Lightweight Two-Factor Mutual Authentication for IoT Applications

Geeta Sharma[1], Rajni Bedi[2], Vikram Dhiman[3]

School of Computer Applications, Lovely Professional University, Phagwara[1]
Department of CSE, Lyallpur Khalsa College Technical Campus, Jalandhar[2,3]
Corresponding author: Geeta Sharma, Email: geeta.26875@lpu.co.in

The advancement of diverse smart devices has led to the emergence of applications such as smart healthcare, military, agriculture, etc. through which users can access data at any part of the globe. These IoT networks are growing exponentially. This poses the challenge of authenticating remote users. This paper proposes a smart card-based lightweight user authentication scheme for IoT deployment. Security analysis confirms the security of our scheme. Furthermore, the simulation results of our scheme in AVISPA validate its resilience to attacks. The scheme is lightweight, robust, and practically achievable in IoT deployment.

Keywords: Authentication, AVISPA, IoT, Security

2023. In Vikram Dhiman & Pooja Dhand (eds.), *Emerging Trends in Engineering and Management*, 85–90. Computing & Intelligent Systems, SCRS, India.
https://doi.org/10.56155/978-81-955020-3-5-10

1. Introduction

The emergence of diverse heterogeneous smart devices has led to the development of numerous applications such as smart healthcare, smart transportation, smart cities and many more [1, 2]. The vast amount of data is being collected using these smart devices such as sensors, smart phones, mobile devices, and RFID tags. Several other sensors are deployed in environment or on a particular area to sense and collect data around it. These smart devices exchange data with the help of Internet. IoT network consists of three participants, users, gateway node and sensor nodes. Sensor nodes are deployed in the specific region to collect and sense data. This sensed data is transmitted to the gateway node using the wireless channel. This data is stored on the cloud for later use. This data is required by industries, companies and every sector of the economy.

Figure 1 shows the IoT network consisting of diverse sensor nodes which are sensing data and sending data to the gateway node. At last, end user can access any sensor node through a gateway node. As the communication takes place in unreliable public environments, intruders can access and manipulate the data easily. Thus, user authentication is one of the crucial design factors in such environments. Additionally, sensor nodes have limitations of computational power, battery power and communication capability. The security mechanism employed to authenticate remote user must be computationally lightweight.

Several user authentication mechanisms have been proposed in the literature [4-14]. Song [3] analysed existing authentication schemes and found that most of the schemes cannot withstand impersonation attack. Song [3] putforth an improvised scheme. Yeh et al. [4] presented an Elliptic Curve Cryptography based user authentication scheme. However, the scheme has memory overhead. Jiang et al. [5] showed that the existing work is not worthy and is vulnerable to password guessing attack. Moreover, Jiang et al. [5] proposed an enhanced scheme which remove the shortcomings of previous schemes. Xue et al. [6] suggested password based and temporal credential based authentication schemes respectively. Later, in two different papers Xu and Wang [7] and Turkanovic and Hölbl [8] found Xue et al. [6] failed to resist forgery attacks. They proposed improvised schemes. The claims made by Xue et al. [6] were nullified by Li et al. [9]. They also found security flaws in the scheme. Turkanovic et al. [10] suggested authentication protocol for ad-hoc WSNs using the concept of the IoT. They claimed their scheme has low computation cost and attack resistant. But Farash et al. [11] and Ruhul and Biswas [12] found Turkanovic et al. [10]'s scheme insecure to impersonation and forgery attacks. Sharma and Kalra [13] has proposed several user authentication schemes for cloud-IoT environment [14].

1.1 Structure of the paper

The paper is structured as follows. Section 1 describes the need for authentication in IoT environment and related work in the field of IoT. Section 2 proposes a lightweight user authentication scheme. Section 3 rigorous security analysis of our proposed scheme. Section 4 shows simulation results of our scheme using AVISPA. Section 5 concludes the paper.

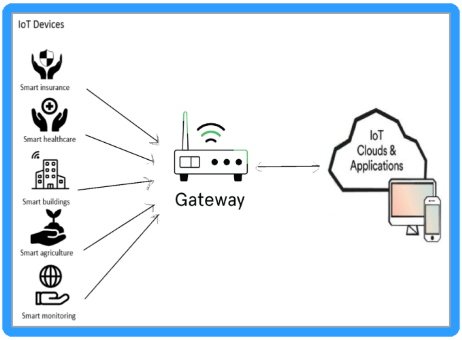

Fig. 1: Proposed framework of WSNs in Cloud-IoT applications

2. Proposed Scheme

This section proposes a two-factor remote user authentication scheme for IoT deployment. After mutual authentication, session key is generated and further communication takes place after encrypting messages with the session key. Notations used in the scheme are depicted in Table 1.

Table 1. Notations

Symbol	Meaning
U_i	i^{th} User
U_{ID}	Identity of user
PW_i	Strong user password
SC	Smart card
S_{Key}	Shared session key
$h(\cdot)$	Hash operation
$\|\|$	Concatenation operation
$\oplus$	XOR operation

2.1 Setup Phase

In this phase, involved entities, gateway nodes and sensor nodes exchanges parameters to initiate secure communication

.

Step 1: GN submits identity ID_{GN}, calculates pseudo-identity PID_{GN} to sensor node SW using secure channel.
Step 2: SW uses secret parameter Z to calculate $A_1 = h(ID_{SW} || PID_{GN} || Z)$, $A_2 = h(ID_{GN} || Z)$ stores ID_{GW} and sends $\{A_1, A_2, ID_{SW}\}$ to GN.
Step 3: GW stores $\{C_1, C_2, ID_{SW}, ID_{GW}, ID_{SN}\}$.

2.2 Registration Phase

In this phase, user registers himself/herself with involved nodes. The process is shown below.

Step 1: U_i randomly selects identity ID_i, PW_i. Ui generates nonce N_1 to calculate pseudo parameters $PID_i = h(ID_t || N_1)$, $PPW_i = h(PW_i || N_1)$ and sends $\{ID_i, PID_i\}$ to SW.
Step 2: SW checks submitted ID_i. If identity is already registered, new identity is requested. Else, SW calculates $A_3 = h(PID_i || ID_{SW} || Z)$, $A_4 = h(ID_i || Z)$, stores ID_i in database and sends $\{A_3, A_4, ID_{SW}\}$ to U_i using secure channel.
Step 3: U_i calculates $B_1 = A_3 \oplus PPW_i$, $B_2 = A_4 \oplus h(ID_i || PPW_i)$, $B_3 = h(ID_i || PW_i) \oplus N_1$.
Step 4: U_i stores $\{B_1, B_2, B_3, PID_i, ID_{SW}\}$ into smart card SC.

2.3 Authentication Phase

In this phase, mutual authentication takes place between involved entities. After successful authentication, session key is generated. This key is used for encrypting further messages.

Step 1: U_i inserts smart card SC, enters $\{ID_i, PW_i\}$. U_i generates a nonce N_2 and fresh pseudo-identity PID'_i, calculates $C_1 = B_3 \oplus h(Id_i || PW_i)$, $PPW_i = h(PW_i || C_1)$, extracts $A_3 = B_1 \oplus PPW_i$, extracts $A_4 = B_2 \oplus h(ID_i || PPW_i)$,

Step 2: Further, U_i computes $C_2 = A_3 \oplus N_2$, $C_3 = h(N_2 || PID_i || ID_{SW}) \oplus ID_i$, $C_4 = A_4 \oplus h(ID_i || PPW_i) \oplus PID'_i \oplus h(N_2 || ID_i)$, $C_5 = h(ID_i || PID_i || PID'_i || B_2 || C_3)$. U_i communicates $\{PID_i, C_1, C_2, C_3, C_4\}$ to SW.
Step 3: GN selects fresh PID'_{GN}, generates nonce N_3, calculates $C_6 = A_1 \oplus N_3$, $C_7 = H(N_3 || ID_{GN} || ID_{SW}) \oplus ID_{GN}$, $C_8 = A_2 \oplus PID'_{GN} \oplus h(N_3 || ID_{GN})$, $C_9 = h(PID_{GN} || ID_{GN} || PID'_{GN} || N_3 || C_8)$. GN transmits $\{PID_i, C_2, C_3, C_4, C_5, ID_{GN}, C_7, C_8, C_9\}$ to SW.
Step 4: SW extracts $N_2 = C_2 \oplus h(PID_i || ID_{SW} || Z)$, $ID_i = C_3 \oplus h(N_2 || PID_i || ID_{SW})$, $PID'_{SW} = C_4 \oplus h(Id_i || Z) \oplus h(N_2 || ID_i)$. It validates if ID_i and $C_5 = h(ID_i || PID_i || PID'_{SN} || N_2 || C_4)$?. If condition fails, the process is aborted. Otherwise, process moves to next step.
Step 5: SW extracts $N_3 = C_6 \oplus h(ID_{GN} || ID_{SW} || Z)$, $ID_{GN} = C_7 \oplus h(N_3 || ID_{GN} || ID_{SW})$, $PID'_{GN} = C_8 \oplus h(ID_{GN} || Z) \oplus h(N_3 || ID_{GN})$, checks ID_{GN} and $C_9 = h(ID_{GN} || ID_{GN} || PID'_{GN} || N_3 || C_8)$?. If fails, session is terminated.
Step 6: Otherwise, SW generates nonce N_4, calculates session key $SK_{SW} = h(N_2 \oplus N_3 \oplus N_4)$,
Step 7: Further, SW calculates $C_{10} = h(PID'_{SW} || ID_{SW} || Z) \oplus h(N_3 || PID'_{SW})$, $C_{11} = h(PID'_{SW} || N_3 || ID_{GN}) \oplus h(N_2 || N_4)$, $C_{12} = h(SK_{SW} || C_{10} || C_{11} || h(ID_{GN} || Z))$, $C_{13} = h(PID'_{SW} || ID_{SW} || Z) \oplus h(N_2 || PID'_{SW})$, $C_{14} = h(PID'_{SW} || N_2 || PID_{SW}) \oplus (N_3 \oplus N_4)$, $C_{15} = h(SK_{SW} || C_{13} || C_{14} || h(ID_i || Z))$ and sends $\{C_{10}, C_{11}, C_{12}, C_{13}, C_{14}, C_{15}\}$ to GN.
Step 8: GN extracts $(N_2 \oplus N_3) = C_{11} \oplus h(PID'_{GN} || N_3 || ID_{GN})$, $SK_{GN} = h(N_4 \oplus N_3 \oplus N_2)$, verifies $C_{12} = h(SK_{GN} || C_{10} || C_{11} || A_2)$?. If not satisfied, process terminates.
Step 9: GN calculates $A_{1new} = C_9 \oplus h(N_3 || PID'_{GN})$ and replaces A_1 with A_{1new} and ID_{GN} with PID'_{GN}. Further, sends $\{C_{13}, C_{14}, C_{15}\}$ to U_i.
Step 10: SC extracts $(N_3 \oplus N_4) = C_{14} \oplus h(PID'_i || N_2 || PID_i)$, $SK_U = h(N_2 \oplus N_3 \oplus N_4)$. It validates $C_{15} = h(SK_U || C_{13} || C_{14} || A_4)$?. If holds, SC proceeds $B_{1new} = C_{13} \oplus h(N_2 || PID'_i) \oplus PPW_i$. It replaces B_1 with B_{1new} and PID_i with PID'_i.

2.4 Password Update Phase

This phase permits user to update his/her password.

Step 1: U_i chooses new PW_i'. Ui generates nonce N_1 to calculate pseudo parameters $PID_i = h(ID_t || N_1)$, $PPW_i' = h(PW_i' || N_1)$ and sends $\{ID_i, PID_i'\}$ to SW.
Step 2: SW checks submitted ID_i'. If identity is already registered, new identity is requested. Else, SW calculates $A_3' = h(PID_i' || ID_{SW} || Z)$, $A_4' = h(ID_i' || Z)$, stores ID_i' in database and sends $\{A_3', A_4', ID_{SW}\}$ to U_i using secure channel.
Step 3: U_i calculates $B_1' = A_3' \oplus PPW_i$, $B_2' = A_4' \oplus h(ID_i || PPW_i')$, $B_3' = h(ID_i || PW_i') \oplus N_1$.
Step 4: U_i replaces $\{B_1, B_2, B_3, PID_i, ID_{SW}\}$ with $\{B_1', B_2', B_3', PID'_i, ID_{SW}\}$ into smart card SC.

3. Security Analysis

This section shows security analysis of our scheme with existing related schemes. Our scheme resilient to major network attacks and achieves all security attributes. The comparison is depicted in Table 2.
Table 2: Security analysis with related schemes

Security Features	Song [3]	Yeh et al. [4]	Jiang et al. [5]	Xue et al. [6]	Farash et al. [11]	Sharma & Kalra [13]	Proposed scheme
S1	Yes	No	Yes	Yes	Yes	Yes	Yes
S2	No	No	No	No	No	Yes	Yes
S3	No	Yes	Yes	Yes	Yes	Yes	Yes
S4	No	No	No	No	Yes	Yes	Yes
S5	Yes	No	No	Yes	Yes	Yes	Yes
S6	No	No	No	No	No	No	Yes
S7	No	No	No	No	Yes	Yes	Yes
S8	No	No	No	No	Yes	Yes	Yes
S9	No	No	No	No	No	No	Yes
S10	No	No	No	No	No	Yes	Yes
S11	No	No	No	No	No	Yes	Yes

S1: Provides mutual authentication, S2: Resists malicious user attack S3: Provides forward secrecy, S4: Resists user anonymity, S5: Resists replay attack, S6: Resists online password guessing attack, S7: Resists insider attack, S8: Provides smart card revocation, S9: Resists hidden server attack, S10: Resists server spoofing attack, S11: Resists offline password guessing attack

4. Simulation Results

This section provides the explanation of simulation procedure of the proposed scheme using the AVISPA. Our scheme has been simulated using popularly used tool Automated Validation of Internet Security Protocols and Applications (AVISPA) [15]. This tool is extensively used to validate the security of the internet security protocols. AVISPA protocols are written in HLPSL (High Level Protocol Specification Language). HLPSL2IF is a translator that translates a HLPSL protocol to an Intermediate Format (IF) specification. This is given as input to one of the four back-ends. For our proposed scheme, it has been simulated on CL-AtSe (Constraint Logic based Attack Searcher). The simulation result is depicted in Figure 2.

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web−interface−computation/
./tempdir/workfilevOpMGm.if
GOAL
As_Specified
BACKEND
CL-AtSe
STATISTICS
Analysed: 13 states
Reachable: 13 states
Translation: 0.04 nodes
Computation: 0.02 seconds
```

Fig. 2: Simulation results on CL-AtSe

5. Conclusion

The advancement of heterogeneous smart devices has led to emergence of applications through which users can access data at any part of globe. These IoT networks are growing exponentially. This poses the challenge of authenticating remote users. This paper proposes a smart card based lightweight user authentication scheme for IoT deployment. Security analysis confirms security of our scheme. Furthermore, simulation results of our scheme in AVISPA validates its resilience to attacks. The scheme is lightweight, robust, and practically achievable in IoT deployment.

References

[1] Shah, S. H., Iqbal, A., & Shah, S. S. A. (2013, October). Remote health monitoring through an integration of wireless sensor networks, mobile phones & cloud computing technologies. In *2013 IEEE Global Humanitarian Technology Conference (GHTC)* (pp. 401-405). IEEE.

[2] Xiong, Z., Sheng, H., Rong, W., & Cooper, D. E. (2012). Intelligent transportation systems for smart cities: a progress review. *Science China Information Sciences*, *55*(12), 2908-2914.

[3] Song R. (2010). Advanced smart card based password authentication protocol. Computer Standards & Interfaces, 32(5):321-5.

[4] Yeh, H. L., Chen, T. H., Liu, P. C., Kim, T. H., & Wei, H. W. (2011). A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, *11*(5), 4767-4779.

[5] Jiang Q, Ma J, Li G, Li X. (2013). Improvement of robust smart-card-based password authentication scheme. Int J Commun Syst, 28(2):383-393.

[6] Xue, K., Ma, C., Hong, P., & Ding, R. (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, *36*(1), 316-323.

[7] Xu, S., & Wang, X. (2013). A new user authentication scheme for hierarchical wireless sensor networks. *Int. Rev. Comput. Softw*, *8*(6), 197-203.

[8] Turkanovic, M., & Holbl, M. (2013). An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Elektronika ir Elektrotechnika*, *19*(6), 109-116.

[9] Li, C. T., Weng, C. Y., & Lee, C. C. (2013). An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. *Sensors*, *13*(8), 9589- 9603.

[10] Turkanović, M., Brumen, B., & Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*, *20*, 96-112.

[11] Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Networks*, *36*, 152-176.

[12] Amin, R., & Biswas, G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks*, *36*, 58-80.

[13] Sharma, G., & Kalra, S. (2018). A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. *Journal of information security and applications*, *42*, 95-106.

[14] Sharma, G., & Kalra, S. (2020). Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications. *Journal of Ambient Intelligence and Humanized Computing*, *11*(4), 1771-1794.

[15] Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on information theory*, *29*(2), 198-208.