A Cryptanalysis of the Authentication Protocol for IoD Security

Priyanshi Thakkar, Nishant Doshi, Soham Patel

Pandit Deendayal Energy University, Gandhinagar, Gujarat.

ABSTRACT – *The emergence of smart cities and the growing demand for drones have led to the rise of Internet of Drones (IoD), offering numerous benefits in academia and industry. IoD integrates infrastructure, Internet of Things (IoT), and Flying Ad-Hoc Networks (FANET) to provide services including applications like traffic and environmental monitoring within smart city settings. However, IoD communication faces security vulnerabilities due to insecure channels, especially in unattended environments. In response to these challenges, in 2023, the authors introduced SLAP-IoD, a secure and lightweight authentication protocol employing Physical Unclonable Functions (PUF) to guarantee dependable services in smart cities. It establishs the security of SLAP-IoD through formal and informal analyses, comparing its performance with related schemes and claimed it ot be secure against various attacks. However, in this paper we have done the cryptanalysis of the SLAP-IoD and prove that it is vulnerable to various attacks.*

KEYWORDS – Physical un-clonable functions (PUF), Internet of Drones (IoD), smart city, authentication, security protocol.

1. INTRODUCTION

In the rapidly evolving landscape of the Internet of Things (IoT) [2-4], the security of cloud-assisted IoT environments has emerged as a critical concern. In this scenario, authentication protocols are paramount for upholding the confidentiality, integrity, and availability of data and services [5-8]. One such authentication protocol, the 'Authentication Protocol for Cloud Assisted IoT Environment,' stands as a fundamental component in the defence against potential threats and vulnerabilities that could compromise IoT systems.

This research paper meticulously examines a specific authentication protocol, aiming to assess its security robustness and effectiveness comprehensively. Beyond evaluating the mechanisms protecting

sensitive data and verifying identities, the research delves into vulnerability identification, uncovering potential flaws exploitable by malicious actors. Successful attacks are demonstrated, offering concrete evidence of uncovered vulnerabilities. Importantly, this analysis not only highlights weaknesses but also contributes to IoT security by providing valuable insights for enhancing security practices within the field.

We advocate for a re-evaluation of the protocol's security posture in light of our findings. The goal is to encourage its developers and users to consider necessary adjustments and enhancements to mitigate the vulnerabilities [9-12] we've exposed and bolster the overall security of cloud-assisted IoT environments. The stakes are undeniably high in the realm of IoT, where the integrity and confidentiality of sensitive data are paramount [13-16]. By spotlighting these attacks and vulnerabilities, our research seeks to fortify the security measures governing cloud-assisted IoT environments, ultimately contributing to the ongoing efforts to protect against the evolving and sophisticated threats that constantly challenge this dynamic field. This examination underscores the imperative need for a continuous and proactive approach to enhancing security measures in IoT systems to effectively counter the ever-evolving threat landscape and safeguard the future of IoT.

In [17-18], the authors have proposed and mentioned the various extension of IoT based protocols in the various domain like smart city as shown in Fig 1. Recently in [1], the authors have proposed the enhanced approach of IoT with drone in the smart city and claimed to be efficient as well secure as to predecessors. Nevertheless, our analysis in this paper reveals that the scheme presented in [1] remains vulnerable to multiple types of attacks.

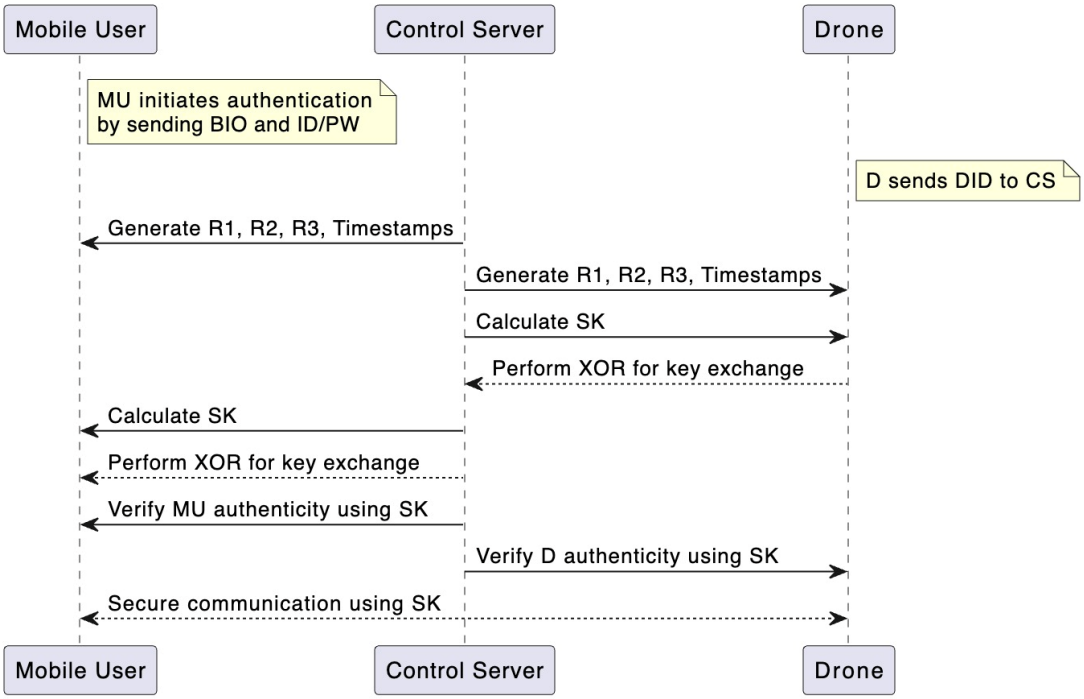

Fig-1 Review Methodology

1.1 Literature Review

Authentication procedures are essential in the context of IoT security to guarantee the privacy, availability, and integrity of data and services. Upon analysis, the 'Authentication Protocol for Cloud Assisted IoT Environment' exposes weaknesses that malevolent actors might exploit. To counteract new threats and protect sensitive data, authentication systems must be continuously evaluated and improved.

As the examination of the SLAP-IoD authentication mechanism shows, cryptanalysis is essential for finding weaknesses in security protocols. Through the discovery of flaws like time synchronisation vulnerabilities and user identity attacks, researchers highlight how crucial strong security measures are for Internet of Device connectivity. In order to minimise computational complexity and resource overhead and enable safe user authentication and key agreement, lightweight and secure authentication algorithms have been suggested for wireless sensor networks.

In general, the research emphasises how important authentication methods are to the security of IoT systems, especially those involving smart cities and IoD connectivity. Researchers work to improve the security posture of IoT devices and guard against unauthorised access and data breaches using cryptanalysis and vulnerability evaluations.

1.2 Our Contribution

In this paper, we have given the analysis of the SLAP-IoD scheme and showed the following attacks.

- User Identity attack: A malicious actor tricks the system into accepting a false drone identity, potentially compromising security.
- Time synchronization: An attacker intercepts a user's registration data to impersonate them, highlighting the need for more secure registration processes.
- Overhead on control server for each Session Key: An adversary manipulates communication timing to disrupt authentication, underlining the importance of precise timing.
- Stolen verifier: Increasing computational complexity and storage requirements for session keys to protect against resource overload on the control server.

1.3 Paper Organization

In Section 2, a comprehensive analysis of the SLAP-IoD Authentication Protocol is presented, delving into its intricate components. Progressing to Section 3, an exhaustive evaluation of the protocol is performed, focusing on Cryptanalysis and Vulnerability Assessment. Acknowledgment of the paper is featured in Section 4. Section 5 summarizes our findings in the Conclusion and proposes potential directions for Future Work. Finally, Section 6 provides an inventory of the References utilized throughout this study.

Scheme of Slap-Iod

In this section we have discussed the scheme of SLAP-IoD [1]. The notation are as shown in Table 1.

Table 1 Notations

Icon	Represents
MU_i	Mobile User
D_j	Drone
CS	Control Server
BIO_i	Biometric of MU_i
ID_i,PW_i	Identity and Password of MU_i
DID_j	Identity of D_j
R1, R2, R3	Random Nonce Values
T_i	Timestamp
SK	Session key between MU_i and D_j
MSK	Control Server Master key
h(.)	Cryptographic hash function with collision resistance
PUF (.)	PUF function
$\oplus$	Exclusive OR operation
$\|$	String concatenation

The approach outlined in [1] is segmented into different stages as follows.

2.1 Mobile User

- ID_i (Selects a unique identity)
- PW_i (Selects a unique password)
- r_i (Generates a random number)
- Computes $RPW_i = h\ (PW_i \| r_i)$
- $MU_i \dashrightarrow \{ID_i, RPW_i, r_i\}$

Biometric Computations:

- Computes:
- $\gamma i = PUF\ (BIO_i)$
- Generates (α_i, β_i) using Gen$(\gamma_i\gamma_i)$
- Computes:
- $\beta_i{}^* = \beta \oplus h(ID_i \| PW_i \| \gamma_i)$
- $X_i{}^* = X_i \oplus h\ ID_i \| \alpha_i \| r_i$
- $RID^*I = RID_i \oplus h\ (\alpha_i \| ID_i \| RPIW_i)$

- $DID^{*}j = DID_j \oplus h\ (ID_i \parallel RPWi \parallel \alpha_i)$
- $C^{*}i = h(RID^{*}i \parallel \alpha_i \parallel X_i^{*} \parallel ri)$

Storage and Replacement:

- Replaces { $RID\hat{}i, X\hat{}i$ } with { RID_i, X_i }
- Stores {$beta\hat{} * \_i, C\hat{} * i, DID\hat{} * j$ } in the mobile device

2.2 DRONE REGISTRATION PROCESS

Drone (D_j) → Control Server (CS)

- (DID_j) (Chooses an identity)
- (b_j) (Selects a random number)
- Sends $\{b_j, DID_j\}$ via secure channel
- Stores $\{N_j, E_j\}$ in the memory Chooses an identityDID_j.

Control Server (CS)

- Identity Verification:
- ($DID^{*}_j = DID_j$)
- Selects a challenge set (C_j)
- Computes ($Res_j = PUF\ (C_j)$
- Generates (R_j, D_j) using Gen (Res_j)
- Computes
- $(Z_j = h\ (DID_j \parallel MSK)$
- $(N_j = Z_j \oplus h(DID_j \parallel bj)$
- $E_j = d_j \oplus^{h\ (Z_j \parallel bj \parallel DID_j)}$
- Stores { $\{Z_j, (C_j, R_j)\}$in a secure database
- Sends $\{N_j, E_j\}$ via secure channel

Mobile User ($M\ U_i$) → Drone (D_j)U_i: Inserts Smart Card.

Computations:

- $\gamma_i = PUF(BOI_i)$
- $\beta_i = \beta^{*} \oplus\ h(ID_i \parallel PWi \parallel\ \gamma_i)$
- $\alpha_i = Rep\ (\gamma_i i, \beta_i)$ • $RPWi = h(PWi \parallel\ ri)$
- $Xi = X^{*} \oplus\ h(ID_i \parallel \alpha_i \parallel ri)$
- $RID_i = RID^{*} \oplus\ h(\alpha_i \parallel ID_i \parallel RPWi)$
- $DIDj = DID * j \oplus\ h(IDi \parallel RPWi \parallel \alpha i)$
- $C * i\ =\ h(RIDi \parallel \alpha i \parallel Xi \parallel ri)$

Verification:

- Check whether $C\ i = C_i$

Random Nonce and Timestamp:

- R1, T1 (Random nonce and timestamp selection)

Additional Computations:

- $M1 = (R1 \parallel DID_j) \oplus h(RID_j \parallel X_i \parallel T1)$
- $Aut^{h_{us}} = h(RID_i \parallel R1 \parallel X_i \parallel T1)$

Timestamps and Freshness:

- T5 (Generation of timestamp)
- Check freshness: $|T5 - T4| \leq \Delta T$

Challenge Set and PUF:

- C_j= Challenge set selection
- $Res_j = PUF(C_j)$
- $(R_j, D_j) = Gen(Res_j)$

Additional Computations:

- $Z_j = h(DID_j \parallel MSK)$
- $N_j = Z_j \oplus h(DID_j \parallel b_j)$
- $E_j = d_j \oplus^{h} (Z_j \parallel bj \parallel DID_j)$

Timestamps and Freshness:

- T2 (Generation of timestamp)
- Check freshness: $|T2 - T1| \leq \Delta T$ *More computations:*
- $(R1 \parallel DID_j) = M1 \oplus h(RID_i \parallel Xi \parallel T1)$
- $Aut^{h_{us}} = h(RID_i \parallel R1 \parallel Xi \parallel T1)$

Retrieval and Nonce:

- Retrieve $(C_j, R_j)\ from\ DID\_j$
- R2 (Random nonce selection)

Additional Computations:

- $M2 = (R1 \parallel R2) \oplus h(DID_j \parallel R_j \parallel Z_j \parallel T2)$
- $Aut^{h_{sd}} = h(DID_j \parallel R2 \parallel Z_j \parallel T2)$

Timestamps and Freshness:

- T4 (Generation of timestamp)
- Check freshness: $|T4 - T3| \leq \Delta T$ *More Computations:*
- $R3 = M3 \oplus h(R_j \parallel R2 \parallel T3)$
- $Aut^{h_{ds}} = h(DID_j \parallel R2 \parallel R3 \parallel R_j \parallel T3)$

Final Computations:

- $M4 = (R2 \parallel R3 \parallel R_j) \oplus h_{(RID_i \parallel DID_j} \parallel R1 \parallel X_i \parallel T4)$
- $Aut^{h_{su}} = h(RID_i \parallel R1 \parallel R2 \parallel X_i)$

Drone(D_j) Equations:

Identity and Random Number:

- $DID_j =$ (Choosing an identity)
- bj (Selecting a random number)

Secure Channel Transmission:

- Send $\{b_j, DID_j\}$ via secure channel

Memory Storage:

- Store$\{N_j, E_j\}$in memory

Identity Verification:

- Check whether $DID^* = DID_j$

Challenge Set and PUF:

- Challenge set selectionC_j
- $Res_j = PUF(C_j)$
- $(R_j, d_j) = Gen(Res_j)$

Additional Computations:

- $Z_j = h(DID_j \| MSK)$
- $N_j = Z_j \oplus h_{(DID_j \| b_j)}$
- $E_j = d_j \oplus h(Z_j \| b_j \|_{DID_j})$

Timestamps and Freshness:

- T2 (Generation of timestamp)
- Check freshness: $|T2 - T1| \leq \Delta T$

Secure Channel Transmission:

- Send $\{N_j, E_j\}$ via secure channel

Timestamps and Freshness:

- T4 (Generation of timestamp)

Check freshness: $|T4 - T3| \leq \Delta T$

Retrieval:

- Retrieve $\{C_j, R_j\}$ from DID_j

Random Nonce:

- R2 (Random nonce selection)

Additional Computations:

- $M2 = (R1 \| R2) \oplus h_{(DID_j \| R_j \| Z_j \| T2)}$
- $Authsd = h(DIDj \| R2 \| Zj \| Rj \| T2)$ *Timestamps and Freshness:*
- T3 (Generation of timestamp)

Check freshness: $|T3 - T2| \leq \Delta T$

Final Computations:

- $M3 = R3 \oplus h(R_j \| R2 \| T3)$
- $SK = h(R1 \| R3 \| R_j)$
- $Aut^{h_{ds}} = h_{(DID_j \| R2 \| T3)}$
- $Aut^{h_{du}} = h(R1 \| R2 \| R_j \|_{DID_j \| SK})$

Session Key Establishment:

- Both MU_i and D_j establish the common session key SK.

2. ANALYSIS

In this section, we have provided an analysis of the SLAP-IoD scheme [1] as follows.

User Identity Attack:

1. Attacker intercepts a legitimate drone's registration message ($DID_j$and b_j).
2. Attacker impersonates the drone, exploiting vulnerabilities in identity verification.
3. CS mistakenly accepts the attacker's message, compromising security.
4. Emphasizes the need for improved identity verification processes.

Stolen Verifier:

1. Attacker intercepts a legitimate mobile user's registration data (ID_i,RPW_i and ri).
2. Attacker independently calculates RID_i and Xi using intercepted data.
3. Attacker can impersonate the user and gain unauthorized access.
4. Calls for enhanced registration security to prevent credential theft.

Time synchronization:

1. Attacker manipulates message delays to disrupt authentication.
2. Causes timestamps to appear invalid, leading to authentication issues.
3. Highlights the importance of accurate time synchronization and timestamp validation mechanisms.

Overhead on Control server for each Session Key:

1. Suggests increasing computational complexity for session key generation.
2. Using resource-intensive cryptographic operations and larger key sizes.
3. Storing session keys for extended periods, leading to increased server storage overhead.
4. Balancing security measures to prevent resource overload on the control server.

3. ACKNOWLEGEMENT

The work is supported by the workstation purchased under the grant GUJCOST/STI/2021-22/3867 by the Gujarat Council of Science and Technology, Government of Gujarat, India.

4. CONCLUSION AND FUTURE WORK

The integration of technologies, including Internet of Drones, sensors, and Cloud computing, is presently leading the way in shaping our future. Authentication and key agreement, as discussed, remain pivotal challenges within these technologies. This paper delves into the examination of the SLAP-IOD approach, revealing vulnerabilities to various attacks. In the future, there is an opportunity to develop a more robust and efficient scheme to address these security concerns.

5. REFERENCES

[1]. SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments Sungjin Yu , Ashok Kumar Das , Senior Member, IEEE, Youngho Park , Member, IEEE, and Pascal Lorenz , Senior Member, IEEE.

[2]. 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.

[3]. Rashid, B.; Rehmani, M.H. Applications of wireless sensor networks for urban areas: A survey. J. Netw. Comput. Appl. 2016, 60,192–219.

[4]. Pierce, F.J.; Elliott, T.V. Regional and on-farm wireless sensor networks for agricultural systems in Eastern Washington. Comput.Electron. Agric. 2008, 61, 32–43.

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. Das, M.L. Two-factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. 2009, 8, 1086–1090.

[10]. He, D.; Gao, Y.; Chan, S.; Chen, C.; Bu, J. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad HocSensorWirel. Netw. 2010, 10, 361–371.

[11]. 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.

[12]. 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.

[13]. 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.

[14]. 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.

[15]. Shuai, M.; Yu, N.;Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security.Comput. Secur. 2019, 86, 132–146.

[16]. 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.

[17]. 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.

[18]. Kalra, S.; Sood, S.K. Advanced password based authentication scheme for wireless sensor networks. J. Inf. Secur. Appl. 2015, 20,37–46.