REVIEW ARTICLE

SAMRIDDHI Volume 14, Issue 2, 2022 Print ISSN: 2229-7111 Online ISSN: 2454-5767

Session Handover among Fog Devices using Polynomials

Priyank Nayak, Ravi K.S. Pippal

Vedica Institute of Technology Ram Krishna Dharmarth Foundation University, Bhopal, Madhya Pradesh, India

Abstract

In the past, authentication and authorization issues were not considered especially in the context of Fog computing. They were discussed in the context of machine-to-machine and smart grids communications. The employable authentication and authorization techniques in Fog computing have been discussed earlier. However, they may not be appropriatefor Fog computing as none of them have discussed the facility of session handover among registered fog devices. If due to some problem/unavailability/down of fog devices, any user desires to switch the present fog device then they were not allowed to migrate among all registered fog devices.This study proposes a session handover scheme among fog devices using Lagrange Interpolating Polynomial. Use of Lagrange Interpolating Polynomial instead of costly, time-consuming exponential computation makes it feasible for practical implementation. If due tosome problem, any user desires to switch the present fog device then our scheme allows him/her to migrate among all registered fog devices.

Keywords: Attacks, Authentication, Fog devices, Interpolation, Password, PFS, Security, Smart Card.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2022); DOI: 10.18090/samriddhi.v14i03.20

Introduction

Fog processing is proposed to resolve the issue related with Cloud registering worldview to fulfill the need of portability support, area mindfulness and low inactivity.[1] As Fog registering is executed at the edge of the organization, it offers exceptionally low dormancy, area mindfulness with worked on Quality-of-Services (QoS) for ongoing applications. In the Fog worldview, verification of imparting parties is essential. In any case, single element verification isn't adequate. Accordingly, two element verification plans were proposed and suggested by various creators. In this unique circumstance, Chang and Wu.[2] proposed a confirmation conspire in view of passwords which kills the job of check table to endure every one of the expected assaults. These secret key based brilliant card validation plans are additionally ordered into two significant classes: timestamp based and nonce based.[3] In any case, it is shown that these plans have inadequacies.[4,5] To lessen the clock synchronization execution cost, nonce based plans have been recommended.[6,7] As of late, verification in view of shrewd card has been sent constantly in various parched regions like distributed computing,[8] medical care,[9] key trade in IPTV broadcasting,[10] remote organizations,[11] multi-server validation,[12] and remote sensor networks.[13] Consequently, it is important to deal with recognized potential assaults alongside all security prerequisites related with secret word based savvy card validation plans.[14]

Before, the issues connected with confirmation and approval were not viewed as particularly with regards to Fog registering. They were talked about with regards to machine-to-machine[15] and shrewd lattices correspondences.[16] The verification and approval strategies that can be utilized in Fog figuring have been talked about before at the same time, not a solitary one of them have examined the office of meeting relocation among enlisted haze gadgets. In the event that in light of some issue/inaccessibility, any client wants to switch the current mist gadget then he/she has not been permitted to move among all enlisted haze gadgets.

The remainder of this paper is coordinated as follows. Section 2 presents the proposed brilliant card based meeting movement conspire among haze gadgets. Section 3 finishes up the paper.

Corresponding Author: Priyank Nayak, Vedica Institute of Technology Ram Krishna Dharmarth Foundation University, Bhopal, Madhya Pradesh, India, e-mail: nayak.priyank123@gmail.com

How to cite this article: Nayak, P., Pippal, R.K.S. (2022). Session Handover among Fog Devices using Polynomials. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 14(3), 376-380.

Source of support: Nil

Conflict of interest: None

Smart Card based Session Handover Scheme among Fog devices

The notations/symbols used in this paper are given in Table 1.

Table 1: Symbols with their meaning

Notations	*Their Meaning*
FD	Fog Devices
CAS	Cloud Authentication Server
x	Secret key of CAS
P	Large prime number
g	Primitive element in Z_P^*
ID, PW	Identity and password chosen by User
$ID_1, ID_2, \ldots, ID_m$	Identity of 'm' FDs that user wants to register
VT_j	Validity time period of FD 'j'
$h(\bullet)$	Secure one way hash function
$E_k(\bullet)$	Encryption operation using key 'k'

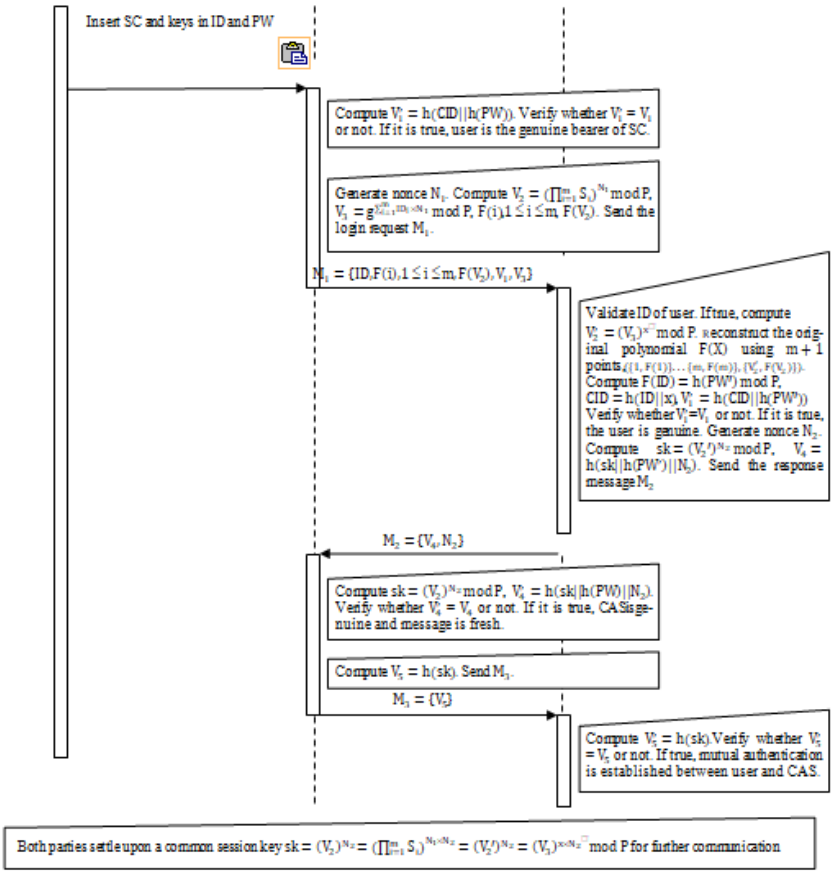

Figure1: Login and Authentication phase of our proposed session handover scheme

The proposed scheme consists of three stages:

- Registration,
- Login and Verification and
- Session handover/switch

Registration Phase

In this phase, user selects ID, PW and IDs of 'm' FDs which he/she wants to register $(ID_1, ID_2, \ldots, ID_m)$, computes $h(PW)$ and submits $\{ID, h(PW), ID_1, ID_2, \ldots, ID_m\}$ to the CAS. After receiving the registration request from user, the CAS computes $CID = h(ID||x)$, $V_1 = h(CID||h(PW))$, $S_i = g^{(ID_i \times x)} \bmod P$, $1 \le i \le m$ and constructs the lagrange interpolating polynomial

$$F(X) = \sum_{j=1}^{m} (VT_j) \frac{(X - ID)}{(S_j - ID)} \times \prod_{j=1, j \neq k}^{m} \frac{(X - S_j)}{(S_k - S_j)} + h(PW) \prod_{i=1}^{m}$$

$$= C_m X^m + C_{m-1} X^{m-1} + C_{m-2} X^{m-2} + \ldots + C_1 X + C_0$$

CAS issues a smart card over secure channel to user by storing $\{CID, V_1, S_1, S_2, \ldots S_m, h(\bullet), E(\bullet), F(X), P\}$ into smart card memory.

Login and Verification Phase

In this phase, user inserts his/hersmart card into the card reader and keys in IDand PW. After this, the smart card computes $V_1' = h(CID||h(PW))$and verifies whether the value of stored $V_1$and computed V_1' are equal or not (Figure 1). If it is true, then the useris the genuine and legitimate

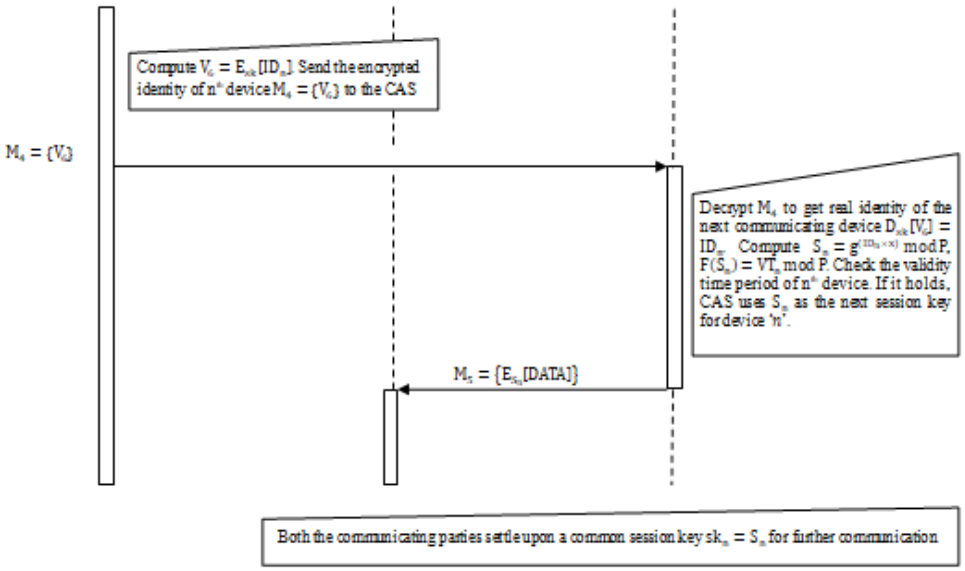

Figure 2: Session Handover/Switch phase of our proposed session handover scheme

bearer of smart card. After this, the smart cardgenerates a random nonce N_1, computes $V_2 = (\prod_{i=1}^{m} S_i)^{N_1} \bmod P$, $V_3 = g^{\sum_{i=1}^{m} ID_i \times N_1} \bmod P$, $F(i),\ 1 \le i \le m,\ F(V_2)$ and sends the login request $M_1 = \{ID, F(i), 1 \le i \le m, F(V_2), V_1, V_3\}$ to the CAS. Upon receiving the login request $M_1 = \{ID, F(i), 1 \le i \le m, F(V_2), V_1, V_3\}$; CAS first checks the validity of ID to accept/reject the login request. If true, CAS computes $V_2' = (V_3)^x \bmod P$.

Theorem1 The CAS can get $V_2 = (\prod_{i=1}^{m} S_i)^{N_1} \bmod P$ using received V_3 and its secretly stored key 'x'.

Proof After getting V_3 from the received login request $M_1 = \{ID, F(i), 1 \le i \le m, F(V_2), V_1, V_3\}$; CAS can compute V_2' by using its own secret key 'x' as follows:

$$V_2' = (V_3)^x \bmod P$$
$$= \left(g^{\sum_{i=1}^{m} ID_i \times N_1}\right)^x \bmod P$$
$$= (g^{ID_1 \times N_1 + ID_2 \times N_1 \ldots\ldots ID_m \times N_1})^x \bmod P$$
$$= (g^{(ID_1 + ID_2 \ldots\ldots ID_m) N_1 \times x}) \bmod P$$
$$= (g^{(ID_1 \times x + ID_2 \times x \ldots\ldots ID_m \times x) N_1}) \bmod P$$

UserSC TerminalCAS

Insert SC and keys in ID and PW

$M_1 = \{ID, F(i), 1 \le i \le m, F(V_2), V_1, V_3\}$

$M_2 = \{V_4, N_2\}$

$M_3 = \{V_5\}$

$$= ((g^{ID_1 \times x}) \times (g^{ID_2 \times x}) \times \ldots . (g^{ID_m \times x}))^{N_1} \bmod P$$

$$= (\prod_{i=1}^{m} S_i)^{N_1} \bmod P.$$

Using these $m+1$ points, $(\{1, F(1)\}, \{2, F(2)\}, \{3, F(3)\}, \ldots \{m, F(m)\}, \{V_2', F(V_2)\})$ CAS reconstructs original interpolation polynomial $F(X) = C_m X^m + C_{m-1} X^{m-1} + C_{m-2} X^{m-2} + \ldots + C_1 X + C_0$ m and finds $h(PW')$ by calculating $F(ID) = h(PW') \bmod P$.

Theorem 2 The CAS can get user's secret information $h(PW')$ from the polynomial $F(ID)$.

Proof After reconstructing the original polynomial $F(X)$, the CAS can get $h(PW')$ as follows:

$$F(ID) = \sum_{j=1}^{m} (VT_j) \frac{(ID - ID)}{(S_j - ID)} \times \prod_{j=1, j \ne k}^{m} \frac{(ID - S_j)}{(S_k - S_j)} + h(PW')$$

$$\prod_{l=1}^{m} \frac{(ID - S_l)}{(ID - S_l)} \bmod P$$

$$F(ID) = 0 \times \prod_{j=1, j \ne k} \frac{(ID - S_j)}{(S_k - S_j)} + h(PW') \times 1 \bmod P$$

$$F(ID) = h(PW') \bmod P.$$

After computing$h(PW')$, CAS computes $CID = h(ID||x)$, $V_1' = h(CID||h(PW'))$ and verifies whether it is equal to received V_1 or not. If it is true, user is genuine. Now, CAS generates random nonce N_2, computes $sk = (V_2')^{N_2} \bmod P$, $V_4 = h(sk||h(PW')||N_2)$ and sends the response message $M_2 = \{V_4, N_2\}$ back to the user. Once the response message $M_2 = \{V_4, N_2\}$ is received, smart card computes $sk = (V_2)^{N_2} \bmod P$, $V_4' = h(sk||h(PW)||N_2)$ and verifies whether it is equal to received V_4 or not. If it holds, CAS is genuine and message is fresh else terminates the session. Consequently, the smart card computes $V_5 = h(sk)$ and sends $M_3 = \{V_5\}$ to the CAS. Once received, CAS can easily verify it. Finally, mutual authentication is accomplished between user and CAS. Both the communicating parties settle upon a common shared session key $sk = (V_2)^{N_2} = (\prod_{i=1}^{m} S_i)^{N_1 \times N_2} = (V_2')^{N_2} = (V_3)^{x \times N_2} \bmod P$ for further communication.

Session Handover/ Switch Phase

If because of some problem, userdesires to switch the present FD to FD 'n' ($1 \le n \le m$) then the user computes $V_6 = E_{sk}[ID_n]$ and sends particular FD'sencrypted identity $M_4 = \{V_6\}$ to the CAS. After receiving M_4, CAS decrypts it and gets real identity of the next communicating FD by computing $D_{sk}[V_6] = ID_n$. To check whether the FD 'n' is valid or not, CAS computes $S_n = g^{(ID_n \times x)} \bmod P$ and $F(S_n)$.

$$F(S_n) = \sum_{j=1}^{m} (VT_j) \frac{(S_n - ID)}{(S_j - ID)} \times \prod_{j=1, j\neq k}^{m} \frac{(S_n - S_j)}{(S_k - S_j)} + h(PW) \prod_{l=1}^{m} \frac{(S_n - S_l)}{(ID - S_l)} \bmod P$$

$$h(PW) \prod_{l=1}^{m} \frac{(S_n - S_l)}{(ID - S_l)} \bmod P = \frac{(S_n - S_n)}{(ID - S_n)} \times h(PW) \prod_{l=1, l\neq n}^{m} \frac{(S_n - S_l)}{(ID - S_l)} \bmod P = 0$$

If $j \neq n$, then

$$\prod_{j=1, j\neq k}^{m} \frac{(S_n - S_j)}{(S_k - S_j)} = \frac{(S_n - S_j)}{(S_n - S_j)} \times \prod_{j=1, j\neq k j\neq n}^{m} \frac{(S_n - S_j)}{(S_k - S_j)} \bmod P = 0$$

Hence,

$$F(S_n) = (VT_n) \frac{(S_n - ID)}{(S_n - ID)} \times \prod_{j=1, j\neq k}^{m} \frac{(S_n - S_j)}{(S_n - S_j)} + 0 \bmod P = (VT_n) \bmod P$$

Finally, CASverifies the validity time period of FD 'n'. If it holds, CAS uses S_n as the next session key for FD 'n'. As all the connected FDs were initially registered with the CAS, no need to again verify the authenticity of the FDs. Only a genuine FD can get the data coming from the CAS as it has the information about S_i, ($1 \le i \le m$) stored in its memory securely (Figure 2).

Conclusion

In the past, the issues related to authentication and authorization were not considered especially in the context of Fog computing. They were discussed in the context of machine-to-machine and smart grids communications.The authentication and authorization techniques that can be used in Fog computing have been discussed earlier but, none of them have discussed the facility of session handover among registered fog devices. If because of some problem/ unavailability, any user desires to switch the present fog device then they have not been allowed to switch among all registered fog devices.

This paper proposes a session handover scheme among fog devices using Lagrange Interpolating Polynomial. Use of Lagrange Interpolating Polynomial instead of costly, time-consuming exponential computation makes it feasible for practical implementation. To handle the problem of synchronized clocks among between users's registered FDs and the CAS especially in large systems, random nonce is used instead of timestamp. The presented scheme provides the facilities through which CAS can efficiently verify the identity of user's registered FDs earlier than granting the privileges to access data from the CAS. As all the connected FDs were initially registered with the CAS, no need to again verify the authenticity of the registered FDs.

Usernth Registered FDCAS

Acknowledgments

The authors would like to thank Vedica Institute of Technology, Bhopal for providing the academic support.

References

[1] Bonomi F. Connected vehicles, the internet of things, and Fog computing. The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA, 2011; 13–15.

[2] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," IEE Proceedings E: Computers and Digital Techniques, vol. 138, 1991, pp. 165-168.

[3] R. Song, "Advanced smart card based password authentication protocol," Computer Standards & Interfaces, vol. 32, no. 5-6, 2010, pp. 321-325.

[4] R. S. Pippal, Jaidhar C. D. and S. Tapaswi, "Comments on symmetric key encryption based smart card authentication scheme," In Proceedings of the 2nd International Conference on Computer Technology and Development, Cairo, Egypt, 2010, pp. 482-484.

[5] R. S. Pippal, Jaidhar C. D. and S. Tapaswi, "Security vulnerabilities of user authentication scheme using smart card," In Proceedings of the 26th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy, Paris, France, 2012, pp. 106-113.

[6] J. Y. Liu, A. M. Zhou and M. X. Gao, "A new mutual authentication scheme based on nonce and smart cards," Computer Communications, vol. 31, no. 10, 2008, pp. 2205-2209.

[7] R. S. Pippal, Jaidhar C. D. and S. Tapaswi, "Highly secured remote user authentication scheme using smart cards," In Proceedings of the 7th IEEE Conference on Industrial Electronics and Applications, Singapore, 2012, pp. 1001-1005.

[8] Z. Hao, S. Zhong and N. Yu, "A time-bound ticket-based mutual authentication scheme for cloud computing," International Journal of Computers, Communications and Control, vol. 6, no. 2, 2011, pp. 227-235.

[9] Jiankun Hu, Hsiao-Hwa Chen and Ting-Wei Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/ security regulations," Computer Standards and Interfaces, vol. 32, no. 5-6, 2010, pp. 274-280.

[10] R. S. Pippal, S. Tapaswi and Jaidhar C. D., "Secure key exchange scheme for IPTV broadcasting", Informatica, vol. 36, no. 1, 2012, pp. 47-52.

[11] D. He, M. Ma, Y. Zhang, C. Chen and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," Computer Communications, vol. 34, no. 3, 2011, pp. 367–374.

[12] S. K. Sood, A. K. Sarje and K. Singh, **"**A secure dynamic identity based authentication protocol for multi-server architecture," Journal of Network and Computer Applications, vol. 34, no. 2, 2011, pp. 609-618.

[13] R. Fan, D. He, X. Pan and L. Ping, "An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks," Journal of Zhejiang University-SCIENCE C (Computers and Electronics), vol. 12, no. 7, 2011, pp. 550-560.

[14] R. S. Pippal, Jaidhar C. D. and S. Tapaswi, "Security issues in smart card authentication scheme", International Journal of Theory and Engineering, vol. 4, no. 2, 2012, pp. 206-211.

[15] Lu R, Li X, Liang X, Shen X, Lin X. GRS: the green, reliability, and security of emerging machine to machine communications. IEEE Communications Magazine 2011; 49(4):28–35.

[16] Wang W, Lu Z. Survey cyber security in the smart grid: survey and challenges. Computer Networks 2013; 57(5):1344–1371.