t \in Z_q^*, T = t.P$
	$R = H_2(T\|\|HID\|\|H_1PW)$
	$C_i = T \oplus HID$
	$B_i = H_3(H_1PW\|\|R\|\|C_i)$
$\xleftarrow{\{C_i\}}$	
$W_i = H_1(ID_u\|\|PW) \oplus r$	
$V_i = C_i \oplus r$	
$Z_i = \alpha \oplus H_1(HID\|\|HPW)$	
Smart card save the value of $\{W_i, V_i, Z_i\}$	

- At the end, the user deletes the value of $\{C_i\}$ and the TA deletes the values of $\{R, B_i\}$ from their respective memories to evade the privileged insider attack.

5.2.2 Server registration

The server registration is as follows:

- The server generates the identity ID_s, random number $r_s \in Z_q^*$, calculates the value of $R_s = r_s.P$, and then relays the ID_s value to the TA.
- After getting the value, the TA generates a new random number, $r_t \in Z_q^*$ and calculates $R_t = r_t.P$. After that, the TA computes two values, $A_s = s.H(ID_s)$ and $L = s.r_t$. TA then transfers the calculated values (L, A_s, r_t, C_i) to the server.
- The Server generates a new random value $x \in Z_q^*$, $X = x.P$ and determines the secret key $S_s = x + A_s$ upon getting the values from TA. The server then computes the value of $S_{sp} = S_s.P$, $L_1 = (r_s + L).P$ and $M = (r_s||R_s||r_t||x||X) \oplus C_i$ and saves the value of $\{M, S_s, S_{sp}, L_1\}$ in the database.
- Lastly, the TA and the server erase the value of $\{C_i\}$ from their memories to abstain from the privileged insider attack. The whole process is summarized in Table 5.

5.2.3 PDA registration

The PDA registration phase is as follows :

Table 5 Server registration phase

Server	TA
Generate $ID_s \in Z_q^*$	
$r_s \in Z_q^*, R_s = r_s.P$	
$\xrightarrow{\{ID_s\}}$	
	Genaerate $r_t \in Z_q^*$
	$R_t = r_t.P$
	$A_s = s.H(ID_s)$
	$L = s.r_t$
$\xleftarrow{\{L,A_s,r_t,,C_i\}}$	
$x \in Z_q^*, X = x.P$	
$S_s = x + A_s$	
$S_{sp} = S_s.P$	
$L_1 = (r_s + L).P$	
$M = (r_s\|\|R_s\|\|r_t\|\|x\|\|X) \oplus C_i$	
Server will save the value of $\{M, S_s, S_{sp}, L_1\}$	

- The PDA generates the identity, $ID_p \in Z_q^*$ and the random number, $r_\phi \in Z_q^*$,. It then computes the value of $R_\phi = r_\phi.P$ and delivers (ID_p,R_ϕ) to the TA.
- After getting the values, the TA calculates $A_t = \frac{1}{H(ID_p)+s}.P$ and $\phi_2 = \{H_1(ID_p||R_\phi) + r_t.s\}$, and forwards these values to the PDA.
- Upon receiving values A_t and ϕ_2, the PDA calculates a random number, $y \in Z_q^*$ and calculate his secret key $S_{pd} = (\phi_2 + y)$ and also compute $S_{pdp} = S_{pd}.P$
- At the end, the PDA stores the values of { S_{pd}, S_{pdp}, A_t, Y} and R_ϕ in server's memory.

The entire process are summarized in Table 6.

Table 6 PDA registration phase

PDA	TA
Generate $ID_p \in Z_q^*$	
$r_\phi \in Z_q^*, R_\phi = r_\phi.P$	
$\xrightarrow{\{ID_p,R_\phi\}}$	
	$A_t = \frac{1}{H(ID_p)+s}.P$
	$\phi_2 = \{H_1(ID_p\|\|R_\phi) + r_t.s\}$
$\xleftarrow{\{\phi_2,A_t\}}$	
$y \in Z_q^*, Y = y.p$	
$S_{pd} = (\phi_2 + y)$	
$S_{pdp} = S_{pd}.P$ PDA will save the value of $\{S_{pd}, A_t, Y, S_{pdp}\}$	

5.3 Login phase

In login phase, the server authenticates the user. The process is as follows:

- Firstly, the user inserts his smart card in server machine and then enter the values $< ID_u, PW >$.
- On receiving $< ID_u, PW >$ and the stored smart card value, W_i, the server begets the value of long term secret r' using $W_i \oplus H_1(ID_u||PW) = r'$. The value of r' is used to get the masked value of identity and password, i.e., $HID' = H_1(ID_u||r')$ and $HPW' = H_1(PW||r')$.

  Using the stored smart card value V_i and the value of r', the server estimates C_i'. The server then computes another long-term secret $\alpha' = Z_i \oplus H_1(HID'||HPW')$. Using α', the server calculates the second masked password, $H_1PW' = HPW' \oplus \alpha'$. To get the value of T, the server uses the value of C_i' and H_1PW' and computes the value of $R' = H_2(T||HID'||H_1PW')$.
- At last, the server verifies the value of B_i. If the value equals the value of $H_3(H_1PW'||R'||C_i')$, then the user is authorized access, else the server aborts the login.

The whole process is summarized in the Table 7.

5.4 Authentication and key establishment phase

In this phase, the server and the PDA mutually authenticate each other and generate the session key for future communication. The steps are as follows:

- The server generates a new random number, $z \in Z_q^*$, and calculates the value of $Z = z.P$. After that, the server computes $C_i' \oplus M = (r_s||R_s||r_t||x||X)$,

Table 7 Login phase

User	Server
Insert Smart card and enter the credentials	
$< ID_u, PW >$	
$\xrightarrow{\{ID_u PW\}}$	
	$W_i \oplus H_1(ID_u\|\|PW) = r'$
	$HID' = H_1(ID_u\|\|r')$
	$HPW' = H_1(PW\|\|r')$
	$V_i \oplus r' = C_i'$
	$Z_i \oplus H_1(HID'\|\|HPW') = \alpha'$
	$H_1PW' = HPW' \oplus \alpha'$
	$C_i' \oplus H_1PW' = T$
	$R' = H_2(T\|\|HID'\|\|H_1PW')$
	$B_i? = H_3(H_1PW'\|\|R'\|\|C_i')$

$T_t = x.z$, $\mathfrak{F} = g^{T_t}$, $\wedge_1 = T_t(H(ID_p).P + P_{pu})$, $\wedge_2 = \mathfrak{F} \oplus (R_s||r_t||X||Z||B_i||T_1)$, and a verifier, $\wedge_3 = r_s + H_1(ID_p||R_\phi)$. The server finally sends $\{\wedge_1,\wedge_2,\wedge_3,T_1\}$ to the PDA.

- After receiving these values, the PDA first checks the validity of the message using $|T_2 - T_1| \leq \Delta T$. This showcases that the message is not repeated. Here, ΔT represents the maximum transmission delay.
- The PDA computes $\mathfrak{F}' = e(A_t, \wedge_1)$ and $\mathfrak{F}' \oplus \wedge_2 = (R_s||r_t|||X||Z||B_i||T_1)$. Next, it determines two values, $\rho_1 = \wedge_3.P + P_{pu}.r_t + Y$ and $\rho_2 = S_{pdp} + R_s$, and verifies if ρ_1 is equal to ρ_2. If true, it indicates the server's authenticity and message integrity, else the PDA aborts the session.
- PDA chooses a new random number $f \in Z_q^*$ and computes $F = f.P$, $\rho_3 = Z.f||(R_s + P_{pu}.r_t)$ and $\rho_4 = H(ID_s).P_{pu} + X$. After calculating these values the PDA estimates the value of $\rho_5 = (\rho_3 \oplus \rho_4)$ and $\rho_6 = (\rho_2 \oplus \rho_4)$. At last, the PDA reckons the shared session key, $S.K. = (ID_s||ID_p||\rho_2||\rho_3||\rho_4||B_i||T_3)\mathbf{mod}q$. After that the PDA transfers $\{\rho_5,\rho_6,F,T_3\}$ to the server.
- Subsequently, the server checks $|T_4 - T_3| \leq \Delta T$ and computes $\wedge_4 = (z.F||L_1)$, $\wedge_5 = S_{sp}$, and then examines the PDA's message integrity and authenticity using $\rho_5? = (z.F||L_1 \oplus S_{sp})$. It also verifies that the message is coming from the authorized PDA.
- At the end of the session, the server calculates $\rho_2' = \rho_6 \oplus \wedge_5$ and the value of the shared session key $S.K. = (ID_s||ID_p||\rho_2'|| \wedge_4 || \wedge_5 ||B_i||T_3)\mathbf{mod}q$ for future communication.

The overall process is summarized in Table 8.

- *Proof of correctness*

Table 8 Authentication and key establishment phase

Server	PDA
$z \in Z_q^*, Z = z.P$	
$C_i' \oplus M = (r_s||R_s||r_t||x||X)$	
$T_t = x.z$	
$\mathfrak{F} = g^{T_t}$	
$\wedge_1 = T_t(H(ID_p).P + P_{pu})$	
$\wedge_2 = \mathfrak{F} \oplus (R_s||r_t||X||Z||B_i||T_1)$	
$\wedge_3 = r_s + H_1(ID_p||R_\phi)$	
$\xrightarrow{\{\wedge_1,\wedge_2,\wedge_3,T_1\}}$	
	$Check|T_2 - T_1| \leq \Delta T$
	$\mathfrak{F}' = e(A_t, \wedge_1)$
	$\mathfrak{F}' \oplus \wedge_2 = (R_s||r_t|||X||Z||B_i||T_1)$
	$\rho_1 = \wedge_3.P + P_{pu}.r_t + Y$
	$\rho_2 = S_{pdp} + R_s$
	Verify $\rho_1? = \rho_2$
	$f \in Z_q^*, F = f.P$
	$\rho_3 = Z.f||(R_s + P_{pu}.r_t)$
	$\rho_4 = H(ID_s).P_{pu} + X$
	$\rho_5 = (\rho_3 \oplus \rho_4)$
	$\rho_6 = (\rho_2 \oplus \rho_4)$
	$S.K. = (ID_s||ID_p||\rho_2||\rho_3||\rho_4||B_i||T_3)\mathbf{mod}q$
$\xleftarrow{\{\rho_5,\rho_6,F,T_3\}}$	
$Check|T_4 - T_3| \leq \Delta T$	
$\wedge_4 = (z.F||L_1)$	
$\wedge_5 = S_{sp}$	
Check $\rho_5? = ((z.F||L_1) \oplus S_{sp})$	
$\rho_2' = \rho_6 \oplus \wedge_5$	
$S.K. = (ID_s||ID_p||\rho_2'|| \wedge_4 || \wedge_5 ||B_i||T_3)\mathbf{mod}q$	

$$
\begin{aligned}
e(A_t, \wedge_1) &= e(\frac{1}{H(ID_p)+s}.P, x.z(H(ID_p).P + P_{pu})) \\
&= e(\frac{1}{H(ID_p)+s}.P, x.z(H(ID_p).P + s.P)) \\
&= e(\frac{1}{H(ID_p)+s}.P, x.z.P(H(ID_p) + s)) \\
&= e(P,P)^{\frac{1}{H(ID_p)+s}.x.z.(H(ID_p)+s)} \\
&= e(P,P)^{x.z} \\
&= g^{x.z}
\end{aligned}
$$

6 Security analysis

In this section, we address the security of our proposed protocol. The section is divided into four subsections. The first subsection, covers the informal security analysis, while the second subsection addresses the formal security analysis using the BAN logic. The third section, analyzes the security using a mathematical model, and the last section, discusses the AVISPA simulation tool for security verification.

6.1 Informal security analysis

- *Mutual authentication* The server and the PDA authenticate each other and generate the session key for future communication. In the proposed protocol, the PDA verifies the server on the value of $\{\wedge_3\}$ by using his secret key, and the server verifies the PDA for the value of $\{\rho_5\}$ using his secret key. The two-way verification process illustrates that the proposed protocol provides mutual authentication.
- *User anonymity* The identities of server, user and the PDA are hidden in the messages, $\{\wedge_1, \wedge_2, \wedge_3, T_1\}$, where the value of $\wedge_1 = T_t(H(ID_p).P + P_{pu})$, $\wedge_2 = \mathfrak{F} \oplus (R_s||r_t||X||Z||B_i||T_1)$ and $\wedge_3 = r_s + H_1(ID_p||R_\phi)$. To get the PDA identity, the adversary needs to compute the value $\mathfrak{F} = g^{T_t}$ from $\wedge_1 = T_t(H(ID_p).P + P_{pu})$. Whereas, $\{\wedge_2\}$ message is used to scratch the user identity. Nevertheless, the adversary will encounter the hard problem, k-mBIDH. Thus, our scheme is secure against the user anonymity problem.
- *Resistance to man-in-middle-attack* The proposed protocol establishes the session key, which is used by the server and the PDA to authenticate each other. To secure an authentication with the PDA, the adversary needs the legal messages, $\wedge_1 = T_t(H(ID_p).P + P_{pu})$, $\wedge_2 = \mathfrak{F} \oplus (R_s||r_t||X||Z||B_i||T_1)$ and $\wedge_3 = r_s + H_1(ID_p||R_\phi)$. However, the adversary cannot manufacture a legal message as it wasn't exposed to the long-term secrets, r_s, r_t. Also, the adversary won't be able to fetch the value of $\mathfrak{F} = g^{t_t}$ from $\wedge_1 = T_t(H(ID_p).P + P_{pu})$ because of k-mBIDH hard problem.

  When the adversary sends the legal message, $\{\rho_5, \rho_6, F, T_3\}$, due to unknown long-term secrets it is unable to generate the legal messages and fails to establish a connection. This shows that the adversary is unable to generate the legal messages and therefore cannot breach the mutual authentication process. Thus, our proposed protocol can resist man-in-middle-attacks.
- *Offline password guessing attack* The adversary compromises the secret information stored in the user's smart card, i.e.,$\{W_i, V_i, Z_i\}$, and launches the offline dictionary attack. To get the users' password, the adversary intercepts the saved details, but the value of $W_i = H_1(ID_u||PW) \oplus r$ and $Z_i = \alpha \oplus H_1(HID||HPW)$ are stored in the hashed form. Firstly, to get the password from value W_i, the adversary needs to know the value of long-term secret "r" and the one-way hash function. Moreover, to get the value of PW from Z_i, the adversary needs to know the values of "r, "α", and the one way hash function. This shows that the adversary cannot access the user's password and the proposed protocol is therefore secure against the offline password guessing attack.
- *Perfect forward secrecy* Assume that the server and the PDA's long-term secrets are disclosed to the adversary, and the adversary intercepted all the exchanged messages between the server and the PDA on a public channel. To obtain the value of the session key $S.K. = (ID_s||ID_p||\rho_2'|| \wedge_4 || \wedge_5 ||B_i||T_3)$, the adversary knows the random numbers and timestamps. The adversary is also capable of solving the CDH problem. Since, a new key is generated in each session and there is no connection between the session keys. So, even if the previous ones are compromised the current one is perfectly secure. This ensures perfect forward secrecy of the proposed protocol.
- *Privileged insider attack* An adversary may be internal or external. Let us assume that the privileged insider is a trusted authority. In proposed protocol, as there is no information stored related to the password, and the use of masked password and deletion of C_i from the TA during registration, ensures that any adversary from an insider cannot fetch information that harms our proposed protocol. Therefore, our proposed protocol is secure against the privileged insider attack.
- *Replay attack* In each exchanged message, we have used the timestamp values, and ensured in each session, we have checked the freshness of our timestamp values ensuring that our proposed protocol is secure against the replay attack.

- *Untraceability* In the proposed protocol, the random number $\{z, f\}$ is selected in every new session of the authentication and key establishment phase. Hence, the message exchanged between the server and the PDA through the public channel is different in each session. The adversary is unable to co-relate the messages between the two sessions. Therefore, our proposed protocol guarantees that it is untraceable.

6.2 Formal security analysis using BAN logic

In this section, we have included the detailed description of the formal security analysis of our proposed protocol using the concept of Burrows-Abadi-Needham(BAN) logic (Burrows et al. 1989). To analyze the proposed protocol using the BAN logic, we will first discuss about the three basic items used in BAN logic,i.e. Principals, Keys, and the statements.

Let's assume that $\{X, Y\}$ are the principals, $\{S, T\}$ are the statements and the "K" is the key. Then the basic logical notations used in the BAN logic is as follows:

- $X| \equiv S$: X believes in the Statement and S is the true statement.
- $X \lhd S$: X sees the statement S,i.e., S is coming from another principal and getting by principal X.
- $X| \sim S$: X once said the statement S.
- $X| \Rightarrow S$: X has jurisdiction over S.
- $\#(S)$: The mean of this notation is the statement S is fresh and never used in previous session.
- $[A \overset{K}{\leftrightarrow} B]$: The principals A and B used the shared key K for communication.
- $(S)_K$: A Statement S hashed with a key K.

After knowing about the notation of BAN logic, there are also some basic postulates for BAN logic which is used to proof the algorithm:-

* *Message meaning rule*

$$\frac{A| \equiv A \overset{K}{\leftrightarrow} B, A \lhd (S)_K}{A| \equiv B| \sim S}$$

* *Nonce-verification rule*

$$\frac{A| \equiv \#(S), A| \equiv B| \sim S}{A| \equiv B| \equiv S}$$

* *Jurisdiction rule*

$$\frac{A| \equiv B| \Rightarrow S, A| \equiv B| \equiv S}{A| \equiv S}$$

* *Freshness rule*

$$\frac{A| \equiv \#(S)}{A| \equiv \#(S, T)}$$

* *Belief Rule*

$$\frac{A| \equiv B| \equiv (S, T)}{A| \equiv B| \equiv (S)}$$

* *Elimination of multipart message*

$$\frac{A \lhd (S, T)}{A \lhd (S)}$$

To proof our proposed protocol using the BAN logic we have to follow the four essential steps,i.e.,

- Goals : The goals of our proposed protocol.
- Idealize message : We have to convert the transmitted message in the idealize form.
- Assumptions: We have to take the initial assumptions to proof the protocol goals.
- Proof: Using the assumption and idealize message we have to proof the protocol goals. In our proposed protocol we have to mutually authenticate the server and the PDA so our goal is to proof the security. Here we use notations,i.e.,

"Se" : The Server,
"P" : The PDA So our goals for the proposed protocol are:

1) $Se| \equiv P| \equiv (Se \overset{S_s}{\underset{S_{pd}}{\leftrightarrow}} P)$
2) $P| \equiv Se| \equiv (Se \overset{SK}{\leftrightarrow} P)$
3) $Se| \equiv P| \equiv (Se \overset{SK}{\leftrightarrow} P)$
4) $Se| \equiv P(Se \overset{s}{\leftrightarrow} P)$
5) $P| \equiv Se| \equiv (Se \overset{s}{\leftrightarrow} P)$
6) $Se| \equiv P| \equiv (Se \overset{s}{\leftrightarrow} P)$

The next step of BAN logic is to idealize the messages which were transmitted between the server and the PDA

Message 1:

$$P \lhd [(x, z, H(ID_p), Se \overset{s}{\leftrightarrow} P),$$
$$(R_s, r_t, X, Z, C_i, T, Se \overset{s}{\leftrightarrow} P)_{g^{xz}}, (R_\phi, Se \overset{S_{pd}}{\leftrightarrow} P)_{r_s}]$$

Message 2 :

$$Se \lhd [(Z, X, R_s, P_{pu}, Se \overset{s}{\leftrightarrow} P)_{H(ID_s)},$$
$$(S_{pd}, r_t, X, Se \overset{S_s}{\leftrightarrow} P, Se \overset{SK}{\leftrightarrow} P)_{H(ID_s)}]$$

In next step we have to make some assumption which will help to proof the BAN logic goals:

$A_1 : P| \equiv \#(X)$
$A_2 : P| \equiv \#(R_\phi)$
$A_3 : Se| \equiv \#(R_s)$
$A_4 : Se| \equiv \#(r_{g^{xz}})$
$A_5 : P| \equiv (Se \overset{r_s}{\leftrightarrow} P)$
$A_6 : P| \equiv (Se \overset{H(ID_s)}{\leftrightarrow} P)$
$A_7 : Se| \equiv (Se \overset{SK}{\leftrightarrow} P)$
$A_8 : Se| \equiv P| \Rightarrow (Se \overset{SK}{\leftrightarrow} P)$

The proof of the goals of the proposed protocol
Using Message 1:

- Using the elimination postulate and the message 1 we got the $B_1 : P \lhd ((R_s, r_t, X, Z, C_i, T, Se \overset{s}{\leftrightarrow} P)_{g^{xz}})$
- Using the Assumption A_5 and B_1 and the message meaning rule we got the $B_2 : P| \equiv Se \sim (R_s, r_t, X, Z, C_i, T, Se \overset{s}{\leftrightarrow} P)$
- Using the concept of freshness rule and the assumption A_1 we got the $B_3 : P| \equiv \#(R_s, r_t, X, Z, C_i, T, Se \overset{s}{\leftrightarrow} P)$
- Using the B_2, B_3 and nonce verification rule we got the $B_4 : P| \equiv Se| \equiv (R_s, r_t, X, Z, C_i, T, Se \overset{s}{\leftrightarrow} P)$
- Using the belief rule and the B_4 we got the $B_5 : P| \equiv Se| \equiv (Se \overset{s}{\leftrightarrow} P)$ **Goal 5** Again using Message 1 and the elimination rule we got $B_6 : P \lhd (R_\phi, Se \overset{S_{pd}}{\leftrightarrow} P)_{r_s}$
- Using the Assumption A_6 and B_6 and the message meaning rule we got the $B_7 : P| \equiv Se \sim (R_\phi, Se \overset{S_{pd}}{\leftrightarrow} P)$
- Using the concept of freshness rule and the assumption A_2 we got the $B_8 : P| \equiv \#(R_\phi, Se \overset{S_{pd}}{\leftrightarrow} P)$
- Using the B_7, B_8 and nonce verification rule we got the $B_9 : P| \equiv Se| \equiv (R_\phi, Se \overset{S_{pd}}{\leftrightarrow} P)$
- Using the belief rule and the B_9 we got the $B_{10} : P| \equiv Se| \equiv (Se \overset{S_{pd}}{\leftrightarrow} P)$ **Goal 2**
- Using the message 2 and the elimination rule we got the $B_{11} : Se \lhd (Z, X, R_s, P_{pu}, Se \overset{s}{\leftrightarrow} P)_{H(ID_s)} B_{12} : Se \lhd (S_{pd}, r_t, X, Se \overset{S_s}{\leftrightarrow} P)_{H(ID_s)} B_{13} : Se \lhd (S_{pd}, r_t, X, Se \overset{SK}{\leftrightarrow} P)_{H(ID_s)}$
- Using the Assumption A_7 and B_{11}, B_{12}, B_{13} and the message meaning rule we got the $B_{14} : Se| \equiv P \sim (Z, X, R_s, P_{pu}, Se \overset{s}{\leftrightarrow} P) B_{15} : Se| \equiv P \sim (S_{pd}, r_t, X, Se \overset{S_s}{\leftrightarrow} P) B_{16} : Se| \equiv P \sim (S_{pd}, r_t, X, Se \overset{SK}{\leftrightarrow} P)$
- Using the concept of freshness rule and the assumption A_3 we got the $B_{17} : Se| \equiv \#(Z, X, R_s, P_{pu}, Se \overset{s}{\leftrightarrow} P)$
- Using the concept of freshness rule and the assumption A_4 we got the $B_{18} : Se| \equiv \#(S_{pd}, r_t, X, Se \overset{S_s}{\leftrightarrow} P) B_{19} : Se| \equiv \#(S_{pd}, r_t, X, Se \overset{SK}{\leftrightarrow} P)$
- Using the B_{14}, B_{17} and nonce verification rule we got the $B_{20} : Se| \equiv P \equiv (Z, X, R_s, P_{pu}, Se \overset{s}{\leftrightarrow} P)$
- Using the belief rule and the B_{20} we got the $B_{21} : Se| \equiv P \equiv (Se \overset{s}{\leftrightarrow} P)$ **Goal 6**
- Using the B_{15}, B_{18} and nonce verification rule we got the $B_{22} : Se| \equiv P| \equiv (S_{pd}, r_t, X, Se \overset{S_s}{\leftrightarrow} P)$
- Using the belief rule and the B_{22} we got the $B_{23} : Se| \equiv P| \equiv (Se \overset{S_s}{\leftrightarrow} P)$ **Goal 1**
- Using the B_{16}, B_{19} and nonce verification rule we got the $B_{24} : Se| \equiv P| \equiv (S_{pd}, r_t, X, Se \overset{SK}{\leftrightarrow} P)$
- Using the belief rule and the B_{24} we got the $B_{25} : Se| \equiv P| \equiv (Se \overset{SK}{\leftrightarrow} P)$ **Goal 3**
- Using the concept of jurisdiction rule, assumption A_8, and B_{25} we got the $B_{26} : Se| \equiv (Se \overset{SK}{\leftrightarrow} P)$ **Goal 4**

Using the concept of BAN logic we prove the Goal 1 to Goal 6 and it shows that the formal security analysis using the BAN logic will be done and it insures the security of our proposed protocol.

6.3 Security analysis based on mathematical model

This section will show our proposed protocol security using the concept of a Real or random (ROR) model (Abdalla et al. 2005). We occupied the concept of Bellare and Rogaway (1993) to define our proposed protocol security model. According to the model, the adversary has to differentiate between the real session key and random numbers. In many mutual authentications and key agreement(MAKA) protocol (Agrahari and Varma 2021; Abbasinezhad-Mood et al. 2019), the ROR model is used to prove the session key security.

In our proposed protocol, there are two participants associated with the mutual authentication and key agreement protocol. The following components are associated with the ROR model. The components of our scheme are as follows:-

Participants

Server "S" and PDA "P" is the two participants of our proposed protocol. Let us assume that t_1 and t_2 are the two instances of our participants represented as $\Psi_S^{t_1}$ and $\Psi_P^{t_2}$ respectively.

Accepted state

When the instance Ψ^t gets the final message of the proposed protocol, it enters the final state. All the sent and the received message are arranged according to the accepted state, and at last, the session identification will form for the current session.

Partnering

Two instances of the participants, $\Psi_S^{t_1}$ and $\Psi_P^{t_2}$, are known to be a partner when they follow the following properties:-

- Both instances in an acceptable state.
- Both instances are mutually authenticating to each other and also have the same session identification.
- Both instances are mutual partner of each other.

Freshness

The session key between the two participants, "S", "P", was unable to leak using the reveal query, then only the instances $\Psi_S^{t_1}$ and $\Psi_P^{t_2}$ are fresh.

Adversary

Let's assume that $\boldsymbol{A}$ is an adversary who is having control of the entire network. Here, the control shows that adversary can read or modify all the messages through the public channel, and the adversary can also construct the message or delete the message in the network. $\boldsymbol{A}$ has to run the following queries:

- Execute$\{\Psi_S^{t_1}, \Psi_P^{t_2}\}$: This query works like a passive attack where $\boldsymbol{A}$ will try to obtain the message, which will be transferred between the S and P. It's like an eavesdropping attack.
- Send $\{\Psi^t, \mathrm{M}\}$: This query works like an active attack where $\boldsymbol{A}$ will try to impersonate the participant to send a message to another participant.
- CorruptSC : When adversary $\boldsymbol{A}$ runs this query, he will get the all information stored in the smart card. This kind of attack is possible by the the side channel attack.
- Capture$\{\Psi^t\}$: When adversary $\boldsymbol{A}$ runs this query, then he will get the secrets information of the server"S" or PDA "P'.
- Test$\{\Psi^t\}$: When the adversary runs this query, it can simulate the session key's semantic security using the unbiased coin C. The query output returns the random number of the same key size when the value of $C = 0$, if the value of $C = 1$, then the output is session key. Otherwise, the output is the null value..

The adversary has no restriction over the execution of test query, but the capture and corruptSC query will run a limited number of times.

Semantic security To make our proposed MAKA protocol is semantic secure, we will implement the game between the oracle $\mathcal{O}$ and $\boldsymbol{A}$. $\boldsymbol{A}$ can make many queries to $\mathcal{O}$, and the $\mathcal{O}$ will respond accordingly. When $\boldsymbol{A}$ makes the test query then the $\mathcal{O}$ response the C'. If the $C' == C$ then the adversary wins the game. Let *Succ* denotes the event when the adversary $\boldsymbol{A}$ wins the game. So, the advantage of $\boldsymbol{A}$ to break the semantic security of our proposed protocol $\mathcal{P}$ in the polynomial time t is represented as

$$Adv_A^{\mathcal{P}}(t) = |2.Pr[Succ] - 1|.$$

Theorem *Suppose $\boldsymbol{A}$ is a polynomial time 't' bound adversary and $Adv_A^{\mathcal{P}}(t)$ be the advantage of breaking the proposed scheme's semantic security. Then this is denoted as*

$$Adv_A^{\mathcal{P}}(t) \leq \frac{q_h^2}{|Hash|} + \frac{(q_s + q_e)^2}{(2^{p-1})} + \frac{2.q_s}{|D_{id}||D_{pw}|} + 2.Adv_A^{k-mBIDH}$$

Where,

q_h = Number of hash query
q_s= Number of send query
q_e = Number of execute query
$|Hash|$ = Range space of h(.)
p = Bit length of random number
D_{id}= Uniformly distributed dictionary of user identity
D_{pw} Uniformly distributed dictionary of user password

Proof In the following proof of the games $G_i, 0 \leq i \leq 4$, Adversary $\boldsymbol{A}$ will do a five attacks. $Succ_i$ denotes the probability of $\boldsymbol{A}$ winning the game G_i . So the result of game G_0 to G_4 demonstrates that adversary $\boldsymbol{A}$ can breach the semantic security of the session key in the polynomial-time or not.

−Game G_0: The game G_0 defines as a real attack in the network, which is done by $\boldsymbol{A}$. The bit C chosen by the adversary at the starting of the game, Therefore by definition

$$Adv_A^{\mathcal{P}}(t) = |2.Pr[Succ_0] - 1| \tag{1}$$

□

−Game G_1: Under this game, the eavesdropping attack has been implemented. The Adversary $\boldsymbol{A}$ runs the execute query,i.e., Execute$\{\Psi_S^{t_1}, \Psi_P^{t_2}\}$, and gets the transmitted message between the server "S" and the PDA "P",i.e., $\{\wedge_1,\wedge_2,\wedge_3,T_1\}$ and $\{\rho_5,\rho_6,F,T_3\}$ after that, $\boldsymbol{A}$ runs the Test(Ψ^t) query. At last, $\boldsymbol{A}$ requires to verify the session key. In our proposed algorithm, the session key is SK = $(ID_s||ID_p||\rho_2'||\wedge_4||\wedge_5||B_i||T_3)$. However, none of the messages can use to implement the session key, and also, the secret credential is not revealed in the intercepted message. The possibility of $\boldsymbol{A}$ winning the game using the eavesdropping attack is not increased, So we conclude that

$$Pr[Succ_1] = Pr[Succ_0] \tag{2}$$

−GameG_2: The difference between the previous game and this game is that we consider the collision in the hash query and transcript. $\boldsymbol{A}$ performs the active attack and runs the send and hash query to mislead the node to accepting the illegal messages. However, in the proposed scheme, all messages are dynamic because they have random numbers and timestamps. So no collision occurs in the transcript messages and the hash oracle messages. According to the birthday paradox, the hash query's collision probability is at most $\frac{q_h^2}{2.|Hash|}$ and the collision probability for random number is $\frac{(q_s+q_e)^2}{(2^p)}$. So the result is

$$|Pr[Succ_2] - Pr[Succ_1]| \leq \frac{q_h^2}{2.|Hash|} + \frac{(q_s + q_e)^2}{(2^p)} \quad (3)$$

−Game G_3: In this game, the adversary $\boldsymbol{A}$ performs the CorruptSC(Ψ^t) and capture query to obtain the secret information store in the smart card, server, and PDA. If $\boldsymbol{A}$ obtains the correct ID and PW, then $\boldsymbol{A}$ will win the game. However, in proposed scheme the adversary could not get the secret information using the card data because it is in masked form and encrypted using the one way hash function. So the result obtain as:

$$|Pr[Succ_3] - Pr[Succ_2]| \leq \frac{q_s}{|D_{id}||D_{pw}|} \quad (4)$$

−GameG_4: Adversary $\boldsymbol{A}$ eavesdrops on the messages sent between the "S" and "P". To obtain the session key to breach the semantic security, the adversary must solve the k-mBIDH problem in polynomial time. But it is hard to solve the k-mBIDH problem in polynomial time, so the result obtain as

$$|Pr[Succ_4] - Pr[Succ_3]| \leq Adv_A^{k-mBIDH} \quad (5)$$

$\boldsymbol{A}$ runs all the queries to obtain the value of the session key to break the semantic security. So, at last, the adversary guess the bit value of C to win the game, so it generates:

$$|Pr[Succ_4]| = \frac{1}{2} \quad (6)$$

From equation (1) and (2)

$$Adv_A^{\mathcal{P}}(t) = |2.Pr[Succ_0] - 1|$$
$$Adv_A^{\mathcal{P}}(t) = |2.Pr[Succ_1] - 1|$$
$$Adv_A^{\mathcal{P}}(t) = 2.|Pr[Succ_1] - \frac{1}{2}|$$

using equation (6)

$$Adv_A^{\mathcal{P}}(t) = 2.|Pr[Succ_1] - Pr[Succ_4]|$$

Applying triangular inequality

$$|Pr[Succ_1] - Pr[Succ_4]| \leq |Pr[Succ_1] - Pr[Succ_2]| + |Pr[Succ_2] - Pr[Succ_3]| + |Pr[Succ_3] - Pr[Succ_4]| \quad (7)$$

From Eqs. (3), (4), (5) and (7) we get the result

$$Adv_A^{\mathcal{P}}(t) \leq \frac{q_h^2}{|Hash|} + \frac{(q_s + q_e)^2}{(2^{p-1})} + \frac{2.q_s}{|D_{id}||D_{pw}|} + 2.Adv_A^{k-mBIDH}$$

Hence our proposed protocol insures the semantic security.

6.4 Security verification using AVISPA tool

This part officially verifies our proposed protocol utilizing the Automated Verification Security Protocol and Analysis (AVISPA) simulation tool. It is a push button tool that is used for checking the cryptographic protocols and recognizing whether those security protocols are SAFE or UNSAFE against different active and passive attacks.

AVISPA utilizes High-Level Protocol Specification Language(HLPSL) [30] for code execution to confirm the security vulnerabilities in a protocol.

AVISPA incorporates four back-ends, to be specific (1) On-the-fly-Model-Checker (OFMC), (2) Constraint-Logic-based Attack Searcher (CL-AtSe),(3) SAT-based Model-checker (SATMC), and (4)Tree Automata dependent on Automatic Approximations for the Analysis of Security Protocols (TA4SP), with HLPSL to analyze the protocol. In the AVISPA tool, the HLPSL code is initial changed over into the intermediary form(IF) with the assistance of the HLPSL2IF interpreter. This IF code is given to back-ends for security checks, and afterward its yield shows whether the protocol is protected or attacked.

The yield design contains the accompanying significant fields:

SUMMARY It Shows that the protocol is SAFE or UNSAFE.
DETAILS Depicting conditions in which text protocol is declared to be protected or attack discovering condition.
PROTOCOL Name of the protocol.
GOAL The objective of the analysis.
BACKEND Shows which back-end is used.
STATISTICS Shows the parse-time, search-time, visited hubs, and the profundity of the hub in executing of the protocol.

6.4.1 Implementation and results

The HLPSL code of our proposed protocol run in the SPAN simulation tool. To run this simulation tool, we have used a personal computer. The configuration of our system is

Processor: Intel(R) Core(TM) i3-3220 CPU @3.30GHz
RAM: 6GB
System type: 64 bit OS

The result of the SPAN simulation tools shows in Table 9. The output of the AVISPA code is categorized based on the backend tool and its model type. According to the simulation result, We have used the OFMC backend tool for the bounded number of the session then the statistics for the proposed protocol is as follows: it is visited

Table 9 Simulation results of AVISPA tool

Version	Backend tool	Details	Statistics	Goal	Summary
Basic	OFMC	Bounded number of Session	Parse time :.00s, Search time:.31s, Visited nodes: 167, Depth : 4plies	As specified in HLPSL code	SAFE
Basic	CL-AtSe	Bounded number of Session Typed model	Analysed: 15 states, Reachable :15 states, Translation : .01s, Computation: .00s	As specified in HLPSL code	SAFE
Basic	CL-AtSe	Bounded number of Session Untyped model	Analysed: 15 states, Reachable :15 states, Translation : .00s, Computation: .00s	As specified in HLPSL code	SAFE

Table 10 Execution time of the cryptographic operation According to Kilinc and Yanik (2013)

Operation	Description	time(ms)
T_b	Time to compute the bilinear pairing operation	5.811
T_h	Time to compute the hash operation	0.0023
T_m	Time to compute point multiplication	2.226
T_e	Time to compute exponentiation operation	3.85

167 nodes with the depth of 4 plies where the search time is .31 second.

The statistics for CL-AtSe backend tool for the typed and untyped model for the bounded number of session is as follows: it will analyze 15 states and reach all the states in the .01s in the typed model and .00s for the untyped model. Whereas the computation time for both the model is .00s.

This simulation result shows that our proposed protocol is secure against the various attacks.

7 Performance analysis

In this section, we will illustrate the performance of the proposed protocol for wireless body area networks. The analysis is based on computation cost and security threats. Finally, we provide a comprehensive discussion of the effectiveness of the proposed protocol compared to some existing protocols.

7.1 Computation cost analysis

In this section, we compare the computation cost of our proposed protocol with some similar existing protocols, such as, Wang and Zhang (2015); Wu et al. (2016); Liu et al. (2013); Xiong and Qin (2015); Abbasinezhad-Mood et al. (2019); Zhang et al. (2020); Li et al. (2016); Tsai and Lo (2015); He et al. (2016). We have considered many cryptographic functions in the proposed protocols. We defined the notations and computation time in Table 10, which we used further. We have referred the Kilinc et al. work to get the computation cost of the cryptographic operation. In Kilinc and Yanik (2013) using the version 0.5.12 of PBC library by using 32 bit OS of ubuntu 12.04.1 , CPU:2.2GHz and RAM: 2GB to get the computation time.

The computation time of the proposed scheme is $1.T_b + 9.T_h + 8.T_m + 1.T_e \approx 27.52$ ms. The comprehensive comparison of the proposed protocol with some existing protocol is as follows :

- The computation cost of the Wang and Zhang (2015) is $2.T_b + 10.T_h + 5.T_m \approx 22.79$ ms. The scheme is approximately 17.18% more efficient compared to the proposed scheme, but it is not secure against the session key attack, replay attack, impersonation attack, and also fails in user anonymity and untraceability.
- The computation cost of the Wu et al. (2016) is $1.T_b + 5.T_h + 7.T_m + 4.T_e \approx 36.83$ ms. The scheme is approximately 33.83% less efficient compared to the proposed scheme.
- The computation cost of the Liu et al. (2013) is $1.T_b + 4.T_h + 7.T_m + 1.T_e \approx 25.28$ ms, The scheme is approximately 8.14% more efficient compared to the proposed scheme, but it has the key escrow problem, and is also not secure against impersonation attack .
- The computation cost of the Xiong and Qin (2015) is $9.T_b + 11.T_h + 5.T_m + 15.T_e \approx 121.21$ ms. The scheme is approximately 340.44% less efficient compared to the proposed scheme.
- The computation cost of the Abbasinezhad-Mood et al. (2019) is $1.T_b + 11.T_h + 12.T_m + 1.T_e \approx 36.44$ ms. The scheme is approximately 32.41% less efficient compared to the proposed scheme.
- The computation cost of the Zhang et al. (2020) is $1.T_b + 11.T_h + 8.T_m + 1.T_e \approx 27.52$ ms, which is approximate equally efficient to the proposed scheme, but does not handle the key escrow issue.
- The computation cost of the Li et al. (2016) is $2.T_b + 8.T_h + 7.T_m + 2.T_e \approx 34.95$ ms. The scheme is

approximately 27.00% less efficient compared to the proposed scheme.

- The computation cost of the Tsai and Lo (2015) is $4.T_b + 10.T_h + 9.T_m + 2.T_e \approx 51.03$ ms. The scheme is approximately 85.42% less efficient compared to the proposed scheme.
- The computation cost of the He et al. (2016) is $1.T_b + 11.T_h + 5.T_m + 6.T_e \approx 45.89$ ms. The scheme is approximately 66.75% less efficient compared to the proposed scheme.

The complete comprehensive analysis of all cryptographic operations and total computational cost is enumerated in Table 11. Additionally the computation cost-related graph is shown in Fig 2. Whereas, Table 12 shows the Efficiency of the existing schemes with respect to the proposed scheme.

Fig. 3 mentions the computation cost of the server. According to Fig 3, when we increases the number of servers, the server's computation time increases. However, the server's time of the proposed scheme is better than the existing schemes except Wang and Zhang (2015) scheme. According to Table 13, the Wang scheme is not

Table 11 Total cryptographic operation and total computation cost

Scheme	Server side cryptographic operation	PDA side cryptographic operation	Total cryptographic operation	Computation time (ms)
Wang and Zhang (2015)	$1.T_b + 5.T_h + 2.T_m \approx 10.27$	$1.T_b + 5.T_h + 3.T_m \approx 12.52$	$2.T_b + 10.T_h + 5.T_m$	≈ 22.79
Wu et al. (2016)	$3.T_h + 4.T_m + 2.T_e \approx 16.61$	$1.T_b + 2.T_h + 3.T_m + 2.T_e \approx 20.21$	$1.T_b + 5.T_h + 7.T_m + 4.T_e$	≈ 36.83
Liu et al. (2013)	$1.T_b + 2.T_h + 2.T_m + 1.T_e \approx 14.13$	$2.T_h + 5.T_m \approx 11.16$	$1.T_b + 4.T_h + 7.T_m + 1.T_e$	≈ 25.28
Xiong and Qin (2015)	$8.T_b + 3.T_h + 4.T_e \approx 61.89$	$1.T_b + 8.T_h + 5.T_m + 11.T_e \approx 59.32$	$9.T_b + 11.T_h + 5.T_m + 15.T_e$	≈ 121.21
Abbasinezhad-Mood et al. (2019)	$1.T_b + 5.T_h + 5.T_m \approx 16.95$	$6.T_h + 7.T_m + 1.T_e \approx 19.49$	$1.T_b + 11.T_h + 12.T_m + 1.T_e$	≈ 36.44
Zhang et al. (2020)	$1.T_b + 6.T_h + 4.T_m \approx 14.73$	$5.T_h + 4.T_m + 1.T_e \approx 12.79$	$1.T_b + 11.T_h + 8.T_m + 1.T_e$	≈ 27.52
Li et al. (2016)	$2.T_b + 4.T_h + 3.T_m + 1.T_e \approx 22.16$	$4.T_h + 4.T_m + 1.T_e \approx 12.79$	$2.T_b + 8.T_h + 7.T_m + 2.T_e$	≈ 34.95
Tsai and Lo (2015)	$4.T_b + 4.T_h + 2.T_m + 1.T_e \approx 31.55$	$6.T_h + 7.T_m + 1.T_e \approx 19.48$	$4.T_b + 10.T_h + 9.T_m + 2.T_e$	≈ 51.03
He et al. (2016)	$2.T_b + 5.T_h + 2.T_m + 3.T_e \approx 27.62$	$6.T_h + 3.T_m + 3.T_e \approx 18.26$	$2.T_b + 11.T_h + 5.T_m + 6.T_e$	≈ 45.89
Proposed scheme	$8.T_h + 4.T_m + 1.T_e \approx 12.77$	$1.T_b + 1.T_h + 4.T_m \approx 14.75$	$1.T_b + 9.T_h + 8.T_m + 1.T_e$	≈ 27.52

Table 12 Efficiency With respect to the proposed scheme

Schemes	Efficiency with respect to proposed scheme	Security remark
Wang and Zhang (2015)	17.18% more efficient	Not secure against the session key attack, replay attack, impersonation attack
Wu et al. (2016)	33.83% less efficient	Not secure against the replay attack , impersonation attack and also having the key escrow issue
Liu et al. (2013)	8.14% more efficient	Not secure against impersonation attack and also having a key escrow issue
Xiong and Qin (2015)	340.44% less efficient	Not secure against the impersonation attack and also having the key escrow and perfect forward secrecy issue
Abbasinezhad-Mood et al. (2019)	32.41% less efficient	Not secure against the impersonation attack and also not proof the protocol using BAN logic
Zhang et al. (2020)	Equally efficient(Approx)	Not handle the key escrow issue and also not secure against the privileged insider attack
Li et al. (2016)	27.00% less efficient	Not satisfy the Perfect forward secrecy property]
Tsai and Lo (2015)	85.42% less efficient	Not resist a smart card and privileged insider attack and also have the key escrow issue
He et al. (2016)	66.75% less efficient	Not secure against the impersonation attack and also not proof the protocol using any predefined model or tool like RoR model, BAN logic or AVISPA tool

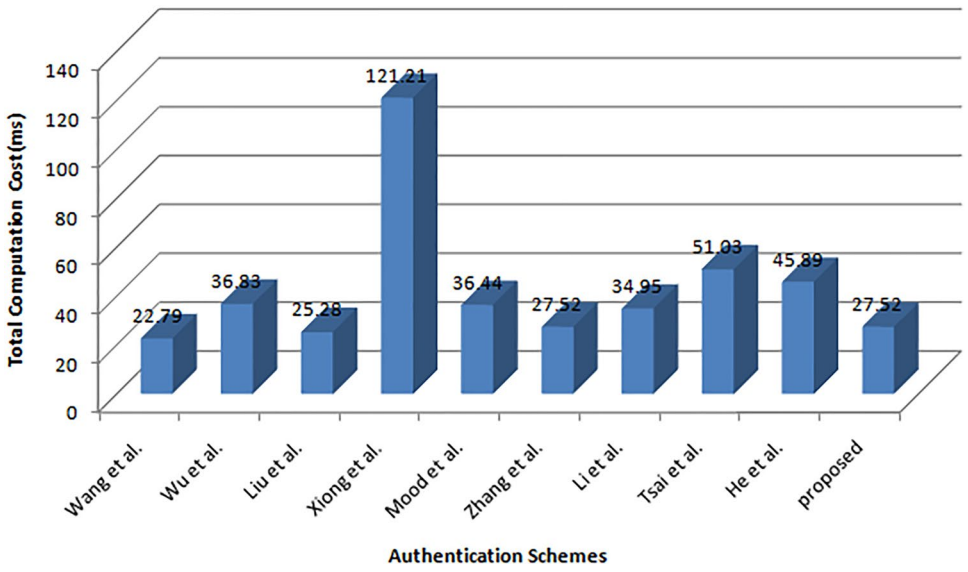

Fig. 2 Computation cost

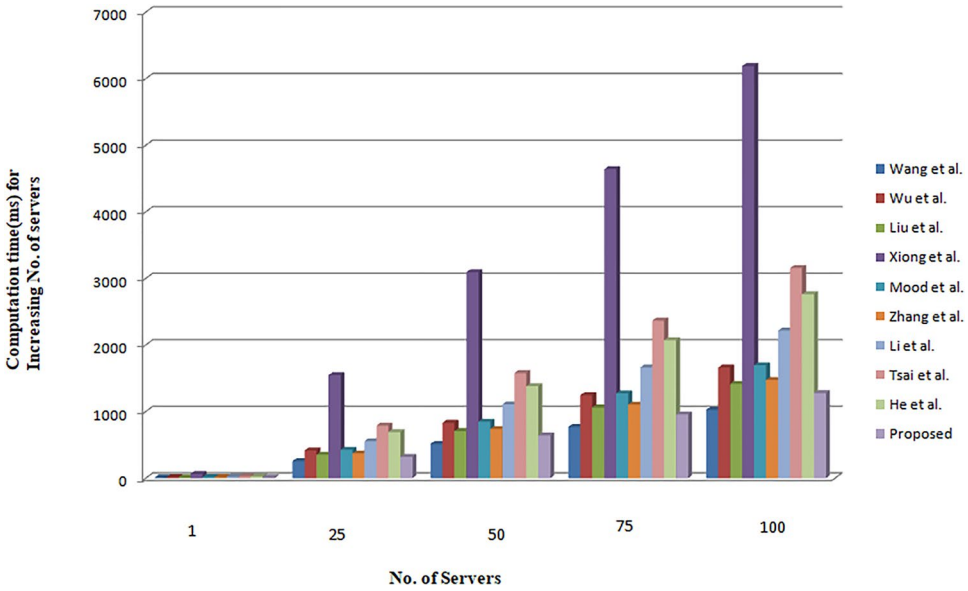

Fig. 3 Computation cost on server

secure against many predefined attacks like perfect forward secrecy, replay attack, impersonation attack, and does not establish mutual authentication. Hence, it takes less server time than the proposed scheme, but does not fulfill the security requirements.

7.2 Security analysis

This section is completely dedicated to the comparison of our proposed authentication scheme with the other existing schemes on the basis of the features, functionality and their security requirements. The notations "*N*", "*Y*", and "–" are used which means security requirements are not fulfilled, security requirements are fulfilled and security requirements are not included simultaneously.

The main security requirement is whether the schemes have focused on the mutual authentication between the server and the PDA. Among all, the Wang and Zhang (2015); Wu et al. (2016); Liu et al. (2013), and Tsai and Lo (2015) could not achieve the mutual authentication requirements in their schemes. The scheme avoided the key escrow problem. The key escrow problem is when the trusted authority knows the secret keys of the user. While our proposed protocol is able to avoid this problem, the schemes of Wu et al., Liu et al., Xiong et al., Zhang et al., and Tsai et al. have not even considered this problem.

The proposed scheme is also secure against the privileged insider attack which Zhang et al., and Tsai et al. fail to secure. User is traceable in Wang and Zhang (2015); Liu et al. (2013), and Tsai and Lo (2015). Additionally,

Table 13 Security requirements

Security requirements	Wang and Zhang (2015)	Wu et al. (2016)	Liu et al. (2013)	Xiong and Qin (2015)	Zhang et al. (2020)	Kompara et al. (2019)	Tsai and Lo (2015)	Proposed protocol
Resistance to replay attack	N	N	Y	Y	Y	Y	Y	Y
Resistance to impersonation attack	N	N	N	N	Y	N	N	Y
Resistance to Man in the middle attack	Y	Y	Y	Y	Y	N	N	Y
Resistance to Password guessing attack	–	–	Y	Y	Y	–	Y	Y
Resistance to smart card attack	–	–	–	–	Y	–	N	Y
Resistance to privileged insider attack	–	–	Y	Y	N	Y	N	Y
Resistance to key escrow problem	–	N	N	N	N	–	N	Y
Perfect forward secrecy	N	Y	N	N	Y	Y	Y	Y
Session key security	N	Y	Y	Y	Y	Y	N	Y
User untraceability	N	Y	N	Y	Y	Y	N	Y
User anonymity	N	Y	Y	Y	Y	Y	N	Y
Mutual authentication	N	N	N	Y	Y	Y	N	Y

the scheme is also secure against impersonation and man-in-the-middle attacks.

The comprehensive security requirements comparison is summarized in the Table 13.

8 Conclusion and future work

Security is the primary goal in a healthcare environment when crucial data are transferred via the public channel. This paper has designed a new authentication scheme where the legitimate user can register through a trusted authority. The server and the PDA have to authenticate each other in order to send or receive the sensitive information mutually. Our primary focus is to avoid the key escrow problem and establish a new session key between the server, and the PDA, which will be used for future communication. The formal security analysis of the proposed protocol is done using the BAN logic and ROR model. While the Security verification is done using the AVISPA tool. In addition, a detailed comparative analysis for the communication cost is also included. This analysis, verification, and comparison prove that the proposed protocol is secure against prevailing attacks and better among the other existing protocols.

However, the proposed scheme has certain limitations, such as assuming the PDA (sensors) remain undamaged once installed in the patient body. In contrast, this is not the case in the real world. We have to replace the sensors after they are damaged. Another concern is that we are using the centralized server for our scheme, which incurs some latency even in the best case. So, in the future, we would try to extend our work and shift our paradigm towards edge computing which is the extension of cloud computing for resolving latency. Additionally, we will try to inculcate the private blockchain to make the system transparent and immutable. Last but not least, we would try to work on the real dataset and execute the proposed work in the real environment.

References

Abbasinezhad-Mood D, Ostad-Sharif A, Nikooghadam M, Mazinani SM (2019) A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid. IEEE Trans Ind Inf 16(3):1495–1502. https://doi.org/10.1109/TII.2019.2927512

Abdalla M, Fouque P. A., Pointcheval D (2005) Password-based authenticated key exchange in the three-party setting. In: International workshop on public key cryptography. Springer, Berlin, pp 65–84. https://doi.org/10.1007/978-3-540-30580-46

Abualigah LMQ (2019) Feature selection and enhanced krill herd algorithm for text document clustering. Springer, Berlin, pp 1–165. https://doi.org/10.1007/978-3-030-10674-4

Abualigah L, Diabat A (2021) Advances in sine cosine algorithm: a comprehensive survey. Artif Intell Rev. https://doi.org/10.1007/s10462-020-09909-3

Abualigah L, Yousri D, Abd Elaziz M, Ewees AA, Al-qaness MA, Gandomi AH (2021a) Aquila optimizer: a novel meta-heuristic optimization algorithm. Comput Ind Eng 157:107250. https://doi.org/10.1016/j.cie.2021.107250

Abualigah L, Diabat A, Mirjalili S, Abd Elaziz M, Gandomi AH (2021b) The arithmetic optimization algorithm. Comput Methods Appl Mech Eng 376:113609. https://doi.org/10.1016/j.cma.2020.113609

Agrahari AK, Varma S (2020) Authentication in RFID scheme based on elliptic curve cryptography. Saf Secur Reliab Robot Syst Algorithms Appl Technol. https://doi.org/10.1201/9781003031352

Agrahari AK, Varma S (2021) A provably secure RFID authentication protocol based on ECQV for the medical internet of things. Peer-to-Peer Netw Appl 14(3):1277–1289. https://doi.org/10.1007/s12083-020-01069-z

Amin R, Islam SH, Biswas GP, Giri D, Khan MK, Kumar N (2016) A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments. Secur Commun Netw 9(17):4650–4666. https://doi.org/10.1002/sec.1655

Assunção MD, Calheiros RN, Bianchi S, Netto MA, Buyya R (2015) Big Data computing and clouds: trends and future directions. J Parall Distrib Comput 79:3–15. https://doi.org/10.1016/j.jpdc.2014.08.003

AVISPA (2018) Automated validation of Internet Security protocols and applications. http://www.avispa-project.org. Accessed May 2018

Bellare M, Rogaway P (1993) Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of the 1st ACM conference on computer and communications security, pp 62–73. https://doi.org/10.1145/168588.168596

Burrows M, Abadi M, Needham RM (1989) A logic of authentication. Proc R Soc Lond A Math Phys Sci 426(1871):233–271. https://doi.org/10.1098/rspa.1989.0125

Canetti R, Krawczyk H (2001) Analysis of key-exchange protocols and their use for building secure channels. In: International conference on the theory and applications of cryptographic techniques. Springer, Berlin, pp 453–474. https://doi.org/10.1007/3-540-44987-628

Cao X, Kou W, Du X (2010) A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Inf Sci 180(15):2895–2903. https://doi.org/10.1016/j.ins.2010.04.002

Debiao H, Jianhua C, Jin H (2012) An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security. Inf Fus 13(3):223–230. https://doi.org/10.1016/j.inffus.2011.01.001

Dolev D, Yao A (1983) On the security of public key protocols. IEEE Trans Inf Theory 29(2):198–208. https://doi.org/10.1109/TIT.1983.1056650

He D, Kumar N, Khan MK, Wang L, Shen J (2016) Efficient privacy-aware authentication scheme for mobile cloud computing services. IEEE Syst J 12(2):1621–1631. https://doi.org/10.1109/JSYST.2016.2633809

https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

Irshad A, Sher M, Ahmad HF, Alzahrani BA, Chaudhry SA, Kumar R (2016) An improved multi-server authentication scheme for distributed mobile cloud computing services. TIIS 10(12):5529–5552. https://doi.org/10.3837/tiis.2016.12.021

Jia X, He D, Kumar N, Choo KKR (2019) A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing. IEEE Syst J 14(1):560–571. https://doi.org/10.1109/JSYST.2019.2896064

Jiang Q, Ma J, Wei F (2016) On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst J 12(2):2039–2042. https://doi.org/10.1109/JSYST.2016.2574719

Karati A, Islam SH, Biswas GP (2018a) A pairing-free and provably secure certificateless signature scheme. Inf Sci 450:378–391. https://doi.org/10.1016/j.ins.2018.03.053

Karati A, Islam SH, Karuppiah M (2018b) Provably secure and lightweight certificateless signature scheme for IIoT environments. IEEE Trans Ind Inf 14(8):3701–3711. https://doi.org/10.1109/TII.2018.2794991

Kilinc HH, Yanik T (2013) A survey of SIP authentication and key agreement schemes. IEEE Commun Surv Tutor 16(2):1005–1023. https://doi.org/10.1109/SURV.2013.091513.00050

Kompara M, Islam SH, Hölbl M (2019) A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. Comput Netw 148:196–213. https://doi.org/10.1016/j.comnet.2018.11.016

Koya AM, Deepthi PP (2018) Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. Comput Netw 140:138–151. https://doi.org/10.1016/j.comnet.2018.05.006

Li F, Han Y, Jin C (2016) Cost-effective and anonymous access control for wireless body area networks. IEEE Syst J 12(1):747–758. https://doi.org/10.1109/JSYST.2016.2557850

Li X, Peng J, Kumari S, Wu F, Karuppiah M, Choo KKR (2017) An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. Comput Electr Eng 61:238–249. https://doi.org/10.1016/j.compeleceng.2017.02.011

Liu J, Zhang Z, Chen X, Kwak KS (2013) Certificateless remote anonymous authentication schemes for wirelessbody area networks. IEEE Trans Parallel Distrib Syst 25(2):332–342. https://doi.org/10.1109/TPDS.2013.145

Omala AA, Ali I, Li F (2018) Heterogeneous signcryption with keyword search for wireless body area network. Secur Priv 1(5):e25. https://doi.org/10.1002/spy2.25

Singh S, Chaurasiya VK (2021) Mutual authentication scheme of IoT devices in fog computing environment. Clust Comput 24(3):1643–1657. https://doi.org/10.1007/s10586-020-03211-1

Sowjanya K, Dasgupta M, Ray S (2020) An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. Int J Inf Secur 19(1):129–146. https://doi.org/10.1007/s10207-019-00464-9

Suriyakrishnaan K, Sridharan D (2018) Reliable packet delivery in wireless body area networks using TCDMA algorithm for e-health monitoring system. Wirel Pers Commun 103(4):3127–3144. https://doi.org/10.1007/s11277-018-5998-5

Tsai JL, Lo NW (2015) A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst J 9(3):805–815. https://doi.org/10.1109/JSYST.2014.2322973

Wang D, Ma CG (2013) Cryptanalysis of a remote user authentication scheme for mobile client-server environment based on ECC. Inf Fus 14(4):498–503. https://doi.org/10.1016/j.inffus.2012.12.002

Wang C, Zhang Y (2015) New authentication scheme for wireless body area networks using the bilinear pairing. J Med Syst 39(11):1–8. https://doi.org/10.1007/s10916-015-0331-2

Wu L, Zhang Y, Li L, Shen J (2016) Efficient and anonymous authentication scheme for wireless body area networks. J Med Syst 40(6):134. https://doi.org/10.1007/s10916-016-0491-8

Xiong H, Qin Z (2015) Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE Trans Inf Forensics Secur 10(7):1442–1455. https://doi.org/10.1109/TIFS.2015.2414399

Yang JH, Chang CC (2009) An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Comput Secur 28(3–4):138–143. https://doi.org/10.1016/j.cose.2008.11.008

Yoon EJ, Yoo KY (2009) Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc. In: 2009 International conference on computational science and engineering, vol 2. IEEE, pp 633–640. https://doi.org/10.1109/CSE.2009.363

Zhang Y, Zou J, Guo R (2020) Efficient privacy-preserving authentication for V2G networks. Peer-to-Peer Netw App. https://doi.org/10.1007/s12083-020-01018-w

Zhao Z (2014) An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. J Med Syst 38(2):1–7. https://doi.org/10.1007/s10916-014-0013-5