Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 220 (2023) 886–891

Procedia Computer Science

www.elsevier.com/locate/procedia

The 6th International Workshop on Recent Advances on Internet of Things: Technology and Application Approaches (IoT-T&A)
March 15-17, 2023, Leuven, Belgium

Cryptanalysis of Authentication Protocol for Cloud Assisted IoT Environment

Nishant Doshi, Payal Chaudhari*

Pandit deendayal Energy Unviersity, Gandhinagar, Gujarat, India

Abstract

In today's wireless based applications, sensors are playing the vital role due to its pluses like low cost, low maintenance, hostile environment etc. On other end, cloud based technologies are increasing day-by-day to make its presence in the life of people for processing large chunk of data. Also, Internet of Things (IoT) is making its way by utilizing the sensors for various internet based applications and to connect to them with cloud. In all of these technologies, the major issue is authentication i.e. user from distance can access the server and authenticate via insecure channel. Recently, Lee et al. proposed the authentication scheme in IoT based environment using sensors and claimed it to be secure against various attacks. However, in this research we have analyzed the scheme and prove that it is yet susceptible to key control, time synchronization and stolen verifier. In addition, there will be overhead for verification which can lead to the DoS attack for large setup.

Keywords: IOT; Cloud; Sensors; Authentication Protocols;

1. INTRODUCTION

Internet of Things (IoT) is making its way in today's technology in various areas of the human life like smart city, smart agriculture, smart transportation etc. [1-8]. Sensors are applying the vital role in IoT based applications for

* Corresponding author. Tel.: +91-792-325-359
E-mail address: payal.ldrp@gmail.com

10.1016/j.procs.2023.03.120

required tasks in hostile environments. On the other side, cloud based technologies makes its vital role due to high level of data from the IoT based applications.

One of the prevalent issues in this scenario is authentication from sensor device to the end server. Thus, to resolve this issue in [9], Lamport firstly propose the scheme of remote user authentication protocol in which user can set the session key with server apart from authentication even though the physical distance between them is much larger.

Indeed, key agreement as well as authentication is prime issue for any data transfer to begin. The existing schemes can be broadly classified into various categories like one factor, two factor and three factors [10-39]. Indeed, three factor will be more secures however requires more infrastructure as to others. As the messages are transmitted on the open channel, the channel is susceptible to the various attacks like stolen smart card, man-in-middle, etc.

Afterwards in research [40-46], many researchers have proposed various key agreement protocols as well as given the cryptanalysis of the earlier schemes. Recently in [47], Lee et al proposed the three factor authentication scheme and proved to be efficient as well as secure as compared to the earlier schemes. However, in this paper we have proved that the scheme is yet susceptible to the various attacks.

1.1. Our Contribution

In this paper, we have given the analysis of the Lee et. al [47] scheme and showed the following attacks.

- Key Control : session key will be control from one side of authority.
- Time synchronization : any delay in time requires the resend of same message multiple times.
- Replay attack : detecting the same message at various level requires more resources.
- Stolen verifier : compromise of data from either entity can lead to compromise of session key.

1.2. Paper Organization

In section 2, we have given the scheme of Lee et al.[47]. In section 4, we have given the cryptanalysis of Lee et al [47] scheme. In Section 5, we have given the conclusion with scope of future work. References are at the end.

2. SCHEME OF LEE ET AL

In this section we have given the scheme of Lee et al.[47]. It is divided into various phases as follows.

Service User Registration Phase

It will be between Service User U_i and Gateway GW.

- U_i: Inputs ID_i and PW_i and imprints B_i.
- U_i: Generates α and R_u.
- U_i: Computes GEN(B_i) = (R_i, P_i),
- U_i: $HID_i = h(ID_i \| R_i)$,
- U_i: $HPW_i = h(ID_i \| PW_i \| R_u \| R_i)$.
- $U_i \rightarrow GW$: $<HID_i, HPW_i \oplus \alpha>$
- GW: Secret Key : K_{gw}
- GW: Checks Uniqueness ofHID_i
- GW: Generate a random nonce R_{gw}
- GW: Computes $A_i = h(HID_i \| K_{gw} \| R_{gw})$,
- GW: $B_i = A_i \oplus (HPW_i \oplus \alpha)$,
- GW: C_i = h($A_i \| HID_i$).
- GW: Generates temporary user identity $THID_i$.
- GW: Stores {($HID_i, THID_i$),R_{gw}, honey_list = null}
- $GW \rightarrow U_i$: SC = $< B_i, C_i, THID_i >$ via secure channel
- U_i: $L_i = h(ID_i \| PW_i \| R_i) \oplus R_u$,

- U_i: $B'_i = B_i \oplus \alpha = A_i \oplus, HPW_i,$
- U_i: $C'_i = h(C_i \| HPW_i)$.
- U_i: Store $\{L_i, B'_i, C'_i, THID_i\}$ into SC.

Sensing Device Registration Phase

It will be between Sensing Device SD_j and Gateway GW

- SD_j: Picks identity SID_j and Challenge C_j.
- SD_j: Generate random nonce R_{sd}.
- SD_j:Compute $Req_j = SID_j \oplus h(R_{sd})$,
- SD_j: $R_j = PUF(C_j)$.
- SD_j: $GEN(R_j) = < SDR_j, SDP_j >$
- SD_j: $HSID_j = h(SID_j || SDR_j$
- $SD_j \rightarrow GW$: $< Req_j, R_{sd}, HSID_j, C_j >$ via secure channel
- GW: Computes $SID_j = Req_j \oplus h(R_{sd})$.
- GW: Generate random secret keyRK_j.
- GW: Computes $PSID_j = h(HSID_j || RK_j)$,
- GW: $SI_j = h(PSID_j || h(K_{gw} || RK_j))$.
- GW: Stores $\{(HSID_j, PSID_j), PSID_j, RK_j, C_j\}$
- $GW \rightarrow SD_j$: $< PSID_j, SI_j >$ via secure channel
- SD_j: Stores $\{SID_j, PSID_j, SI_j, SDP_j\}$

Login and Authentication Phase

It will be between Service User U_i, Sensing Device SD_j and Gateway GW

- U_i: Inserts Smart Card.
- U_i: Inputs ID_i, PW_i, B_i.
- U_i: Smart Card Computes
- U_i: $REP(B_i, P_i) = R_i, HID_i = h(ID_i || R_i)$,
- U_i: $R_u = L_i \oplus h(ID_i \| PW_i \| R_i)$.
- U_i: $HPW_i = h(ID_i \| PW_i \| R_u \| R_i)$.
- U_i: $A_i = B'_i \oplus HPW_i,$
- U_i: $C *_i = h(h(A_i || HID_i) \| HPW_i)$.
- U_i: Checks if $C_i = C *_i$? If so,
- U_i: Generates a random nonce N_u and timestamp T_1.
- U_i: Computes $Msg_1 = \mathrm{h}(\mathrm{h}(N_u || A_i) \| A_i || HID_i || PSID_j)$,
- U_i: $V_1 = \mathrm{h}(N_u || A_i) \oplus h(HID_i || A_i || T_1)$.
- $U_i \rightarrow GW$: $< Msg_1, V_1, THID_i, PSID_j >$ via insecure channel
- GW: Checks if $|T_1 - T *_1| < \Delta$ T?
- GW: Retrieves HID_i corresponding to $THID_i$.
- GW: Computes $A_i = h(HID_i || K_{gw} \| R_{gw})$,
- GW: $\mathrm{h}(N_u || A_i) = \mathrm{h}(HID_i || A_i || T_i) \oplus V_1$,
- GW: $Msg *_1 = \mathrm{h}(\mathrm{h}(N_u \| A_i) || A_i || HID_i PSID_j)$
- GW: Checks if $Msg_4 = Msg *_4$? If not,
- GW: $A *_i$is inserted into honey_list
- GW: Fetch, (C_j, RK_j) corresponding to $PSID_j$.

- GW: Generates a random nonce N_g and timestamp T_2
- GW: Computes $SI_j = h(PSID_j||h\left(K_{gw}\middle||RK_j\right)\big)$,
- GW: $V_2 = C_j \oplus h(PSID_j|\big|PSI_j)$,
- GW: $V_3 = \mathrm{h}(\mathrm{h}(N_u||A_i)||h(N_g||SI_j) \oplus \mathrm{h}(HSID_j||C_j||SI_j)$
- GW: $Msg_2 = h(\mathrm{h}(\mathrm{h}(N_u||A_i)||h(N_g||SI_j))||T_2||HSID_j||C_j||SI_j$
- $GW \rightarrow SD_j$: $< Msg_2, V_2, V_{3,}T_2 >$ via insecure channel
- SD_j: Checks if $|T_2 - T*_2|<\Delta$ T?
- SD_j: Computes $C_j = V_2 \oplus \mathrm{h}(PSID_j|\big|SI_j)$,
- SD_j: PUF($C_j) = R_j$,
- SD_j: REF($R_j, SDP_j) = SDR_j$,
- SD_j: $HSID_j = h(SID_j|\big|SDR_j)$,
- SD_j: K_{gs}(=h(h($N_u||A_i)||h(N_g||SI_j))) = V_3 \oplus \mathrm{h}(HSID_j||C_j||SI_j)$,
- SD_j: $Msg*_2 = h(K_{GS}||T_2HSID_j||C_j|\big|SI_j)$.
- SD_j: Checks if $Msg_2 = Msg*_2$? If so,
- SD_j: Generates a random nonce N_{sd} and Timestamp T_3.
- SD_j: Computes a session key
- SD_j: Skey = $h(N_{sd}||\ K_{gs})$
- SD_j: $V_4 = Skey\ \oplus \mathrm{h}(HSID_j||SI_j||C_j||T_3)$,
- SD_j: $Msg_3 = h(C_j||HSID_j||Skey)$.
- $SD_j \rightarrow GW$: $< Msg_3, V_4, T_3 >$ via insecure channel
- GW: Computes a Skey
- GW: Skey = $V_4 \oplus \mathrm{h}(HID_i|\big|SI_j\big||C_j||T_3)$,
- GW: $Msg*_3 = \mathrm{h}(C_j||HSID_j||Skey)$.
- GW: Checks if $Msg_3 = Msg*_3$? If so,
- GW: Computes $THID_{inew} = \mathrm{h}(\mathrm{h}(N_u||A_i)||N_g||THID_i)$,
- GW: $V_5 = Skey \oplus \mathrm{h}(\mathrm{h}(N_u||A_i)||HID_i)$,
- GW: V_6 = h(Skey || $THID_{inew}$).
- $GW \rightarrow U_i$: $< Msg_4, V_5, V_6 >$ via insecure channel
- U_i : Computes a Skey
- U_i : Skey = $V_5 \oplus \mathrm{h}(\mathrm{h}(N_u||A_i)||\ HID_i)$,
- U_i : $V_6 = THID_{inew} \oplus h(HID_i||THID_i\mathrm{h}(N_u||A_i))$,
- U_i : $Msg*_4 = h(Skey||THID_{inew})$
- U_i : Check if $Msg_4 = Msg*_4$? If so,
- U_i : The session key is authentic, and user updates $THID_{inew}$.

3. Analysis

In this section we have given the analysis on the scheme of Lee et al [47] as follows.

Key Control: The scheme is said to be vulnerable to the key control attack if one side of entity can set the session key. In scheme of Lee et al. Sensing device (SD_j) is making the step $h(N_{sd}\big|\big|K_{gs})$ in which both variables will be selected by SD_j only. Thus, the scheme of Lee et al is vulnerable to key control attack.

Time synchronization: The scheme is said to be insure against the time synchronization if it requires the involving entities to be using the same clock. In the scheme of Lee et al. U_i, SD_j and GW requires the same clock to be verify for all message communication. Thus, any delay in message as well as synchronization of same clock requires the continuous internet support. Thus, the scheme of Lee *et al* is vulnerable to time synchronization attack.

Replay attack: The scheme is said to be insure against replay attack if sending the same message will be detected late and requires computation power of the involving entities. The broader version of this attack lead to the Denial of Service (DoS) attack. In the scheme of Lee *et al.* the required operations are as follows.

Table 1. Operational Analysis of the Scheme by Lee *et al.*

Operation	U_i	GW	SD_j
Hash (h)	4	5	7
Concatenation (‖)	4	12	10
Bitwise X-OR ($\oplus$)	2	2	2

Considering the time taken for each operation, this will lead to the overhead on the entities for large number of communications.

Stolen Verifier: The scheme is said to insecure against stolen verifier attack if compromising the stored values at users cannot compromise the sessions. In the scheme of Lee et al., gateway node GW is storing the value of user's credentials i.e. $THID_i, HID_i$. Thus, compromising this value will also compromise the other session values and finally the session key.

4. Conclusion and Future Work

IoT, sensors, Cloud are today's technology which are playing the key role in shaping our future. As discussed, authentication and key agreement is the vital issue in any of these technologies. The recent approach by Lee et al is being analyzed in this paper and found to be insecure against various attacks. In future, one can design the more secure and efficient scheme.

Acknowledgements

Authors are thankful to GUJCOST for providing financial assistance through major research project "Developing a Privacy Preserving Framework for securing Organizational Data Publication" initiated in 2022.

References

[1]. AZhang, Y.; Zhao, H.; Xiang, Y.; Huang, X.; Chen, X. A key agreement scheme for smart homes using the secret mismatch problem. IEEE Internet Things J. 2019, 6, 10251–10260.
[2]. Rashid, B.; Rehmani, M.H. Applications of wireless sensor networks for urban areas: A survey. J. Netw. Comput. Appl. 2016, 60,192–219.
[3]. Wazid, M.; Bagga, P.; Das, A.K.; Shetty, S.; Rodrigues, J.J.P.C.; Park, Y. AKM-IoV: Authenticated key management protocol in fogcomputing-based Internet of vehicles deployment. IEEE Internet Things J. 2019, 6, 8804–8817.
[4]. Kwon, D.; Yu, S.; Lee, J.; Son, S.; Park, Y. WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensornetworks. Sensors 2021, 21, 936.
[5]. Fu, X.;Wang, Y.; Yang, Y.; Postolache, O. Analysis on cascading reliability of edge-assisted Internet of Things. Reliab. Eng. Syst.Saf. 2022, 223, 108463.
[6]. Fu, X.; Pace, P.; Aloi, G.; Li,W.; Fortino, G. Cascade Failures Analysis of Internet of Things under Global/Local Routing Mode.IEEE Sensors J. 2021, 22, 1705–1719.
[7]. Das, M.L. Two-factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. 2009, 8, 1086–1090.
[8]. He, D.; Gao, Y.; Chan, S.; Chen, C.; Bu, J. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad HocSensor Wirel. Netw. 2010, 10, 361–371.
[9]. Kumar, P.; Lee, H.J. Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks. InProceedings of the Wireless Advanced, London, UK, 20–22 June 2011; pp. 241–245.
[10]. Turkanovi´c, M.; Brumen, B.; Hölbl, M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wirelesssensor networks, based on the Internet of Things notion. Ad Hoc Netw. 2014, 20, 96–112.
[11]. Amin, R.; Biswas, G.P. A secure light weight scheme for user authentication and key agreement in multi-gateway based wirelesssensor networks. Ad Hoc Netw. 2016, 36, 58–80.
[12]. Wu, F.; Xu, L.; Kumari, S.; Li, X.; Shen, J.; Choo, K.R.; Wazid, M.; Das, A.K. An efficient authentication and key agreement schemefor multi-gateway wireless sensor networks in IoT deployment. J. Netw. Comput. Appl. 2017, 81, 72–85.
[13]. Shuai, M.; Yu, N.;Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security.Comput. Secur. 2019, 86, 132–146.

[14]. Zou, S.; Cao, Q.;Wang, C.; Huang, Z.; Xu, G. A Robust Two-Factor User Authentication Scheme-Based ECC for Smart Home inIoT. IEEE Syst. J. 2021, 16, 4938–4949.
[15]. Chunka, C.; Banerjee, S.; Goswami, R.S. An efficient user authentication and session key agreement in wireless sensor networkusing smart card. Wirel. Pers. Commun. 2021, 117, 1361–1385.
[16]. Kalra, S.; Sood, S.K. Advanced password based authentication scheme for wireless sensor networks. J. Inf. Secur. Appl. 2015, 20,37–46.
[17]. Amintoosi, H.; Nikooghadam, M.; Shojafar, M.; Kumari, S.; Alazab, M. Slight: A lightweight authentication scheme for smarthealthcare services. Comput. Elec. Eng. 2022, 99, 107803.
[18]. He, D.; Kumar, N.; Chen J.; Lee, C.-C.; Chilamkurti, N.; Yeo, S.-S. Robust anonymous authentication protocol for health-careapplications using wireless medical sensor networks. Multimedia Syst. 2015, 21, 49–60.
[19]. Wu, F.; Xu, L.; Kumari, S.; Li, X. An improved and anonymous twofactor authentication protocol for health-care applications withwireless medical sensor networks. Multimedia Syst. 2017, 23, 195–205.
[20]. Wang, C.; Xu, G.; Li, W. A secure and anonymous two-factor authentication protocol in multiserver environment. Secur. Commun.Netw. 2018, 2018, 1–15.
[21]. Amin, R.; Islam, S.H.; Biswas, G.; Khan, M.K.; Leng, L.; Kumar, N. Design of an anonymity-preserving three-factor authenticatedkey exchange protocol for wireless sensor networks. Comput. Netw. 2016, 101, 42–62.
[22]. Jiang, Q.; Zeadally, S.; Ma, J.; He, D. Lightweight three-factor authentication and key agreement protocol for internet-integratedwireless sensor networks. IEEE Access 2017, 5, 3376–3392.
[23]. Ostad-Sharif, A.; Arshad, H.; Nikooghadam, M.; Abbasinezhad-Mood, D. Three party secure data transmission in IoT networksthrough design of a lightweight authenticated key agreement scheme. Future Gener. Comput. Syst. 2019, 100, 882–892.
[24]. Mo, J.; Chen, H. A lightweight secure user authentication and key agreement protocol for wireless sensor networks. Secur.Commun. Netw. 2019, 2019, 1–17.
[25]. Yu, S.; Park, Y. SLUA-WSN: Secure and lightweight three-factor-based user authentication protocol for wireless sensor networks.Sensors 2020, 20, 4143.
[26]. Hajian, R.; Erfani, S.H.; Kumari, S. A lightweight authentication and key agreement protocol for heterogeneous IoT with specialattention to sensing devices and gateway. J. Supercomput. 2022, 1–43.
[27]. Aghili, S.F.; Mala, H.; Shojafar, M.; Peris-Lopez, P. LACO: Lightweight three-factor authentication, access control and ownershiptransfer scheme for e-health systems in IoT. Future Gener. Comput. Syst. 2019, 96, 410–424.
[28]. Maes, R. Physically unclonable functions: Properties. In Physically Unclonable Functions; Springer: Berlin/Heidelberg, Germany,2013; pp. 49–80.
[29]. Juels, A.; Ristenpart, T. Honey encryption: Encryption beyond the brute-force barrier. IEEE Secur. Privacy 2014, 12, 59–62.
[30]. Juels, A.; Ristenpart, T. Honey encryption: Security beyond the brute-force bound. In Proceedings of the Annual InternationalConference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014; pp. 293–310.
[31]. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. ACM Trans. Comput. Syst. 1990, 8, 18–36.
[32]. Abdalla, M.; Fouque, P.-A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In LectureNotes in Computer Science, Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'05),Les Diablerets, Switzerland, 23–26 January 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 65–84.
[33]. Scyther Tool—Cas Cremers. Available online: https://people.cispa.io/cas.cremers/scyther/ (accessed on 23 July 2022).
[34]. Lamport, L. Password authentication with insecure communication. Commun. ACM 1981, 24, 770–772.
[35]. Dolev, D.; Yao, A.C. On the security of public key protocols. IEEE Trans. Inf. Theory 1983, 29, 198–208.
[36]. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In Advances in Cryptology; Springer Science+Business Media: Berlin,Germany; New York, NY, USA, 1999; pp. 388–397.
[37]. Aman, M.N.; Chua, K.C.; Sikdar, B. Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet of Things J. 2017, 4, 1327–1340.
[38]. Frikken, K.B.; Blantonm, M.; Atallahm, M.J. Robust authentication using physically unclonable functions. In Proceedings of theInternational Conference on Information Security, Pisa, Italy, 7–9 September 2009; Springer: Berlin/Heidelberg, Germany, 2009;pp. 262–277.
[39]. Chatterjee, U.; Chakraborty, R.S.; Mukhopadhyay, D. A PUF-based secure communication protocol for IoT. ACM Trans. EmbeddedComput. Syst. 2017, 16, 1–25.
[40]. Son, S.; Lee, J.; Park, Y.; Park, Y.; Das, A.K. Design of blockchain-based lightweight V2I handover authentication protocol forVANET. IEEE Trans. Netw. Sci. Eng. 2022, 9, 1346–1358.
[41]. Oh, J.; Yu, S.; Lee, J.; Son, S.; Kim, M.; Park, Y. A secure and lightweight authentication protocol for IoT-based smart homes.Sensors 2021, 21, 1488.
[42]. Yu, S.; Park, Y. A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and PhysicallyUnclonable Functions. IEEE Internet Things J. 2022.
[43]. Kim, M.; Lee, J.; Oh, J.; Park, K.; Park, Y.; Park, K. Blockchain based energy trading scheme for vehicle-to-vehicle usingdecentralized identifiers. Appl. Energy 2022, 322, 119445.
[44]. Lee, J.; Kim, G.; Das, A.K.; Park, Y. Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks.IEEE Trans. Netw. Sci. Eng. 2021, 8, 2412–2425.
[45]. Gope, P.; Sikdar, B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. IEEE Internet Things J.2019, 6, 580–589.
[46]. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Rodrigues, J.J.; Park, Y. Physically secure lightweight anonymous userauthentication protocol for internet of things using physically unclonable functions. IEEE Access 2019, 7, 85627–85644.
[47]. Lee, JoonYoung, JiHyeon Oh, DeokKyu Kwon, MyeongHyun Kim, SungJin Yu, Nam-Su Jho, and Youngho Park. 2022. "PUFTAP-IoT: PUF-Based Three-Factor Authentication Protocol in IoT Environment Focused on Sensing Devices" Sensors 22, no. 18: 7075