Authentication of IoT device with the enhancement of One-time Password (OTP)

[1]Alice Su Wei Tang, [2]Jie Hui Bong, [3]Quor Ling Teh, [4]Shanmugapiriya Sivalingam, [5]Sharon Suet Yan Chan, [6]Shi Yee Khoo, [7]Tahmid Mutashim Nafy

Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia
email: [1]alicetsw11@gmail.com, [2]huibong97@gmail.com, [3]quorling@gmail.com, [4]shanmugapiriya95@gmail.com, [5]sharon199717@gmail.com, [6]shiyee530@gmail.com, [7]tmnafy95@gmail.com.

Date received: 24 August 2021
Date accepted: 2 October 2021
Date published: 28 October 2021

Abstract - *The Robust and Energy Efficient Authentication Protocol works for Industrial Internet of Things. The Internet of Things (IoT) is an arising innovation and expected to give answers for different modern fields. The IoT enable connection of physical devices all around the world to the internet by collecting and sharing critical and real-time data among each other. The increment of devices increases the computational cost during data transmission between devices and towards the internet. In this paper we proposed a solution that is a multi-factor authentication protocol to enhance the protocol proposed by Li et al. For Industrial IoT by adding One Time Password (OTP) after the biometric information of the user is checked by the Gateway Node (GWN) to be able to tackle additional network attack aside from those that are overcome by Li et al. scheme. Our contribution for this project is, we proposed the solution that a multi-factor authentication protocol to enhance the protocol proposed. For Industrial IoT by adding One Time Password (OTP) after the biometric information of the user is checked by the Gateway Node (GWN) to be able to tackle additional network attack aside from those that are overcome. The idea of adding OTP is inspired by where they scheme correlates to biometric of user as well. Our proposal is lower cost than the three protocols regarding authentication overhead and computational cost perspectives. Challenges and future directions of this paper examined the security shortcomings of a client confirmation convention for WSN, which is as proposed by Chang and Le. To address the normal security shortcomings of past protocols, we proposed a strong and energy effective three-factor authentication protocol for WSN.*

Keywords: IoT, Multi-factor authentication, One-time password, WSN

1 Introduction

Mutual authentication and specifically multifactor authentication mechanism is not a new research paradigm. Several researchers have proposed several methods to ensure secure authentication mechanisms in any communication protocols (Khan et al., 2021) (Khan et al., 2019) (Maikol et al., 2020) (Khan et al., 2015) (Balan et al., 2018). The Internet of Things (IoT) is an arising innovation and expected to give answers for different modern fields. IoT is referring to the connection between millions and billions of physical devices that allows sharing and collecting of data (Ranger, 2020). (WSN) wireless sensor networks as one of the essential innovations of the IoT that can be utilized to gather the necessary climate boundaries for explicit applications. There are three sorts of members in WSN; they are users, sensor nodes and gateway. Sensor nodes have restricted calculation, power sources and gateway. Two authentication protocols for WSN and they are safer with amazing forward mystery another one is lightweight. They are comparable, and the two plans contain of three stages, and they are password change, registration, and authentication (Li et al., 2018).

The problem statement is that the IoT enable connection of physical devices all around the world to the internet by collecting and sharing critical and real-time data among each other (Gope & Sikdar, 2019). The increment of devices increases the computational cost during data transmission between devices and towards the internet. This

gives rise to network congestion as the algorithms of encryption and number of operations performed in each session escalates with the number of devices. Moreover, as the IoT devices are deployed in open and public spaces of the internet, it is more prone for adversary to deploy internal and external attacks towards the network such as Impersonation attack, spoofing, Replay attack etc (Gope & Sikdar, 2019) (Varanasi, 2020). It is needed to propose a multifactor authentication scheme for IoT that involved lower computational cost and authentication cost plus increase of network security assurance for the users.

Thus, our proposed solution to address the problem statement stated is a multi-factor authentication protocol to enhance the protocol proposed by Li et al. (Li et al., 2018). The ideation of adding OTP is inspired by Imran et al. (2017) where their scheme correlates to the biometric information of user as well. Method to solve the problem is mainly on the Authentication phase where the OTPi sent from the Gateway for the user device to enter and sent back to Gateway Node (GWN) to counter check (Imran et al., 2017). The OTP_i is only sent to the device that request for login access and it is only available for one login session, thus it is impossible to have the same OTPi used for different session (Digital Guide Ionos, 2020).

Our contribution for this project is to propose a multi-factor authentication protocol to enhance the protocol proposed by Li et al. (Li et al., 2018). For Industrial IoT by adding One Time Password (OTP) after the biometric information of the user is checked by the GWN to be able to tackle additional network attack aside from those that are overcome. The attacks that are able to be mitigated from the enhancement of the scheme should overcome attacks that is to be discussed in Section V.

Aside from that, computational and authentication cost of the proposed scheme are considered as well to ensure the proposed scheme is lightweight yet brings secure for IoT devices. Three other proposed schemes are taken for comparison with our proposed scheme and more in depth explanation is in Section VI

Furthermore, this paper examined the shortcomings in security of a client confirmation convention for WSN proposed by Chang and Le. It is presented in the examination that it able to forestall normal attacks at most time and gives some ideal usefulness. In the interim, the security and execution correlations show that the proposed protocol is strong than other comparable conventions with low computational cost, decreases the power consumption and lightweight. Take IoT-based brilliant medical services for instance, the plan of lightweight confirmation convention for asset restricted wearable gadgets, protection saving clinical information total plan, and security saving clinical information distributing are open issues (Sethia et al., 2018). The proposed work can be extended to enhance end to end security mechanism in network intrusion detection system or malware detection system (Ahmad el al., 2021; Dildar et al., 2017; Khan et al., 2021; Khan et al.2017).

2 Related Work

In these recent years, communication between different IoT devices in various domain have been secured with the implementation of authentication. Such implemented are introduced and constantly proposing an enhancement of authentication in various work.

Sethia et. al (2018) presented a unique structure aimed at the NFC Secure Element (SE)-centred attestation and mutual authentication on behalf of IoT admission utilizing NFC-based Host Card Emulation (HCE) style with an end-client gadget such as a portable device. Near field communication (NFC) is a small-scale wireless machinery that allows electronic devices to communicate easily and securely within a short distance that is only a few centimeters (Christensson, 2019). Their proposed scheme provides a developer-friendly platform and even support mutual communication and large amounts of storage, as well as other NFC modes. It uses an asymmetric algorithm – RSA, and symmetric algorithm - AES encryption algorithms.

Feng (2020) enhanced the security protocol from Safkhani and Vasilakos (2019) to overcome the drawbacks of security problems in RFID for healthcare system such as impersonation attacks, traceability attacks, replay attacks, desynchronization attacks, time measurement attack and secret disclosure attacks (Feng, 2020). Mutual authentication, message of tag in two different sessions, adding in random number etc. are the implementation introduced in Feng proposed protocol. However, the proposed protocol possesses higher computational cost despite lower risk of encountering network attack.

Banerjee et al. (2019) proposed a robust lightweight anonymous authentication protocol for IoT ecosystem that is able to counter new attack like device impersonation. Their proposed protocol based on lightweight operations such as "Physically Unclonable Functions (PUFs)", "fuzzy extractor functions", "one-way hash functions", and "bitwise XOR operations" (Banerjee et al., 2019). The PUFs are intended to match an entry only to an output based on a computer's physical microstructure. Each PUF circuit has its own challenge-response pair, which is an input-output pair. While a high degree of reliability of a PUF can be established, noise in PUF remains a significant problem. Therefore, fuzzy extractor is used to overcome the problem. The fuzzy extractor is affected by two approaches, the probabilistic Gen (·) function and the deterministic Rep (· function). One-way hash functions for data integrity are extensively used. Cryptographic one-way hash functions are engineered to be extremely sensitive to even minor changes in the input. The proposed scheme requires the user U, the gateway node GN, and the smart system SD to execute during the login and authentication process.

Gope and Sikdar (2019) stated that IoT devices are often installed in open and public spaces, making them susceptible to physical attack and the cloning attack. Traditional password or a hidden key using an authentication system, in which a mutual secret is the only authentication factor, are insufficient to solve the security issues in these scenarios. He proposed that any attempt to tamper with the computer, on the other hand, changes the actions of the PUF embedded in it, rendering the PUF useless. Aside from that, his proposed protocol also employs the key-hash feature and the challenge-response principle to not allow the adversary to attack. Plus, PUFs are resistant to cloning which then makes it secure against the specific attack.

Cao et al. (2019) work on access authentication and distribution protocol with aggregation signcryption with no bilinear pairings in the 5G network and it is also applicable in LTE network. However, it is not resistant towards Quantum attack. By enhancing their previous proposed protocol, in Cao et al. (2019), an addition of lattice-based homomorphic encryption is used. Encrypted messages from NB-IoT devices are sent using the public key of AMF (access and mobility manage function) during the transmission. It will be able to mitigate MiM attack. This is due to private key of AMF is needed to decrypt the message. Aggregation signcryption (signature encryption) was used to mitigate DoS attack which also contributes towards avoidance of network congestion. Quantum attack that occurs in the previous proposed schemes by Cao et al. (2019) is mitigated as well by the usage of private key for decryption that disable the attacker to forge signcryption.

Li et al. (2020) designed SLAKA by applying the cryptographic hash function, the blurry extractor method, and the XOR operations. It will be able to overcome attacks which are stolen or lost mobile terminal attacks, stolen or lost wearable device attacks, man-in-the-middle attacks, password change attacks, user impersonation attacks, wearable device impersonation attacks, and replay attacks. SLAKA uses timestamps during the message transmission that is good in countering replay attack. Computational and communication costs of SLAKA protocol is lower than the other existing schemes that are proposed in other work as comparison.

Li et al. (2018) proposed a strong and energy effective three-factor authentication protocol for WSN that involves with user, password and biometric. Examination shows it can forestall most normal attacks and gives some ideal usefulness. In the interim, the security and execution correlations show that the proposed protocol is strong than other comparable conventions with low computational cost, decreases the power consumption and lightweight. Hence, their proposed protocol is vigorous furthermore, proficient for IoT applications. IoT advancements can be utilized in numerous fields, for example, brilliant network and keen medical services, and there are numerous securities also, security insurance issues to be settled. Take IoT-based brilliant medical services for instance, the plan of lightweight confirmation convention for asset restricted wearable gadgets, protection saving clinical information total plan, and security saving clinical information distributing are open issues.

3 Review Li et. Al Scheme

In this paper, we will be enhancing the proposed scheme stated by Li et al. (2018). Figure 1 below presents the current scheme that is proposed by Li et al. (2018). From this scheme, we will be adding in OTP during the authentication phase between the user and the gateway.

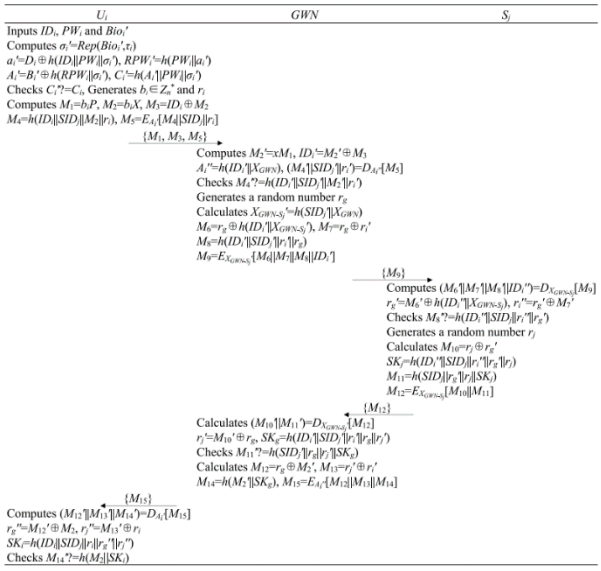

Figure 1 : Proposed scheme by Li et al. (2018)

4 Proposed Solution

For this section, we have proposed a multi-factor authentication protocol to enhance the protocol proposed by Li et al. (2018) for Industrial IoT by adding One Time Password (OTP) after the biometric information of the user is checked by the Gateway Node (GWN) to be able to tackle additional network attack aside from those that are overcome by Li et al. (2018) scheme . The ideation of adding OTP is inspired by Imran et al. (2017) where they scheme correlates to identifying biometric information of user as well. Table 1 display the notation that is used in the protocol.

Table 1 : Notations

Notation	Description
U_i	User
ID_i	Corresponding identity
PW_i	Password
Bio_i	Biometric information
a_i , r_j	Random number
RPW_i	Masked password
GWN, X_{GWM}	Gateway node and its master secret key
S_j , SID_j	The sensor node and its identity
OTP_i	One Time Password
X_{GWN-Ui}	Secret key shared between GWN and U_i
TSM	Timestamp
X_G	Secret key only known by gateway
X_{GW}	Gateway key that is shared with user

4.1 Initiation Phase

During initialization of the system, a long term secret key chosen by GWN, X_{GWN}, hash function as $h(\cdot)$, implementing symmetric cryptography that includes encryption and decryption algorithm labelled $E_k(\cdot)$ and $D_k(\cdot)$ respectively.

Apart from that, elliptic curve E selected by GWN is dependant with the finite field F_P. Then, an order of large prime n by subgroup G of E is chosen by GWN while point P is the generator. Afterwards, private key represent by x is bring out by GWN and the corelated public key X is calculated, where $x \in Z_n^*$ n and $X = xP$. Lastly, x is being kept secretly by GWN and parameters $\{E(F_p), G, P, X\}$ are produced.

For initializing sensor network, sensor node S_j has its identity SID_j selected by GWN. After that, the shared secret key $X_{GWN-Sj} = h(SID_j \| X_{GWN})$ is calculated by GWN. X_{GWN-Sj} is kept by GWN into the memory of S_j, and the target area will be having sensor nodes deployed in it.

4.2 Registration Phase

For the user to be recognized being an eligible user for the system, the mentioned steps below are to be conducted between the user U_i and the gateway node GWN. By completing the registration phase, it will result of allowing the U_i to access the sensor data through their mobile devices according to real-time.

Step 1: U_i chooses an identity ID_i, a password PW_i and a random number. In the meanwhile, Biometric information Bio_i will be provided by U_i and extracted with fuzzy extractor [1] through their mobile device, alongside $Gen(Bio_i) = (\sigma_i, \tau_i)$ is obtained. Next, masked password $RPW_i = h(PW_i \| a_i)$ is calculated by U_i, $\{ID_i, RPW_i, \sigma_i\}$ is submitted for GWN to register U_i mobile device.

Step 2: When registration request from U_i is received, GWN will first examine whether ID_i is in the database. If yes, a new identity will be asked from U_i for submission. Else, $A_i = h(ID_i \| X_{GWN})$ and $B_i = A_i \oplus h(RPW_i \| \sigma_i)$ will be computed by GWN, and GWN sends $\{B_i, E_k(\cdot), D_k(\cdot), X\}$ to U_i through an authentic manner.

Step 3: After obtaining the parameters sent by GWN, U_i determines $A_i = B_i \oplus h(RPW_i \| \sigma i)$, $C_i = h(A_i \| PW_i \| \sigma_i)$, $D_i = a_i \oplus h(ID_i \| PW_i \| \sigma_i)$, and stores $\{B_i, C_i, D_i, E_k(\cdot), D_k(\cdot), Gen(\cdot), Rep(\cdot), X, \tau_i\}$ into mobile devices of U_i .

4.3 Authentication and Key Agreement Phase

Whenever there is a need for U_i to access S_j sensor data, with the additional of OTP_i during the authentication process, U_i, GWN, and S_j performed the stated authentication steps as listed below. By the end of authentication

phase, a session key is shared among these three parties. Figure 1 presents the processes that is implemented during this phase.

Step 1: U_i uses their mobile devices inputting ID_i and PW_i plus have their biometric information, Bio_i imprinted with fuzzy extractor. Then $\sigma_i' = Rep\,(Bio_i', \tau_i)$, $a_i' = D_i \oplus h(ID_i \,||PW_i \,||\, \sigma_i')$, $RPW_i' = h(PW_i \,||a_i')$, $A_i' = B_i' \oplus h(RPW_i' \,||\sigma_i')$, $C_i' = h(A_i'||PW_i||\sigma_i')$ is calculated by the mobile devices, and checks $C_i \stackrel{?}{=} C_i$. If there is more than one out of the three factors mentioned is invalid, login request will be refuse by the mobile device. Else, next step will be performed. Two random numbers is produced, $b_i \in Z_n^*$and r_i, and computes $M_1 = b_iP$, $M_2 = b_iX$, $M_3 = ID_i \oplus M_2$, $M_4 = h(ID_i \,||\, SID_j \,||M_2 \,||\, r_i)$ and $M_5 = E_{A_i'}[M_4 || SID_j||r_i]$. The login request $\{M_1,M_3,M_5, TSM_1\}$ to GWN is then being submitted from the mobile device.

Step 2: Upon login request is received, GWN calculates $M_2 = xM_1$, $ID_i = M_2' \oplus M_3$, $A_i = h(ID_i \,||\, X_{GWN})$,$(M_4' \,||\, SID_j||r_i') = D_{A_i'}[M_5]$, and checks $M_4' \stackrel{?}{=} h(ID_iSID_jM_2\ r_i)$. TSM_1 is checked to ensure real-time transmission as it can be evaluated that is it being attacked by the adversary when there is a delay. GWN will stop the login request when the equation does not hold. Otherwise, GWN generates the OTP_u . OTP_u is generated by $z_u = x_u \oplus OTP_u$, $x_u = h(ID_i \,||\, X_{GWN-Ui})$, $y_u = h(Bio_i \,||\, X_{GWN-Ui})$. GWN then sends back < z_u, x_u, y_u, TSM_2> to U_i.

Step 3: U_i extract $OTP_u = x_u \oplus y_u$ and send back the OTP_u received by the GWN with $e_u = OTP_u \oplus y_u$.

Step 4: When GWN receives e_u from U_i mobile device, GWN extract $OTP_u^* = e_u \oplus y_u$ and Checks $OTP_u^* \stackrel{?}{=} OTP_u$. If the OTP_u* obtained is the same as OTP_u , a random number r_g is generated by GWN, and calculates $X'_{GWN-S_j} = h(SID_j'||X_{GWN})$, $M_6 = r_g \oplus h(ID_i'||X'_{GWN-S_j})$, $M_7 = r_g \oplus r_i'$, $M_8 = h(ID_i'|| \,SID_j'||r_i'||r_g)$, $M_9 = E_{X'_{GWN-S_j}}[M_6||M_7||M_8||ID_i']$. At last, GWN sends $\{M_9\}$ to S_j.

Step 5: When S_j receives messages from GWN, $(M'_6 \,||\, M'_7 \,||\, M'_8 \,||\, ID'_i{}') = D_{X_{GWN-S_j}}[M_9]$, $r_g' = M_6' \oplus h(ID_i'' \,||X_{GWN-S_j})$, $r_i'' = r_g' \oplus M_7'$ is calculated by S_j and checks $M_8' \stackrel{?}{=} h(ID_i''|| \,SID_j \,||\, r_i''|| \,r_g')$. If $M_8' \stackrel{?}{=} h(ID_i''|| \,SID_j \,||\, r_i''|| \,r_g')$ is not equivalent, the termination of session is conducted. If not, S_j generates a random number r_j, and calculates $M_{10} = r_j \oplus r_g'$, $SK_j = h(ID_i'' \,||\, SID_j \,||r_i''|| \,r_g'|| \,r_j)$, $M_{11} \stackrel{?}{=} h(SID_j \,||r_g'|| \,r_j \,||\, SK_j)$ and $M_{12} = E_{X_{GWN-S_j}}[M_{10} \,||\, M_{11}]$. Then S_j responses $\{M_{12}\}$ to GWN.

Step 6: Upon receiving response message by S_j, $(M'_{10}||M'_{11}) = D_{X'_{GWN-S_j}}[M_{12}]$, $r'_j = M'_{10} \oplus r_g$, $SK_g = h(ID'_i \,||\, SID'_j \,||\, r'_i \,||\, r_g|| \,r'_j)$ is calculated by GWN, $M'_{11} \stackrel{?}{=} h(SID'_j \,||r_g|| \,r'_j \,||\, SK_g)$ is checked afterwards. If they are not equal, the session will be terminated. Otherwise, GWN calculates $M_{12} = r_g \oplus M'_2$, $M_{13} = r'_j \oplus r'_i$, $M_{14} = h(M'_2 \,||\, SK_g)$, and $M_{15} = E_{A'i'}[M_{12} \,||\, M_{13}|| \,M_{14}]$. Then, GWN submits $\{M_{15}\}$ to U_i.

Step 7: When receiving $\{M_{15}\}$ from GWN, U_i calculates $(M'_{12}|| \,M'_{13}|| \,M'_{14}) = D_{A'_i}[M_{15}]$, $r_g'' = M_{12}' \oplus M_2$, $r_j'' = M_{13}' \oplus r_i$,$SK_i = h(ID_i \,||\, SID_j \,||\, r_i \,||\, r''_g \,||\, r''_j)$, and $M'_{14} \stackrel{?}{=} h(M_2 \,||\, SK_i)$. Termination of session is conducted if it is not equal. Else, mutual authentication is achieved among U_i, GWN and S_i, and a shared session key $SK_i (= SK_g = SK_j)$ is provided between these three parties to ensure continuous communication yet secure.

Figure 2 exhibit the process during the registration phase and authentication and key agreement phase.

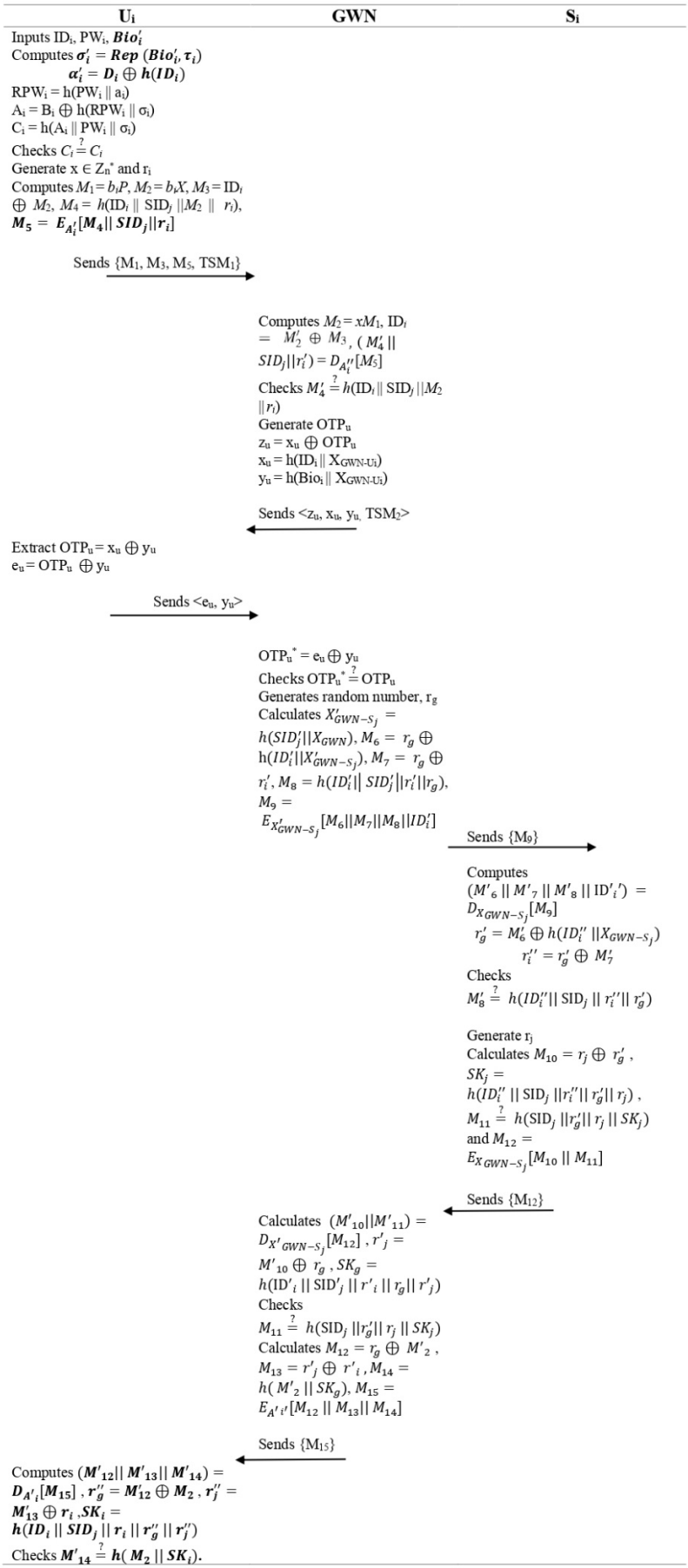

Figure 2: Proposed scheme diagram

4.4 Password Change Phase

In an event where the user forgotten or wanted to renew their static password, this phase allows them to change the password. The users able to change their password without sending any request to the GWN.
U_i utilized their mobile devices and inputs ID_i, PW_i, and imprints the biometric information Bio_i' with fuzzy extractor. Next, a request of password change is sent by the user. The mobile device from user then calculates $\sigma_i' = Rep(B_i',\ \tau_i)$, $a_i' = D_i \oplus h(ID_i \,||\, PW_j \,||\, \sigma_i')$, $RPW_i' = h(PW_i||\, a_i')$, $A_i' = B_i' \oplus h(RPW_i' \,||\, \sigma_i')$, and $C_i' = h(A_i' \,||\, PW_i \,||\, \sigma_i')$, and checks $C_i' \stackrel{?}{=} C_i$. If one of the three factors is invalid from the user's input, the user's mobile device will decline the request for password change. Otherwise, U_i a new password PW_i^{new} can be filled in by U_i. In the end, $C_i^{new} = h(A_i' \,||\, PW_i^{new}||\sigma_i')$, $D_i^{new} = a_i' \oplus h(ID_i||\, PW_i^{new}||\sigma_i')$ is calculated by the U_i mobile device and replaces $\{B_i, C_i, D_i\}$ with $\{B_i^{new}, C_i^{new}, D_i^{new}\}$.

5 Security Analysis

Through the improvement by adding in timestamps and OTP into the protocol, we were able to analyze the types of network attack that can be mitigated and being more secure from adversary or ill-intention people. This section provides a clearer picture on how the improvements and computational processes is implemented in the protocol to mitigate attacks.

5.1 Quick Detection for Unauthorized login

Three factors are used in the proposed protocol to ensure authentication implemented is appropriate. If the verification of user's biometric, identity, and password passed, the sensor data may only be accessed by the user. Mobile device will be able to find out and decline unwanted logins triggered by incorrect password with the error password checking mechanism. This verification procedure involved with three-factor is in AKA phase step 1.

5.2 Proper Mutual Authentication

GWN and U_i's mutual authentication is based on the shared secret information $A_i = h(ID_i \,||\, X_{GWN})$ and $M_2 = b_i xP$, where M_2 is created by U_i. A_i may be obtained from B_i and D_i using identity, password, and biometric data. GWN may obtain M_2 and A_i from U_i's login request message $\{M_1, M_3, M_5, TSM_1\}$ using x. GWN and U_i may authenticate each other using the shared secret information A_i and M_2.
The shared secret key = $h(SID_j \,||\, X_{GWN})$, which is kept in S_j's memory and may be obtained by GWN when it receives SID_j via the login request message, is used for mutual authentication between GWN and S_j. GWN appear to be a trustworthy towards sensor nodes and users in the proposed protocol. If both U_i and S_j are authenticated by GWN, they think each other is legitimate.

5.3 User Anonymity and Untraceability

Assume that A intercepts the login request message $\{M_1, M_3, M_5\}$, where $M_1 = b_i P$, $M_2 = b_i X$, $M_3 = ID_i \oplus M_2$, , $M_4 = h(ID_i \,||\, SID_j \,||\, M_2 \,||\, r_j)$,and the two random numbers $b_i \in$ and r_i . It is noticeable that without knowing x, A unable to expose ID_i through the login request message, thus achieved user anonymity with the suggested protocol. GWN, on the other hand, may retrieve U_i's identification ID_i by utilizing x, user identification verification is enabled by our proposed protocol. Furthermore, with the variability of random numbers $b_i \in$ *and* r_i, dynamic changes take place for each of the element in login request message. As a result, A is unable to track a specific user over the public channel.

.

5.4 Resist Mobile Device Loss Attack

Mobile device loss attack is when through the exploitation of one's devices such as tablets and smartphones to get information or to download malicious application (Ismail et al., 2017). If A obtains U_i's lost mobile device, A can use power analysis attacks to extract the parameters $\{B_i, C_i, D_i, E_k(\cdot), D_k(\cdot), Gen(\cdot), Rep(\cdot), X, \tau_i\}$ from the device. $B_i = h(ID_i \,||\, X_{GWN}) \oplus h(h(PW_i \,||\, a_i) \,||\, \sigma_i)$, $C_i = h(h(ID_i \,||\, X_{GWN}) \,||\, PW_i \,||\, \sigma_i)$, $D_i = a_i \oplus h(ID_i \,||\, PW_i \,||\, \sigma_i)$, and U_i's biometric data extracts a random string σ_i. Since B_i, C_i and D_i are computed from at least two of three unknown lengthy random strings X_{GWN}, a_i and σ_i, the parameters retrieved from the mobile device by an attacker A will not be able to correctly determine the identity and password. Hence, it will prevent mobile device loss attack

5.5 Resist Impersonation Attack

According to the AKA phase description, attacker require the ID_i and $A_i = h(ID_i \| x)$'s information in order to impersonate a trusted user and produce a successful login request. However, based on the description on user anonymity and untraceability, the proposed protocol ensures user anonymity, with no party other than GWN being able to get the user's identity ID_i. According to the AKA phase, A_i can also be computed by GWN using x when he/she obtains ID_i or obtained by U_i from B_i with the presence of PW_i, a_i and σ_i. As a result, attacker A will be unable to get A_i without possessing the necessary information, and our protocol will be able to prevent a user impersonation attack. Furthermore, x and X_{GWN} as the secret keys are needed for an attacker to produce legitimate communication messages to impersonate the GWN. However, GWN is the only one who knows about x and X_{GWN}, therefore the suggested protocol can prevent a gateway impersonation attack.

5.6 Resist Replay Attack

To prevent replay attacks, the suggested protocol uses a random number method. U_i, S_j and GWN, respectively, produce random numbers $b_i \in$, r_i, r_g and r_j in each session of the AKA phase to calculate the communication messages. Because the random numbers change constantly with each session, and the fresh random numbers ensure the freshness of the communication in each session. As a result, our protocol is protected against replay attacks. The timestamp used during the login request sent from user and the OTP sent from gateway able to counter this attack as well as if the messages is sent and received longer than as expected, it indicates that the adversary trying to get the message packets through the network and alter the contents of the messages (Kaspersky, 2021).

5.7 Sensor Node Anonymity

The identification of the sensor node is not sent in plaintext across the public channel in the proposed protocol. Encryption of S_j's identity SID_j in the login request message M_5 is done and enables retrieval of GWN with x from M_5 when U_i wishes to access S_j's sensor data. Any attacker who does not know x is unable to get the identity of a sensor node, SID_j, thus the proposed protocol achieves sensor node anonymity.

5.8 Friendly Password Change

The proposed protocol enables the mobile device to rapidly identify illegal logins caused by incorrect passwords and allows users to renew their passwords once the mobile device has validated their identification, biometrics, and earlier password. As a result, password change phase in the proposed protocol is user-friendly, and it is stated in the password change phase.

5.9 Resist Against Spoofing Attack

Spoofing is the where the adversary imitates or impersonates a trusted contact or brand to obtain one's sensitive information (Belcic & Farrier, 2021). The use of OTP can counter this attack as the adversary will be unable to login although they obtained the user's login details. Upon receiving the login details from the user U_i, the gateway will send out the OTP_u back to the user for them to insert accordingly through their mobile devices. The gateway will then counter check whether the OTP_u received from the mobile device is the same as what is sent out by $OTP_u^* \stackrel{?}{=} OTP_u$, where OTP_u^* is obtained from the mobile device. Without the user's device, the adversary is unable to obtain the OTP_u to impersonate the user to login.

5.10 Ensure Identity Privacy

The session key is generated, $SK_i = h(ID_i \| SID_j \| r_i \| r''_g \| r''_j)$ when mutual authentication is achieved during the $M'_{14} \stackrel{?}{=} h(M_2 \| SK_i)$ is established upon receiving $\{M_{15}\}$ from GWN and U_i computes it. A session key is an encryption and decryption key that allows continuous communication between the parties. This can secure the identity of U_i as a new session key will be generated by random and it will be discarded after the session is ended. Thus, the use of session key will halt the attack from an adversary as each session comes with a random session key which then secures the user's identity (SearchSecurity, 2021).

6 Complexity Analysis

In order to facilitate the computational overhead comparisons, some notations are defined as follows.

T_h : Time taken for a hash function operation
T_{XOR} : Time taken for a XOR operation
T_m : Time taken of a scalar multiplication using ECC
T_S : Time taken of a symmetric encryption/decryption
T_{AS}: Time taken of an asymmetric RSA time using Chinese remainder theorem
T_f: Time taken of a fuzzy extractor operation
T_{ms}: Time taken of modular squaring
T_{SR}: Time taken of squaring root solving
T_p: Time taken of pseudo random number generation

Usually, T_m is larger than T_h and T_S. T_h is the same with the T_S. By using the simulation result of the Intel T5870 2.00 GHz experimental platform (Wang et al., 2015), we have $T_m = 1.226ms$, $T_S = 0.0021ms$ and $T_h = 0.0026ms$ respectively. By considering other schemes, we have $T_{AS} = 12.06ms$ (Feng, 2020), $T_f = 63.075ms$ (Banerjee et al., 2019), $T_{ms} = 0.021ms$, $T_{SR} = 3.481ms$ and $T_p = 0.021ms$ (Gope & Sikdar, 2019) respectively. The bit-wise XOR operation (T_{XOR}) is not included in this analysis because it is negligible as compared to other operations.
For the analysis of the authentication overhead, we assume 160 bits for the gateway's identity and sensor node's identity respectively. The user's identity length and timestamps are 80 and 32 bits respectively. Besides, the output of the hash function and random numbers are also 160 bits. It is supposed that the point on the elliptic curve $P = (P_x, P_y)$ is 320 bits as P_x and P_y are x and y coordinates respectively which is 160 bits. ECC security remains the same because RSA public key length uses 1024 bits (Barker, 2018). The ciphertext block is 128 bits. We additionally suppose that the OTP length is 64-bits strings which will be shown as 8 decimal digits (Huang et al., 2013).
We compare authentication and computational overheads with related protocols during the authentication phase are shown in Table 2 and Table 3 (Feng, 2020) (Banerjee et al., 2019) (Sethia et al., 2018).

Table 2: Comparison of Computational Overhead among the proposed protocol and other schemes.

Protocol	**Total cost**	**Total time**
Sethia et al.	$46T_h + 258T_S + 26T_{AS}$	$314.21ms$
Banerjee et al.	$31T_h + 2T_f$	$126.23ms$
Feng	$8T_h + 2T_{ms} + 26T_{SR} + 2T_p$	$10.84ms$
Our proposed protocol	$20T_h + 8T_S + 3T_m$	$3.746ms$

During the authentication phase, the computational overhead of the proposed protocol is $7T_h + 2T_S + 2T_m$ for each user, $9T_h + 4T_S + T_m$ for the gateway and $4T_h + 2T_S$ for the sensor node. The total computational overhead is $20T_h + 8T_S + 3T_m = 3.746ms$. Table 2 summarizes the computational overhead for the compared schemes. The computational overhead of Sethia et al. (2018) protocol is the highest as they consider more about the RSA and AES encryption algorithms for asymmetric and symmetric encryption respectively. Banerjee et al. (2019) protocol is higher than Feng (2020) protocol because of the addition of the fuzzy extractor operator. It is clear that the proposed protocol is the lowest computational overhead as compared to that for other protocols. For the proposed protocol, the sensor node carries out symmetric encryption/decryption operations and hash function only.

Table 3: Comparison of Authentication Overhead among the proposed protocol and other schemes.

Protocol	**No of messages**	**No of bits**
Sethia et al.	10	27936
Banerjee et al.	3	2048
Feng	7	3648
Our proposed protocol	6	3360

Table 3 shows the authentication overhead of all protocols. We can observe that the proposed protocol is lower than Sethia et al. (2018) protocol and Feng (2020) protocol but is higher than Banerjee et al. (2019) protocol. The total authentication overhead of the proposed protocol with six exchanged messages is 3360 bits. Sethia et al. (2018) protocol is the highest authentication overhead which requires 10 messages with around 27936 bits for communication since it uses much of the symmetric encryption. The proposed protocol is acceptable as compared to the overheads of the Banerjee et al. (2018) protocol since the proposed protocol has four factor authentication compared to three factor authentication of Banerjee et al. (2018) protocol.

7 Conclusion

The Internet of Things (IoT) is a new technology that is predicted to revolutionize a variety of industrial sectors. The IoT allows physical devices worldwide to connect to the Internet by gathering and exchanging important and real-time data. As the number of devices rises, the computational cost associated with data transfer between devices and to the internet increases. In this paper, we have proposed an improved scheme of Li et al. scheme (2018) which is resist against spoofing attack and ensure identity privacy. The proposed scheme is to improve the protocol presented by Li et al. with a multi-factor authentication protocol by adding OTP once the user's biometric information is verified by the GWN. We have examined the security of our scheme and demonstrated that it is impervious to several well-known attacks such as impersonation attack, replay attack, and spoofing attack. Furthermore, complexity analysis that includes computational and authentication cost evaluations demonstrated that the enhancement of the proposed method is more reliable than existing protocols with lower cost in computational and presents reduction in power consumption significantly. IoT technology may be applied in a variety of sectors, including smart healthcare and smart grid, several security and privacy concerns are needed to be addressed. For example, in IoT-based smart healthcare, to create a authentication system that is lightweight for resource-restricted wearable devices, the aggregation of medical data for privacy protection and the publication of medical data protection remained as unresolved challenges. As for future work, researchers would need to further study and specifies the privacy and security needs for applications that are IoT-based and create solutions that are suited to overcome these challenges.

Acknowledgements

The authors would like to thank Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak to support this research work. This work is carried out as a short term research based class project.

References

Ahmad, Z., Khan, A. S., Shiang, C.W., Abdullah, J. & Ahmad, F., Network intrusion detection system: A systematic study of machine learning and deep learning approaches, *Transactions on Emerging Telecommunications Technologies,* vol. 32 no.1, pp. e4150, 2021, 10.1002/ett.4150

Banerjee, S., Odelu, V., Das, A., Chattopadhyay, S., Rodrigues, J. J. & Park, Y. (2019). Physically secure lightweight anonymous user authentication protocol for internet of things using physically unclonable functions. *IEEE Access.* 7, 85627-85644.

Balan, K., Khan, A.S., Julaihi, A.A., Tarmizi, S. & Pillay, K.S., RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks, *International Journal of Advanced Computer Science and Applications* (IJACSA) Volume 9 No 12 December 2018; pp. 298-304

Barker, E. (2018). Recommendation for Key Management. NIST, Gaithersburg, MD, USA. Tech. Rep.

Belcic, I. & Farrier, E. (2021). *What is spoofing and how can you prevent it?* Retrieved from https://www.avast.com/c-spoofing

Cao, J., Yu, P., Ma, M. & Gao, W. (2019). Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network. *IEEE Internet Thing J,* 6(2), 1561-1575.

Cao, J., Yu, P., Xiang, X.Y., Ma, M. & Li, H. (2019). Anti-Quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system. *IEEE Internet of Things Journal,* 6(6), 9794-9805. https:/doi.org/10.1109/JIOT.2019.2931724

Christensson, P. (2018, April). *NFC Definition.* Retrieved from https://techterms.com

Digital Guide Ionos. (2020). *One-time password (OTP)-more security online*. Retrieved from https://www.ionos.com/digitalguide/server/security/what-is-a-one-time-password-otp/

Dildar, M.S., Khan, N., Abdullah, J.B. & Khan, A.S., Effective way to defend the hypervisor attacks in cloud computing, *2nd International Conference on Anti-Cyber Crimes (ICACC),* pp. 154-159, 2017, 10.1109/Anti-Cybercrime.2017.7905282.

Feng, Z. (2020). A Secure RFID Mutual Authentication Protocol for Healthcare Systems. *Special Section on Lightweight Security and Provenance for Internet of Health Things,* 8, 192192-192205.

Gope, P. & Sikdar, B. (2019). Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things. *IEEE Internet of Things Journal,* 6(1), 580-589.

Huang, Y., Huang, Z., Zhao, H. & Lai, X. (2013). A new One-time Password Method. *IERI Procedia*, 4, 32-37

Imran, M.A., Mridha, M.F. & Rahman, M. (2017). *A Lightweight One Time Pad (OTP) and Biometric based Secure authentication scheme for IoT environment*. Retrieved from https://www.researchgate.net/publication/320034057_A_Lightweight_One_Time_Pad_OTP_and_Biometric_based_Secure_Authentication_Scheme_for_IoT_Environment/stats

Ismail, K.A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P. & Zulkefi, Z. (2018). Security Strategies for Hindering Watering Hole Cyber Crime Attack. *Procedia Computer Science*, 127, 656-663.

Kaspersky. (2021). *What is a Reply Attack?* Retrieved from https://www.kaspersky.com/resource-center/definitions/replay-attack

Khan, A.S., Ahmad, Z., Abdullah, J. & Ahmad, F. A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network, *IEEE Access*, 2021, *9*, 87079–87093.

Khan, N., Abdullah, J. & Khan, A.S. Defending malicious script attacks using machine learning classifiers, Wireless Communications and Mobile Computing, vol. 2017; doi:10.1155/2017/5360472

Khan, A.S., Balan, K., Javed, Y., Abdullah, J. & Tarmizi, S. Secure trust-based blockchain architecture to prevent attacks in VANET. Sensors (Switzerland), 2019, 19(22), 1.

Khan, A. S., Lenando, H., Abdullah, J. & Fisal, N. Secure authentication and key management protocols for mobile multihop WiMAX networks. Jurnal Teknologi, 2015, 73(1), 75–81.

Khan, A.S., Javed, Y. & Abdullah, J., Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS), Journal of Ambient Intelligence and Humanized Computing, 2021, 10.1007/s12652-021-02968-6.

Li, J., Zhang, N., Chen, J. & Du, R. (2020). Secure and Lightweight Authentication with Key Agreement for Smart Wearable Systems. *IEEE Internet of Things Journal,* 7(8), 7334-7344.

Li, X. Peng, J.Y., Liao, J. & Choo, K.K.R. (2018). Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things. *IEEE Internet of Things Journal,* 5(3), 1606-1615.

Ranger, S. (2020, February). *What is the IoT? Everything you need to know about the Internet of Things right now.* Retrieved from https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

Maikol, S.O., Khan, A.S., Javed, Y. & Bunsu, A.L.A., Petrus, C., A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities, *International Journal of Integrated Engineering,* vol. 13, no. 2, pp. 127-135, 2020.

Safkhani, M. & Vasilakos, A. (2019). A new secure authentication protocol for telecare medicine information system and smart campus. *IEEE Access,*7, 23514-23526.

SearchSecurity (2021). *Session Key.* Retrieved from https://searchsecurity.techtarget.com/definition/session-key

Sethia, D., Gupta, D. & Saran, H. (2018). NFC secure element-based mutual authentication and attestation for IoT access. *IEEE Transactions on Consumer Electronics*, 64(4), 470-479.

Varanasi,P. (2020, October). *Learn About Internal and External Cyber Attacks & Ideas to be safe from them.* CloudCodes. Retrieved from https://www.cloudcodes.com/blog/internal-external-cyber-attacks.html

Wang, D., He, D., Wang, P. & Chu, C. (2015). Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment. *IEEE Transactions on Dependable and Secure Computing*, 12(4), 428-442. 10.1109/TDSC.2014.2355850.