Lightweight and Efficient ECC-Based Authentication for Dew computing-assisted 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: The dew computing ($\mathcal{DC}$) is the most promising technology that provide data access without the internet. However, $\mathcal{DC}$ presents new difficulties, especially in regard to privacy and security. Key agreement and authentication provide significant issues in the $\mathcal{DC}$ paradigm that need to be considered. The goal of proposed work is to provide a safe authentication system based on *ECC* for Internet of Things (*IoT)*. The proposed strategy has also been contrasted with analogous schemes in terms of a number of security aspects, including resilience to replay and denial of service (*DoS*) attacks, anonymity, key agreement, mutual authentication, and perfect forward secrecy. The informal security analysis is conducted, which indicates the proposed approach is resilience to cryptographic attacks.

Keywords: Mutual authentication; Cryptographic attacks; Dew computing; ECC.

1. Introduction

IoT is a network of physical objects that may be connected with sensors, actuators, and software stacks to create a centralized platform for data interchange and communication with cloud servers [1]. The concept of cloud computing has significantly developed during the past few years in order to solve the problem of sharing resources to the IoT applications [2]. IoT and cloud computing are merged together called cloud computing-assisted IoT networks, which have been used in many smart applications such as smart transportation, smart healthcare, smart city and smart home [3]. However, the cloud computing is unable to fulfil the need of delay sensitive IoT applications, where faster response time is required to process the information. The latency and bandwidth are the major drawback of cloud computing enabled IoT model. To address the issues of cloud computing, the post cloud computing paradigms emerges to solve the services of delay-sensitive IoT applications. The post cloud computing model brings the processing power closer to the IoT devices [4]. The common post cloud computing models are fog, edge and $\mathcal{DC}$ illustrated in the Figure 1.

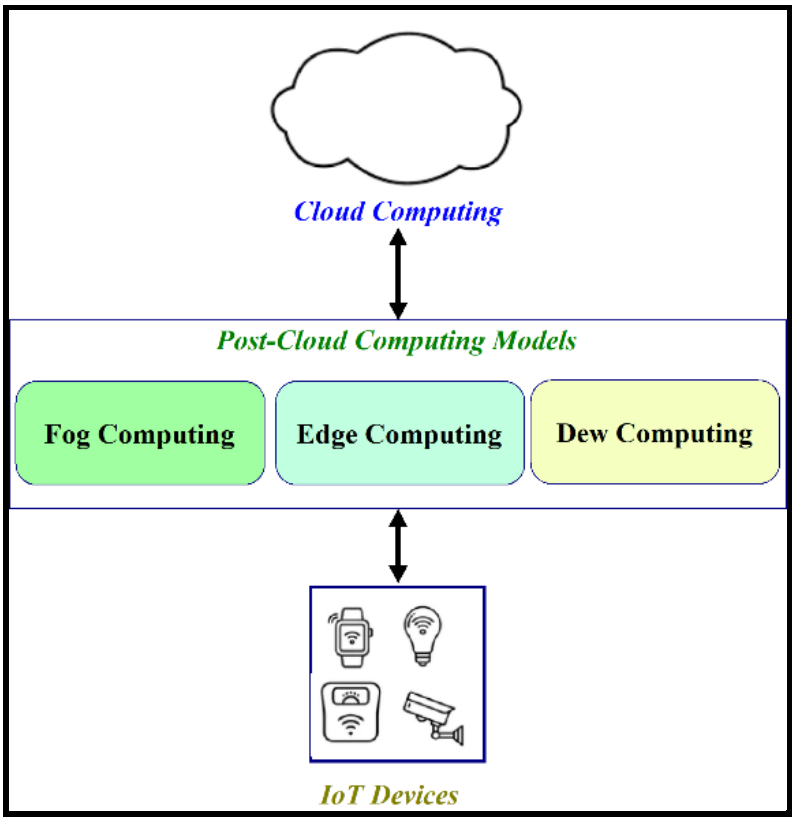

Figure 1. *Post-Cloud Computing Architecture Empowered by IoT*

As per the figure, fog and edge computing provides services to the user with the help of internet connection. If the internet connection is not available, then in this situation services won't be accessed by the user. In these situations, $\mathcal{DC}$ has been developed to confirm the accessibility with the devices. IoT and $\mathcal{DC}$ are combined with each other to realize the dew-assisted IoT networks. Dew-assisted IoT networks provide all services to the IoT device without internet access [5].

In $\mathcal{DC}$ environment, $\mathcal{DC}$ server provides services to the IoT devices in the absence of internet between dew server and IoT devices. Due to instable connection between dew server and *IoT* device, a security is the major concern and the authentication is the supreme requirement in this case. Therefore, secure authentication protocol is required for the dew-assisted IoT networks, which should be lightweight and computationally efficient in the resource constrained networks. As per literature, there are some existing protocols have been proposed in the dew-assisted networks [6-9]. However, they are unable to provide common security requirement such as perfect forward secrecy, anonymity, and location privacy. The existing protocol are not resilience against the common cryptographic attacks such as replay, *MITM* and *DoS* attacks. Therefore, we proposed an efficient authentication protocol for dew-assisted IoT networks, which utilized *ECC*.

Research Contributions

- The proposed system employed *ECC*-cryptographic primitives to develop secure anonymous authenticated key agreement for dew-assisted IoT networks.
- Informal security analysis has carried out, which shows the proposed scheme ensures common security requirements with resilience to various cryptographic attacks.

Organization of paper Section 2 discusses the related works. Section 3 addresses the preliminaries which contains network model and attack model. The proposed scheme is outlined in the Section 4. Section 5 presents the informal security analysis. Section 6 concludes the proposed work.

2. Related Works

$\mathcal{DC}$ emerged more recently compared to cloud and fog computing. Research is still exploring foundational aspects like architecture, communication models, and use cases. Hence, few authentication schemes have been proposed specifically for it so far. An *ECC* based authentication scheme was presented by Wang et al. [10]. A mutual authentication method for dew-assisted IoT networks was proposed by Rana et al. [6]. There is no anonymity in their strategy. Another authentication protocol for dew-assisted IoT devices was proposed by Ma et al. [11]. They have discussed Rana et al. [6] security issue and then claimed that the Rana et al. [6] scheme was suffered to offer user anonymity and forward security. Braeken et al. [7] proposed an authenticated key agreement technique for dew-assisted IoT system. Their strategy demonstrates how Rana et al. [6] are susceptible to a number of cryptographic assaults. Yadav et al. [12] conducted a new investigation and examined the protocol that Ma et al. [11] proposed. According to their review, the strategy presented by Ma et al. [11] has security issues, such as common shared keys and malicious trusted third parties (TTP).

3. Preliminaries

i. Network Model

Network model is the physical arrangement that explains the connections and interactions between IoT devices and dew server. In the network model, the IoT device is able to access services from the dew server in the absence of internet connections. Figure 2 depicts the network model.

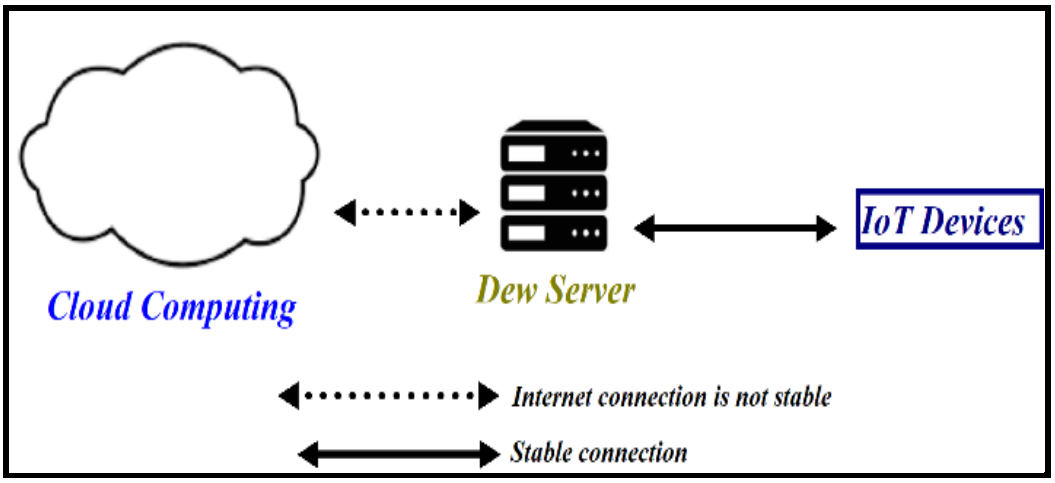

Figure 2. *Network model*

ii. Attack Model

This section describes the attack model, which can be used by adversary to deduce confidential and sensitive information.

- The adversary intercepts and modifies the message transferred between network entities.
- The adversary may impersonate as device and contact to the real dew server.
- The messages are altered, replayed and broadcast by the adversary.
- The adversary intercepts the previous transmitted message among the network entities.

4. Proposed scheme

This section describes the working procedure of proposed authenticated key agreement approach. The flow chart of proposed strategy is depicted in Figure 3.

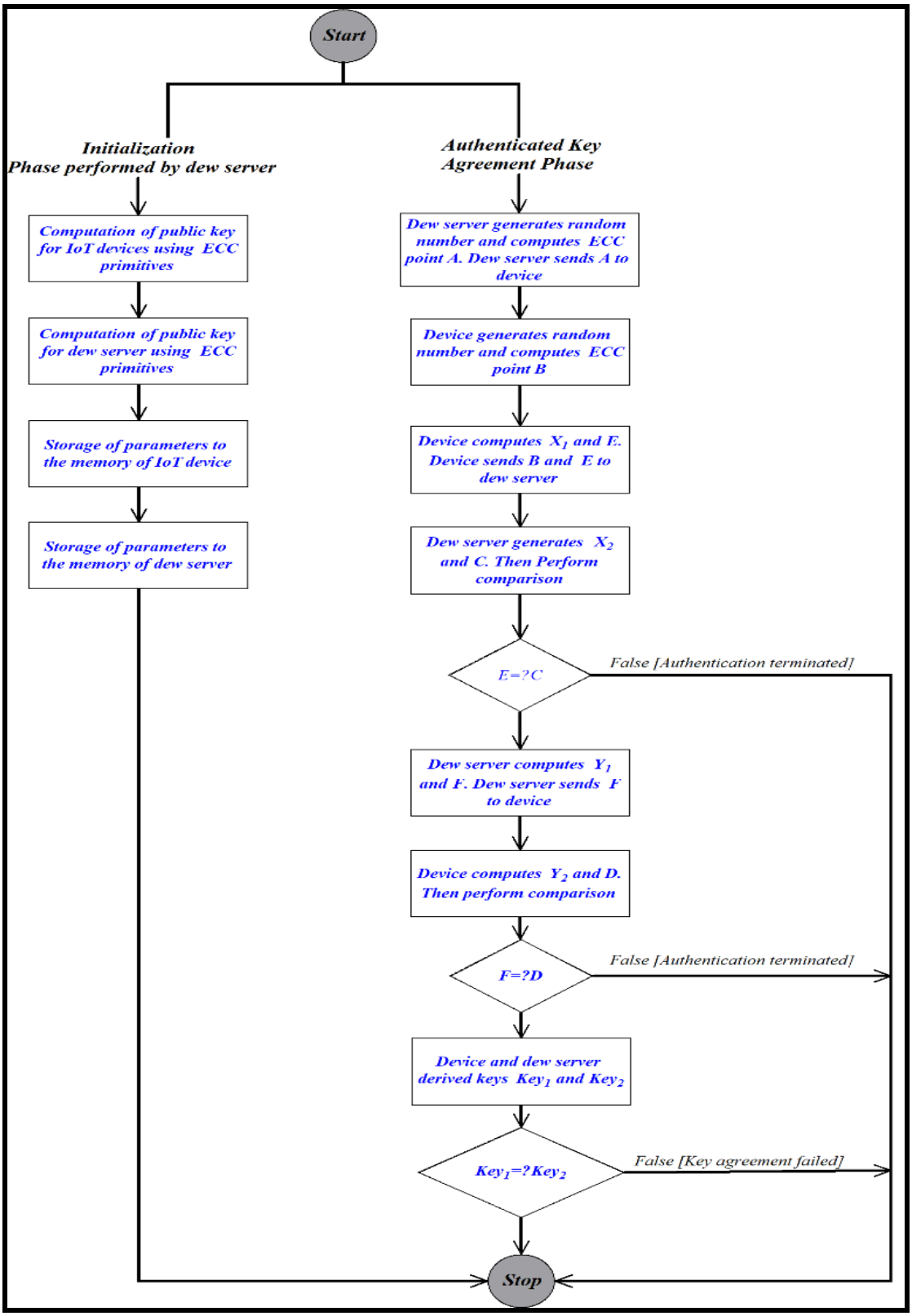

Figure 3. *Flow chart of proposed scheme*

Table 1 gives the various notations used in the proposed strategy.

Table 1. *Notation used in this article*

Notations	***Meaning***
EC_p	*Elliptic over prime number p*
PU	*Public key*
PR	*Private key*
r_1, r_2	*Random numbers*
H	*One-way hash function*
Key_1	*Key generates by device*
Key_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: Initialization phase and authenticated key agreement phase.

i. Initialization Phase

This section describes the generation of few system parameters and how the parameters are distributed by the dew server.

- The dew server selects a elliptic curve EC_p over prime number p and selects private key and computes public key for device using as $device(PU) = device(PR) \cdot BP$.
- The dew server chooses private key and computes public key using *ECC* as $dew(PU) = dew(PR) \cdot BP$.
- Dew server stores few parameters to the memory of device: *{H, device(PU), device(PR), dew(PU)}*
- Dew server stores few parameters to its memory: *{H, dew(PU), dew(PR), device(PU)}*.

ii. Authenticated key agreement phase

This section describes how dew server and device are mutually authenticated with each other and also generates a common session key. This phase has following steps:

1. Dew server generates random number r_1 and computes *ECC* point *A* as $A = r_1 \cdot BP$. Parameter *{A}* is transmitted to device.
2. Upon receiving *{A}*, device generates random number r_2 and computes *ECC* point *B* as $B = r_2 \cdot BP$.
3. Device generated X_1 as $X_1 = A \cdot device(PR)$.
4. Device computes $E = H(B \ //A \ //X_1)$. Parameters *{B}* and *{E}* are transmitted to dew server.
5. Upon receiving *{B}* and *{E}*, dew server generates X_2 as $X_2 = r_1 \cdot device(PU)$.
6. Dew server computes *C* as $C = H(B \ //A \ //X_2)$. Dew server compares *E* and *C* as *E=? C*. If false then authentication process is suspended, otherwise continue to next step.
7. Dew server computes Y_1 as $Y_1 = B \cdot dew(PR)$ and *F* as $F = H(Y_1 \ //C)$. The parameter *{F}* is transmitted to device.

8. Device computes Y_2 as $Y_2 = r_2 \cdot dew(PU)$ and D as $D = H(Y_2 \ // E)$. Device compares E and D as $F =? D$. If false then authentication process is suspended, otherwise continue to next step.
9. Device generates Key_1 as $Key_1 = r_2 \cdot A$.
10. Dew server generates Key_2 as $Key_2 = r_1 \cdot B$.

In step 9 and step 10, Key_1 and Key_2 are equivalent with each other as $Key_1 = r_2 \cdot A = r_2 \cdot r_1 \cdot BP = r_1 \cdot B = Key_2$.

5. Informal Security Analysis

i. Mutual authentication

Device computes parameter *{E}* and sends to dew server. The dew server generates *{C}* and perform comparison between *{E}* and *{C}*. If both are equivalent, then authentication process continues. Similarly, dew server computes *{F}* and sends to device. The device computes *{D}* and perform comparison between *{F}* and *{D}*. If both are equivalent, then authentication process continues. Therefore, the proposed scheme achieves the mutual authentication.

ii. Anonymity

The proposed scheme uses the random number r_1 and r_2. It is infeasible to compute the r_1 and r_2 due to elliptic curve discrete logarithm problem (*ECDLP*). Moreover, these parameters are also protected from one-way hash function. Hence, the proposed scheme provides anonymity.

iii. Protection from impersonation attack

The adversary has credential *{A}* and *{F}* to impersonate IoT device and *{B, E}* to impersonate dew server. However, *{E}* and *{F}* are protected by *H*. *{A}* and *{B}* generated by r_1 and r_2 and r_1, r_2 are never shared during the communication.

iv. Protection from replay attack

All exchanged parameters are computed using random numbers and private credential i.e. private key of dew server and device. Therefore, the proposed method is safe against replay attack.

v. Protection from MITM attack

The parameter *{B}* is transferred between dew sever and device. The parameter *{B}* is produced by r_1 and r_2. intruder can't get the useful information without r_1 and r_2.

vi. Protection from MITM attack

Dew server and device should create a shared key without disclosing the secret parameters. The device produces Key_1 as $Key_1 = r_2 \cdot A$. Dew server generates Key_2 as $Key_2 = r_1 \cdot B$. The Key_1 and Key_2 are equivalent with each other as $Key_1 = r_2 \cdot A = r_2 \cdot r_1 \cdot BP = r_1 \cdot B = Key_2$. The random number r_1 and r_2 are used to generate Key_1, Key_2 and r_1, r_2 are never shared between dew server and device. Therefore, the proposed strategy offers secure key agreement between dew server and device.

6. Conclusions

This work provides a comprehensive analysis of authentication schemes in post-cloud computing model. This study emphasizes the challenges of IoT-Cloud computing paradigm, along with how the post-cloud computing models address these challenges. The post-cloud computing model delivers services closer to the user's premises. However, this proximity increases the attack surface, making communications potentially more vulnerable to security threats. The emerging security challenges in the post-cloud computing model, including inadequate authentication, insufficient anonymity, lack of untraceability, and reduced resilience against cryptographic attacks.

The paper shows the realization procedure of authentication scheme, which provides valuable insights that can guide researchers in exploring future research directions.

References

1. Milenkovic, Milan. Internet of things: concepts and system design. Vol. 8. Berlin/Heidelberg, Germany: Springer, 2020. https://link.springer.com/book/10.1007/978-3-030-41346-0

2. Sadeeq, Mohammed Mohammed, Nasiba M. Abdulkareem, Subhi RM Zeebaree, Dindar Mikaeel Ahmed, Ahmed Saifullah Sami, and Rizgar R. Zebari. IoT and Cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal, Vol. 1, No. 2, pp. 1-7, 2021. https://journal.qubahan.com/index.php/qaj/article/view/36

3. Khan, L.U., Yaqoob, I., Tran, N.H., Kazmi, S.A., Dang, T.N. and Hong, C.S. Edge-computing-enabled smart cities: A comprehensive survey. IEEE Internet of Things journal, Vol. 7, No. 10, pp.10200-10232, 2020. https://ieeexplore.ieee.org/abstract/document/9063670/

4. Zhou, Yuezhi, Di Zhang, and Naixue Xiong. Post-cloud computing paradigms: a survey and comparison. Tsinghua Science and Technology, Vol. 22, No. 6, pp. 714-732, 2017. https://ieeexplore.ieee.org/abstract/document/8195353/

5. Ray, P.P. and Skala, K. Internet of things aware secure dew computing architecture for distributed hotspot network: a conceptual study. Applied Sciences, Vol. 12, No. 18, p.8963, 2022. https://www.mdpi.com/2076-3417/12/18/8963

6. Rana S, Obaidat MS, Mishra D, Mishra A, Rao YS, Efficient design of an authenticated key agreement protocol for dew-assisted IoT systems. J Supercomputing, 2021. https://link.springer.com/article/10.1007/s11227-021-04003-z

7. Braeken, A. Authenticated key agreement protocols for dew-assisted IoT systems. The Journal of Supercomputing, Vol. 78, No. 10, pp.12093-12113, 2022. https://link.springer.com/article/10.1007/s11227-022-04364-z

8. Jan, S.U., Ghani, A., Alzahrani, A., Tariq, M.U., Algarni, F. and Naqvi, H.A. SKALP: Secure key agreement and lightweight protocol for dew-assisted IoT enabled edge computing. Transactions on Emerging Telecommunications Technologies, Vol. 35, No. 9, p.e5035, 2024. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.5035

9. Verma, U. and Sohani, M. An efficient lightweight authentication scheme for dew-assisted IoT networks. Security and Privacy, Vol. 7, No. 2, p.e360, 2024. https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.360

10. Wang KH, Chen CM, Fang W, Wu TY. A secure authentication scheme for internet of things. Pervas Mob Comput. Vol. 42, pp. 15-26, 2017. https://www.sciencedirect.com/science/article/pii/S1574119216304369

11. Ma Y, Ma Y, Cheng Q. Cryptanalysis and enhancement of an authenticated key agreement protocol for dew-assisted IoT systems. SecurCommun Netw. Vol. 2022, No. 1, pp. 7145491, 2022. https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/7125491

12. Yadav AK, Braeken A, Misra M. Symmetric key-based authentication and key agreement scheme resistant against semi-trusted third party for fog and dew computing. J Supercomput. Vol. 79, pp. 1-39, 2023. https://link.springer.com/article/10.1007/s11227-023-05064-y