An Improved and Secured 3-Factor Authentication Scheme for WSN in IoT based Applications

Ramesh Sengodan
Presidency School of Computer Science and Engineering, Presidency University, Bangalore, Karnataka, India.
ramesh.sengodan@presidencyuniversity.in

Correspondence should be addressed to Ramesh Sengodan : ramesh.sengodan@presidencyuniversity.in

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202404088
Received 16 March 2024; Revised from 24 April 2024; Accepted 25 July 2024.
Available online 05 October 2024.

Abstract – Wireless Sensor Networks (WSN) has top-notch capacity for numerous domains of utility due to the potential to sense and apprehend unattended environments. IoT is playing an increasingly more essential position in clever healthcare, smart transportation and elegant grid using WSN. Therefore, challenges like privacy and data security associated with IoT wireless sensor networks because of sensor node being captured easily, consume less computing energy and low storage. Designing a secure authentication scheme will enable secure communication in WSN. Here, we proposed a improved three-factor authentication scheme for WSN utilizing biometric, password and smart card withstand against security attacks. Subsequently, by comparing the security, functional and performance parameters of our proposed scheme to the other schemes, our scheme provides better and efficient one. Therefore, our scheme is fairly workout in real time IoT applications involved in WSN scenario.

Keywords – Session Key, Internet of Things, Mutual Authentication, ECC, Biometric, Wireless Sensor Network.

I. INTRODUCTION

With quick advancement of network communication over wireless, intelligence of computer and embedded technology, Wireless Sensor Networks (WSN) are generally taken advantage of as far as colossal appropriateness and have been utilized in different fields like smart home, smart industries, health cares, military services, and environmental monitoring. Not at all as most of the traditional networks have, WSN itself had huge number of sensor nodes (SN) which are asset restricted in brilliant gadgets (things, sensors, and so forth) that may know about the surroundings and communications in not connected networks. The sensor node fetches the data, forward it to the remote user (U) for later processing over gateway node (GWN) through wireless channel. WSN is facing big problems such as limited energy, computing capacity, transmission in wireless, deployment in unattended network. Sensor nodes energy consumption is directly proportional to the space between the communique party and the sensor node. Users communicate with sensors of WSN to keep the identity and their privacy in a secure manner without any adversary's disturbances. In order to achieve the desirable security level as well as to maintain the user anonymity and un-traceability. Numerous fields, such as health, industry, education, agriculture, smart cities and homes, etc., heavily rely on the Internet of Things. One of the most significant uses of IoT, for instance, is integrating data processing and communication control in transportation systems. Using wireless sensors in the fleet management system, an IoT platform may continuously monitor the conditions and situations of the cargo and assets and notify management in specific cases, like a delay. To effectively address security concerns pertaining to privacy, secrecy, authentication, and integration, To address these needs, a multitude of key agreements and authentication schemes have been proposed; nevertheless, because to the difficulties in the networks operating on the internet platform, including IoT, their security remains vulnerable to a variety of attacks. . In the security, concern attackers initiate the potential threat such as eavesdropping, tampering or intercepting the transmission of the sensitive information. The significant that the user need be verified before get permission to acquire the distance sensor data. The only solution is user authentication scheme, which are mutually authenticate between user and sensor by establishing the shared session key away from WSN with less computation and withstand well-known attacks from the adversaries, not allow any unauthorized third parties involve in the communication. **Fig 1** shows an authentication model in wireless sensor network.

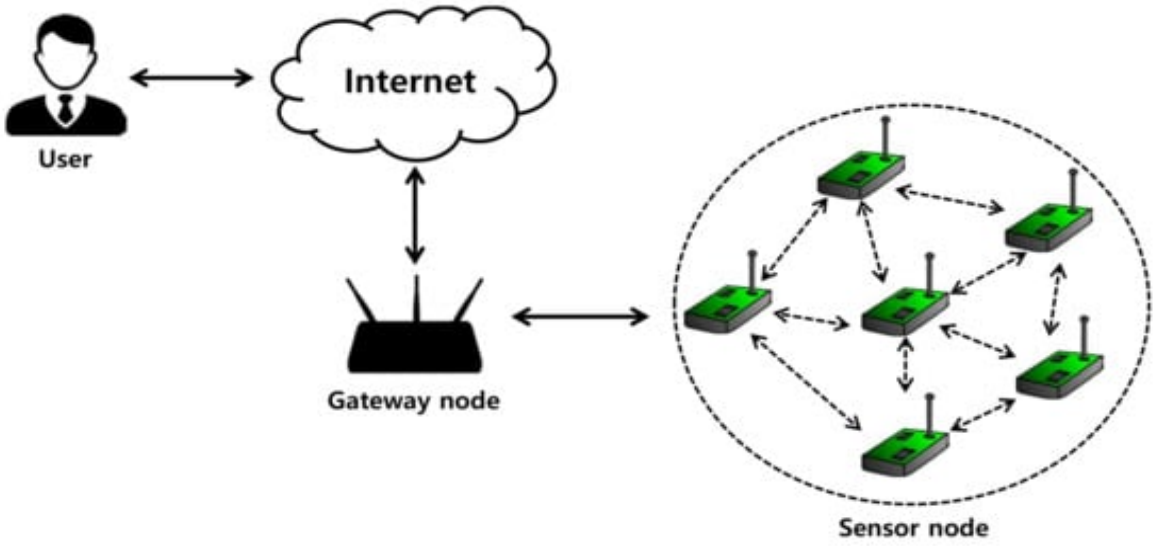

Fig 1. Authentication Model in Wireless Sensor Network. (Source: [13])

II. RELATED WORKS

To this point many authentication schemes had been proposed to prevent unauthorized get entry to between the transmitted facts inside WSN from malicious customers or adversaries [1]. 2016 Jiang et al. [20] proposed a 2FA using ECC which is a temporal credential scheme that remove the short comings of security flaws. Li et al. [14] proposed a three-factor authenticated protocol that remove flaws in Das scheme that lack the facility of impersonation attack and user anonymity in 2019. In the same year Mo and Chen [3] defined a Lightweight three factor authentication protocol for WSN withstand against known security attacks. In 2021 Liu et al. [2] expressed a 3FA protocol which is safe that is suitable in WSN based IoT applications. Shuai et al. [15] proposed an enhanced 3FA scheme for WSN, using a bio-hash function to provide security. Shin et al. [16] defined a 3FA key agreement protocol can achieve security features with efficiency. Zhu et al. [4] remove the shortcomings of Shin et al. [16] and improve the performance. Jiang et al. [17] defined a 2-factor untraceable authentication protocol using ECC. Later Li et al. [5] remove the deficiencies of [17] and defined a 3FA keeps the computational efficiency satisfy security and functional features. Saqib et al. [6] expressed a 3FA protocol that uses ECC baaed operations in it rather than encryption. In 2018 Wu et al. [9] found Das scheme was not reliable for WSN and does not have security critical information. Ryu et al. [7] eliminate the faults faced by [9] and redefined protocol that withstands the security attacks. Chen et al. [8] proposed an improved 3FA that utilize the WSN in health and medical oriented applications using IoT. A. K. Das [18] developed a modified Jiang et al.'s [17] two factor user authentication scheme into a new 3-factor authentication scheme for WSNs to remove the shortcomings. Fan Wu et al. [9] defined 3FA scheme of WSN eliminate the weakness of Das et al. scheme. In 2016, Liu and Chung [19] expressed an authentication scheme using bilinear pairings. In his scheme a trusted third authority to validate the user. Challa et al. [10] defined a ECC based method prefer the legal user allow to change the password and bio- metrics without contacting the trusted third authority. Shin and Kwon [16] proposed a scheme provide better security against the active and passive attacks. Mo et al. [11] proposed a protocol in 2021 using chebyshev mapping for WSN which improved the security and reduce computation overhead. Kim and Kapito [12] proposed a better security and successful of IoT and provide the facility of IoT security and privacy concerns. Yu and Park [13] SLUA-WSN protocol prevent any kind of security threats in addition ensure functional features.

III. PRILIMINARIES

Fuzzy Extractor

Fuzzy extractor is mostly used to resolve the problems facing in biometric template authentication. The biometric based extractor use two functions (Gen, Rep) convert the biometric data into random value. The fuzzy extractor taking biometric template B_i as input and produce biological key δ_i and public parameter $\tau_i$with the help of error correcting code technology. Two algorithms demonstrate fuzzy extractor.

$Gen(B_i) = (\delta_i, \tau_i)$ is a probabilistic generation algorithm. This algorithm accepts B_i as biometric template is input and generate output as a random pseudo string $\delta_i$with support of auxiliary pseudo stringτ_i.

$Rep(B_i^*, \tau_i) = \delta_i$ is a deterministic reproducing generation algorithm. This algorithm accepts B_i^* as biometric-template input as accepted an error tolerant range and the auxiliary random string τ_i.This function will returnδ_i.

Biometric authentication can be achieved by comparing the biometric template stored in the database with the captured image of biometric template with error tolerance specified.

Elliptic Curve Cryptography

Elliptic curve is expressed by the equation $y^2 = x^3 + ax + b \, mod \, p, 4a^3 + 27b^2 \, mod \, p \neq 0$ with $a, b \in F_p$, through the prime finite field F_p in which $E_p(a, b)$ be a set of elliptic curve points. An elliptic curve group *G* is defined on E_{F_P} with generator *P*. Private key is n_A, public key is $p_A = n_A XG$.Encrypt p_m is done by the selection of the random number k as $C_m = \{kG, P_m + kP_B\}$.Decrypt by $P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B(kG) = P_m$

Hash Function

A one-way collision resistant hash function $h: \{0,1\}^* \rightarrow \{0,1\}^n$ that accepts binary string with any arbitrary length $x \in \{0,1\}^*$ as input, and then outputs be a binary string of fixed size length n , say $y \in \{0,1\}^n$ such that $y = h(x)$. Here, y is known as the hash digest of input x.

IV. PROPOSED SCHEME

We derived an efficient, secure and a light weight 3-parties involved authenticated scheme for exchanging key for IoT applications. Three participants involved in this scheme they are remote user (Ui) who are the consumers of the services, group of providers or sensor nodes (S_j) and trusted gateway node (GWN). The proposed methodology is organized into following phases namely initialization/setup phase, registration phases, login phase, verification/authentication phase, key generation phase and password update/change phase. **Table 1** shows the notations.

Table 1. Notations

Symbol	Description
GWN	Gate Way Node
U_i	User
S_j	Sensor Node
ID_i	User Identity
PW_i	User Password
SID_j	Sensor Node Identity
K_i	Secret/Private key of U_i
K_j	Secret/Private key of S_j
K_G	Master key of GWN
B_i	User Biometric
E_K/D_K	Symmetric Encryption/Decryption
T_i	Time stamp
SK	Session Key
$\boldsymbol{SC}$	Smart Card
$h(.)$	Hash function
$\oplus$	Exclusive OR
$\|\|$	Concatenation operation

Initialization/Pre-Deployment Phase

Compute the user and sensor node secret keys and distribute to it. In this phase of the scheme, each user(U_i) and IoT sensor node (S_j)is register with gateway node(GWN). This phase include the following steps.

Step 1

GWNchoose the identity of $SID_j$for the sensor node S_j and computes$K_j = h(SID_j||K_G)$. GWNsends $\{SID_j, K_j\}$ in a secured channel toS_j . .

Step 2

GWNchoose the identity of U_i as $ID_i$and computes $K_i = h(ID_i||K_G)$. GWNsends $\{ID_i, K_i\}$ in a secured channel to U_i.

IoT Sensor Node Registration Phase

On this segment of the scheme, each IoT sensor node is register with gateway node. Any subordinate nodes or auxiliary can be included dynamically. This phase include the next coming steps.

Step 1

$S_i$received the message from $GWN$and compute $h(SID_i||K_i)$. This value is stored in a secret memory of the sensor nodeS_i.

Remote User Registration Phase

User (U_i) wants or gain to access IoT resources, he//she initially register with GWN. Perform the registration process $U_i$will initiate the subsequent steps.

Step 1

U_i select freely his/her identity ID_i and password PW_i. Next, he/she input his/her biometric finger printB_i.

Step 2

Then U_i computes $Gen(B_i) = \{\delta_i, \tau_i\}$, $MPW_i = h(PW_i||\delta_i)$ and $C_i = h(ID_i||PW_i||\delta_i)$. Next U_i send $\{ID_i, MPW_i\}$ to GWNin a secure channel.

Step 3

Once received GWNgenerate a secret nonce $N_G$and calculate $MID_i = h(ID_i||N_G||K_G)$ and store N_G in a secure or protected database. GWN insertsMID_i,C_i into smart card SC and issue it to U_i.

Login Phase

After the complete the registration phase, user U_i access the services through the sensor node. Various process involved in the login phases are depicted as come after.

Step 1

User U_i inputs his/her credentials such as identity ID_i and password PW_i. Next imprints his/her biometric finger print B_i^*into the biometric device and input the SCin to the smart card reader.

Step2

Compute $\delta_i^* = Rep(B_i^*, \tau_i)$ parameters $MPW_i^* = h(PW_i||\delta_i^*)$ and $C_i^* = h(ID_i||MPW_i^*||\delta_i^*)$. Check if $C_i$and C_i^* are equal, if it equals continue with next or coming step or else aborts the session.

Step 3

$U_i$generate the random nonce N_U and timestamp T_1. The U_i compute the message components send to GWN $m_1 = MID_i \oplus (N_U||K_i)$, $M_{UG} = h(ID_i||N_U||K_i||T_1)$ $M_1 = \{ID_i, MID_i, m_1, M_{UG}, T_1\}$ and send the encrypted $E_{h(ID_i||K_i)}(M_1)$ to GWNinsecure channel.

Authentication or Verification Phase

Step 1

Upon received the login request message GWNdecrypt by $D_{h(ID_i||K_i)}(M_1)$. Check the validity of T_1 and calculate $MID_i^* = h(ID_i||K_G||N_G)$,$N_U^*||K_i = m_1 \oplus MID_i^*$,$M_{UG}^* = h(ID_i||K_i||N_U^*||T_1)$ and check $M_{UG}^*$with M_{UG},if it holds GWNcalculate $m_2 = (N_G \,||\, K_G) \oplus h(SID_j \,||\, K_j \,||\, T_2)$ $M_{GS} = h(ID_i||SID_i||N_U||K_i||N_G||K_G||T_2)$ and $M_2 = \{MID_i, m_1, m_2, M_{GS}, T_2\}$send $E_{h(SID_i||K_i)}(M_2)$ to the $S_i$in a insecure channel.

Step 2

When received the message by $S_i$then decrypt it as $D_{h(SID_i||K_i)}(M_2)$ and verify the validity of T_2if it ok computes the following $(N_G||K_G) = m_2 \oplus h(SID_i||K_i||T_2)$ $N_U^* \,||\, K_i = m_1 \oplus MID_i^*$ $M_{GS}^* = h(ID_i||SID_i||N_U||K_i||N_G||K_G||T_2)$ Whether $S_i$verified the comparison $M_{GS}^* = M_{GS}$ then find to hold it or not. If it holds, accept the session or otherwise discard the session.

Key Generation Phase

Step 1

After the verification, process $S_i$generates a pseudo random nonce $N_S$and timestamp T_3. Calculate

$m_3 = (N_S||K_i) \oplus h(N_U||SID_i||K_i||T_3)$

$M_{SG} = h(N_S||K_i||N_G||K_G||MID_i||SID_i) SK = h(N_S||K_i||N_G||K_G||K_U||N_U)$

$M_{SU} = h(SK)$ $M_3 = \{MID_i, m_3, M_{SG}, M_{SU}, T_3\}$and sends $E_{h(SID_i||K_i)}(M_3)$ to GWNin a secure channel.

Step 2

Upon receive the acknowledged encrypted message GWNthen decrypt it$D_{h(SID_i||K_i)}(M_3)$. Check the validity of $T_3$and calculate $(N_S \,||\, K_j) = m_3 \oplus h(N_U \,||\, SID_j \,||\, K_j \,||\, T_3)$ $M_{SG}^* = h(N_S||K_i||N_G||K_G||MID_i||SID_i)$ check if $M_{SG}^* ?= M_{SG}$. If it holds then GWNgenerate timestamp$T_4$and calculate

$SK = h(N_S||K_i||N_G||K_G||K_U||N_U)$

$m_4 = (N_S \,||\, K_j) \oplus h(MID_i \,||\, K_i \,||\, T_4)$ $M_{GU} = h(N_U||N_G||K_G||MID_i||K_i||T_4)$

$m_5 = N_G \,||\, K_G$ $M_4 = \{MID_i, m_4, m_5, M_{GU}, M_{SU}, T_4\}$ and sends $E_{h(ID_i||K_i)}(M_4)$ insecure channel to U_i.

Step 3

After message received, U_i decrypt it by $D_{h(ID_i||K_i)}(M_4)$ verify the validity of $T_4$and compute $(N_S||K_i) = m_4 \oplus h(MID_i||K_i||T_4)$ $M_{GU}^* = h(N_U||N_G||K_G||MID_i||K_i||T_4)$ and checks$M_{GU} ?= M_{GU}^*$. If the condition is satisfied $U_i$compute $SK = h(N_S||K_i||N_G||K_G||K_U||N_U)$ and confirmed it by compute$M_{SU}^* = h(SK)$. Then after check $M_{SU} ?= M_{SU}^*$. If the condition is correct $U_i, S_i, GWN$are mutually authenticate each other.

Password Change Phase

When user U_i willing or wants to change/update her/his password, the following subsequent procedure are followed.

Step 1

U_i input his/her old identityID_i^{old}, old password $PW_i^{old}$and imprints old biometric fingerprintB_i^{old}. After the inputs U_i computes $Gen(B_i^{old}) = \langle \delta_i^{old}, \tau_i^{old} \rangle$and $MPW_i^{old} = h(PW_i^{old}||\delta_i^{old})$. Next sends $\{ID_i^{old}, MPW_i^{old}\}$to the SCin a secured way.

Step 2

Upon the message received, the SCcalculate the

$MID_i^{old} = h(ID_i^{old} \,||\, N_G^{old} \,||\, K_G^{old})$ $C_i^{old} = h(ID_i^{old}||PW_i^{old}||\delta_i^{old})$ and sends message to U_i

Step 3

After message received, the U_i selects his/her new identity ID_i^{new}, new password $PW_i^{new}$and imprints new biometric fingerprint B_i^{new}.Then $U_i$calculates $Gen(B_i^{new}) = \langle \delta_i^{new}, \tau_i^{new} \rangle MPW_i^{new} = h(PW_i^{new}||\delta_i^{new})$. Next sends $\{ID_i^{new}, MPW_i^{new}\}$ to the SCin a secured channel.

Step 4

After the message received, SC calculates $MID_i^{new} = h(ID_i^{new} \| N_G^{new} \| K_G^{new}$ $\boldsymbol{C_i^{new} = h(ID_i^{new} \| PW_i^{new} \| \delta_i^{new})}$. Next $\langle MID_i^{old}, C_i^{old} \rangle$ replace with $\langle MID_i^{new}, C_i^{new} \rangle$

V. DISCUSSIONS

Security Analysis

To analyze the proposed scheme, by performing with different security features in informal way. The scheme is withstand against various attacks meet out the security requirement of WSN. **Table 2** shows the summary of the security analysis.

Resist Masquerade Attack

In this type of attack, the adversary tries out to masquerade as like the original user by intercepting the flowing message in the insecure channel. In our scheme, message flowing between any two entities such as U-GWN, GWN-S, S-GWN and GWN-U. are encrypted. There is no such possibility of this particular attack.

Resist Password Guessing Attack

Malicious users initiate attack by extracting the information from SC or trapping through login request of the user in an unsecure public channel. So the attacker still not able to guess the password without knowing the other two components identity and biometric finger print. All the messages related to the password are masked, so that it infeasible to guess it.

Resist Replay Attack

In our scheme, we are using timestamp and random nonce in all parts of request and reply message transmitted between any two communication ends such as U-GWN, GWN-S, S-GWN and GWN-U. Any intruder may initiate this type of attack by intercepting message and modify and resend is difficult without knowing the values of timestamp and nonce.

Resist Sensor Node Impersonation Attack

Sensor nodes may be installed or placed in hostile or unmanned locations, and then the attacker may easily seize the sensor nodes. They may try to pretend as like sensor nodes, but there is not feasible in our proposed scheme because each sensor have unique identity and secret key.

Resist Stolen Verifier Attack

This kind of attack taken at verifier table stored in GWN usually called password table. Normally attackers carry out the malicious attack on it. This is prevent in our scheme by attackers not obtain the password in the open network environment in such a way that masked with encrypted values are passed.

Resist Man in Middle Attack

This is normally happen when an attackers sits in between the message exchange between the communication entities. They steal and capture the message and modify and resend to the other end of the communication. This attack is prevent in our scheme by authentication checkup procedure installed at the communication end.

Table 2. Security Analysis

Security Parameter	Zhu et. al [4]	Taheer et. al [2]	Xie et al. [1]	Yu et. al [13]	Mo-Chen [8]	Ours
SP1	√	√	√	√	√	√
SP2	×	√	√	×	√	√
SP3	√	√	√	√	√	√
SP4	√	√	×	√	√	√
SP5	√	√	√	√	×	√
SP6	√	√	√	√	√	√

Note SP1 – Replay attack SP2 – Man in middle attack SP3 – Insider attack SP4 – password guessing attack SP5 – Masquerade attack SP6 – Sensor node capture attack

Functional Analysis

Strength of the authentication scheme can be analyzed by taking consideration of various functional parameters. **Table 3** shows the summary of the functional analysis.

User Anonymity
It is the real identity which is a protected one without know by any adversaries normally it is feature of authentication scheme. In our proposed scheme, original user identity does not reveal in any message exchanges. Any adversary does not get users identity from message communications. In our scheme ID is implied with the message, even though the message is encrypted form. In this way our scheme is achieved with user anonymity.

User Traceability
Any adversary cannot trace on different sessions when exchanged in a public channel. In our scheme each entity involved in the communication generated the random number for every session. In addition message is encrypted with key that also involved with the identity and secret key. In such a way our authentication scheme incorporated with non-traceable.

Time Synchronization
To prevent the replay attack, authentication schemes employed use any one of the two methods namely timestamp based or nonce based. By avoiding the time synchronization problem in the authentication scheme that is implemented with time stamp. Our scheme is involved with both timestamp and nonce.

Mutual Authentication
Each entity involved in the communication performs the mutual agreement before authentication happens. Upon get the authenticated message, every time there is a verification process involved in it. If the verification is successful then only it permits to authenticate. In our scheme any type of request or response message involved in message exchanges the verification process is a mandatory one. In such a way scheme achieved mutual authentication.

Session Key Agreement
After successful authentication or verification completes for future communication between user and sensor node there is in a need of session key. In our scheme user U_i, sensor nodeS_i and gateway node involve for the generation of session key with the help of nonce and secret keys.

Forward Secrecy
Suppose an adversary captured the private keys of user and sensor node, master key of GWN accidently. He may intercepted the message in insecure public channel. He may not get the previous session key. Every time of communication, the authentication will use the private key and master keys. Previous values of the keys cannot considered in the account of current session key generation in addition it also uses one way hash function.

Table 3. Functional Analysis

Functional Parameters	Zhu et. al [4]	Taheer et. al [2]	Xie et al [1].	Yu et. al [13]	Chen et al. [8]	Ours
FP1	√	√	√	√	√	√
FP2	√	×	√	×	√	√
FP3	×	√	√	√	×	√
FP4	√	√	√	√	√	√
FP5	√	√	√	√	√	√
FP6	√	√	√	√	√	√

Note FP1 – User anonymity FP2 – User traceability FP3 – Time Synchronization FP4 – Mutual authentication FP5 – Session agreement FP6 – Forward secrecy

Performance Analysis
To assess the overall performance of the proposed scheme encompass three factors computation, communication and garage cost. Compare the proposed scheme with different associated schemes.

Computational Cost
To evaluate the computational cost considering hash functions, encryption and decryption functions excluding XOR and OR function that are neglected. Taking account of all phases exclude the password change phase. T_h- hash function time cost, T_E- symmetric encryption/ decryption time cost of. T_R- Rep operation time cost. T_M- elliptic curve multiplication operation time cost. Execution time of $T_E$is greater than the execution time of T_h. Evaluate the proposed scheme with different associated schemes is indexed inside **Table 4**. By conducting the experiment with a CPU of 3.2GHz and 3 GB RAM. Execution time for hash function is 0.32ms and encryption 0.40ms and elliptic multiplication 0.12ms and rep function o.21ms.

Communication Cost

This cost is calculated by the amount of bits in a message transfer between the three entities U_i user, S_i sensor node and GWN gateway node. The numbers of message exchange around the three entities are listed in **Table 5**.

Table 4. Computational Cost

Scheme	U_i	GWN	S_i	Total	Exec Time
Zhu et. al [4]	$11T_h$	$10T_h$	$6T_h$	$27T_h$	8.64ms
Taher et. al [2]	$12T_h$	$14T_h$	$3T_h$	$29T_h$	9.28ms
Xie et al [1]	$9T_h + 3T_E$	$5T_h + 2T_E$	$8T_h + T_E$	$22T_h + 6T_E$	9.44ms
Yu et. al [13]	$11T_h$	$11T_h$	$6T_h$	$28T_h$	8.96ms
Chen et al. [8]	$12T_h + T_R + 2T_M$	$10T_h + T_E$	$5T_h + 2T_M + T_E$	$24T_h + T_R + 4T_M + 2T_E$	9.4ms
Ours	$11T_h$	$10T_h$	$6T_h$	$27T_h$	8.64ms

Table 5. Communication Cost

Scheme	Message count	Bit count
Zhu et. al [4]	4	2048
Taher et. al [2]	4	1664
Xie et al [1]	4	2048
Yu et. al [13]	4	2208
Chen et al. [8]	4	3328
Ours	6	2208

Storage Cost

Amount of bits kept/stored in SC smart card is described in the **Table 6**. According to the login request message initiated by user the number of bits is stored/reserved in SC smart card in the login phase of the scheme.

Table 6. Storage Cost in Smart Card

Scheme	No of bits
Zhu et. al [4]	512
Taher et. al [2]	512
Xie et al [1]	1024
Yu et. al [13]	512
Chen et al. [8]	512
Ours	256

VI. CONCLUSION

Despite the reality that many three-factor mutual authentication schemes had been supplied for the WSN environments, maximum of them had been located to be unprotected from several attacks. Moreover, the proposed scheme is relaxed towards recognized security attacks. In the end, the overall performance evaluation assessment in phrases of computation and communication prices established that our protocol showed correct one and overall performance as compared to those of recent related protocols and is extra appropriate for practical IoT WSN environments

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests

References

[1]. Q. Xie, Z. Ding, and B. Hu, "A Secure and Privacy-Preserving Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things," Security and Communication Networks, vol. 2021, pp. 1–12, Sep. 2021, doi: 10.1155/2021/4799223.

[2]. B. H. Taher, H. Liu, F. Abedi, H. Lu, A. A. Yassin, and A. J. Mohammed, "A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications," Journal of Sensors, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/8871204.

[3]. J. Mo and H. Chen, "A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks," Security and Communication Networks, vol. 2019, pp. 1–17, Dec. 2019, doi: 10.1155/2019/2136506.

[4]. L. Zhu, H. Xiang, and K. Zhang, "A Light and Anonymous Three-Factor Authentication Protocol for Wireless Sensor Networks," Symmetry, vol. 14, no. 1, p. 46, Dec. 2021, doi: 10.3390/sym14010046.

[5]. X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," Journal of Network and Computer Applications, vol. 103, pp. 194–204, Feb. 2018, doi: 10.1016/j.jnca.2017.07.001.

[6]. M. Saqib, B. Jasra, and A. H. Moon, "A lightweight three factor authentication framework for IoT based critical applications," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 9, pp. 6925–6937, Oct. 2022, doi: 10.1016/j.jksuci.2021.07.023.

[7]. J. Ryu, T. Song, J. Moon, H. Kim, and D. Won, "Cryptanalysis of Improved and Provably Secure Three-Factor User Authentication Scheme for Wireless Sensor Networks," Computational Science and Technology, pp. 49–58, Aug. 2018, doi: 10.1007/978-981-13-2622-6_5.

[8]. Y. Chen, Y. Ge, Y. Wang, and Z. Zeng, "An Improved Three-Factor User Authentication and Key Agreement Scheme for Wireless Medical Sensor Networks," IEEE Access, vol. 7, pp. 85440–85451, 2019, doi: 10.1109/access.2019.2923777.

[9]. F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and provably secure three-factor user authentication scheme for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 11, no. 1, pp. 1–20, Aug. 2016, doi: 10.1007/s12083-016-0485-9.

[10]. S. Challa et al., "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," Computers & Electrical Engineering, vol. 69, pp. 534–554, Jul. 2018, doi: 10.1016/j.compeleceng.2017.08.003.

[11]. J. Mo, Z. Hu, and W. Shen, "A Provably Secure Three-Factor Authentication Protocol Based on Chebyshev Chaotic Mapping for Wireless Sensor Network," IEEE Access, vol. 10, pp. 12137–12152, 2022, doi: 10.1109/access.2022.3146393.

[12]. H. Kim and B. O. D. Kapito, "Security Considerations on Three-Factor Anonymous Authentication Scheme for WSNs," Journal of Computer and Communications, vol. 09, no. 03, pp. 1–9, 2021, doi: 10.4236/jcc.2021.93001.

[13]. S. Yu and Y. Park, "SLUA-WSN: Secure and Lightweight Three-Factor-Based User Authentication Protocol for Wireless Sensor Networks," Sensors, vol. 20, no. 15, p. 4143, Jul. 2020, doi: 10.3390/s20154143.

[14]. Y. Lu, G. Xu, L. Li, and Y. Yang, "Anonymous three-factor authenticated key agreement for wireless sensor networks," Wireless Networks, vol. 25, no. 4, pp. 1461–1475, Nov. 2017, doi: 10.1007/s11276-017-1604-0.

[15]. M. Shuai, N. Yu, H. Wang, L. Xiong, and Y. Li, "A Lightweight Three-Factor Anonymous Authentication Scheme With Privacy Protection for Personalized Healthcare Applications," Journal of Organizational and End User Computing, vol. 33, no. 3, pp. 1–18, May 2021, doi: 10.4018/joeuc.20210501.oa1.

[16]. S. Shin and T. Kwon, "A Lightweight Three-Factor Authentication and Key Agreement Scheme in Wireless Sensor Networks for Smart Homes," Sensors, vol. 19, no. 9, p. 2012, Apr. 2019, doi: 10.3390/s19092012.

[17]. Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," Journal of Network and Computer Applications, vol. 76, pp. 37–48, Dec. 2016, doi: 10.1016/j.jnca.2016.10.001.

[18]. A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 9, no. 1, pp. 223–244, Dec. 2014, doi: 10.1007/s12083-014-0324-9.

[19]. C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," Computers & Electrical Engineering, vol. 59, pp. 250–261, Apr. 2017, doi: 10.1016/j.compeleceng.2016.01.002.

[20]. Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," Journal of Network and Computer Applications, vol. 76, pp. 37–48, Dec. 2016, doi: 10.1016/j.jnca.2016.10.001.