# Analysis of Fuzzy Based Provably Secure Multi-Server Authentication Remote User Authentication Scheme

NISHANT DOSHI
Department of Computer Science and Engineering
Pandit Deendayal Petroleum University
Raisan, Gandhinagar, Gujarat
INDIA
Doshinikki2004@gmail.com http://orsp.pdpu.ac.in/adminfacviewprofile.aspx?facid=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* and *perfect forward secrecy attack*.

*Key-Words:* - Multi-Server, Fuzzy Commitment, Information Security.

## 1 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 factor and three factor schemes. In two factor only the identity and password with smart card is considered while in three factor 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.

### 1.1 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

### 1.2 Paper organization

In Section 2, we have given the preliminaries that we will use throughout this paper. In section 3, we have given the scheme of Barman et al. in Section 4, the detailed analysis is given. Conclusion and references are at the end.

## 2 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.

**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. |
| $C_{T_x}$ | $U_x$'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 |
| $\Delta T$ | 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 $S_y$ |
| $f(\cdot)$ | 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 parameter. 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 can not 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].

# 3 Scheme of Barman et al.

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

## 3.1 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 $PSK_y = h(SID_y || X_{RC})$

$RC \rightarrow S_y$: $PSK_y$

## 3.2 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 $\{AM_{xy}, BM_{xy} | j \in [1, m + m']\}, T_P, H_R, P, h(\cdot), \varepsilon_{enc}(\cdot), \varepsilon_{dec}(\cdot)$ into $SC_x$

## 3.3 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 $M_9 = h(h(M_5||PSK_y)||N_1) \oplus N_2, SK_{xy} = h(M_5||h(SID_y||PSK_y)||N_1||N_2||TS_x||TS_y), M_{10} = h(h(M_5 \| PSK_y) \| SK_{xy} \| N_2)$.

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

$SC_x$ : 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.

# 4 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.

## 4.1 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. ■

## 4.2 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. ■

## 4.3 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.

### 4.3.1 Compromise of secret credential of server *j*

Assume that the attacker gets the secret credential of server $y$i.e. $SID_y, PSK_y$. 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 $SK_{xy} = h(ID_x||SV_y||N_1||N_2||TS_x||TS_y)$.

#### 4.3.2 Compromise of secret credential of RC

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 $SK_{xy} = h(ID_x||SV_y||N_1||N_2||TS_x||TS_y)$

#### 4.3.3 Compromise of secret credential of user

Assume that the attacker compromise the secret credential of user i.e. $ID_x$,$PW_x$ and $BIO_x$. The attacker perform the following to get session key $SK_{xy}$

- Calculate $C'_{T_x} = f(BIO_x, T'_{P_x}), R'_c = H_i \oplus C'_{T_x}, R'_{cx} = \varepsilon_{dec}(R'_c)$.
- Calculate $r'_x = h(R_{cx}||ID_x||PW_x)$
- 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. ■

## 5 Conclusion and Future Work

With increasing usage as well as demand data over the internet, it's not only require 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 future, we hope to have lightweight scheme that to be practical in real time scenario.

*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 password authenticated 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 anonymity preserving 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, Debasis Samanta, 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).