Cryptanalysis and Improvement of Barman et al.’s Secure Remote User Authentication Scheme

Chintan Patel, Nishant Doshi

Abstract— In past people used to send the messages in plain text over the public channel. However, this protocol susceptible to various attacks like anyone can read the message, no proper authentication of sender and receiver, tampering, etc. Indeed, Remote User Authentication (RUA) is a technique is the key to solution of all these problems. RUA is scheme in which any remote user can not only authenticate but also transfer the messages over insecure medium to server even though the extraneous physical distance between them. With advancement in technology, the system moved to multi server in which user can connect to the any server and have the secure established session over public channel. Recently, in IEEE Access, Barman et al. proposed the multi-server remote user authentication scheme using the notion of fuzzy commitment and claimed to secure against various attack. However, in this paper we prove that the scheme due to Barman et al. is failed to provide the countermeasure against *user anonymity, server anonymity, Stolen Verifier Attack and perfect forward secrecy attack, lack of level-based authentication*. In this paper, we also propose the novel level dependent authentication scheme for the environment where user wants to get access of live data from the sensor via gateway device. At last, we provide informal security analysis for the proposed scheme. We conclude this paper with some future direction.

Keywords—Multi-Server, Fuzzy Commitment, Information Security, Level-based authentication.

I. Introduction

In today’s world, Information and Communication Technology (ICT) is the key point for any nation to progress. Indeed, ICT relies on the advancement of the technology and importantly the communication. In data communication, not only the speed matters but also security plays vital role due to nature of data. One way to achieve this is to establish the secure communication between all participating entities. However, it will be costly in installation as well as maintenance. In 1981, Lamport [1] proposed the first remote user authentication technique in which any remote user can establish the secure session over the public channel and also authenticate each other too.

These communication systems broadly classified in two categories i.e. single server and multi-server. In single server, only single point of server is there to which all users will connect. In multi-server, more than one server is available, and users are required to connect to either server for possible communication. in general, one Resource Center (RC) will be there for initial setup. Each of the single and multi-server system is categorized either into two factors or three factor schemes. In two factors only the identity and password with smart card is considered while in three factors scheme the biometric identity of user also considered in addition to identity and password.

In [2-22], the authors have proposed the single server-based schemes. In [23-38], the authors have proposed the multi-server-based schemes. Recently in 2018, Barman et al. [39] proposed the multi-server scheme based on the fuzzy commitment analysis and claimed that it is secure against various attacks.

A. Our Contributions

In this paper we have cryptanalysis the fuzzy based multi-server three factor authentication scheme which proposed by the Barman et al. We have shown the following attacks in the scheme of barman et al.

- User anonymity
- Server anonymity
- Perfect Forward secrecy
    - By compromising user’s secret credentials
    - By compromising server’s secret credentials
    - By compromising RC’s secret credentials
- Stolen Verifier Attack

In this paper, we also propose novel ECC based level dependent authentication scheme which is also suitable for Wireless Sensor Network (WSN) and IoT based environment. By keeping the real time scenario in the mind, as an improvement of the proposed scheme, we propose the authentication scheme for User -Gateway/Server – Sensor based environments.

B. Paper organization

In Section II, we have given the preliminaries that we will use throughout this paper. In section III, we have given the

Chintan Patel is PhD Scholar with the Computer Science and Engineering Department, Pandit Deendayal Petroleum University, Gandhinagar, India (e-mail: Chintan.p592@gmail.com).

Nishant Doshi is faculty with the Computer Science and Engineering Department, Pandit Deendayal Petroleum University, Gandhinagar, India (Contact : 792-327-5458 e-mail: doshinikki2004@gmail.com).

scheme of Barman et al. in Section IV, the detailed cryptanalysis is given. In section V, we discuss the proposed scheme. Conclusion and references are at the end.

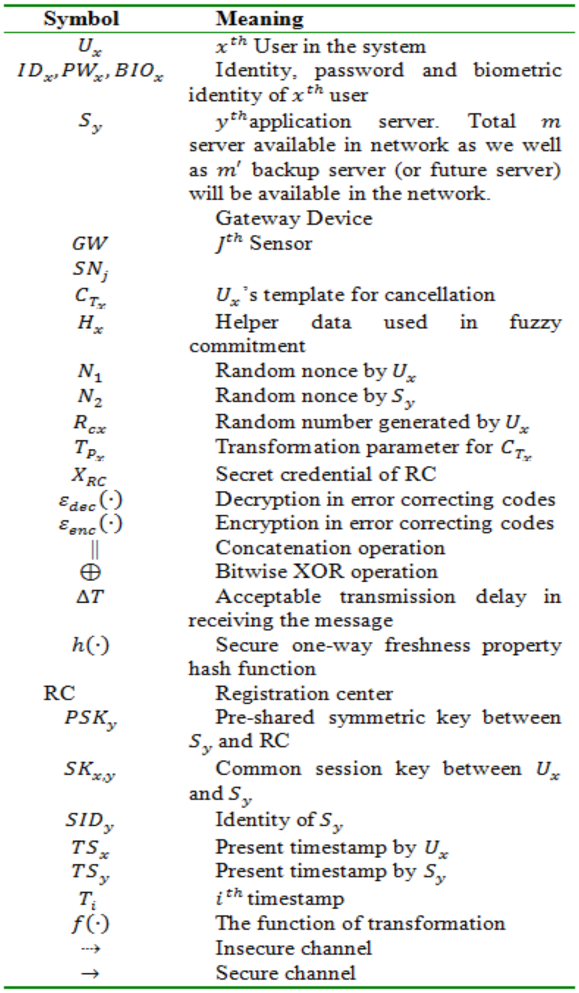
II. PRELIMINARIES

In this section, we will give the preliminaries as well as notations that we will use in the explanation of the Barman et al.'s scheme as well as in the cryptanalysis. Table 1 shows the list of notations.

In addition to the notations, we have given the brief introduction the fuzzy commitment as follows.

As the scheme of Barman et al. uses the biometric as one of the parameters. We can use the one-way hash function to compute the *h(BIO$_x$)*. However, slight change (even single bit) in input of user's biometric can result in invalid entry thus we cannot use hash property for biometric. Thus, researcher come up with fuzzy based commitment.

Table 1. Notations



Symbol	Meaning
U_x	x^{th} User in the system
ID_x, PW_x, BIO_x	Identity, password and biometric identity of x^{th} user
S_y	y^{th}application server. Total m server available in network as we well as m' backup server (or future server) will be available in the network.
	Gateway Device
GW	J^{th} Sensor
SN_j	
C_{T_x}	U_x's template for cancellation
H_x	Helper data used in fuzzy commitment
N_1	Random nonce by U_x
N_2	Random nonce by S_y
R_{cx}	Random number generated by U_x
T_{P_x}	Transformation parameter for C_{T_x}
X_{RC}	Secret credential of RC
$\varepsilon_{dec}(\cdot)$	Decryption in error correcting codes
$\varepsilon_{enc}(\cdot)$	Encryption in error correcting codes
$\|\|$	Concatenation operation
$\oplus$	Bitwise XOR operation
ΔT	Acceptable transmission delay in receiving the message
$h(\cdot)$	Secure one-way freshness property hash function
RC	Registration center
PSK_y	Pre-shared symmetric key between S_y and RC
$SK_{x,y}$	Common session key between U_x and S_y
SID_y	Identity of S_y
TS_x	Present timestamp by U_x
TS_y	Present timestamp by S_y
T_i	i^{th} timestamp
$f(\cdot)$	The function of transformation
$\dashrightarrow$	Insecure channel
$\rightarrow$	Secure channel

In addition to the notations, we have given the brief introduction the fuzzy commitment as follows.

As the scheme of Barman et al. uses the biometric as one of the parameters. We can use the one-way hash function to compute the *h(BIO$_x$)*. However, slight change (even single bit) in input of user's biometric can result in invalid entry thus we cannot use hash property for biometric. Thus, researcher come up with fuzzy based commitment scheme to work with biometric data. More details about this is given in [40-41].

A. *Elliptic Curve Cryptography*

The ECC is a light-weight cryptography defined on the finite field F of order n. The algebraic equation for the Elliptic Curve is defined as follow:

$$Y^2 = X^3 + ax + b \ mod \ n$$

Where X and Y are the point of the elliptic curve while a and b are the constants which must satisfy the following equation.

$$4a^3 + 27b^2 \neq 0$$

In the proposed scheme, we use the elliptic curve point multiplication operation which satisfies the Elliptic Curve Diffie-Hellman and Elliptic Curve Discrete Logarithm Property [40].

III. SCHEME OF BARMAN ET AL.

The scheme of barman et al. is dividing into following main phases.

A. *Server Registration Phase*

The following procedure will be done by all $m + m'$ server in the system.

$S_y \rightarrow RC$: SID_y
RC : Compute $PSK_y = h(SID_y||X_{RC})$
$RC \rightarrow S_y$: PSK_y

B. *User Registration Phase*

The following procedure will be done user U_x and RC
U_x : Choose ID_x, PW_x and T_{P_x}.
Scan biometric data to capture BIO_x.
Select random k.
Compute $C_{T_x} = f(BIO_x, T_{P_x}), RPW_x = h(PW_x||C_{T_x})$.
$U_x \rightarrow RC$: $ID_x, RPW_x \oplus k$
RC : For $\forall j, j \in [1, m + m']$
$US_y = h(ID_x||PSK_y)$
$SV_y = h(SID_y||PSK_y)$
$BM_y = SV_y \oplus (RPW_x \oplus k)$
Store $\{SID_y, AM_y, BM_y\}$ into smart card SC_x
$RC \rightarrow U_x$: SC_x
U_x : Compute $R_c = \varepsilon_{enc}(R_{cx}), H_x = C_{T_x} \oplus R_c, R = h(R_{cx}), r_x = h(R_{cx}||ID_x||PW_x), P = h(R_x), AM_{xy} = (AM_y \oplus k) \oplus r_x, BM_{xy} = (BM_y \oplus k) \oplus r_x$
Store $\{AM_{xy}, BM_{xy}|j \in [1, m + m']\}, T_P, H_x, R, P, h(\cdot), \varepsilon_{enc}(\cdot), \varepsilon_{dec}(\cdot)$ into SC_x

C. *Mutual Authentication with Key Generation Phase*

In this phase user (U_x)/smart card (SC_x) will mutually authenticate the server S_y and if successful than derive the session key Sk_{xy}.

U_x : Scan biometric and extract BIO_x.

$U_x \rightarrow SC_x$: ID_x, PW_x, BIO_x

SC_x : Calculate $C'_{T_x} = f(BIO_x, T'_{P_x}), R'_c = H_i \oplus C'_{T_x}, R'_{cx} = \varepsilon_{dec}(R'_c)$.
Check if $h(R'_{cx}) = R$holds else terminate.
Calculate $r'_x = h(R_{cx}||ID_x||PW_x)$
Check if $h(r'_x) = r_x$ holds else terminate.
Compute $US_y = h(ID_x||PSK_y), SV_y = h(SID_y||PSK_y)$.
Generate random N_1 in time stamp TS_x.
Compute $M_1 = h(ID_x||US_y), M_2 = ID_x \oplus h(SV_y||TS_x), M_3 = M_1 \oplus N_1, M_4 = h(ID_x||M_1||M_2||TS_x||N_1)$

$SC_x \dashrightarrow S_y$: M_2, M_3, M_4, TS_x

S_y : Check if $|TS'_x - TS_x| < \Delta T$ holds else terminate
Compute
$M_5 = M_2 \oplus h(h(SID_y||PSK_y)||TS_x), M_6 = h(M_5||h(M_5||PSK_y)), M_7 = M_3 \oplus M_6 = N_1, M_8 = h(M_5||M_6||M_2||TS_x||M_7)$.
Check if $M_4 = M_8$ holds else terminate
Generate random N_2 in time stamp TS_y
Compute
$M_9 = h(h(M_5||PSK_y)||N_1) \oplus N_2, SK_{xy} = h(M_5||h(SID_y||PSK_y)||N_1||N_2|| TS_x||TS_y), M_{10} = h(h(M_5 \parallel PSK_y) \parallel SK_{xy} \parallel N_2)$.

$S_y \dashrightarrow SC_x$: M_9, M_{10}, TS_y

SC_x : Check if $|TS^*_{xy} - T_y| < \Delta T$ holds else terminate
Compute
$N'_2 = M_9 \oplus h(US_y||N_1), SK'_{xy} = h(ID_x||SV_y||N_1||N'_2||TS_x||TS_y),$
$M_{11} = h(US_y||SK'_{xy}||TS_y||N'_2)$.
Check if $M_{10} = M_{11}$ holds else terminate

$SC_x \rightarrow U_x$: SK'_{xy}

S_j : Store SK_{xy} for secure communication.

IV. CRYPTANALYSIS OF BARMAN ET AL'S SCHEME.

In this section we have proved that the scheme of Barman et al. is susceptible to the various attacks as follows.

A. User Anonymity

The scheme is said to insecure against user anonymity attack if any messages from open channel reveals the identity of user. Let's consider the typical scenario involving two system users U_{x1}, U_{x2} and server S_j. Barman et al. claimed that the system provides the user anonymity as no one can get the identity of user from M_2, M_3, M_4, TS_x. However other users of system can easily guess the identity of users as follows. Consider that U_{x1} send the message < M_2, M_3, M_4, TS_{x1} > to server S_j . U_{x2} follows the steps as below.

- Compute $SV_y = BM_y \oplus (RPW_{x2} \oplus k_{x2})$
- Compute $h(SV_y||TS_{x1}) \oplus M_2 = h(SV_y||TS_{x1}) \oplus ID_{x1} \oplus h(SV_y||TS_{x1}) = ID_{x1}$

Thus, the scheme of Barman et al. is prone to the user anonymity attack.

B. Server Anonymity

The scheme is said to be insecure against server anonymity if identity of server is known from open channel messages. Even though it is not mentioned in M_2, M_3, M_4, TS_x, the user U_x need to specify the server j out of $m + m'$ servers. Thus, the scheme of Barman et al. is prone to the server anonymity attack.

C. Perfect Forward Secrecy

The scheme is said to be insecure against perfect forward secrecy if compromise of long secrets of involving parties can reveal the past as well as present session keys.

- ***Compromise of secret credential of server j***

In this attack, we assume that the attacker gets the secret credential of server yi.e. SID_y, PSK_y. Then the attacker performs the following steps to get the session key SK_{xy},

  - Compute $SV_y = h(SID_y||PSK_y)$
  - From message $< M_2, M_3, M_4, TS_x >$,compute ID_x as discussed in 4.2.
  - Compute $US_y = h(ID_x||PSk_y)$
  - Compute $N_1 = M_3 \oplus h(US_y||ID_x)$
  - Compute $N_2 = M_9 \oplus h(N_1||US_y)$
  - Finally compute $SK_{xy} = h(ID_x || SV_y||N_1||N_2||TS_x||TS_y)$.

This assumption is specifically valid in the situation when attacker lies as an internal member of the system.

- ***Compromise of secret credential of RC***

In this attack, we assume that the attacker compromises the secret credential of RC i.e. X_{RC}. The attacker follows the following steps.

  - Compute $PSK_y = h(X_{RC}||SID_y)$ for any server y

- Compute $SV_y = h(SID_y||PSK_y)$
- From message $< M_2, M_3, M_4, TS_x >$,compute ID_x as discussed in 4.2.
- Compute $US_y = h(ID_x||PSk_y)$
- Compute $N_1 = M_3 \oplus h(US_y||ID_x)$
- Compute $N_2 = M_9 \oplus h(N_1||US_y)$
- Finally compute $SK_{xy} = h(ID_x||SV_y||N_1||N_2||TS_x||TS_y)$

- ***Compromise of secret credential of user***

  In this attack, we assume that the attacker compromises the secret credential of user i.e. ID_x, PW_x and BIO_x. The attacker performs the following to get session key SK_{xy}

  - Calculate $C'_{T_x} = f\left(BIO_x, T'_{P_x}\right), R'_c = H_i \oplus C'_{T_x}, R'_{cx} = \varepsilon_{dec}(R'_c)$.
  - Calculate $r'_x = h\left(R_{cx}||ID_x||PW_x\right)$
  - Compute $US_y = h(ID_x||PSK_y), SV_y = h(SID_y||PSK_y)$.
  - Compute $M_1 = h(ID_x||US_y), N_1 = M_3 \oplus M_1, N_2 = M_9 \oplus h(US_y||N_1)$.
  - Finally compute $SK_{xy} = h(ID_x||SV_y||N_1||N_2||TS_x||TS_y)$

  Thus, the scheme of Barman et al. is prone to the perfect forward secrecy attack.

D. Stolen Verifier Attack

The scheme is prone to stolen verifier attack, if server stores any data relevant to users of the system.

As in Barman's scheme, the server requires to store the *ID* of all system users to be check during the mutual authentication and key agreement phase. Thus, compromising the server's database can compromise the identity of all system users.

E. Lack of Level based Authentication

The scheme of Barman et al. is not suitable for the environment where the Multi-level entities are involved. The environment where the User want to get the live data from the uni-sensor or from the multi-server. The scheme of Barman et al. discusses client-server-based environment which is rare environment in the century of Sensor Network and IoT.

V. PROPOSED SCHEME

In this section, we put forward the proposed level dependent authentication designed using Elliptic Curve Cryptography (ECC). In the proposed scheme, we assume that the gateway device is fully trusted and secure device. The proposed scheme has two phases. 1. Initialize phase and 2. Mutual authentication scheme. In the initialize phase, the gateway device generates required parameters like random numbers, public key for the User device U_i, sensor device SN_j, and Gateway device GW_k. In the mutual authentication phase, the user U_i and sensor node SN_j perform mutual authentication via gateway device GW_k and generates session key. In the proposed scheme, we consider the real time scenario in which user's at different level in the hierarchy will have access of the different level of sensing devices. Example. In the smart university, the students, admin staff, academic staff, and dean will have access of different sensors. The dean will have access of all the sensors while faculty will have access of the sensors of the classroom in which they take lecture and the cabin in which they seat. So, in the proposed scheme, we consider that the User at level will have access of the sensor at level *j* only if $i \leq j$. In the proposed scheme, we make use ECC encryption and decryption protected by random private key [40].

A. Initialize Phase

In the initialize phase, the gateway device generates basic parameters like random numbers, public key and level verification variable for each device involved in offline environment.

- ***Gateway Node Initialize Phase***
  - Gateway Node generates random number as a private key for itself called as$RGWN_k$.
  - Gateway Node generates random number as a master secret for itself called asK_s.
  - Gateway Node computes public key for $RGWN_k$ as a PUB_{RGWN_k} =$RGWN_k * P$.

- ***User U_i Initialize Phase***
  - Gateway Node generates random number as a private key for each user U_i called asRU_i.
  - Gateway Node computes public key for user U_i as a PUB_{U_i} =$RU_i * P$.
  - Gateway node computes $B_1 = H(PUB_{U_i}||K_s)$ and $B_2 = H(l_i||K_s || H(PUB_{U_i}))$ where l_i is level of i^{th} user based on its role in organization.

- ***Sensor Node S_J Initialize Phase***
  - Gateway Node generates random number as a private key for each sensor node SN_j called as RSN_j.
  - Gateway Node compute public key for RSN_j as a $PUB_{SN_j} = RSN_j * P$.
  - Gateway node computes $D_1 = H(PUB_{SN_j}||K_s)$ and $D_2 = H(l_j||K_s || H(PUB_{SN_j}))$ where l_j is level of j^{th} user based on its role in organization.

Gateway node stores private key and public key of each user and sensor in memory securely. All public key will be available to intruders/ attackers/ adversaries.

B. Mutual Authentication Phase

In this subsection, we discuss mutual authentication phase between user U_i and Sensor N_j. The mutual authentication phase consists of following steps.

- $U_i \rightarrow GW_k$

  - Generate random number $r_1 \in F_p$. F_p is finite field on which elliptic curve is defined.
  - $M_1 = H(r_1 || B_1)$.
  - Get current time stamp T_1 .
  - $M_2 = H(M_1 ||PUB_{U_i}|| T_1)$.
  - $M_3 = M_2 \oplus PUB_{U_i}\}$
  - $M_4 = M_1 \oplus M_3$.
  - $M_5 = Enc_{PUB\,RGWN_k}(r_1, PUB_{U_i}, PUB_{RSN_j})$
  - Send (M_3, M_4, M_5, T_1)
- $GW_k \rightarrow S_j$
  - Verify time stamp $\Delta T = T_1^* - T_1$.
  - $M_1^* = M_3 \oplus M_4$
  - Get $(r_1^*, PUB_{U_i}, PUB_{RSN_j}) = Dec_{RGWN_k}(M_5)$
  - Verify $M_1^{**} = H(r_1^* || H(PUB_{U_i}||K_S))$
  - Compute $Tmp\_1 = H(PUB_{RGWN_k}||H(PUB_{RSN_j}||K_s) || T_2)$ and send to sensor S_j with T_2 .
- $S_j \rightarrow GW_k$
  - Verify time stamp $\Delta T = T_2^* - T_2$
  - $Tmp_1^* = H\left(PUB_{RGWN_k}||D_1||T_2\right) =?\ Tmp_1$.
  - Send $M\_6 = H(PUB_{RGWN_k}||D_1||T_3)$, T_3, D_2 to GWN_k.
- $GW_k \rightarrow S_j$
  - Verify time stamp $\Delta T = T_3^* - T_3$
  - $M_6^* = H(PUB_{RGWN_k}|| H(PUB_{RSN_j}||K_s) || T_3)?= M_6$
  - Get l_i and l_j from B_2 and D_2
  - if $l_i \leq l_j$ than allow else deny
  - Compute current time stamp T_4
  - Generate random number k_1
  -

    $M_7 = H(k_1 || PUB_{RGWN_k}||PUB_{RSN_j}||PUB_{U_i}||r_1^* ||$
  - $T_4)$
  - $M_8 = PUB_{RGWN_k} \oplus PUB_{U_i}$
  - $M_9 = Enc_{PUB\,RSN_j}(k_1, r_1^*)$
  - $M_{10} = Enc_{PUB_{U_i}}(k_1)$
  - Send M_7, M_8, M_9, T_4 to SN_j
- $GW_k \rightarrow U_i$
  - Send M_{10}, T_4 to user
- $U_i \rightarrow SN_j$
  - Verify time stamp Verify time stamp $\Delta T = T_4^* - T_4$.
  - Get $k_1^* = Dec_{RU_i}(M_{10})$
  - Generate r_2 .
  - $M_{11} = Enc_{PUB\,RSN_j}(r_2)$
  - Send (M_{11}, T_5) to SN_j
- Session key at User U_i
  - $SK = H((r_1 ||PUB_{U_i}), H(k_1^*||PUB_{RGWN_k}||PUB_{RSN_j}||PUB_{U_i}||r_1), r_2, T_5)$.
- Computation at S_j
  - Verify time stamp Verify time stamp $\Delta T = T_4^* - T_4$.
  - Get $k_1^*, r_1^{**} = Dec_{RSN_j}(M_9)$.
  - $M_7^* = H(k_1^* || PUB_{RGWN_k}||PUB_{RSN_j}||PUB_{U_i}\, r_1^* * ||T_3)?= M_7$
  - if yes than user and gateway mutually Verified
  - $X_1 = H(k_1^* || PUB_{RGWN_k}||PUB_{RSN_j}||PUB_{U_i}||$
  - $r_1^{**})$
  - $X_2 = H(r_1 || RU_i)$ and sleep.
  - Wake up and Verify time stamp $\Delta T = T_5^* - T_5$ after receiving message from user U_i
  - Get $r_2^* = Dec_{RSN_j}(M_{11})$
  - Verify $X_2^* = H(r_1 ||RU_i^*)?= X_2$
- Session key at Sensor S_j
  - $SK = H(X_2 ||X_1 || r_2^* || T_5)$.

VI. CONLUSION

With increasing usage as well as demand data over the internet, it's not only required the security but also the authentication as same time too. Indeed, remote user authentication scheme is the key to this problem. In this paper we have cryptanalysis the fuzzy extractor based multi-server remote user authentication scheme and claim that the scheme is yet vulnerable against various known attack which makes the scheme impractical for real time applications. In this paper, we propose the authentication real-time level dependent authentication scheme which provides secure and reliable session key generation for any sensor network-based data access. The key generation mechanism in the attacked scheme can be used only for the client-server architecture while the proposed scheme can be used for client-server based as well as all IoT based future devices. The level dependent authentication assures that the user who registers for single time, can access all the sensors for which he is eligible. So the computation cost at user side will be significantly reduced. So overall this paper discusses various attacks on the previously published scheme as well as provides unique and more reliable authentication scheme.

REFERENCES

[1] L. Lamport, Password authentication with insecure communication, *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. (1981).

[2] C.-I. Fan, Y.-C. Chan, and Z.-K. Zhang, Robust remote authentication scheme with smart cards, *Comput. Secur*., vol. 24, no. 8, pp. 619–628, (2005).

[3] W.-S. Juang, S.-T. Chen, and H.-T. Liaw, Robust and efficient passwordauthenticated key agreement using smart cards, *IEEE Trans. Ind. Electron.*, vol. 55, no. 6, pp. 2551–2556, Jun. (2008).

[4] D.-Z. Sun, J.-P. Huai, J.-Z. Sun, J.-X. Li, J.-W. Zhang, and Z.-Y. Feng, Improvements of Juang's password-authenticated key agreement scheme using smart cards, *Comput. Standards Interfaces*, vol. 56, no. 6, pp. 2284–2291, (2009).

[5] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, A secure authentication scheme for telecare medicine information systems, *J. Med. Syst.*, vol. 36, no. 3, pp. 1529–1535, (2012).

[6] D. He, C. Jianhua, and Z. Rui, A more secure authentication scheme for telecare medicine information systems, *J. Med. Syst.*, vol. 36, no. 3, pp. 1989–1995, (2012).

[7] Z. Zhu, An efficient authentication scheme for telecare medicine information systems, *J. Med. Syst.*, vol. 36, no. 6, pp. 3833–3838, (2012).

[8] P. Kocher, J. Jaffe, and B. Jun, Differential power analysis, in *Advances in Cryptology—CRYPTO*. Santa Barbara, CA, USA: Springer, pp. 388–397 (1999).

[9] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, Examining smart-card security under the threat of power analysis attacks, *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May (2002).

[10] M. L. Das, A. Saxena, and V. P. Gulati, A dynamic ID-based remote user authentication scheme, *IEEE Trans. Consum. Electron*., vol. 50, no. 2, pp. 629–631, May (2004).

[11] M.-S. Hwang and L.-H. Li, A new remote user authentication scheme using smart cards, IEEE Trans. *Consum. Electron*., vol. 46, no. 1, pp. 28–30, Feb. (2000).

[12] M. Sandirigama, A. Shimizu, and M. T. Noda, Simple and secure password authentication protocol (SAS), *IEICE Trans. Commun.*, vol. E86, no. B6, pp. 1363–1365, (2000).

[13] H. Arshad and M. Nikooghadam, An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC, *Multimedia Tools Appl.*, vol. 75, no. 1, pp. 181–197, (2016).

[14] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York, NY, USA: Springer-Verlag, (2003).

[15] J. K. Lee, S. R. Ryu, and K. Y. Yoo, Fingerprint-based remote user authentication scheme using smart cards, *Electron. Lett.*, vol. 38, no. 12, pp. 554–555, Jun. (2002).

[16] J. Xu, W. T. Zhu, and D. G. Feng, Improvement of a fingerprint-based remote user authentication scheme, in *Proc. Int. Conf. Inf. Secur. Assurance* (ISA), Apr., pp. 87–92. (2008)

[17] C. I. Fan and Y. H. Lin, Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics, *IEEE Trans. Inf. Forensics Security,* vol. 4, no. 4, pp. 933–945, Dec. (2009).

[18] M. K. Khan and J. Zhang, An efficient and practical fingerprint-based remote user authentication scheme with smart cards, in Proc. *Inf. Secur. Pract. Experience,* K. Chen, R. Deng, X. Lai, and J. Zhou, Eds. Berlin, Germany: Springer, 2006, pp. 260–268. (2006)

[19] C. C. Chang and I. C. Lin, Remarks on fingerprint-based remote user authentication scheme using smart cards, *ACM SIGOPS Oper. Syst. Rev.*, vol. 38, no. 4, pp. 91–96, (2004).

[20] Y. L. C. H. Lin, A flexible biometrics remote user authentication scheme, *Comput. Standards Interfaces,* vol. 27, no. 1, pp. 19–23, (2004).

[21] C.-T. Li and M.-S. Hwang, An efficient biometrics-based remote user authentication scheme using smart cards, *J. Netw. Comput. Appl.,* vol. 33, no. 1, pp. 1–5, Jan. (2010).

[22] C. J. Mitchell and Q. Tang, Security of the Lin-Lai smart card based user authentication scheme, Dept. Math., Royal Holloway, Univ. London, Egham, U.K., Tech. Rep. RHUL-MA-2001-0, 2005.

[23] M.-C. Chuang and M. C. Chen, An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics, *Expert Syst. Appl.,* vol. 41, no. 4, pp. 1411–1418, Mar. (2014).

[24] S. K. Sood, A. K. Sarje, and K. Singh, A secure dynamic identity based authentication protocol for multi-server architecture, *J. Netw. Comput*. Appl., vol. 34, no. 2, pp. 609–618, (2011).

[25] B. Wang and M. Ma, A smart card based efficient and secured multiserver authentication scheme, *Wireless Pers. Commun*., vol. 68, no. 2, pp. 361–378, (2013).

[26] D. Yang and B. Yang, A biometric password-based multi-server authentication scheme with smart card, in Proc. *Int. Conf. Comput. Design Appl.*, vol. 5, 2010, pp. 554–559. (2010)

[27] D. Mishra, A. K. Das, and S. Mukhopadhyay, A secure user anonymitypreserving biometric-based multi-server authenticated key agreement scheme using smart cards, *Expert Syst. Appl.,* vol. 41, no. 18, pp. 8129–8143, (2014).

[28] X. Li, Y. Xiong, J. Ma, and W. Wang, An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards, *J. Netw. Comput. Appl.,* vol. 35, no. 2, pp. 763–769, (2012).

[29] A. K. Das, V. Odelu, and A. Goswami, A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in *TMIS, J. Med. Syst*., vol. 39, no. 9, pp. 1–24, (2015).

[30] R. Amin and G. P. Biswas, A novel user authentication and key agreement protocol for accessing multi-medical server usable in *TMIS, J. Med. Syst.*, vol. 39, no. 3, pp. 1–17, (2015).

[31] Y. Lu, L. Li, X. Yang, and Y. Yang, Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards, *PLoS ONE*, vol. 10, no. 5, p. e0126323, (2015).

[32] C. Wang, X. Zhang, and Z. Zheng, Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme, *PLoS ONE*, vol. 11, no. 2, p. e0149173,(2016).

[33] D. He and D. Wang, Robust biometrics-based authentication scheme for multiserver environment, *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. (2015).

[34] V. Odelu, A. K. Das, and A. Goswami, A secure biometrics-based multiserver authentication protocol using smart cards, *IEEE Trans. Inf. Forensics Security,* vol. 10, no. 9, pp. 1953–1966, Sep. (2015).

[35] A. G. Reddy, A. K. Das, V. Odelu, and K. Y. Yoo, An enhanced biometric based authentication with key-agreement protocol for multi-server architecture based on elliptic curve cryptography, *PLoS ONE,* vol. 11, no. 5, p. e0154308, (2016).

[36] A. G. Reddy, E. J. Yoon, A. K. Das, V. Odelu, and K. Y. Yoo, Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment, *IEEE Access*, vol. 5, pp. 3622–3639, (2017).

[37] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment, *IEEE Trans. Dependable Secure Comput.,*doi: 10.1109/TDSC.2016. 2616876. (2018)

[38] S. Kumari et al., A provably secure biometrics-based authenticated key agreement scheme for multi-server environments, *Multimedia Tools Appl.,* vol. 77, no. 2, pp. 2359–2389, (2018).

[39] Subhas Barman, Ashok Kumar Das, DebasisSamanta, Samiran Chattopadhyay, Joel J. P. C. Rodrigues and Youngho Park., Provably Secure Multi-Server Authentication Protocol Using Fuzzy Commitment", *IEEE Access,* vol. 6, pp. 38578-38594, (2018).

[40] Patel, Chintan, and Nishant Doshi. Internet of Things Security: Challenges, Advances, and Analytics. Auerbach Publications, 2018.

Chintan Patel is a research scholar in the Department of Computer Engineering at Pandit Deendayal Petroleum University, Gandhinagar Gujarat. Mr. Patel is having more than 4 years of experience in academics. He has completed masters from SRM University, Chennai India, and Pursuing Ph.D. from PDPU, Gandhinagar India. With the active academic, he is an active researcher and has published papers in various reputed journals like Springer. His main area of interest includes Cryptography, Wireless Sensor Network, and the Internet of Things. M.r Patel has also published an article with springer's reputed journal Wireless personal communication. Recently he has published book titled "Internet of Things Security Challenges, Advances, and Analytics" with CRC Press. He has also worked as a Microsoft student partner for SRM University. He is an active member of IEEE, Computer Society of India and Many other international organizations. Mr. Patel has authored various books with TATA Macgraw hill and Amazon. Currently, he is working on the Internet of Things and Cryptography

Dr. Nishant Doshi is an academician and researcher with more than 6 years' experience. Currently, he is a faculty member in the Department of Computer Engineering at PDPU, Gandhinagar, India since 2016.India. His main research interests include algorithms, cryptography, and remote user authentication, information protection in general. He has completed masters from DA-IICT, Gandhinagar in 2009 and doctorate from National Institute of Technology, Surat in 2014. Along with active researcher and editorial members of various reputed journals like Springer.

Dr.Doshi is a reviewer of various reputed journals like springers and IEEE Transactions. he is Editor-in-Chief of journals like IJCES, IJECEE, IJME, IJMES, and IJSCE. He has also authored books on cryptography and programming with various reputed publications like CRC and Amazon. He was rewarded as Young Scientist Award of India from Venus International Foundation for 2015 and 2017. Dr. Doshi is a member of IEEE, ACM and many more international and national scientific bodies.