A Secure Authenticated Key Agreement Scheme for Post-cloud computing–based IoT networks

Upendra Verma[1], Dr. Divya Midhunchakkaravarthy[2], Dr. Pawan Kumar Chaurasia [3]
[1] Post Doc Researcher, Lincoln University College, Malaysia; [2] Director, Centre of Postgraduate Studies, Lincoln University College, Malaysia; [3] Associate Professor, Babasaheb Bhimrao Ambedkar University, A Central University, Lucknow, India
drupendra.pdf@lincoln.edu.my

Abstract: In the past few years, the post-cloud computing model has become one of the most noteworthy technological development because of its competence to process an extensive range of response-intensive internet of things (IoT) applications. The IoT devices have limited computational resources in response-intensive IoT networks. Therefore, security and privacy are critical concerns, and authentication plays a vital role in post-cloud computing–based IoT networks. In this paper, we propose ECC-based authenticated key agreement approach to address authentication challenges in post-cloud computing–based IoT networks. The Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation program under the Dolev-Yao (DY) attack model is used to formally verify the security of the proposed approach. The proposed scheme is compared with existing authentication schemes in terms of computational complexity, and the results confirm its effectiveness for post-cloud computing–based IoT networks. Finally, comparative analysis of security features confirms that the proposed scheme outperforms existing schemes.

Keywords: IoT networks; Security and Privacy; Authentication; AVISPA; Computational complexity

1. Introduction

The applications for the IoT can be found nowadays in many different areas and businesses, such as smart transportation, smart healthcare, smart grids, and industrial automation. [1]. To satisfy the real-time requirements of certain applications, novel computing models such as dew, edge and fog computing have been introduced [2]. Through cloud computing, users have begun to profit from the on-demand availability of computing resources for processing power and data storage in the IoT applications. The demands of ubiquitous networks, fast evolving pervasive devices, and recently developed network applications and services cannot be satisfied by cloud computing's intrinsic centralized processing features. Unfortunately, cloud computing paradigm is not appropriate for the delay sensitive IoT applications due to resource constrained nature of IoT networks [3]. In order to handle response-intensive IoT applications, post-cloud computing architecture for IoT applications known as "Post-cloud computing–based IoT networks" are essential. The post-cloud computing provides various services that are more in line with IoT applications. Table 1 illustrates the difference among cloud and post-cloud computing.

Table 1. Contrast between Cloud and Post-Cloud Computing

Attributes	***Cloud Model***	***Post-Cloud Model***
Energy consumption	High	Low
Latency	High	Low
Architecture	Centralized	Distributed
Bandwidth constraints	High	Low
Storage	High	Limited
Computational power	High	Limited
Scalability	Low	High
Location awareness	Partially supported	Supported
Number of nodes	Few	More
Mobility support	Limited	Fully supported

In 2011, Cisco introduced the idea of fog computing [4]. Fog computing is an abstracted framework that facilitates communication, storage, and processing between cloud centers and end devices. European Telecommunications Standards Institute (ETSI) first put up the idea of mobile edge computing in 2014 [5]. Mobile edge computing offers IT service infrastructures and virtualization abilities to content producers and application developers at the edge of mobile networks. In 2012, the academic community launched dew computing [6]. Without an internet connection, dew computing offers services nearer to IoT devices. The post-cloud computing paradigms are fully distributed computing architectures that are extremely vulnerable to different cryptographic attacks because of their open nature, multiple network points, and absence of centralized control. Therefore, secure authentication protocol is required for the post-cloud computing–based IoT networks, which should be lightweight and computationally efficient in the resource constrained networks. According to the literature, several authenticated key agreement schemes for post-cloud computing–based IoT networks have been proposed [7-11]. Nevertheless, the existing protocols do not provide various security features such as anonymity, privacy, key agreement and untraceability. Moreover, they are not resistant against the common security threats such as DoS, MITM, impersonation and replay attacks. Therefore, we proposed an efficient authentication protocol for post-cloud computing–based IoT networks, which utilized ECC, XOR operation and one-way hash function.

Key Contributions

- Lightweight cryptographic primitives like hash functions, XOR operations, and ECC were used in the proposed authenticated key agreement approach to create an authentication approach for post-cloud computing–based IoT networks.
- The AVISPA simulation formally verifies the propounded approach using the DY attack model.
- The proposed strategy and the existing scheme are compared in terms of various security features. According to the analysis, the proposed approach is well suited for post-cloud computing–based IoT networks.

Organization of paper Section 2 deliberates the existing works. Section 3 discusses the desgined authentication and key agreement scheme. The experiments and results are outlined in the Section 4. Section 5 concludes the proposed work.

2. Related work

Table 1 presents a summary of related work based on three parameters: post–cloud computing paradigms, strengths, and limitations.

Table 2. Summary of related works

Authentication schemes	***Post–cloud computing paradigms***	***Strengths***	***Limitations***
Braeken [12], 2022	Dew computing	Anonymity; Can resist against replay and insider attacks	Can't provide key agreement
Chen et al. [13], 2021	Fog computing	Resilience against dictionary attack	Unable to provide anonymity
Shahidinejad et al., [14], 2021	Edge computing	Protected from MITM and eavesdropping with anonymity	Very high computational complexity
Wu et al. [15], 2021	Fog computing	Resilience against MITM and replay attacks	Cann't resist against smart card loss attack
Ma et al. [16], 2022	Dew computing	Provide anonymity and resistant against replay attack	Problem in key agreement
Liu et al. [17], 2024	Fog computing	Resilience to MITM and session key attack	Susceptible to impersonation attack
Rakeei et al. [18], 2022	Edge computing	Provide PUF feature	Can't resist against DoS attack
Tomar et al. [19], 2022	Fog computing	Provides anonymity	Can't resist against replay attack
Rana et al. [20], 2021	Dew computing	Provide mutual authentication and anonymity	Can't provide forward secrecy

3. Proposed Method

This segment describes the working procedure of proposed authenticated key agreement approach. Table 3 gives the various notations used in the proposed strategy.

Table 3. Notations and their meaning

Notations	***Meaning***
EC_p	Elliptic over prime number p
D_{IoT}	IoT device
$P\text{-}Cloud_{Server}$	Post-cloud computing servers i.e. dew, fog or edge servers
PU_k	Public key
PR_k	Private key
n_1, n_2	Random nonce
$H(\cdot)$	One-way hash function
K_1	Key generates by device
K_2	Key generates by dew server
A, B, E, F	Parameters shared between dew server and device

The proposed strategy is divided into two distinct phases: setup phase and authenticated key agreement phase.

i. Setup Phase

This section describes the generation of few system parameters and how the parameters are distributed by the $P\text{-}Cloud_{Server}$.

- The $P\text{-}Cloud_{Server}$ selects a elliptic curve EC_p over prime number p and chooses PR_k and computes PU_k for D_{IoT} using as $D_{IoT}\ (PU_k) = D_{IoT}\ (PR_k) \cdot GP$.
- The $P\text{-}Cloud_{Server}$ chooses PR_k and computes PU_k using ECC as $P\text{-}Cloud_{Server}\ (PU_k) = P\text{-}Cloud_{Server}\ (PR_k) \cdot GP$.
- $P\text{-}Cloud_{Server}$ stores few parameters to the memory of D_{IoT}: $\{H(\cdot), D_{IoT}\ (PU_k), D_{IoT}\ (PR_k), P\text{-}Cloud_{Server}\ (PU_k)\}$
- $P\text{-}Cloud_{Server}$ stores few parameters to its memory: $\{H(\cdot), P\text{-}Cloud_{Server}\ (PU_k), P\text{-}Cloud_{Server}\ (PR_k), D_{IoT}\ (PU_k)\}$.

ii. Authenticated key agreement phase (AKA)

This section describes how $P\text{-}Cloud_{Server}$ and D_{IoT} are jointly authenticated with each other and also generates common key. This phase has following steps:

- $P\text{-}Cloud_{Server}$ creates nonce n_1 and computes ECC point A as $A = n_1 \cdot GP$. Parameter $\{A\}$ is transmitted to D_{IoT}.
- Upon receiving $\{A\}$, D_{IoT} produces nonce n_2 and computes ECC point B as $B = n_2 \cdot GP$.
- D_{IoT} generated X_1 as $X_1 = A \cdot D_{IoT}\ (PR)$.
- D_{IoT} computes $E = H(B\ //\ A\ //X_1)$. Parameters $\{B\}$ and $\{E\}$ are transmitted to $P\text{-}Cloud_{Server}$. Upon receiving $\{B\}$ and $\{E\}$, $P\text{-}Cloud_{Server}$ generates X_2 as $X_2 = n_1 \cdot D_{IoT}\ (PU)$.
- $P\text{-}Cloud_{Server}$ computes C as $C = H(B\ //\ A\ //\ X_2)$. $P\text{-}Cloud_{Server}$ compares E and C as $E=?\ C$. If false then authentication process is suspended, otherwise continue to next step.
- $P\text{-}Cloud_{Server}$ computes Y_1 as $Y_1 = B \cdot P\text{-}Cloud_{Server}\ (PR)$ and F as $F = H(Y_1\ //\ C)$. The parameter $\{F\}$ is transmitted to D_{IoT}.
- D_{IoT} computes Y_2 as $Y_2 = n_2 \cdot P\text{-}Cloud_{Server}\ (PU)$ and D as $D = H(Y_2\ //\ E)$. D_{IoT} compares E and D as $F =?\ D$. If false then authentication process is suspended, otherwise continue to next step.
- D_{IoT} generates K_1 as $K_1 = n_2 \cdot A$.
- $P\text{-}Cloud_{Server}$ generates K_2 as $K_2 = n_1 \cdot B$.

It is noted that K_1 and K_2 are equivalent with each other as $K_1 = n_2 \cdot A = n_2 \cdot n_1 \cdot BP = n_1 \cdot B = K_2$.

4. Experiments and Results

The experiment of proposed scheme is conducted using AVISPA simulation tools [21]. It is a formal verification tool for analyzing and validating cryptographic protocols against many types of attacks, particularly key-agreement and authentication methods. AVISPA is used to determine whether a cryptographic protocol is secure or susceptible. The following is the experimental configuration for the proposed scheme:

- ***Processor:*** *Intel ® Core ™ i5-8265U CPU @ 1.80 GHz*
- ***Installed memory (RAM):*** *6GB*
- ***System type:*** *64-bit Operating System, x64-based processor*

- ***SPAN:** Security Protocol Animator*
- ***Intruder Model:** DY attack model*
- ***Backend:** OFMC and AtSE*

The formal security validation of propounded method is conducted using OFMC and CL-AtSE backends. There is no attack trace found during the security verification of proposed scheme. Therefore, the proposed authentication scheme is SAFE under the DY attack model. Figure 1 depicts the simulation results of the proposed scheme.

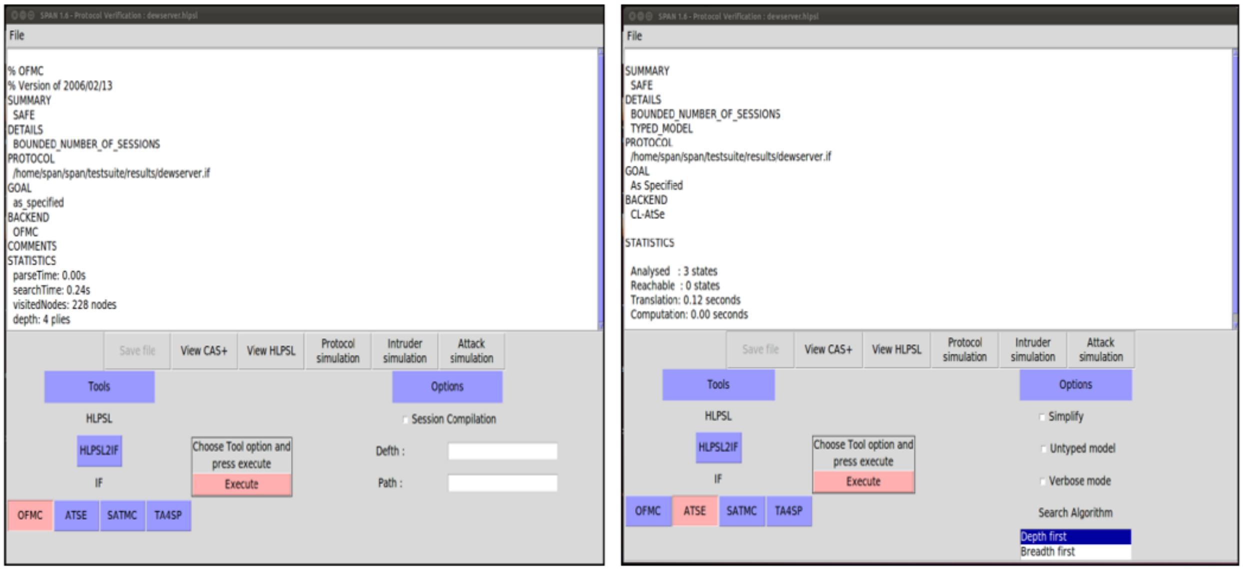

Figure 1. Simulation results

5. Conclusions

In this work, we proposed a secure and efficient AKA protocol for post-cloud computing–based IoT networks. The proposed technique offers typical security properties like anonymity, mutual authentication, and forward secrecy, while the present AKA does not meet these requirements. The proposed AKA scheme is suitable for resource constrained nature due to lightweight operations such as XOR, ECC and hash function. The formal security verification under AVISPA is conducted, which shows that our scheme is SAFE under the well-known DY attack model. In future, we would like to devise the proposed scheme for the multi-tier server architecture.

References

1. R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0," *Sensors*, vol. 23, no. 16, Art. no. 7194, 2023. https://doi.org/10.3390/s23167194
2. Y. Zhou, D. Zhang, and N. Xiong, "Post-cloud computing paradigms: A survey and comparison," *Tsinghua Science and Technology*, vol. 22, no. 6, pp. 714–732, 2017. https://doi.org/10.23919/TST.2017.8195346

3. R. O. Aburukba *et al.*, “Scheduling Internet of Things requests to minimize latency in hybrid fog–cloud computing,” *Future Generation Computer Systems*, vol. 111, pp. 539–551, 2020. https://doi.org/10.1016/j.future.2020.05.023
4. C. Puliafito *et al.*, “Fog computing for the Internet of Things: A survey,” *ACM Transactions on Internet Technology*, vol. 19, no. 2, pp. 1–41, 2019. https://doi.org/10.1145/3301614
5. Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, “Mobile edge computing—A key technology towards 5G,” ETSI White Paper No. 11, Sep. 2015. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf?utm_source=chatgpt.com
6. M. Gusev, “What makes dew computing more than edge computing for Internet of Things,” in *Proc. IEEE 45th Annual Computers, Software, and Applications Conf. (COMPSAC)*, Madrid, Spain, pp. 1795–1800, Jul. 12–16, 2021. https://doi.org/10.1109/COMPSAC51774.2021.00269
7. U. Verma and D. Bhardwaj, “A secure lightweight anonymous elliptic curve cryptography-based authentication and key agreement scheme for fog-assisted Internet of Things enabled networks,” *Concurrency and Computation: Practice and Experience*, vol. 34, no. 23, Art. no. e7172, 2022. https://doi.org/10.1002/cpe.7172
8. U. Verma, K. D. Gautam, and S. K. Shukla, “Anonymous Mutual Authentication and Key Agreement Scheme in Edge-enabled Wireless Body Area Networks,” in *Proc. 2025 6th Int. Conf. Recent Advances in Information Technology (RAIT)*, Dhanbad, India, Mar. 6–8, 2025. https://doi.org/10.1109/RAIT65068.2025.11089377
9. U. Verma and R. Dhanare, “A robust ECC-based authenticated key agreement protocol for wireless body area networks,” *Concurrency and Computation: Practice and Experience*, vol. 37, no. 27–28, Art. no. e70361, 2025. https://doi.org/10.1002/cpe.70361
10. Y. Ren *et al.*, “Identity management and access control based on blockchain under edge computing for the industrial Internet of Things,” *Applied Sciences*, vol. 9, no. 10, Art. no. 2058, 2019. https://doi.org/10.3390/app9102058
11. Y.-T. Huang, T.-S. Chen, and S.-D. Wang, “Authenticated key agreement scheme for fog computing in a health-care environment,” *IEEE Access*, vol. 11, pp. 46871–46881, 2023. https://doi.org/10.1109/ACCESS.2023.3274095
12. Braeken, “Authenticated key agreement protocols for dew-assisted IoT systems,” *The Journal of Supercomputing*, vol. 78, no. 10, pp. 12093–12113, 2022. https://doi.org/10.1007/s11227-022-04388-0
13. C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, and M.-E. Wu, “A secure authenticated and key exchange scheme for fog computing,” *Enterprise Information Systems*, vol. 15, no. 9, pp. 1200–1215, 2021. https://doi.org/10.1080/17517575.2020.1837111

14. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar, and S. Kumari, “Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloud environment,” *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 57–63, 2021. https://doi.org/10.1109/MCE.2021.3055406
15. T.-Y. Wu, Z. Lee, L. Yang, J.-N. Luo, and R. Tso, “Provably secure authentication key exchange scheme using fog nodes in vehicular ad hoc networks,” *The Journal of Supercomputing*, vol. 77, no. 7, pp. 6992–7020, 2021. https://doi.org/10.1007/s11227-021-03891-3
16. Y. Ma, Y. Ma, and Q. Cheng, “Cryptanalysis and enhancement of an authenticated key agreement protocol for dew-assisted IoT systems,” *Security and Communication Networks*, vol. 2022, Art. no. 1–11, 2022. https://doi.org/10.1155/2022/1234567
17. J. Liu, H. Wang, J. Bao, R. Sun, X. Du, and M. Guizani, “RPMDA: Robust and privacy-enhanced multidimensional data aggregation scheme for fog-assisted smart grids,” *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 16021–16032, May 2024. https://doi.org/10.1109/JIOT.2024.3352558
18. M. Rakeei and F. Moazami, “An efficient and provably secure authenticated key agreement scheme for mobile edge computing,” *Wireless Networks*, vol. 28, no. 7, pp. 2983–2999, 2022. https://doi.org/10.1007/s11276-022-03005-w
19. Tomar and S. Tripathi, “Blockchain-assisted authentication and key agreement scheme for fog-based smart grid,” *Cluster Computing*, vol. 25, no. 1, pp. 451–468, 2022. https://doi.org/10.1007/s10586-021-03420-2
20. S. Rana, M. S. Obaidat, D. Mishra, A. Mishra, and Y. S. Rao, “Efficient design of an authenticated key agreement protocol for dew-assisted IoT systems,” *The Journal of Supercomputing*, vol. 78, no. 3, pp. 3696–3714, 2022. https://doi.org/10.1007/s11227-021-04003-z
21. J. A. Hurtado Alegría, M. C. Bastarrica, and A. Bergel, “AVISPA: a tool for analyzing software process models,” *Journal of Software: Evolution and Process*, vol. 26, no. 4, pp. 434–450, Apr. 2014. https://doi.org/10.1002/smr.1578