Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.019486
Article

Cryptanalysis of an Online/Offline Certificateless Signature Scheme for Internet of Health Things

Saddam Hussain[1], Syed Sajid Ullah[2,*], Mohammad Shorfuzzaman[3], Mueen Uddin[4] and Mohammed Kaosar[5]

[1]Department of Information Technology, Hazara University, Mansehra, 21120, KPK, Pakistan
[2]Department of Electrical and Computer Engineering, Villanova University, PA, USA
[3]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[4]Digital Science, Faculty of Science, Universiti Brunei Darussalam, Jln Tungku link, Gadong, BE1410, Brunei Darussalam
[5]Discipline of Information Technology, Media and Communications, College of Arts, Business, Law and Social Sciences (ABLSS), Murdoch University, 90 South Street, Murdoch, WA6150, Australia
*Corresponding Author: Syed Sajid Ullah. Email: sullah1@villanova.edu
Received: 15 April 2021; Accepted: 18 May 2021

Abstract: Recently, Khan et al. [An online-offline certificateless signature scheme for internet of health things," Journal of Healthcare Engineering, vol. 2020] presented a new certificateless offline/online signature scheme for Internet of Health Things (IoHT) to fulfill the authenticity requirements of the resource-constrained environment of (IoHT) devices. The authors claimed that the newly proposed scheme is formally secured against Type-I adversary under the Random Oracle Model (ROM). Unfortunately, their scheme is insecure against adaptive chosen message attacks. It is demonstrated that an adversary can forge a valid signature on a message by replacing the public key. Furthermore, we performed a comparative analysis of the selective parameters including computation time, communication overhead, security, and formal proof by employing Evaluation based on Distance from Average Solution (EDAS). The analysis shows that the designed scheme of Khan et al. doesn't have any sort of advantage over the previous schemes. Though, the authors utilized a lightweight hyperelliptic curve cryptosystem with a smaller key size of 80-bits. Finally, we give some suggestions on the construction of a concrete security scheme under ROM.

Keywords: Cryptanalysis; Internet of health things; online-offline signature

1 Introduction

The concept of an online/offline signature was first proposed in 1990 by Evan et al. [1]. The main idea is to divide the signature generation algorithm into two phases (i.e., online and offline phase). The signing algorithm performs the offline step to manage most of the heavy computations and stores without knowing the signed message. Once the signed message arrives, the signature algorithm runs the online step very fast and only light computations are required. Online offline signatures are more useful on some storage limited devices such as smart cards, wireless sensors, and RFID tags, as the offline step can be

done with a background computation during the device manufacturing process or whenever the device power is connected. There are numerous offline/online signature schemes [2–5], designed for different applications.

In 2008, Yu and Tate [3], presents three effective online/offline signature approaches. The authors claim that the given is formally secure in the standard model under the assumptions of RSA. Unfortunately, the given scheme is affected by high-cost consumptions i.e., computation time and communication overhead. Besides, Ma et al. [4], found that the first scheme of Yu and Tate [3], is not secure.

In 2010, Wu et al. [5], suggest an identity-based online/offline signature scheme under ROM using the hardness of bilinear pairing. Unfortunately, the given scheme is affected by high-cost consumptions due to the use of heavy pairing operation which makes it inefficient.

In 2020, Addobea et al. [6], suggest a certificateless online/offline signature scheme for mobile health devices under ROM using the hardness of bilinear pairing. Nonetheless, the given scheme also suffers from high-cost consumptions due to the use of heavy pairing operation that shows the inefficiency of the designed scheme for the resource-constrained devices of mobile health.

1.1 Motivation and Contribution

To minimize the cost consumptions, Khan et al. [7], recently presented a new certificateless online/offline signature scheme for IoHT under the hardness of hyperelliptic curve discrete logarithm problem. The authors also claimed that the given scheme was proven secure "against adaptive chosen-message" in the ROM. In this paper, we analyzed the formal security of Khan et al.'s scheme and proving its insecurity against "adaptive chosen-message and identity attacks". Furthermore, we suggest some comments on the formal security issues of the Khan et al. [7] scheme that should be considered while proposing a concrete security scheme. The following are some of our contributions.

- First, we proved the insecurity of Khan et al. [7] scheme against adaptive chosen message attacks.
- Then, we suggest a concrete construction of the given scheme.
- We performed a comparative analysis of the selective parameters including computation time, communication overhead, security, and formal proof based on Evaluation based on Distance from Average Solution (EDAS). The analysis shows that the designed scheme of Khan et al. doesn't have any sort of advantage over the previous schemes. For comparative analysis, we choose the same environment (hardware and software) and the same online-offline scheme with which the authors compared their scheme.

1.2 Organization of Paper

The rest of the paper is organized as; Section 2 presents the definition for HDLP, Section 3 reviews the construction of the Khan et al. scheme. Section 4, shows the insecurity and Section 5 presents formal correction. Section 6 shows the cost efficiency, while Section concludes our research work.

2 Definition 1: Hyperelliptic Curve Discrete Logarithm Problem (HDLP) Assumptions

- Let $\mathfrak{O}$, $\mathfrak{E}$ $\{1, 2, 3, \ldots n-1\}$ and $\mathcal{R} = \mathfrak{O}.\ \mathcal{D}$, then finding $\mathfrak{O}$ and $\mathcal{R}$ is known as HDLP.

3 Review of Khan et al. Scheme

Here we present the constructions of the Khan et al. [7] scheme. Additionally, the notations used in the constructions are listed in Tab. 1.

Table 1: List of notations

S/N	Notation	Description
1	η	Security parameter
2	$\hbar c$	Hyperelliptic curve
3	$\mathcal{D}$	Divisor of hc
4	$\mathcal{Q}$	Master private key
5	$\mathcal{K}$	Master public key
6	ψ	Global parameter set
7	id_s, id_r	Identities of sender and receiver
8	$\mathcal{S}$	Signature
9	N_s, N_r	Private key of sender and receiver
10	$\mathcal{Z}_s, \mathcal{Z}_r$	Public key of sender and receiver
11	$H_x, H_y, H_z.$	Hash functions
12	$\mathcal{A}_{dv}$	Adversary

Setup:

- Given the security parameter η, the KGC select,
- A hyperelliptic curve ($\hbar c$) with field $f(n)$, where the size of $n \geqslant 2^{80}$
- Devisor ($\mathcal{D}$) from $\hbar c$
- Hash functions H_x, H_y and H_z.
- It also picks $\mathcal{Q} \in \{1, 2, 3, \ldots\ldots n-1\}$ as a master key and computes the public key as $\mathcal{K} = \mathcal{Q}.\mathcal{D}$.
- Finally, produces a public parameter set $\psi = \{\mathcal{K}, H_x, H_y, H_z, \mathcal{D}, \hbar \boldsymbol{c}\}$ $n \geqslant 2^{80}$.

Set Secret value:

The participating entities with identity id_i picks $l_i \in \{1, 2, 3, \ldots\ldots n-1\}$ as a secret value and computes V_i=$l_i.\mathcal{D}$ as a public key.

Set Partial private key:

For an entity with identities id_i the KGC picks $\vartheta_i \in \{1, 2, 3, \ldots\ldots n-1\}$, computes $\mu_i = \vartheta_i.\mathcal{D}$, calculates $\mathcal{W}_i = \vartheta_i + \mathcal{Q}H_x(id_i, V_i, \mu_i)$, and send $\Gamma_i = (\mathcal{W}_i, \mu_i)$ to the entities with id_i using a secure channel.

Set Private key:

The entities, with identity id_i sets $N_i = (\Gamma_i, l_i)$ of its private key.

Set Public key:

The entities, with identity id_i sets $\mathcal{Z}_i = (V_i, \mu_i)$ of its public key.

Signature Generation:

The computations of the sender are divided into two steps;

Offline Step:

Executed on the server equipped with high resources.

- It picks $\mathcal{A} \in \{1, 2, 3, \ldots\ldots n-1\}$ and computes $t = \mathcal{A}.V_s$

- Compute $\mathcal{P} = H_y(id_s, \mu_s, m, t)$ and $\mathcal{X} = H_z(id_s, V_s, m, t)$
- Gives ($\mathcal{A}$, t, $\mathcal{P}$, $\mathcal{X}$) to the sensor nodes

Online phase:

- Compute $\mathcal{S} = l_s.\mathcal{A} - (l_s.\mathcal{X} + \mathcal{P}.\mathcal{W}_s)$
- Set $\phi = (t, \mathcal{S})$ as a signature and send it to the receiver

Verification:

Upon reception ϕ, the receiver can verify $\mathcal{S}$ as follows

- Compute $\mathcal{P} = H_y(id_s, \mu_s, m, t)$ and $\mathcal{X} = H_z(id_s, V_s, m, t)$
- checks if $\mathcal{S}.\mathcal{D} = t.\mathcal{X}V_s - \mathcal{P}(\mu_s + H_x(id_s, V_s, \mu_s)\mathcal{K})$ hold.

4 Analysis of Khan et al. Scheme

An $\mathcal{A}_{dv}$ can forge the valid signature on a message (m) by replacing a public key ($\mathcal{K}$).

- Subsequently after obtaining the (id_s, μ_s), the $\mathcal{A}_{dv}$ randomly choose $\mathcal{W}_{\mathcal{A}_{dv}}$, $l_{\mathcal{A}_{dv}} \in \{1, 2, 3, \ldots\ldots n-1\}$, computes $V_{\mathcal{A}_{dv}} = l_{\mathcal{A}_{dv}}\mathcal{D}$, $H_x(id_s, \mu_s, V_{\mathcal{A}_{dv}})\mathcal{K}' = \mathcal{W}_{\mathcal{A}_{dv}}\mathcal{D} - \mu_s), H_x^{-1}$ and replace the master public key ($\mathcal{K}$) with $\mathcal{K}'$ and id_sV_s with $V_{\mathcal{A}_{dv}}$ so that $\mathcal{W}_{\mathcal{A}_{dv}}\mathcal{D} = \mu_s + H_x(id_s, \mu_s, V_{\mathcal{A}_{dv}})\mathcal{K}'$ holds.
- $\mathcal{A}_{dv}$ set $(\Gamma_{\mathcal{A}_{dv}}, l_{\mathcal{A}_{dv}})$ as their full private key of signer where $\Gamma_{\mathcal{A}_{dv}} = (\mathcal{W}_{\mathcal{A}_{dv}}, \mu_s)$, and sets $(V_{\mathcal{A}_{dv}}, \mu_s)$ as their full public key.
- For signing a message (m), the $\mathcal{A}_{dv}$ select choose $\mathcal{A}_{\mathcal{A}_{dv}} \in \{1, 2, 3, \ldots\ldots n-1\}$, compute $t_{\mathcal{A}_{dv}} = \mathcal{A}_{\mathcal{A}_{dv}}V_{\mathcal{A}_{dv}}$, $\mathcal{P}_{\mathcal{A}_{dv}} = H_y(id_s, \mu_s, m, t_{\mathcal{A}_{dv}})$ and $\mathcal{X}_{\mathcal{A}_{dv}} = H_z(id_s, m, V_{\mathcal{A}_{dv}}, t_{\mathcal{A}_{dv}})$.

Finally, $\mathcal{A}_{dv}$ computes $\mathcal{S}_{\mathcal{A}_{dv}} = l_{\mathcal{A}_{dv}}\mathcal{A}_{\mathcal{A}_{dv}} - (\mathcal{X}_{\mathcal{A}_{dv}}l_{\mathcal{A}_{dv}} + \mathcal{P}_{\mathcal{A}_{dv}}\mathcal{W}_{\mathcal{A}_{dv}})$ and generate the signature $(\mathcal{S}_{\mathcal{A}_{dv}}, t_{\mathcal{A}_{dv}})$ on the given message m.

Because $t_{\mathcal{A}_{dv}} = \mathcal{A}_{\mathcal{A}_{dv}}V_{\mathcal{A}_{dv}} = \mathcal{A}_{\mathcal{A}_{dv}}l_{\mathcal{A}_{dv}}\ \mathcal{P}_{\mathcal{A}_{dv}} = H_y(id_s, \mu_s, m, t_{\mathcal{A}_{dv}})$ and $\mathcal{X}_{\mathcal{A}_{dv}} = H_z(id_s, m, V_{\mathcal{A}_{dv}}, t_{\mathcal{A}_{dv}})$

Thus, $\mathcal{S}_{\mathcal{A}_{dv}}\mathcal{D} = t_{\mathcal{A}_{dv}} - \mathcal{X}_{\mathcal{A}_{dv}}V_{\mathcal{A}_{dv}} - \mathcal{P}_{\mathcal{A}_{dv}}(\mu_s + H_x(id_s, V_{\mathcal{A}_{dv}}, \mu_s)\mathcal{K}')$.

Therefore, we argue that the produced signature can pass through the verification successfully and the A can generate a signature.

5 Proof and Correction

While designing a signature protocol as designed by Khan et al. [7], the public key $\mathcal{K}$ needs to be hashed to eliminate the prospect of this type of forgery. The correction with formal proof is given below.

- While executing partial private key extraction in Khan et al. [7], if the $\mathcal{K}$ is hashed in H_x, the private part $\mathcal{W}_i$ is computed as $\mathcal{W}_i = \vartheta_i + \mathcal{Q}H_x(id_i, V_i, \mu_i, \mathcal{K})$, so a user can authenticate their tuple of the partial private key $(\mathcal{W}_i, \mu_i)$, if $\mathcal{A}_{dv}$ tries to forge the signature as described in Khan et al. scheme, it then randomly pick $\mathcal{W}_{\mathcal{A}_{dv}}$, $l_{\mathcal{A}_{dv}} \in \{1, 2, 3, \ldots n-1\}$, computes $l_{\mathcal{A}_{dv}}\mathcal{D}, H_x(id_i, \mu_i, V_i, \mathcal{K}), \mathcal{K}' = (\mathcal{W}_{\mathcal{A}_{dv}}\mathcal{D} - \mu_s), H_x^{-1}$ and replace the master public key $\mathcal{K}$with $\mathcal{K}'$ and id_sV_s with $V_{\mathcal{A}_{dv}}$.
- On verification, one can prove the equation $\mathcal{W}_i = \vartheta_i + \mathcal{Q}H_x(id_i, V_i, \mu_i, \mathcal{K})$ $\mathcal{W}_{\mathcal{A}_{dv}}\mathcal{D} = V_s + H_x(id_s, \mu_s, V_{\mathcal{A}_{dv}}, \mathcal{K}'), \mathcal{K}'$, which cannot be held. Hence, we can claim that forgery is not possible.

6 Efficiency

In this section, we evaluate the performance of our cryptanalysis in comparison with Khan et al. [7]. For our comparative analysis, we adopt the running time of costly mathematical operations from [8] and [9]. Here, we only consider the operations that are used in the particular scheme of Khan et al. [6]. According to [8] and [9], the cost of a single pairing-based point multiplication (PB_{ML}) is 4.31 milliseconds, the cost of bilinear pairing (B_{Pairing}) is 14.90 milliseconds, the cost of exponentiation (E_{PO}) is 1.25 milliseconds and the cost of a single HCDM is approximately 0.48 milliseconds [8,9]. The total computation cost of signing in the Khan et al. [7] scheme is 4 HCDM and the total computation cost of verification is 3 HCDM.

Note: Here we consider the same schemes with which Khan et al. [7] perform the comparative analysis in terms of computation time and communication overhead. Tab. 2, shows cost analysis of the selected schemes.

Table 2: Cost analysis of the selected schemes

Schemes	Signing time	Verifying time	Total time (ms)	Signature length
Yu and Tate Scheme-I [3]	$1E_{PO} + 3PB_{ML}$	$3E_{PO} + 4PB_{ML}$	$4E_{PO} + 7PB_{ML} = 35.17$	$3\|G\| + \|_m\| = 4096$
Yu and Tate Scheme-II [3]	$2E_{PO} + 3PB_{ML}$	$3E_{PO} + 3PB_{ML}$	$5E_{PO} + 6PB_{ML} = 32.11$	$3\|G\| + \|_m\| = 4096$
Wu et al. [5]	$3PB_{ML}$	$2B_{\text{Pairing}} + 2PB_{ML}$	$2B_{\text{Pairing}} + 5PB_{ML} = 51.41$	$3\|G\| + \|_m\| = 4096$
Addobea et al. [6]	$3PB_{ML}$	$3B_{\text{Pairing}} + 4PB_{ML}$	$3B_{\text{Pairing}} + 7PB_{ML} = 74.93$	$3\|G\| + \|_m\| = 4096$
Khan et al. [7]	4 HCDM	3 HCDM	7 HCDM = 3.36	$2\|_n\| + \|_m\| = 1184$

6.1 Computation Time

- According to Khan et al. [7] the computation time of Yu and Tate [3], is; $1E_{PO} + 3PB_{ML}$ in the signing phase while $3E_{PO} + 4PB_{ML}$ in the Verifying phase.
- The computation time of Yu and Tate [3] scheme 2 is; $2E_{PO} + 3PB_{ML}$ in the signing phase while $3E_{PO} + 3PB_{ML}$ in the Verifying phase.
- The computation time of Wu et al. [5] scheme is; $3PB_{ML}$ in the signing phase while $2B_{\text{Pairing}} + 2PB_{ML}$ in the Verifying phase.
- The computation time of Addobea et al. [6] scheme is; $3PB_{ML}$ in the signing phase while $3B_{\text{Pairing}} + 4PB_{ML}$ in the Verifying phase.
- Similarly, the computation time of Khan et al. [7] scheme is; 4 HCDM in the signing phase while 3 HCDM in the Verifying phase.

6.2 Communication Overhead

- According to Khan et al. [7], the communication overhead of Yu and Tate Scheme-I [3] is; $3|G| + |_m|$.
- The communication overhead of Yu and Tate Scheme-II [3] scheme 2 is; $3|G| + |_m|$.
- The communication overhead of Wu et al. [5] scheme is; $3|G| + |_m|$.
- The communication overhead of Addobea et al. [6] scheme is; $3|G| + |_m|$.
- Similarly, the communication overhead of Khan et al. [7] scheme is; $2|_n| + |_m|$.

6.3 Comparison With Our Cryptanalysis

- The total computation cost of our cryptanalysis is; $7\,(\text{HCDM}) = 7(0.48) = 3.36\,ms$
- The total computation cost of the Khan et al. [7] scheme is; $7\,(\text{HCDM}) = 7(0.48) = 3.36\,ms$

Findings

As we have seen from the aforementioned discussion, Khan et al. [7], perform an analysis of the respective scheme based on two parameters, i.e., computation time and communication overhead. However, these two parameters do not give us a clear advantage of Khan et al. [7], over the others. therefore, we consider four parameters for the performance analysis such as computation time, communication overhead, security, and formal proof respectively. Furthermore, we adopt the technique of EDAS for the performance analysis of the chosen parameters in Section 6.4 below.

6.4 Evaluation based on Distance from Average Solution (EDAS)

In this section, we adopt the multi-criteria decision-making method also known as Evaluation based on Distance from Average Solution (EDAS) [10–13]. The method is considered very useful when we have some conflicting criteria [14,15]. Different performance parameters are identified in the literature are considered for our comparative analysis including computation time, communications overhead, security, and formal proof as shown in Tab. 3. On the other hand, for evaluation, the cross EDAS method is used to extract the cross effective values among the selected schemes based on the chosen parameters. The assessment score (α) is used to obtain the ranking among the selected schemes and to calculate the positive distance from average ($\mathcal{P}_d$) and negative distance from average ($\mathcal{N}_d$) [16,17]. The performance matrices of the selected schemes are shown in Tab. 3.

Table 3: The performance matrices of the selected schemes

Weightage	0.3	0.3	0.2	0.2
Schemes	Total computation Time	Communication overhead	Security	Formal proof (ROM/standard model)
Yu and Tate Scheme-I [3]	35.17	4096	0	1
Yu and Tate Scheme-II [3]	32.11	4096	1	1
Wu et al. [5]	51.41	4096	1	0
Addobea et al. [6]	74.93	4096	1	0
Khan et al. [7]	3.36	1184	0	0
Average	39.396	3513.6	0.6	0.4

Step-I:

Calculate the average solution (ϕ) according to the selected criteria shown below.

$$(\phi) = [\phi_b]_{1\times\beta} \tag{1}$$

Where,

$$(\phi) = \frac{\sum_{i=1}^{y} X_{ab}}{y} \tag{2}$$

The aggregate calculation of the aforementioned Eqs. (1) and (2) can be obtained as an average solution (ϕ) as shown in Tab. 3.

Step-II:

In this particular step, the positive distance from average is calculated using the following equations

$$P_{dav} = \left[(P_{dav})_{ab}\right]_{\beta\times\beta} \tag{3}$$

If the b^{th} scenario is favorable than

$$(P_{dav})_{ab} = \frac{\mathcal{MAX}(0, (Ave_b - X_{ab}))}{Ave_b} \tag{4}$$

If less favorable then

$$(P_{dav})_{ab} = \frac{\mathcal{MAX}(0, (X_{ab} - Ave_b))}{Ave_b} \tag{5}$$

In the above-mentioned equations P_{dav} denote the positive distance from the average solution. The results obtained are shown in Tab. 4.

Table 4: Comparative analysis of positive distance from average (P_{dav})

Schemes	Total computation Time	Communication overhead	Security	Formal proof (ROM/ standard model)
Yu and Tate Scheme-I [3]	0.107269774	0	0	1.5
Yu and Tate Scheme-II [3]	0.184942634	0	0.666666667	1.5
Wu et al. [5]	0	0	0.666666667	0
Addobea et al. [6]	0	0	0.666666667	0
Khan et al. [7]	0.914712154	0.663023679	0	0

Step-III

In this particular step, the negative distance from average (N_{dav}) is calculated using the following equations

$$(N_{dav}) = \left[(N_{dav})_{ab}\right]_{\beta\times\beta} \tag{6}$$

If the b^{th} scenario is favorable than

$$(N_{dav})_{ab} = \frac{\mathcal{MAX}(0, (Ave_b - X_{ab}))}{Ave_b} \tag{7}$$

If less favorable then

$$(N_{dav})_{ab} = \frac{\mathcal{MAX}(0, (X_{ab} - Ave_b))}{Ave_b} \tag{8}$$

In the above-mentioned equations $(N_{dav})_{ab}$ denote the positive distance from the average solution. The results obtained are shown in Tab. 5.

Table 5: Comparative analysis of negative distance from average (N_{dav})

Schemes	Total computation Time	Communication Overhead	Security	Formal proof (ROM/ standard model)
Yu and Tate Scheme-I [3]	0	0.16575592	1	0
Yu and Tate Scheme-II [3]	0	0.16575592	0	0
Wu et al. [5]	0.304954818	0.16575592	0	1
Addobea et al. [6]	0.901969743	0.16575592	0	1
Khan et al. [7]	0	0	1	1

Step-IV:

In this step, the weighted sum of the positive distance ($\mathcal{P}_d$) is calculated using the following equation. The results obtained are shown in Tab. 6.

Table 6: Analysis of $(WS_{\mathcal{P}_d})_a$ based on positive distance

Schemes	Total computation Time	Communication Overhead	Security	Formal proof (ROM/ Standard Model)	$(\mathbf{WS}_{\mathcal{P}_\mathbf{d}})_\mathbf{a}$
Yu and Tate Scheme-I [3]	0.032180932	0	0	0.3	0.332180932
Yu and Tate Scheme-II [3]	0.05548279	0	0.133333333	0.3	0.488816123
Wu et al. [5]	0	0	0.133333333	0	0.133333333
Addobea et al. [6]	0	0	0.133333333	0	0.133333333
Khan et al. [7]	0.274413646	0.198907104	0	0	0.47332075

$$(WS_{\mathcal{P}_d})_a = \sum_{b=1}^{y} \lambda_b (\mathcal{P}_d)_{ab} \tag{9}$$

Step-V:

In this step, the weighted sum of the negative distance ($\mathcal{P}_d$) is calculated using the following equation. The results obtained are shown in Tab. 7.

Table 7: Weighted negative distance from average

Schemes	Total Computation Time	Communication Overhead	Security	Formal proof (ROM/ Standard Model)	$\left(\mathbf{WS}_{\mathcal{N}_d}\right)_{\mathbf{a}}$
Yu and Tate Scheme-I [3]	0	0.049726776	0.2	0	0.249726776
Yu and Tate Scheme-II [3]	0	0.049726776	0	0	0.049726776
Wu et al. [5]	0.091486445	0.049726776	0	0.2	0.341213221
Addobea et al. [6]	0.270590923	0.049726776	0	0.2	0.520317699
Khan et al. [7]	0	0	0.2	0.2	0.4

$$\left(WS_{\mathcal{N}_d}\right)_a = \sum_{b=1}^{y} \lambda_b (\mathcal{N}_d)_{ab} \tag{10}$$

Step-VI:

In this step, the calculated scores obtained from $(WS_{\mathcal{P}_d})_a \& \left(WS_{\mathcal{N}_d}\right)_a$ are normalized as follows,

$$\mathcal{N}(WS_{\mathcal{P}_d})_a = \frac{(WS_{\mathcal{P}_d})_a}{\mathcal{MAX}_a\left((WS_{\mathcal{P}_d})_a\right)} \tag{11}$$

$$\mathcal{N}\left(WS_{\mathcal{N}_d}\right)_a = 1 - \frac{\left(WS_{\mathcal{N}_d}\right)_a}{\mathcal{MAX}_a\left(\left(WS_{\mathcal{N}_d}\right)_a\right)} \tag{12}$$

Step-VII:

In this step, we calculate the appraisal score of all the selected schemes as follows,

$$\psi_a = \frac{1}{2}\left(\mathcal{N}(WS_{\mathcal{P}_d})_a - \mathcal{N}\left(WS_{\mathcal{N}_d}\right)_a\right) \tag{13}$$

Where $0 \preceq \psi_a \succeq 1$.

The result of ψ_a is determined using aggregate score values of the $\mathcal{N}WS_{\mathcal{P}_d} \& \mathcal{N}WS_{\mathcal{N}_d}$.

Step-VII:

In this step, we calculate a sequence of activities to our measurement of evaluation scores (ψ) and determines the ranking of the selected schemes. The results suggest that the best ranking solution has a

higher ψ compared to the other. Therefore, in the following Tab. 8, the scheme of Yu and Tate [3] Scheme 2 has the highest evaluation scores (ψ). So, the last calculated rank result is shown in Tab. 8.

Table 8: Ranking based on performance

Schemes	$(\mathbf{WS}_{\mathcal{P}_d})_a$	$(\mathbf{WS}_{\mathcal{N}_d})_a$	$\mathcal{N}(\mathbf{WS}_{\mathcal{P}_d})_a$	$\mathcal{N}(\mathbf{WS}_{\mathcal{N}_d})_a$	$\boldsymbol{\psi}_a$	Ranking
Yu and Tate Scheme-I [3]	0.332180932	0.249726776	0.679562143	0.52004943	0.599805787	2
Yu and Tate Scheme-II [3]	0.488816123	0.049726776	1.000000001	0.904429974	0.952214988	1
Wu et al. [5]	0.133333333	0.341213221	0.272767871	0.344221383	0.308494627	4
Addobea et al. [6]	0.133333333	0.520317699	0.272767871	2.06368E-10	0.136383936	5
Khan et al. [7]	0.47332075	0.4	0.9683002	0.231238913	0.599769557	3

6.5 Lesson Learned

From the aforementioned evaluation, we conclude that the designed scheme of Khan et al. [7] is efficient in terms of computation time and communication overhead. However, the given is insecure against adaptive chosen message attacks. Further, the proposed scheme of Khan et al. [7] is claimed to be secure under ROM. On the other hand, the given scheme of Yu and Tate [3] Scheme 2 is formally secured under the standard model. Though the given scheme has some limitations in terms of cost efficiencies but secure and proved in the standard model.

7 Conclusion and Future Work

Recently, Khan et al. presented a new certificateless online/offline signature scheme for the Internet of Health Things (IoHT) to fulfill the authenticity requirement for the resource-constrained environment of (IoHT) devices. The authors claim that the newly proposed scheme is secure against Type-I adversary under the Random Oracle Model (ROM). Unfortunately, their scheme is insecure against adaptive chosen message attacks. It is demonstrated that an adversary can forge a valid signature on a message by replacing the public key. Furthermore, we performed a comparative analysis of the selective parameters including computation time, communication overhead, security, and formal proof by employing Evaluation based on Distance from Average Solution (EDAS). The analysis shows that the designed scheme of Khan et al. doesn't have any sort of advantage over the previous schemes. Though, the authors utilized a lightweight hyperelliptic curve cryptosystem with a smaller key size of 80-bits. Finally, we give some suggestions on the construction of a concrete security scheme under ROM. Soon, we intend to improve the security of Khan et al. under the standard model.

Acknowledgement: The authors would like to thank Taif University Researchers Supporting Project number (TURSP-2020/79), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project number (TURSP-2020/79), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest.

References

[1] S. Even, O. Goldreich and S. Micali, "On-line/off-line digital signatures," *Advances in Cryptology—CRYPTO' 89 Proceedings*, vol. 435, pp. 263–275, 2001.

[2] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," *Advances in Cryptology-CRYPTO*, vol. 2139, pp. 355–367, 2001.

[3] P. Yu and S. R. Tate, "Online/offline signature schemes for devices with limited computing capabilities," in *Cryptographers' Track at the RSA Conference 2008 (CT-RSA 2008)*, San Francisco, CA, USA, vol. 4964, pp. 301–317, 2008.

[4] X. L. Ma, Z. W. Wang, L. Z. Gu and Y. Yang, "Remark on Yu et al.'s online/offline signature scheme in CT-RSA 2008," in *2009 Fifth International Conference on Information Assurance and Security*, Xi'an, China, vol. 2, pp. 719–720, 2009.

[5] T. Wu, Y. Chen and K. Lin, "ID-based online/offline signature from pairings," in *Proc. of the International Computer Symposium (ICS2010)*, Tainan City, Taiwan, pp. 198–203, 2010.

[6] A. A. Addobea, J. Hou and Q. Li, "MHCOOS: an offline- online certificateless signature scheme for m-health devices," *Security and Communication Networks*, vol. 2020, pp. 1–12, 2020.

[7] M. A. Khan, S. U. Rehman, M. I. Uddin, S. Nisar, F. Noor *et al.,* "An online-offline certificateless signature scheme for internet of health things," *Journal of Healthcare Engineering*, vol. 2020, pp. 1–10, 2020.

[8] S. Hussain, I. Ullah, H. Khattak, M. Adnan, S. Kumari *et al.,* "A lightweight and formally secure certificate based signcryption with proxy re-encryption (cbsre) for internet of things enabled smart grid," *IEEE Access*, vol. 8, pp. 93230–93248, 2020.

[9] S. S. Ullah, I. Ullah, H. Khattak, M. A. Khan, M. Adnan *et al.,* "A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with internet of things," *IEEE Access*, vol. 8, pp. 98910–98928, 2020.

[10] Y. Y. Li, J. Q. Wang and T. L. Wang, "A linguistic neutrosophic multi-criteria group decision-making approach with EDAS method," *Arabian Journal for Science and Engineering*, vol. 44, no. 3, pp. 2737–2749, 2019.

[11] A. Waheed, A. I. Umar, M. Zareei, N. Din, N. U. Amin *et al.,* "Cryptanalysis and improvement of a proxy signcryption scheme in the standard computational model," *IEEE Access*, vol. 8, pp. 131188–131201, 2020.

[12] L. A. Zadeh, "Fuzzy logic," *Computer*, vol. 21, no. 4, pp. 83–93, 1988.

[13] K. Tanaka, *An introduction to fuzzy logic for practical applications*. Vol. 6. New York: Springer-Verlag, pp. 1–148, 1997.

[14] N. A. Malik and M. Rai, "Enhanced secure and efficient key management algorithm and fuzzy with trust management for MANETs," in *Proc. of the Int. Conf. on Innovative Computing & Communications (ICICC)*, Singapore, Malaysia, pp. 1–8, 2020.

[15] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei and E. M. Mohamed, "A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks," *IEEE Access*, vol. 8, pp. 131397–131413, 2020.

[16] D. Zindani, S. R. Maity and S. Bhowmik, "Fuzzy-EDAS (evaluation based on distance from average solution) for material selection problems," in *Advances in Computational Methods in Manufacturing*, pp. 755–771, 2019.

[17] M. Yazdani, A. E. Torkayesh, E. D. S. Gonzalez and S. K. Otaghsara, "Evaluation of renewable energy resources using integrated shannon entropy-edas model," *Sustainable Operations and Computer*, vol. 1, pp. 35–42, 2020.