Physically Secure and Fog-Enabled Lightweight Authentication Scheme for e-textiles

We analyze the suggested approach's performance efficiency by examining parameters such as computational overhead, communication overhead, and security attributes.

A. COMPUTATIONAL OVERHEAD

To analyze the computational overhead of the proposed scheme, the time consumed by the important cryptographic operations such as the hash function (T_H), PUF (T_{PUF}), reverse fuzzy extractor (T_F), scalar multiplication (T_M) and symmetric cryptography (T_S) of the suggested protocols are considered in this section. The suggested approach is evaluated using Ubuntu 14.04 VMware with an Intel Core i5-8265U processor and 8-GB RAM system. The simulation work was carried out using the JCE library Pbc-05.14 and the computational overhead of different cryptographic operations, such as T_H, T_{PUF}, T_F, T_M, and T_S are calculated as 0.011 ms $(millisecond)$, 0.12 ms, 2.53 ms, 2.6 ms, and 0.041 ms respectively. Table 1 lists the computational overhead of various methods, and it ensures that the suggested approach consumes only 3.024 ms to establish a session key, whereas other related existing approaches, [24-27] consume 8.47 ms, 8.04 ms, 5.77 ms, and 15.79 ms as a communication overhead.

TABLE 1. Computational overhead of various schemes

Methods	eTK_i	FN_i	eT_j	Total
[24]	$2T_S + 8T_H + T_F$	$5T_S + 11T_H + T_F$	$2T_S + 6T_H + T_F + 2T_{PUF}$	$9T_S + 25T_H + 3T_F + 2T_{PUF} = 8.474ms$
[25]	$14T_H + 2T_F + T_{PUF}$	$8T_H$	$8T_H + T_F$	$30T_H + 3T_F + T_{PUF} = 8.04ms$
[26]	$T_S + 10T_H + T_F$	$4T_S + 9T_H$	$3T_S + 5T_H + T_F + T_{PUF}$	$8T_S + 24T_H + 2T_F + T_{PUF} = 5.772ms$
[27]	$3T_M + 6T_H$	$T_M + 6T_H$	$2T_M + 6T_H$	$6T_M + 18T_H = 15.798ms$
Suggested scheme	$15T_H$	$12T_H$	$7T_H + T_F + T_{PUF}$	$34T_H + T_F + T_{PUF} = 3.024ms$

B. COMMUNICATION OVERHEAD

The information communicated among the system entities to establish the session key is considered to analyze the communication overhead of the suggested approach. The bit length of the identity of the system entity, hash function, random number, PUF and block size of symmetric cryptography are 20 bytes, 4 bytes, 20 bytes, 16 bytes, and 16 bytes, respectively [28].

TABLE 2. Communication overhead of various schemes

Methods	No. of messages	Overhead (bytes)
[24]	4	356
[25]	5	360
[26]	6	456
[27]	4	372
Suggested scheme	4	276

The suggested approach communicates four messages such as $\{AID_{eU_i}, K_1, K_2, V_1\}$, $\{AID_{eU_i},\ K_3,\ K_4,\ V_2\}$, $\{K_5,\ V_3\}$ and $\{K_6,\ V_4\}$ to establish the session between eU_i and eT_j. Hence, the communication overhead of the suggested approach is computed as $80 + 116 + 40 + 60 = 276\ bytes$. Table 2 compares the communication overhead of the suggested approach with the existing competitive schemes [24-27]. The suggested approach consumes only 276 bytes as communication overhead, whereas the existing competitive schemes [24-27] consume 356 bytes, 360 bytes, 456 bytes, and 372 bytes, respectively.

C. STORAGE AND ENERGY COSTS

To provide a comprehensive evaluation of the proposed scheme, we include the analysis of storage and energy costs.

Storage Cost: The storage cost involves the amount of memory required to store the security parameters and cryptographic keys for each system entity (eTK_i and eT_j) in the proposed scheme.

Storage Requirements:

- e-Textile Tracker (eTK_i) : It calculates and stores the values $\{M_{eTK_i}, N_{eTK_i}, L_1, L_2, \sigma_{eTK_i}\}$ in the e-Textile Tracker such as a mobile phone. Total storage cost of e-Textile Tracker calculated as 20 + 20 + 16 + 16 + 20 = 92 bytes.
- **e-Textile** (eT_j)**:** It calculates and stores the values $\{h'_{eT_j}, \alpha_{eT_j}\}$ in the e-Textile. Total storage cost of e-Textile Tracker device calculated as 20 + 20 = 40 bytes.

The total storage cost for the proposed scheme is the sum of the storage costs for each entity: 92 bytes (eTK_i) + 40 bytes (eT_j) = 132 bytes.

Energy Costs: Energy costs involve the power consumption required to execute the cryptographic operations during the authentication process. The energy cost can be estimated based on the computational overhead and the energy consumption of each cryptographic operation.

The energy consumption for cryptographic operations is as follows: Hash function (T_H) is 3.5 µJ, PUF (T_{PUF}) is 8 µJ, Reverse fuzzy extractor (T_F) is 6 µJ, Scalar multiplication (T_M) is 9.5 µJ and Symmetric cryptography (T_S) is 4 µJ.

Using the computational overhead values and the energy consumption per operation, the total energy consumption for each entity is calculated as follows:

- e-Textile (eT_j): The computational overhead of eT_j is $7T_H + T_F + T_{PUF}$. The energy cost required for eT_j is calculated as (7×3.5) + 6 + 8 = 38.5 µJ. The total energy cost for the proposed scheme is: 52.5 µJ (eU_i) + 42 µJ (FN_i) + 38.5 µJ (eT_j) = 133 µJ
- e-Textile Tracker (eTK_i): The computational overhead of eU_i is $15T_H$. The energy cost required for eU_i is calculated as 15×3.5 = 52.5 µJ
- Fog Node (FN_i): The computational overhead of FN_i is $12T_H$. The energy cost required for FN_i is calculated as 2×3.5 = 42 µJ.