Authentication Mechanism for IoT Infrastructure

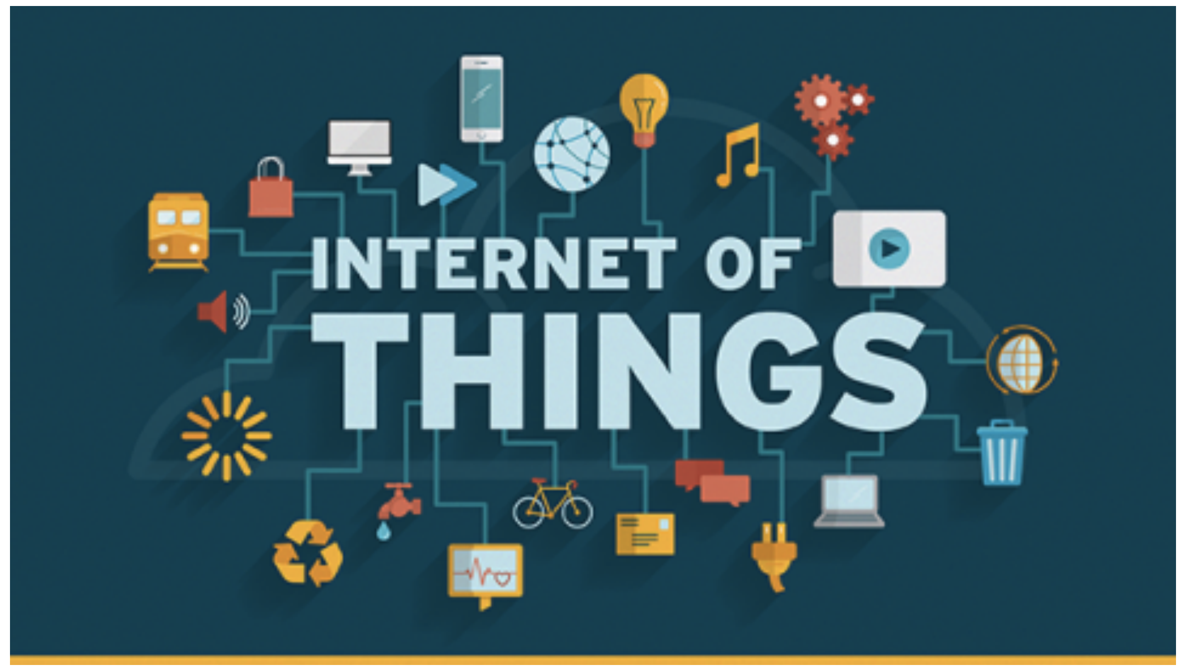
Mini Project

18BCP126, 18BCP150D

Abstract

- Recently, the use of Internet of Things (IoT) Infrastructure has tremendously increased. These difficult COVID-19 times have given a major push to decrease the risk of spreading diseases by limiting human interaction, in turn, relying majorly on IoT and cloud based technologies, in different fields, such as, transportation, healthcare, to name a few. As the reliability and demand for IoT Infrastructure is increasing, there is a definite need to secure the transfer of sensitive information via insecure public channels, with highest achievable efficiency. For the same, *Rana et. al.* proposed a light-weight user authentication scheme for IoT Infrastructure. We have attentively analysed the scheme of *Rana et. al.*, and found out that it is insecure against some attacks, including Server Compromise Attack, Stolen Smart Card (Device) Attack, User Impersonation Attack and Password Change Attack. In turn, we have proposed our own scheme, which is secure against the mentioned attacks. Our scheme is a good fit for high scale IoT systems, since it is light-weight and secure. Finally, we have compared our scheme with various existing schemes, in terms of security against several possible attacks, as well as computation and communication cost.

Introduction



- Internet of Things (IoT) and Cloud Based Infrastructure is all set to replace the current data and communication infrastructure. In recent times, IoT has been widely used to provide services to the general public, as well as various industries of the society [1] [2]. An IoT Infrastructure is a collection of numerous devices / sensors, set up at various places, to communicate with the server database (cloud server). IoT Infrastructure, put together with Cloud Based Infrastructure, is meant to communicate, store and process data.

- The quantity of the IoT and cloud based systems is increasing day by day, especially in these COVID-19 times. The other reason for such popularity and use, is its comparatively lower deployment cost and varying and promising IoT devices and sensors. [3]

- The real time, efficient, secure and accurate access of data in these systems is the key, which helps organisations to manage their resources effectively. In these difficult pandemic times of COVID-19, these systems are proving to be of definite use, since, they are also useful in reducing human involvement. [4] Hence, the use of such IoT systems is highly motivated.

- Since, there is a growth in the demand of usage of such systems, there is a very crucial need to secure the data communication happening between the entities, using insecure public channels. Authentication between the communicating entities is a key requirement to secure the communication. The fruitfulness of these systems will come to reality, only if the security and privacy of users, organisations and institutions is not compromised.

Motivation

- Kaul and Awasthi [5] presented a remote user authentication system based on smart cards, in 2016, in which a client can authenticate with a remote server. In 2021, the review of Kaul and Awasthi's scheme was done by *Rana et al.* [6], and in turn, *Rana et al.* proposed their new improved scheme, which is more secure than *Kaul and Awasthi*'s scheme. But, deeply analysing the scheme of *Rana et al.*, we found that their scheme is insecure against various serious attacks, namely, Server Compromise Attack, Stolen Smart Card (Device) Attack, User Impersonation Attack, and Password Change Attack. Hence, we were motivated to propose a new scheme, which is lightweight and more secure than *Rana et al.*'s scheme.

Contribution

- We have highlighted and pointed out that the scheme of *Rana et al.* [6] is susceptible as well as weak against several basic attacks.
- In turn, we have proposed our own scheme, which is lightweight, highly scalable, and more secure and resistant towards basic and advanced attacks, which will help to provide convenient and effective authorised access to users of the particular IoT system.
- We have implemented both schemes (*Rana et al.*'s scheme and our proposed scheme) in Python 3.9 to carefully analyse them.

Literature Survey

- *Lamport* [7] was the first one to propose an authenticated scheme on an insecure communication channel, which was based on verification tables and verification passwords, in 1981. Verification Tables are unable to provide the amount of security, which the recent and current IoT systems require.
- Keeping efficiency and security as the foremost priority, many authentication schemes [8-11] have been proposed and presented. Their drawback is that they have been proved unresistant to many basic cryptographic attacks.
- *Das et al.* [12] proposed a pseudo ID based scheme, in 2004. It was a new idea, but it was insecure against several attacks.

Literature Survey

(Cont.)

- *Wang et al.* [13] presented a new improved scheme based on *Das et al.*'s scheme, which resisted their weaknesses and was useful on high scale.
- Further, *Chang et al.* [14] found and presented weaknesses in *Wang et al.*'s scheme, and in turn, presenting an improved scheme.
- *Kumari et al.* [15] found out that *Chang et al.*'s scheme is insecure against insider and server impersonation attacks. As a result, *Kumari et al.* [15], proposed an updated scheme, which is resistant to the aforementioned attacks.

Literature Survey

(Cont.)

- *Kaul and Awasthi* [5] presented that *Kumari et al.*'s scheme is still weak and the session key between the server and the user can be found out by an adversary (***A***). Hence, they proposed an updated scheme to counter the vulnerabilities.

- *Rana et al.* [6] reviewed *Kaul and Awasthi*'s scheme to find out its weaknesses and introduced a new scheme for the same.

- In 2017, *Challa et al.* [16] introduced a new user authentication scheme, using digital signature. Their scheme provides untraceability feature. But, their scheme has high computation cost.

Rana et al.’s Scheme

Review

- We have demonstrated Rana et al.’s scheme in this section. We have presented the two phases of their scheme: Registration Phase & Login and Authentication Phase.

Symbols	Detail	Symbols	Detail
$\mathcal{U}_c$	cth legal user	ID_c	cth user identity
PW_c	cth user password	$\mathcal{S}$	Legal server
a, b	Private key and number of server	y_c	Arbitrary number for $\mathcal{U}_c$
SC_c	User’s Smart Card	T_1	Time stamp obtained at User’s side
T_2	Server’s current time stamp	T'	Threshold value
δT_c	Time of transmission delay	$\|$	Concatenation operator
$\oplus$	XoR operator	$h(\cdot)$	Non-collision hash function
SK	Session key	$\mathcal{A}$	Adversary
$\Rightarrow$	Private communication channel	$\rightarrow$	Public communication channel

Rana et al.'s Scheme

Registration Phase

- In this phase, the Server ***S*** registers a user ***U$_c$*** securely. The Server ***S*** doesn't store anything.

User $\mathcal{U}_c$		Server $\mathcal{S}$
Choose ID_c and PW_c		
Choose an arbitrary number m		
Compute $RPW_c = h(m \Vert PW_c)$		
	$\xRightarrow{\{ID_c, RPW_c\}}$	
		Selects an arbitrary number y_c
		$\boxed{\overline{DID_c} = Enc_{ds}(ID_c \Vert y_c)}$
		Compute $\alpha_c = h((ID_c \oplus a) \Vert b)$
		$\beta_c = \alpha_c \oplus h(ID_c \oplus RPW_c)$
		$\gamma_c = y_c \oplus h(\alpha_c \oplus RPW_c)$
		$\chi_c = h(ID_c \Vert RPW_c \Vert y_c \Vert \alpha_c)$
		Stores{ $\beta_c, \gamma_c, \overline{DID_c}, \chi_c, h(.)$} on SC_c
	$\xLeftarrow{\{SC_c\}}$	
Compute $\eta_c = m \oplus h(ID_c \oplus PW_c)$		
Store $\{\eta_c\}$on SC_c		

Rana et al.’s Scheme

Login and Authentication Phase

User $\mathcal{U}_c$	Server $\mathcal{S}$
Login and Authentication Phase	
Input ID_c^*, PW_c^*	
Compute $m = \eta_c \oplus h(ID_c^* \oplus PW_c^*)$	
$RPW_c^* = h(m \| PW_c^*)$	
$\alpha_c^* = \beta_c \oplus h(ID_c^* \oplus RPW_c^*)$	
$y_c^* = \gamma_c \oplus h(\alpha_c^* \oplus RPW_c^*)$	
$\chi_c^* = h(ID_c^* \| RPW_c^* \| y_c^* \| \alpha_c^*)$	
Verify $\chi_c^* \stackrel{?}{=} \chi_c$	
Compute $\omega_c = y_c \oplus h(ID_c \oplus \alpha_c) \oplus h(ID_c \oplus \alpha_c \oplus T_1)$	
$\vartheta_c = h(ID_c \| \alpha_c \| y_c \| (\alpha_c \oplus y_c) \| T_1)$	
$\xrightarrow{\{\overline{DID_c}, \omega_c, \vartheta_c, T_1\}}$	
	Verify $(\acute{T} - T_1) \leq \delta T_c$
	$\boxed{(ID_c \| y_c) = Dec_{ds}(\overline{DID_c})}$
	Compute $\alpha_c^* = h((ID_c^* \oplus a) \| b)$
	$y_c^* = \omega_c^* \oplus h(ID_c^* \oplus \alpha_c^*) \oplus h(ID_c^* \oplus \alpha_c^* \oplus T_1)$
	$\vartheta_c^* = h(ID_c^* \| \alpha_c^* \| y_c^* \| (\alpha_c^* \oplus y_c^*) \| T_1)$
	Verify $\vartheta_c^* \stackrel{?}{=} \vartheta_c$
	Compute $\mu_c = h(ID_c \| y_c \| (\alpha_c \oplus y_c) \| T_2)$
	Generates a new random number
	Computes $\boxed{PID_c = Enc_{ds}(ID_c \| y_{new}) \oplus a_c^*}$
	$\xleftarrow{\{\mu_c, T_2\}}$
Verify $(\acute{T}_2 - T_2) \leq \delta T_s$	
Compute $\mu_c^* = h(ID_c \| y_c \| (\alpha_c \oplus y_c) \| T_2)$	
Verify $\mu_c^* \stackrel{?}{=} \mu_c$	
$\boxed{\overline{DID_c} = PID_c \oplus a_c^*}$	
Initiate SK	
$SK = h(ID_c \oplus \alpha_c \oplus y_c \oplus T_1 \oplus T_2)$	

Rana et al.’s Scheme

Implementation

- Implementation : https://colab.research.google.com/drive/1AAHq1dDiago0uQop98OnxV3zegwqaenV?usp=sharing

Rana et al.'s Scheme

Cryptanalysis

- Server Compromise Attack
- If the server's secret keys ***a*** and ***b*** are compromised, and messages ***M1 (***$\{DID_c, \omega_c, \vartheta_c, T_1\}$***)*** and ***M2 (***$\{\mu_c, T_2\}$***)*** are known to the adversary ***A***, then the session key can easily be found out by ***A***.
- Since DID_c is known to ***A***, he/she can find ID_c and y_c by the following equation:

$$(ID_c \,||\, y_c) = Dec_{ds}\,(DID_c)$$

- $T1$ and $T2$ are known to ***A***, since he/she has the access to messages ***M1 (***$\{DID_c, \omega_c, \vartheta_c, T_1\}$***)*** and ***M2 (***$\{\mu_c, T_2\}$***)***.
- Hence, the session key SK can be found out easily by ***A***, using the following:

$$SK = h(ID_c \oplus a_c \oplus y_c \oplus T1 \oplus T2)$$

Rana et al.'s Scheme

Cryptanalysis

- <u>Stolen Smart Card (Device) Attack</u>
- An adversary ***A*** can steal and gain unprivileged access to a user's smart card (device).
- After getting the unauthorised access, it can guess and find the password of the user, with the following steps:

  1. Suppose, during the registration of User *c*, the adversary ***A*** has got access to the insider information that was transferred via the private channel to the Server ***S*** $\{ID_C, RPW_C\}$
  2. Since, ***A*** has the stolen smart card (device) of the user *c*, he/she can extract all details of the card, via power analysis attacks. $\{\beta_C, \gamma_C, DID_C, \chi_c, \eta_c\}$
  3. Now, ***A*** can calculate the following:

     $\alpha_C{*} = \beta_C \oplus h(ID_C \oplus RPW_C)$
     $y_C{*} = \gamma_C \oplus h(\alpha_C{*} \oplus RPW_C)$
     $\chi{*}_C = h(ID_C \parallel RPW_C \parallel y_C{*} \parallel \alpha_C{*})$

  4. ***A*** will check whether $\chi{*}_C = \chi_C$
  5. If yes, ***A*** will keep guessing a password, until he/she correctly finds it. To check the correctness of the guessed password $PW_c{*}$, ***A*** will do the following:

     $m^* = \eta_C \oplus h(ID_C \oplus PW_C{*})$

     $RPW_C{*} = h(m^* \,||\, PW_C{*})$

     If:

     $RPW_C{*} = RPW_C$

     Then, the guessed password $PW_c{*}$ is the correct password of User *c*

Rana et al.’s Scheme

Cryptanalysis

- User Impersonation Attack
- As described above, as an insider person, adversary ***A*** can have the following information with him/her:
  - $\{ID_c, RPW_c\}$
  - $\{\beta_c, \gamma_c, DID_c, \chi_c, \eta_c\}$
- ***A*** can act as a authorised user *c* and generate a new timestamp $\mathbf{TS_c^f}$ and can send message **M1** to the Server via the open channel.
- The Server S won’t be able to differentiate the user c and adversary A, and will continue its operations in the normal manner.
- In the end, user and server S will calculate the Shared Session Key (SK) using the required parameters.
- Finally, the adversary A will have the shared session key (SK) of the session, authenticated between the Server S and User c.

Rana et al.'s Scheme

Cryptanalysis

- Password Change Attack

- The adversary ***A*** has the ability to find out the password of a User *c*, as described in the Stolen Smart Card (Device) Attack above.

- Hence, ***A*** can easily change the password of user *c*, using the Password Change mechanism of scheme of Rana et al., described below.

Input ID_c^*, PW_c^*, PW_c^N
Compute $m = \eta_c \oplus h(ID_c^* \oplus PW_c^*)$
$RPW_c^* = h(m \| PW_c^*)$
$\alpha_c^* = \beta_c \oplus h(ID_c^* \oplus RPW_c^*)$
$y_c^* = \gamma_c \oplus h(\alpha_c^* \oplus RPW_c^*)$
$\chi_c^* = h(ID_c^* \| RPW_c^* \| y_c^* \| \alpha_c^*)$
Verify $\chi_c^* \stackrel{?}{=} \chi_c$
Compute $RPW_c^N = h(m \| PW_c^N)$
$\beta_c^N = \alpha_c \oplus h(ID_c \oplus RPW_c)$
$\gamma_c^N = y_c \oplus h(\alpha_c \oplus RPW_c)$
$\chi_c^N = h(ID_c \| RPW_c \| y_c \| \alpha_c)$
$\eta_c^N = m \oplus h(ID_c \oplus PW_c)$
Update $\beta_c^N, \gamma_c^N, \chi_c^N, \eta_c^N$ on smart card

Our Scheme

Basic Information

- We have demonstrated our proposed and modified scheme in this section. We have presented the two phases of their scheme: Registration Phase & Login and Authentication Phase.

- We have used user's biometric information to ensure high level of security in our scheme. For the same, we have used a very famous biometrics scheme for its verification, which consists of following two functions:

- $Gen(BIO_{Usr_i}) = (\sigma_{Usr_i}, \tau_{Usr_i})$

- $Rep(BIO'_{Usr_i}, \tau_{Usr_i}) = \sigma_{Usr_i}$

Our Scheme

Symbols

Symbol	Details
U_i	i^{th} user
ID_i	ID (Identity) of User i
S	Server
x, y, z, K	Server's Private Secrets
A	Adversary
PW_i	Password of User i
RPW_i	Hashed Password of User i
h(.)	One-way Collision Resistant Cryptographic Hash Function
Enc_K / Dec_K	Symmetric key encryption/decryption using key K
$rand_1$, $rand_2$, sec, R_i, Y_i	Random Nonces
PID_i	Pseudo ID of User i
BIO_i	Biometrics of User i
Gen(.)	Fuzzy extractor Generation Method
Rep(.)	Fuzzy extractor Reproduction Method
D_i	Device (Smart Card) of User i
TID_i	Temporal ID of User i
TS_i	Timestamp of User Side, during Login Phase of User i
$TS_{S,i}$	Timestamp of Server Side, during Login Phase of User i
ΔT	Maximum Allowable Transmission Delay
SK_i	Session Key of Session between User i & Server S
SKV_i	Session Key Verifier of Session between User i & Server S
$\oplus$	Bitwise XOR Operator
$\|$	Concatenation Operator
$\Rightarrow$	Secure Communication Channel
$\rightarrow$	Public (Insecure) Communication Channel

Our Scheme

Registration Phase

Client (User i)	Server
Input ID_i & PW_i from User i Generate random nonces sec & R_i	
$RPW_i = \mathrm{h}(PW_i \parallel sec)$ $RPW_i' = RPW_i \oplus R_i$	
$M = \{TID_i, ID_i, RPW_i'\}$	
$\Longrightarrow$	
	Generate a random nonce Y_i
	$PID_i = \mathrm{Enc}_K\ (Y_i \parallel ID_i)$ $a_i = \mathrm{h}(x \parallel (ID_i \oplus y) \parallel z)$ $b_i' = a_i \oplus RPW_i'$ $c_i' = Y_i \oplus RPW_i'$ $d_i' = \mathrm{h}(a_i \parallel Y_i \parallel ID_i)$
	Save Pair in Server's DB $\rightarrow \{TID_i,\ PID_i\}$
	$D_i = \{TID_i,\ b_i',\ c_i',\ d_i'\}$
	$\Longleftarrow$
$b_i = (b_i' \oplus RPW_i') \oplus \mathrm{h}(\sigma_i \parallel ID_i \parallel RPW_i)$ $c_i = Y_i \oplus \mathrm{h}(a_i \parallel \sigma_i \parallel ID_i \parallel RPW_i)$ $d_i = \mathrm{h}(\sigma_i \parallel RPW_i \parallel d_i')$ $e_i = sec \oplus \mathrm{h}(\sigma_i \parallel ID_i \parallel PW_i)$	
Update $D_i = \{TID_i,\ b_i,\ c_i,\ d_i,\ e_i,\ \tau_i\}$	

Our Scheme

Login and Authentication Phase

Client (User i)	Server
Input ID_i^*, PW_i^*, BIO_i^* Check whether ID_i^* exists? If NO, then STOP. $\sigma_i^* = \text{Rep}(BIO_i^*, \tau_i)$ $sec = e_i \oplus h(\sigma_i^* \parallel ID_i^* \parallel PW^*)$ $RPW_i^* = h(PW_i^* \parallel \text{sec})$ $a_i^* = b_i \oplus h(\sigma_i^* \parallel ID_i^* \parallel RPW_i^*)$ $Y_i^* = c_i \oplus h(a_i^* \parallel \sigma_i^* \parallel ID_i^* \parallel RPW_i^*)$ $d_i^* = \text{h}(\sigma_i^* \parallel RPW_i^* \parallel \text{h}(a_i^* \parallel Y_i^* \parallel ID_i^*))$ Check $d_i = d_i^*$? If NO, then STOP. Generate a Fresh User Timestamp TS_i Generate a random nonce $rand_1$ $rr_1 = \text{h}(rand_1 \parallel TS_i) \oplus \text{h}(Y_i^* \parallel a_i^* \parallel ID_i^* \parallel TS_i)$ $g_i = \text{h}(a_i^* \parallel (a_i^* \oplus Y_i^*) \parallel Y_i^* \parallel rand_1 \parallel ID_i^* \parallel TS_i)$ $M_1 = \{TID_i, rr_1, g_i, TS_i\}$ $\longrightarrow$	
	Check whether TS_i^* - $TS_i \leq \Delta T$? If NO, then STOP. Fetch PID_i using TID_i from Server DB $(Y_i \parallel ID_i) = \text{Dec}_K\ (PID_i)$ $a_i^* = \text{h}(x \parallel (ID_i \oplus y) \parallel z)$ $rand_1^* = rr_1 \oplus \text{h}(Y_i \parallel a_i^* \parallel ID_i \parallel TS_i)$ $g_i^* = \text{h}(a_i^* \parallel (a_i^* \oplus Y_i) \parallel Y_i \parallel rand_1^* \parallel ID_i \parallel TS_i)$ Check $g_i = g_i^*$? If NO, then STOP. Generate a Fresh Server Timestamp $TS_{S,i}$ Generate a random nonce $rand_2$ Generate new temporal ID of User i, TID_i^{new} $rr_2 = \text{h}(TS_{S,i} \parallel a_i^* \parallel Y_i \parallel ID_i) \oplus \text{h}(rand_2 \parallel TS_{S,i})$ $t_i = \text{h}(TS_{S,i} \parallel (a_i^* \oplus Y_i) \parallel rr_2 \parallel a_i^* \parallel Y_i \parallel ID_i)$ $SK_i = \text{h}((TID_i \oplus TS_i \oplus TS_{S,i} \oplus ID_i \oplus a_i^* \oplus Y_i \oplus$ $\text{h}(rand_2 \parallel TS_{S,i})) \parallel rand_1^*)$ $SKV_i = \text{h}(TS_{S,i} \parallel SK_i \parallel rand_1^*)$ $TID_i^* = TID_i^{new} \oplus \text{h}(TID_i \parallel TS_{S,i} \parallel SK_i)$ $M_2 = \{TID_i^*, t_i, rr_2, SKV_i, TS_{S,i}\}$ $\longleftarrow$
Check whether $TS_{S,i}^*$ - $TS_{S,i} \leq \Delta T$? If NO, then STOP. $t_i^* = \text{h}(TS_{S,i} \parallel (a_i^* \oplus Y_i^*) \parallel rr_2 \parallel a_i^* \parallel Y_i^* \parallel ID_i^*)$ Check $t_i = t_i^*$? If NO, then STOP. $rand_2^* = rr_2 \oplus \text{h}(TS_{S,i} \parallel a_i^* \parallel Y_i^* \parallel ID_i^*)$ $SK_i^* = \text{h}((TID_i \oplus TS_i \oplus TS_{S,i} \oplus ID_i^* \oplus a_i^* \oplus Y_i^* \oplus rand_2^*) \parallel rand_1)$ $SKV_i^* = \text{h}(TS_{S,i} \parallel SK_i^* \parallel rand_1)$ Check $SKV_i = SKV_i^*$? If NO, then STOP. $TID_i^{new} = TID_i^* \oplus \text{h}(TID_i \parallel TS_{S,i} \parallel SK_i^*)$ Update TID_i with TID_i^{new} in D_i	
	Update TID_i with TID_i^{new} in Server's Database (S)

Our Scheme
Implementation

- Implementation : https://colab.research.google.com/drive/1XMoK7xKXrctKSApamqNcvT_SiSRPLTtJ?usp=sharing

Our Scheme

Cryptanalysis

- Server Compromise Attack

- Even if the server's secret keys ***x***, ***y*** and ***z*** are compromised, and messages ***M1*** and ***M2*** are known to the adversary ***A***, then too, the session key can't be found out by ***A***.

- The reason for the same is the inclusion of random nonces used by the User *i* & Server ***S*** to calculate the Shared Session Key (SK).

- Hence, our scheme is secure against Server Compromise Attack.

Our Scheme

Cryptanalysis

- <u>Stolen Smart Card (Device) Attack</u>
- An adversary ***A*** can steal and gain unprivileged access to a user's smart card (device).
- After getting the unauthorised access, ***A*** can't guess the password or find out any other parameter, since for calculating any parameter, there is a requirement of biometrics of User *i* ($\boldsymbol{Bio_i}$) to be known.
- Hence, in any way, ***A*** has no use of the stolen smart card.
- Thus, our scheme is efficient and safe against stolen smart card (device) attacks.

Our Scheme

Cryptanalysis

- <u>User Impersonation Attack</u>
- ***A*** can act as a authorised user i and generate a new timestamp TS_i^f
- But, the new timestamp generated by A will be of no use, as it can't gain access to any other parameter because of unavailability of biometrics of User i (Bio_i), hence, A won't be able to act as an authorised user to S.
- Thus, our scheme is resistant to User Impersonation Attack.

Our Scheme

Cryptanalysis

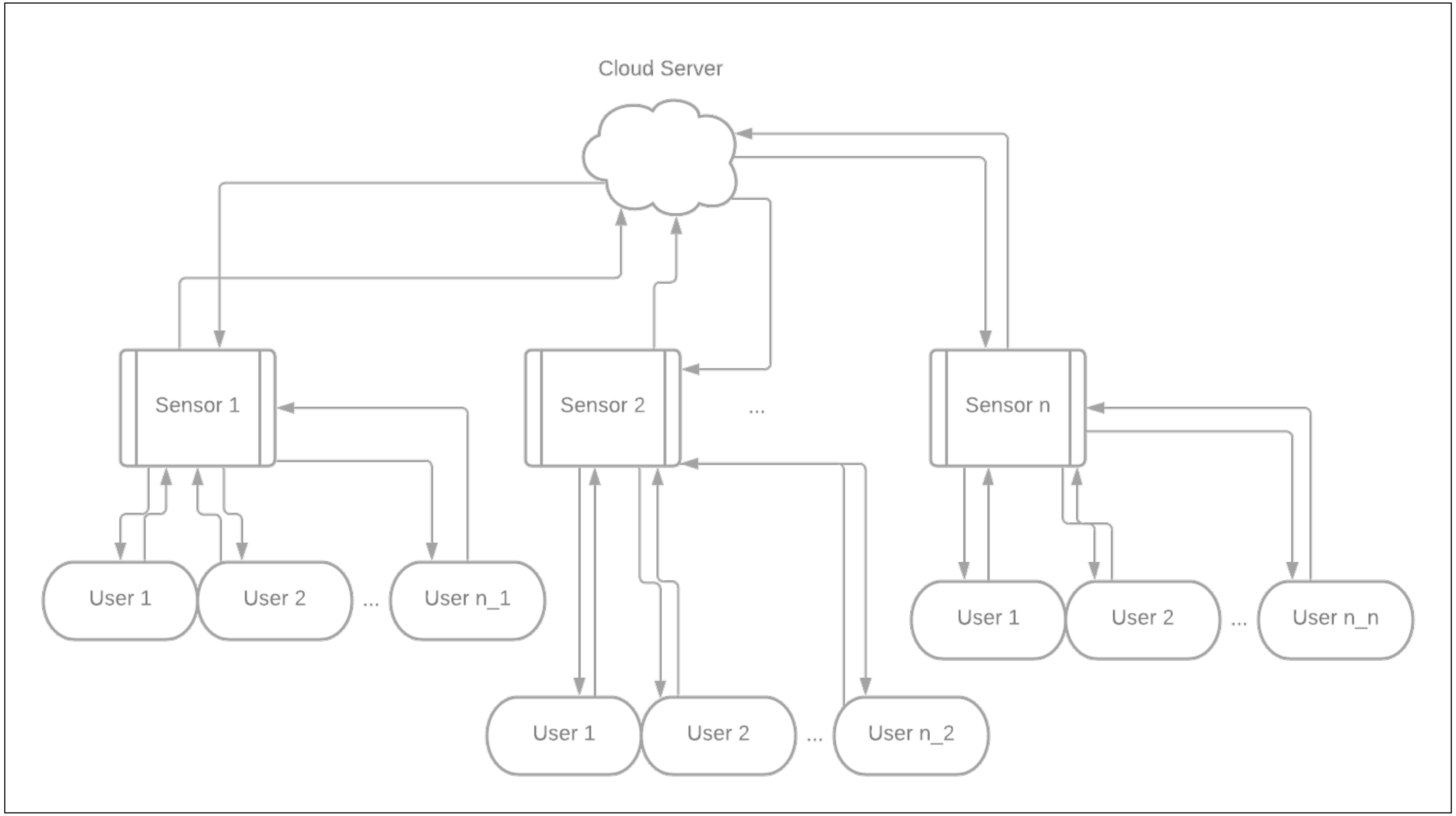
- <u>Password Change Attack</u>

- Since, ***A*** can't find the password of User *i* as described above, hence, ***A*** can't change the password of the user.

- Hence, our scheme is safe against Password Change Attack.

Our Scheme

General Network Diagram



Comparison with Existing Schemes

- In this section, we will compare our scheme with some other existing schemes, with respect to Memory Cost, Communication Cost, Computation Cost and various possible attacks.
- For implementation, we have used PyCrypto Library to implement hash functions in MacOS Catalina.
- We have run our protocol several number of times to measure average computation cost. The average time taken for running collision-resistant hashing function is 0.00080 ms. The average time taken for concatenating is 0.00008 ms. The average times for other operations are negligible and hence aren't taken into account.
- Memory Cost is the memory, in bits, required to store the parameters on the smart card (device) and server's database. In our scheme, we have stored 7 parameters in the smart card (device) and 2 parameters on the server. The memory cost of our scheme is slightly higher than the memory costs of Kaul and Awasthi, Kumari et al., Chang et al. and Rana et al.
- T_h is defined as the time needed for computing hash function
- $T_{||}$ is defined as the time needed for computing concatenation.
- $T_{\oplus}$ is define as the time required for computing XOR operation.
- Communication Cost is the number of bits transferred via the channel during the login and authentication phase of the scheme.
- Computation Cost is the time, in milliseconds (ms), required to run the login and authentication phase.

Comparison with Existing Schemes

(Cont.)

Scheme	Computation Cost	Memory Cost	Communication Cost
Ours	$24T_h + 55T_{\|} + 29T_{\oplus} = 0.0236$ ms	2304 bits	2560 bits
[6]	$20T_h + 27T_{\|} + 29T_{\oplus} = 0.01816$ ms	1536 bits	3296 bits
[5]	$20T_h + 27T_{\|} + 29T_{\oplus} = 0.01784$ ms	1280 bits	2668 bits
[14]	$20T_h + 27T_{\|} + 29T_{\oplus} = 0.01104$ ms	672 bits	2336 bits

Comparison with Existing Schemes
(Cont.)

Resistant to Attack	Ours	[6]	[5]	[14]
Server Compromise Attack	Yes	No	No	No
Password Guessing Attack	Yes	No	No	No
Stolen Smart Card Attack	Yes	No	Yes	Yes
Replay Attack	Yes	Yes	Yes	No
User Impersonation Attack	Yes	No	No	No
Password Change Attack	Yes	No	No	No
Man in the Middle Attack	Yes	Yes	Yes	Yes
Forward and Backward Secrecy	Yes	No	No	No

Future Prospects

- In the future, we want to work further on this scheme and improve it, if we find any other attacks that are possible on the same.
- Other than that, we want to publish this work of mini project as a research paper in a recent upcoming conference. Our preferable conference is MMCITRE-2022 (http://www.mmcitare.com/home.html).

References

[1] Winkler, M., Tuchs, K.-D., Hughes, K., Barclay, G., 2008. Theoretical and practical aspects of military wireless sensor networks. J. Telecommun. Inf. Technol. 37–45.
[2] Kolokotsa, D., 2016. The role of smart grids in the building sector. Energy Build. 116, 703–708.
[3] N. Chen and M. Okada, "Towards 6G Internet of Things and the con- vergence with RoF system," *IEEE Internet Things J.*, early access, Dec. 28, 2020, doi: 10.1109/JIOT.2020.3047613.
[4] Lai, C.-C., Shih, T.-P., Ko, W.-C., Tang, H.-J., Hsueh, P.-R., 2020. Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and corona virus disease-2019 (COVID-19): The epidemic and the challenges. Int. J. Antimicrob. Ag. 105924.
[5] S.D. Kaul, A.K. Awasthi, Security enhancement of an improved remote user authentication scheme with key agreement, Wirel. Pers. Commun. 89 (2) (2016) 621–637.
[6] M. Rana, A. Shafiq, I. Altaf, M. Alazab, K. Mahmood, S. A. Chaudhry, and Y. B. Zikria, "A secure and lightweight authentication scheme for next generation IoT infrastructure," Comput. Commun., vol. 165, pp. 85–96, Jan. 2021.
[7] Lamport, L., 1981. Password authentication with insecure communication. Commun. ACM 24 (11), 770–772.
[8] Z. Zhang, Q. Qi, N. Kumar, N. Chilamkurti, H.-Y. Jeong, A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography, Multimedia Tools Appl. 74 (10) (2015) 3477–3488.
[9] Z. Ali, A. Ghani, I. Khan, S.A. Chaudhry, S.H. Islam, D. Giri, A robust authentication and access control protocol for securing wireless healthcare sensor networks, J. Inf. Secur. Appl. 52 (2020) 102502.
[10] K. Mahmood, X. Li, S.A. Chaudhry, H. Naqvi, S. Kumari, A.K. Sangaiah, J.J. Rodrigues, Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure, Future Gener. Comput. Syst. 88 (2018) 491–500.
[11] S.A. Chaudhry, K. Yahya, F. Al-Turjman, M.-H. Yang, A secure and reliable device access control scheme for IoT based sensor cloud systems, IEEE Access 8 (2020) 139244–139254.
[12] M.L. Das, A. Saxena, V.P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Trans. Consum. Electron. 50 (2) (2004) 629–631.
[13] Y.-y. Wang, J.-y. Liu, F.-x. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, Comput. Commun. 32 (4) (2009) 583–585.
[14] Y.-F. Chang, W.-L. Tai, H.-C. Chang, Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update, Int. J. Commun. Syst. 27 (11) (2014) 3430–3440.
[15] S. Kumari, M.K. Khan, X. Li, An improved remote user authentication scheme with key agreement, Comput. Electr. Eng. 40 (6) (2014) 1997–2012.
[16] Challa, S., Wazid, M., Das, A.K., Kumar, N., Reddy, A.G., Yoon, E.-J., Yoo, K.-Y., 2017. Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access 5, 3028–3043.