

Privacy Preserving Scalable Authentication Protocol with Partially Trusted Third Party for Distributed Internet-of-Things

Hiral S. Trivedi^a and Sankita J. Patel

Department of Computer Engineering, Sardar Vallabhbhai National Institute of Technology, Surat 395007, India


Keywords: Authentication, Anonymity, Security, Scyther, Scalability, Partially Trusted Third Party.

Abstract: *Internet-of-Things* (IoT) has triggered substantial research in real-time applications of distributed networking infrastructure involving disparate entities with heterogeneous protocol configuration stacks. The disparate characteristics of diverse infrastructures elevate the need for improved authentication in distributed IoT. The distributed environment also amplifies the requirement of effective scalability to eliminate halting or restarting of a system whenever any fresh user joins an existing communication channel. Several security protocols using fully trusted third party (TTP) and multi-authority based approaches have been proposed to facilitate reliable distributed networks. These approaches while providing efficient key agreement, have issues such as key escrow and complete rights policy of fully TTP and compulsory user coordination of multi-authority based systems. We propose a novel privacy preserving dynamic new user addition protocol with partially TTP to address fully TTP issues, while achieving efficient scalability to avoid resource wastage in distributed IoT. Formal security analysis is exhibited using a real-or-random model and formal verification under a scyther security verification tool. Finally, we present a performance evaluation to elucidate the utility of our protocol.

1 INTRODUCTION

Widespread IoT adoption has engendered connection of physical objects with cyberspace enabling ubiquitous computing through integrated disparate systems for information sharing via communication networks (Das et al., 2020). IoT advocacy in critical sectors while facilitating pervasive services, has also accentuated information security risk which necessitates a robust authentication requirement for secure and anonymous access to sensitive information. Also, the primary challenges of efficient scalability, uninterrupted communication channel, and cryptographic resource wastage in developing effective distributed systems are higher (Trivedi and Patel, 2020). Several authors have designed fully TTP and multi-authority based protocols, however they rarely jointly achieve robust security and effective privacy. Conventional mechanisms have shortcomings such as fully TTP incorporating complete rights policy and key escrow, while multi-authority based approaches have compulsory user coordination and random authority appointment (Trivedi and Patel, 2020). As a result, none of the standard approaches provide an amalgamated solution to completely mitigate aforementioned limitations. Hence, to satisfy dynamic scalability while pro-

viding reasonable trade-off between security and privacy, we proffer a combined key solution in our novel generic protocol for dynamic fresh user addition with a partially TTP approach. We also present our novelty in achieving dynamic system scalability without interrupting on-going communication channels for fresh node addition. The TTP has partial involvement in performing secure authentication with a fresh node for verification process. After successful verification, a fresh node is granted final communication secret key to participate in the system. We outline three major challenges in designing our protocol as follows. **Robust Security:** Standard Public Key Cryptography (PKC) has higher processing cost while, Symmetric Key Cryptography (SKC) has secret key sharing and trust issues. However, designing light-weight robust authentication for IoT devices remains a challenge. As per Ecrypt II report, a 128 bit symmetric key is equivalent to security strength of 3,248 bit asymmetric key (Babbage et al., 2009). Thereby, we preregister long-term secret for effective key sharing and execute SKC based challenge/response game utilizing one-time dynamic alias identity, hash functions and JSON Web Token (JWT). **Privacy:** An ideal authentication protocol requires efficient trade-off to satisfy between robust security with strong identity and effective privacy with weaker identity to preserve anonymity (Wang, 2018). **Complete Trust Policy:**

^a  <https://orcid.org/0000-0002-2152-8264>

Fully TTP systems with complete rights over cryptographic resources invoke security violations and key escrow problems for encrypting parties.

1.1 Related Work

(Das et al., 2020) proposed *elliptic curve cryptography* (ECC) based RFID authentication protocol to ensure tag's security and privacy. However, the scheme has higher computational requirements. (Gope and Sikdar, 2018) and (Saeed et al., 2018) proposed light-weight privacy preserving authentications. Utilizing fuzzy extractor, physically unclonable function and PKC based certificate-less schemes result in high processing and storage costs. (Chen et al., 2019) and (Zhang et al., 2019) introduced light-weight privacy preserving authentication incorporating PKC and SKC algorithms. However, complete trust and information leakage in their schemes violate security and privacy policies. (Kang et al., 2016) proposed a zero-knowledge based mutual authentication which overlooked secure device registration. (Vijayakumar et al., 2018) utilized anonymous certificates/signatures in their protocol but overlooked calculating communication cost and packet delivery ratio. (Chang and Le, 2015) enhanced (Turkanović et al., 2014) vulnerable scheme by proposing ECC based authentication. However, their approach is still vulnerable to side-channel, brute-force and stolen smart-card attacks. (Lai et al., 2014) proposed privacy preserving authentication using PKC diffie-hellman techniques. However, location and time-based privacy are not considered. (Lin et al., 2015) highlighted impersonation attacks that cheat central server while preserving anonymity in (Alcaide et al., 2013) authentication protocol. (Khan et al., 2011)'s enhanced protocol version of (Wang et al., 2009) enabled insider attack due to password based weak security level.

1.2 Our Contributions

Our contributions are: First, **Partial Rights Policy**: To eliminate complete rights and knowledge sharing, we adopt partially TTP located outside the premises of *Smart Homes* (SH). Second, **Robust Security**: Auto shared key updation in correspondence to JWT session expiry time is designed to boost security. Third, **Complete Anonymity**: We calculate one-time dynamic alias-identity over encrypted identities to preserve complete anonymity of authenticated users. Fourth, **Dynamic Scalability**: Partially TTP is responsible only for verifying fresh node legitimacy by performing secure authentication to allow participation in the existing communication channel. This

prevents frequent halting and restarting of securely configured systems to alleviate communication and computational costs. To the best of our knowledge, this paper proposes the first authentication protocol that jointly addresses partial rights policy, robust security, complete anonymity, and dynamic scalability. Prerequisites for our indigenous protocol model are discussed in Section 2. Section 3 presents privacy preserving secure authentication protocol with partially TTP. Security analysis and verification are hypothesized in Section 4. Performance evaluation and conclusions are elucidated in Section 5 and Section 6.

2 PRELIMINARIES

1. **Indistinguishable Encryption Under Chosen Plain-text Attack (IND-CPA)**: This formally states that two different encryptions of same plain-text do not produce similar cipher-text for symmetric encryption (Trivedi and Patel, 2020): *Definition 1*: This illustrates single/multiple (SI_E/ML_E) eavesdropper in a random oracle. The X encryption oracles are ($E_{k_1}, E_{k_2}, \dots, E_{k_n}$) with encryption keys (Ek_1, Ek_2, \dots, Ek_N), respectively. The advantage function of SI_E/ML_E is $Adv_{SI_E, \mathcal{A}}^{\text{IND-CPA}}(\Phi) = 2 \text{Prob}[SI_E \leftarrow E_{Ek_1} : (b_0, b_1 \leftarrow_R SI_E); \theta \leftarrow_R \{0, 1\}; \gamma \leftarrow_R E_{Ek_1}(b\theta) : SI_E(\gamma) = \theta] - 1$ and $Adv_{ML_E, \mathcal{A}}^{\text{IND-CPA}}(\Phi) = 2 \text{Prob}[ML_E \leftarrow E_{Ek_1}, \dots, E_{Ek_N}; (b_0, b_1 \leftarrow_R ML_E); \theta \leftarrow_R \{0, 1\}; \gamma \leftarrow_R E_{Ek_1}(b\theta), \dots, \gamma_N \leftarrow_R E_{Ek_N}(b\theta) : ML_E(\gamma_1, \dots, \gamma_N) = \theta] - 1$. The Φ is a secure symmetric cipher whose encryption is IND-CPA. It safeguards against (SI_E/ML_E) eavesdropper if $[Adv_{SI_E, \mathcal{A}}^{\text{IND-CPA}}(\Phi), Adv_{ML_E, \mathcal{A}}^{\text{IND-CPA}}(\Phi)]$ is negligible in the Φ for any probabilistic polynomial time.

2. **Architecture**: Partially TTP having own private network is located outside the premises of SH units and a new user wishing to participate in an established communication channel of SH units. It is assumed that inter-network SH units are securely connected for continuous communication. A dynamic new user addition is executed using legitimate partially TTP which holds signature long-term secret for identity verification. In addition, we assume partially TTP is a resource rich entity while new users have resource limited devices to perform authentication on a secure channel. We restrict TTP to validate a fresh user' identity and maintain complete anonymous authenticated user database with partial information to constrain knowledge sharing and complete rights policy. Fig.1 illustrates our design architecture and Table 1 describes the notations.

3. Adversary Model is as follows. **Confidentiality:** An \mathcal{A}_{conf} cannot intercept, tamper or modify the SH_k and T_{JWT} that are secure under our short term secret r_3 and preregistered long term secret $H_{SD_{id}}$.

$$TTP \models TTP \xrightarrow{SH_k} NU_{A_{id}} \wedge TTP \models TTP^c \triangleleft \| T'_{JWT} \wedge$$

$$\frac{TTP \xrightarrow{SH_k} T'_{JWT}}{TTP \models (TTP \cup NU_{A_{id}}) \triangleleft \| T'_{JWT}}$$

Authentication: An \mathcal{A}_{auth} cannot impersonate valid SH_k and a T_{JWT} as r_3 is XORed using $H_{SD_{id}}$. Semantic security is achieved by encrypting T_{JWT} with SH_k and

$$TTP \models TTP \xrightarrow{SH_k} NU_{A_{id}} \triangleleft \| T'_{JWT}$$

$$\frac{TTP \models NU_{A_{id}} \xrightarrow{SH_k} T'_{JWT}}{TTP \models (T_{JWT}) \wedge TTP \triangleleft (T'_{JWT}) \triangleleft (T'_{JWT})}$$

Integrity: An \mathcal{A}_{int} has negligible probability to tamper valid SH_k and T_{JWT} . A T_{JWT} session time will expire while brute-forcing a 128 bit SH_k requiring $5.784e+35$ nanoseconds (ns) (Trivedi and Patel, 2020). Immediately after a T_{JWT} expires, the TTP will update the SH_k and T_{JWT} and discard the old values.

$$\frac{TTP \models (T_{JWT}) \wedge TTP \triangleleft (T'_{JWT}) \triangleleft (T'_{JWT})}{TTP \models \#(T_{JWT})}$$

Replay Attack: Data blocks are appended with unique random numbers and time-stamps which prevent an \mathcal{A}_{rep} to respond to old messages.

$$\frac{TTP \models \#(T_{JWT}) \wedge TTP \triangleleft (T_{JWT}) \triangleleft (T'_{JWT})}{TTP \models \#(T_{JWT})}$$

Anonymity: We preserve anonymity by calculating one-time dynamic alias identity over encrypted identities such that a new user identity remains anonymous for an \mathcal{A}_{anony} and TTP in the system model.

$$I \models \theta(NU_{A_{id}}, r, m) \Rightarrow \mathcal{P}_j[-\theta(i, a)]$$

Table 1: Notations used in our approach.

Acronym	Description
$r_1/r_2/\dots/r_n$	Securely generated pseudo random numbers
NU_{id}	New user's encrypted identity
$NU_{A_{id}}$	New user's one-time alias identity
$TTP_{id}, TTP_{A_{id}}$	TTP's encrypted identity & alias identity
TTP_{MK}	TTP's master key
NU_P, H_{NU_P}	New user's password & Hash of password
$NU_{SD_{id}}$	New user's secret device identification
$H_{SD_{id}}$	Hash of secret device identification
$H(\cdot)$	One-way hash function
$F_{NU_{id}}$	Fresh anonymous identification
S_{E_k/D_k}	Symmetric encryption/decryption functions
$t_1/t_2/\dots/t_n$	Times-stamps
SH_k, T_{JWT}	Symmetric shared key & ID-based JWT
$Q_1/Q_2/Q_3$	Calculated hash values
\mathcal{A}	Adversary
\oplus, \parallel, \perp	XOR, Concatenation & Termination operations

3 PROPOSED PROTOCOL

1. Registration Phase.

- TTP Registration: TTP generates an encrypted identity TTP_{id} and r_1 to calculate $TTP_{MK} = H(TTP_{id} \parallel r_1)$ and $TTP_{A_{id}} = S_{E_k}(TTP_{id})TTP_{MK}$.

- New User Registration: **Step 1:** NU generates NU_{id} , NU_P and r_2 to calculate $H_{NU_P} = (r_2 \parallel NU_P)$. After that NU computes $NU_{A_{id}} = S_{E_k}(NU_{id})_{H_{NU_P}}$ and transmits $(NU_{A_{id}}, H_{NU_P})$ to TTP.

Step 2: After receiving $(NU_{A_{id}}, H_{NU_P})$ from NU, TTP calculates $NU_{id} = S_{D_k}(NU_{A_{id}})_{H_{NU_P}}$ and verifies if NU_{id} is in the database. If yes, TTP generates $F_{NU_{id}} = H(NU_{A_{id}} \parallel H_{NU_P} \parallel H_{SD_{id}} \parallel t_1)$ and transmits $(TTP_{A_{id}}, F_{NU_{id}})$ to NU.

Step 3: Upon receiving $(TTP_{A_{id}}, F_{NU_{id}})$, NU further retrieves $F'_{NU_{id}}$ by calculating hash of legitimate registered $H_{SD_{id}}$ and stores this data.

2. Secure Authentication Phase.

- **Step 1:** $[NU \rightarrow TTP (NU_{A_{id}}, F'_{NU_{id}})]$: Upon obtaining $(TTP_{A_{id}}, F_{NU_{id}})$, NU retrieves $H_{SD_{id}} = H(NU_{SD_{id}})$. Given the parameters $(NU_{id}, F_{NU_{id}})$, NU calculates $F'_{NU_{id}} = H(NU_{id} \parallel H_{NU_P} \parallel H_{SD_{id}} \parallel t_2)$ and transmits $(NU_{A_{id}}, F'_{NU_{id}})$ to TTP.

- **Step 2:** $TTP \rightarrow NU (r'_3, SH'_k, T'_{JWT}, Q_1)$: Upon receiving $(NU_{id}, F'_{NU_{id}})$, TTP verifies $F'_{NU_{id}} \stackrel{?}{=} F_{NU_{id}}$. If $F'_{NU_{id}} = F_{NU_{id}}$, NU's login request is accepted, else rejected. Assuming that NU's request is accepted, TTP will generate a SH_k , r_3 and T_{JWT} . A challenge/response game is enabled through four stages: 1) TTP computes $SH'_k = (SH_k \oplus r_3)$. 2) TTP encrypts $T'_{JWT} = S_{E_k}(T_{JWT})_{SH'_k}$. 3) r_3 is XORed with $H(NU_{SD_{id}})$ such that $r'_3 = (r_3 \oplus H_{SD_{id}})$. 4) TTP computes $Q_1 = H(1 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_3)$ and transmits $(r'_3, SH'_k, T'_{JWT}, Q_1)$ to NU.

- **Step 3:** $[NU \rightarrow TTP (NU_{A_{id}}, Q_2)]$: When obtaining $(r'_3, SH'_k, T'_{JWT}, Q_1)$, NU executes: 1) NU retrieves $r_3 = (r'_3 \oplus H_{SD_{id}})$. 2) NU retrieves $SH_k =$

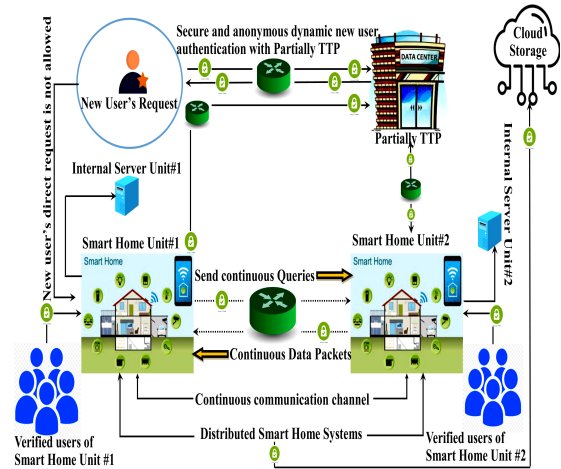


Figure 1: Our proposed generic distributed IoT architecture.

$(SH'_k \oplus r_3)$. 3) NU retrieves $T_{JWT} = S_{D_k}(T'_{JWT})_{SH_k}$.
 4) NU calculates $Q_2 = H(2 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_4)$ and transmits $(NU_{A_{id}}, Q_2)$ to TTP .

- **Step 4:** [$TTP \rightarrow NU (TTP_{A_{id}}, Q_3)$]: Upon receiving NU 's response, TTP verifies $Q_1 \stackrel{?}{=} Q_2$. If $Q_1 = Q_2$ is true, all the values ($r'_3 = r_3, SH'_k = SH_k, T'_{JWT} = T_{JWT}$) have been correctly retrieved. If $Q_1 \neq Q_2$, then it will directly discard the values and \perp the protocol. Assuming the response has been matched and TTP has verified the NU , TTP will transmit $Q_3 = H(3 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_5)$ and $TTP_{A_{id}}$ to complete the protocol.

4 SECURITY ANALYSIS

We prove theoretical analysis and semantic security as per (Chang and Le, 2015). We also demonstrate scyther results in Fig. 2 and Fig. 3 experimented on 100 runs with 10 patterns per claim which prove that our protocol is secure against typical security attacks.

ROR Model: The components of ROR model are as follows: i) **Participants** - u, p of main entities NU and TTP identified as Π^u_{NU}, Π^p_{TTP} . ii) **Partnering** - Π^p_{TTP} of TTP is partnering with Π^u_{NU} and vice-versa. The calculated one-time alias identity $NU_{A_{id}}$ is unique and anonymous for each session in which Π^u_{NU} is a participant. iii) **Freshness** - Assumes that for a given reveal query Π^p_{TTP} , if SH_k is not leaked by an \mathcal{A} , then Π^u_{NU}, Π^p_{TTP} is fresh. iv) **Adversary** - \mathcal{A} can access all communicated messages to perform malicious activities. The queries executed by an \mathcal{A} are: 1) Execute: Π^u, Π^p : It is modeled when an \mathcal{A} eavesdrops on communicated messages between NU and TTP . 2) Send: Π^u, msg : It is an active attack, where an \mathcal{A} transmits a msg to an instance Π^u and accordingly gets a revert from Π^u . 3) Reveal: Π^u : It reveals current SH_k between Π^u and partner Π^p to an \mathcal{A} . 4) Corrupt Π^u_{NU} : It enables an \mathcal{A} for obtaining all the secrets such as $NU_P, r_3, H_{SD_{id}}$ to leak current SH_k . 5) Test Π^u : It is a request by an \mathcal{A} to Π^u to guess a valid SH_k and Π^u replies within the probabilistic polynomial time such that it returns SH_k if $c' = 1$, or some other random value if $c' = 0$. 6) Hash $H(\cdot)$: A one-way hash function denoted as H is a random oracle accessible to an \mathcal{A} and all entities. 7) Semantic security SH_k : It is modeled for an \mathcal{A} to guess valid SH_k by executing test queries from random flipping. An \mathcal{A} wins only if value of $c' = c$. Event S_i is modeled if an \mathcal{A} wins the game. The semantic security of proposed protocol is defined as: $\mathbf{Adv}^{\mathcal{A}}_{PP} = |2\text{Prob}[S] - 1|$. The protocol is secure if, $\mathbf{Adv}^{\mathcal{A}}_{PP} \leq \epsilon$ for small $\epsilon > 0$.

Theorem 1. An \mathcal{A} running in polynomial time t

against our secure authentication protocol in a defined random oracle model. Let $D, q_h, q_{send}, H, |D|$ and $[\mathbf{Adv}^{\text{IND-CPA}}_{SIE, \mathcal{A}}(\Phi), \mathbf{Adv}^{\text{IND-CPA}}_{MLE, \mathcal{A}}(\Phi)]$ be uniformly distributed password dictionary with number of hash queries q_h , number of send queries q_{send} , H range of hash function and $|D|$ the size of D as the advantage of an \mathcal{A} breaking IND-CPA secure Φ . We state that $[\mathbf{Adv}^{\text{IND-CPA}}_{\mathcal{A}}(\Phi) = \mathbf{Adv}^{\text{IND-CPA}}_{SIE, \mathcal{A}}(\Phi), \mathbf{Adv}^{\text{IND-CPA}}_{MLE, \mathcal{A}}(\Phi)]$. Assuming no entity is compromised to have $\mathbf{Adv}^{\mathcal{A}}_{PP} \leq \frac{q^2 h}{|H|} + \frac{2q_{send}}{|D|}$.

Proof: To construct $G_i : [0, 4]$, where $i : [0, 4]$ is the sequence of games demonstrating the probability of an \mathcal{A} 's advantage to break the security and S_i is a semantic security event of our protocol. **G₀**: Illustrates an active attack by an \mathcal{A} choosing bit c of a coin at the beginning in random oracle model. We define this as: $\mathbf{Adv}^{\mathcal{A}}_{PP} = 2\text{Prob}[S_i] - 1$.

G₁: Illustrates an eavesdropping attack using execute query (Π^u, Π^p) to retrieve SH_k . The computation of SH_k is $TTP : SH'_k = (SH_k \oplus r_3)$, $TTP : T'_{JWT} = S_{E_k}(T_{JWT})_{SH_k}$, $TTP : r'_3 = (r_3 \oplus H_{SD_{id}})$ and $TTP : Q_1 = H(1 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_3)$. This requires an \mathcal{A} to calculate r_3 , which is secured under non-transmitted $H_{SD_{id}}$, to retrieve SH_k and T_{JWT} . Without possessing both the secrets, an \mathcal{A} has negligible probability of winning this game. We define this as: $\mathbf{Adv}^{\mathcal{A}}_{PP}[\text{Prob}(S_0)] = \mathbf{Adv}^{\mathcal{A}}_{PP}[\text{Prob}(S_1)]$.

G₂: Illustrates modification in game G_1 with q_{send} and H functions. An \mathcal{A} forwards a fabricated message to convince the honest party to accept. This causes an \mathcal{A} to check collisions in the hash digest by executing q_h . Our protocol incorporates collision-resistant $H(\cdot)$ function to safeguard $H_{SD_{id}} = H(NU_{SD_{id}})$, $TTP : r'_3 = (r_3 \oplus H_{SD_{id}})$, and $TTP : Q_1 = H(1 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_3)$. All secrets, identities and messages are appended with random numbers and timestamps to mitigate collisions using q_{send} and q_h queries. The result of birthday paradox is: $\mathbf{Adv}^{\mathcal{A}}_{PP}|\text{Prob}[S_1] - \text{Prob}[S_2]| \leq \frac{q^2_h}{(2^m|D|)}$.

G₃: Illustrates an \mathcal{A} using dictionary attacks to easily guess low-entropy passwords NU_P . To prevent such illegal access, our authentication system restricts multiple incorrect password attempts which is much smaller than $|D|$ in a random oracle. We define this as: $\mathbf{Adv}^{\mathcal{A}}_{PP} = |\text{Prob}[S_2] - \text{Prob}[S_3]| \leq \frac{q_{send}}{(2^m|D|)}$.

G₄: An \mathcal{A} intercepts NU smart-device after successfully gaining access to NU_P . An \mathcal{A} cannot derive SH_k and T_{JWT} even after gaining access to NU smart device due to non-transmission of long-term secret in the communication channel. The SH_k and T_{JWT} are secured under symmetric encryption cipher Φ . We state that Φ is IND-CPA secure as per Definition 1. We define this as: $\mathbf{Adv}^{\mathcal{A}}_{PP} = |\text{Prob}[S_3] - \text{Prob}[S_4]| \leq$

$Adv_{\mathcal{A}}^{\text{IND-CPA}}(\Phi)(l)$. Finally after computing $G_i; [0, 4]$, an \mathcal{A} guesses bit c of a coin to win this game after launching a test query $Prob[s_4] = \frac{1}{2}$. Thus, we obtain

$$Adv_{PP}^{\mathcal{A}} \leq \frac{q_h^2}{|H|} + \frac{q_{send}^2}{2^{m-1} \cdot |D|} + 2Adv_{\mathcal{A}}^{\text{IND-CPA}}(\Phi)(l). \blacksquare$$

Theorem 2. *Our proposed protocol preserves confidentiality, authenticity and anonymity.*

Proof: A new user's $NU_{SD_{id}}$ is preregistered and independently computed on both the sensing modules such that, $H_{SD_{id}} = H(NU_{SD_{id}})$. Also, our robust security design will enable TTP to auto-update SH_k while brute forcing 128 bit symmetric key which takes $5.784e+35$ ns. Non-transmission of long-term secret $H_{SD_{id}}$ prevents an \mathcal{A} to retrieve data blocks such as $TTP: SH'_k = (SH_k \oplus r_3)$, $TTP: T'_{JWT} = S_{E_k}(T_{JWT})_{SH_k}$, $TTP: r'_3 = (r_3 \oplus H_{SD_{id}})$. This will increase computational hardness for an \mathcal{A} to prove $Q_1 = H(1 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_3)$ and $Q_2 = H(2 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_4)$. Therefore, this will manipulate an \mathcal{A} with invalid SH_k key values. Furthermore, we generate one-time dynamic alias identity over an encrypted identity such as $TTP: TTP_{Aid} = S_{E_k}(TTP_{id})_{TTP_{MK}}$ and $NU: NU_{Aid} = S_{E_k}(NU_{id})_{H_{NU_p}}$ to provide sufficient randomness and anonymity for each new user. Hence, we achieve stated objective of theorem 2. \blacksquare

```

1 hashfunction H;
2 const k:Function;
3 secret R3,R3',SHk,m1,FNUid,TJWT: Nonce;
4 macro m1= {H(I,NUid)}k(I,S);
5 macro m2= {H(I,NUid,NUAid,R3)}k(I,S);
6 macro m3={H(S,{SHk}R3), (S,{TJWT}SHk), (S, {R3}m1)}k(I,S);
7
8 protocol SDUAP (I,S)
9
10 {
11     role I
12     {
13         const NUAid: Data;
14         fresh NUp: Nonce;
15         fresh FNUid: Nonce;
16         var SHk:Nonce;
17         var TJWT: Nonce;
18         const NUDid: Ticket;
19     }
20
21     send_1 (I,S,NUAid,H(NUp,NUAid,R3));
22     recv_2 (S,I, H(FNUid,NUAid, {I,S}m2));
23     send_3 (I,S,NUAid, H(FNUid,NUAid, {I,S}m2));
24     recv_4 (S,I, {I,S}m3);
25     send_5 (I,S,H(SHk,R3,TJWT));
26 }
27
28 role S
29 {
30     const NUAid: Data;
31     var NUp: Nonce;
32     fresh FNUid: Nonce;
33     fresh SHk: Nonce;
34     fresh TJWT: Nonce;
35     const NUDid: Ticket;
36 }
37
38     recv_1 (I,S,NUAid,H(NUp,NUAid,R3));
39     send_2 (S,I, H(FNUid,NUAid, {I,S}m2));
40     recv_3 (I,S,NUAid, H(FNUid,NUAid, {I,S}m2));
41     send_4 (S,I, {I,S}m3);
42     recv_5 (I,S,H(SHk,R3,TJWT));
43 }

```

Figure 2: Code snippet in .spdl using scyther.

Theorem 3. *Our proposed protocol safeguards against impersonation and replay attacks.*

Proof: The computational hardness in deriving $[TTP: r'_3 = (r_3 \oplus H_{SD_{id}})]$ will increase the computational complexity in deciphering T_{JWT} with SH_k due to dynamic SH_k updation that is directly proportional to T_{JWT} session expiry time. Since time-stamps are

SDUAP	I	SDUAP,I1	Secret NUDid	Ok	Verified	No attacks.
		SDUAP,I2	Secret FNUid	Ok	Verified	No attacks.
		SDUAP,I3	Secret NUp	Ok	Verified	No attacks.
		SDUAP,I4	Secret NUAid	Ok	Verified	No attacks.
		SDUAP,I5	Secret TJWT	Ok	Verified	No attacks.
		SDUAP,I6	Secret SHk	Ok	Verified	No attacks.
		SDUAP,I7	Alive	Ok	Verified	No attacks.
		SDUAP,I8	Weakagree	Ok	Verified	No attacks.
		SDUAP,I9	Niagree	Ok	Verified	No attacks.
		SDUAP,I10	Nisynch	Ok	Verified	No attacks.
	S	SDUAP,S1	Secret NUDid	Ok	Verified	No attacks.
		SDUAP,S2	Secret TJWT	Ok	Verified	No attacks.
		SDUAP,S3	Secret SHk	Ok	Verified	No attacks.
		SDUAP,S4	Secret FNUid	Ok	Verified	No attacks.
		SDUAP,S5	Secret NUAid	Ok	Verified	No attacks.
		SDUAP,S6	Secret NUp	Ok	Verified	No attacks.
		SDUAP,S7	Alive	Ok	Verified	No attacks.
		SDUAP,S8	Weakagree	Ok	Verified	No attacks.

Figure 3: Scyther simulation results for security verification.

appended with data blocks $TTP: F_{NU_{id}} = H(NU_{Aid} \parallel H_{NU_p} \parallel H_{SD_{id}} \parallel t_1)$, $NU: F'_{NU_{id}} = H(NU_{Aid} \parallel H_{NU_p} \parallel H_{SD_{id}} \parallel t_2)$, $TTP: Q_1 = H(1 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_3)$ and $NU: Q_2 = H(2 \parallel r_3 \parallel SH_k \parallel T_{JWT} \parallel t_4)$. If, $t' - t \leq \delta t$, where t' is data block received time and t is data block generation time. If time difference is less than δt the data block is accepted else, rejected. Hence, we achieve stated objective of theorem 3. \blacksquare

5 PERFORMANCE ANALYSIS

Table 2 and Table 3 present empirical analysis with $\mathcal{P1}$:(Das et al., 2020), $\mathcal{P2}$:(Kang et al., 2016), $\mathcal{P3}$:(Khan et al., 2011), $\mathcal{P4}$:(Saeed et al., 2018) and $\mathcal{P5}$:(Zhang et al., 2019). We assume communication and computational parameters such as hashing: $T_H = 0.0005$ sec of 160 bit, Symmetric encryption/decryption: $T_{E/D} = 0.0087$ sec, shared key, random number, JWT and pseudo random function: $T_{RF} = 0.0003$ sec of 128 bits, XOR: $T_X = 0.002$ sec, ECC multiplication: $T_M = 0.063075$ sec of 320 bits, identities and password of 64 bits, and timestamps of 16 bits. Energy consumption is calculated with $3(W)$ of power as ($E_{mJ} = Power_W \times Time_{sec}$). As observed our performance is superior to $\mathcal{P2}$, $\mathcal{P4}$ and $\mathcal{P5}$. $\mathcal{P1}$ and $\mathcal{P3}$ have lower costs and energy consumption than ours. The minimal increase in overall performance is acceptable given that our protocol achieves dynamic system expansion, mitigates system restarting and cryptographic wastage, and preserves robust security with effective privacy.

Table 2: Computation and communication costs with energy consumption.

Protocols	User node	Gateway node	Sensor node	Total running cost	Messages	Total cost	Energy
$P1$	$2T_M + 2T_{RF}$	—	$2T_M + 2T_{RF}$	$4T_M + 4T_{RF} = 0.0264 \text{ sec.}$	3	0384 bits	763.6 mJ
$P2$	$2T_E + T_D + 2T_H + 2T_X$	$T_{E/D} + 2T_H + 3T_X$	$T_{E/D} + 3T_H + 4T_X$	$4T_E + 3T_D + 7T_H + 9T_X = 0.0825 \text{ sec.}$	4	1856 bits	247.2 mJ
$P3$	$2T_H + T_X$	—	$10T_H + 9T_X$	$12T_H + 10T_X = 0.026 \text{ sec.}$	4	1200 bits	78 mJ
$P4$	$3T_M + T_E$	—	$3T_M$	$6T_M + T_E = 0.38715 \text{ sec.}$	3	2464 bits	1166.1 mJ
$P5$	$7T_H + T_D$	—	$9T_H + T_D + 2T_E$	$16T_H + 2T_E + 2T_D = 0.04285 \text{ sec.}$	4	1600 bits	128.4 mJ
Ours	$3T_H + T_D + 2T_X$	—	$2T_H + T_E + 2T_X$	$5T_H + T_{E/D} + 4T_X = 0.0279 \text{ sec.}$	4	1088 bits	83.7 mJ

Table 3: Features comparison.

Features	$P1$	$P2$	$P3$	$P4$	$P5$	Ours
Dynamic scalability	×	×	×	×	×	✓
Anonymity	✓	×	✓	✓	✓	✓
Robust security	✓	×	×	✓	✓	✓
No complete rights policy	×	×	×	×	×	✓
Symmetric key cryptography	×	×	✓	×	✓	✓
Formal analysis using ROR model	×	×	×	✓	✓	✓
Security verification	×	×	×	×	×	✓
Safe against impersonation attacks	✓	✓	✓	✓	✓	✓
Safe against replay attacks	✓	✓	✓	✓	✓	✓
IND-CPA secure	×	×	×	✓	✓	✓
Pairing-free scheme	✓	×	×	✓	✓	✓
Efficient token updation	×	×	×	×	×	✓
Efficient shared key updation	×	×	×	×	×	✓
Number of factors used	2	2	2	2	2	2

6 CONCLUDING REMARKS

In this paper, we propose privacy preserving authentication protocol for dynamic system expansion with partially TTP. Our protocol achieves superior trade-off between robust security and effective privacy by adopting one-time alias identity with dynamic JWT and shared key updation during authentication. To achieve dynamic and anonymous scalability we mitigate complete rights policy and knowledge sharing with TTP. Empirical analysis demonstrates that our proposed protocol is light-weight with additional security features as compared to similar modeled schemes.

REFERENCES

Alcaide, A., Palomar, E., Montero-Castillo, J., and Ribagorda, A. (2013). Anonymous authentication for privacy-preserving iot target-driven applications. *computers & security*, 37:111–123.

Babbage, S., Catalano, D., Cid, C., de Weger, B., Dunkelmann, O., Gehrman, C., Granboulan, L., Lange, T., Lenstra, A. K., Mitchell, C., et al. (2009). Ecrypt yearly report on algorithms and key sizes. Technical report.

Chang, C.-C. and Le, H.-D. (2015). A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on wireless communications*, 15(1):357–366.

Chen, Y., Xu, W., Peng, L., and Zhang, H. (2019). Lightweight and privacy-preserving authentication protocol for mobile payments in the context of iot. *IEEE Access*, 7:15210–15221.

Das, M. L., Kumar, P., and Martin, A. (2020). Secure and privacy-preserving rfid authentication scheme for internet of things applications. *Wireless Personal Communications*, 110(1):339–353.

Gope, P. and Sikdar, B. (2018). Lightweight and privacy-preserving two-factor authentication scheme for iot devices. *IEEE Internet of Things Journal*, 6(1):580–589.

Kang, J., Park, G., and Park, J. H. (2016). Design of secure authentication scheme between devices based on zero-knowledge proofs in home automation service environments. *The Journal of Supercomputing*, 72(11):4319–4336.

Khan, M. K., Kim, S.-K., and Alghathbar, K. (2011). Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic id-based remote user authentication scheme’. *Computer Communications*, 34(3):305–309.

Lai, C., Li, H., Liang, X., Lu, R., Zhang, K., and Shen, X. (2014). Cpal: A conditional privacy-preserving authentication with access linkability for roaming service. *IEEE Internet of Things Journal*, 1(1):46–57.

Lin, X.-J., Sun, L., and Qu, H. (2015). Insecurity of an anonymous authentication for privacy-preserving iot target-driven applications. *computers & security*, 48:142–149.

Saeed, M. E. S., Liu, Q.-Y., Tian, G., Gao, B., and Li, F. (2018). Remote authentication schemes for wireless body area networks based on the internet of things. *IEEE Internet of Things Journal*, 5(6):4926–4944.

Trivedi, H. S. and Patel, S. J. (2020). Design of secure authentication protocol for dynamic user addition in distributed internet-of-things. *Computer Networks*, 178:107335.

Turkanović, M., Brumen, B., and Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad Hoc Networks*, 20:96–112.

Vijayakumar, P., Chang, V., Deborah, L. J., Balusamy, B., and Shynu, P. (2018). Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. *Future generation computer systems*, 78:943–955.

Wang, Y.-y., Liu, J.-y., Xiao, F.-x., and Dan, J. (2009). A more efficient and secure dynamic id-based remote user authentication scheme. *Computer communications*, 32(4):583–585.

- Wang, Z. (2018). A privacy-preserving and accountable authentication protocol for iot end-devices with weaker identity. *Future Generation Computer Systems*, 82:342–348.
- Zhang, L., Zhao, L., Yin, S., Chi, C.-H., Liu, R., and Zhang, Y. (2019). A lightweight authentication scheme with privacy protection for smart grid communications. *Future Generation Computer Systems*, 100:770–778.

