Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 22(3): 199-206, Sep. 2024 Regular paper

Differential Authentication Scheme for Electric Charging System through Light Gradient Boosting Machine

Byung-Hyun Lim[1], Ismatov Akobir[1], and Ki-Il Kim[1]*, *Member, KIICE*

[1]Department of Computer Science and Engineering, Chungnam National University, Daejeon 34134, Republic of Korea

Abstract

The network security of Plug-and-Charge (PnC) technology in electric vehicle charging systems is typically achieved through the well-known Transport Layer Security (TLS) protocol, which causes high communication overhead. To reduce this overhead, a differential authentication method employing different schemes for individual users has been proposed. However, decisions use a simple threshold approach and no quantitative performance evaluation should be made. In this study, we determined each user's trust using several machine learning algorithms with their charging patterns and compared them. The experimental results reveal that the proposed approach outperforms the conventional approach by 41.36% in terms of round-trip time efficiency, demonstrating its effectiveness in reducing the TLS overhead. In addition, we show the simulation results for three user authentication methods and capture the performance variations under CPU busy waiting scenarios.

Index Terms: Differential authentication, Data-driven, Electric vehicle charging patterns, Machine learning

I. INTRODUCTION

With the increasing demand for Electric Vehicles (EV) and Charging Stations (CS), ISO/IEC 15118, a worldwide communication standard, is proposed to facilitate seamless charging and improve interoperability between EVs and CSs. Specifically, ISO 15118 Part 2 [1] incorporates Plug-and-Charge (PnC) technology to automatically authenticate customers visiting a CS while charging an EV.

Once the charger is connected to the EV, the PnC technology described in ISO 15118 Part 2 supports all authentication processes, billing information (i.e., payment rates), and controls information exchange over the CS communication network. Transport Layer Security (TLS)-based public key infrastructure authentication is employed to provide secure activities for EV users during PnC activities. However, TLS authentication methods incur additional communication costs and expose certificate validation issues over time [2]. To overcome this issue, previous studies on reducing the overhead of TLS authentication have mainly focused on two methods: lightweight TLS and differential authentication.

The lightweight TLS concept is described in [3,4]. iTLS [3] is a lightweight TLS protocol for Internet of Things (IoT) devices. This protocol allows clients to transmit encrypted data without additional handshaking by dynamically generating an identity authentication key for initial authentication before receiving a server response. The iTLS is suitable for IoT environments that require low power owing to the reduced network traffic overhead and handshaking latency compared with TLS. Another extension of the iTLS was proposed in [4] by analyzing security vulnerabilities using an Open-source Fixed-point Model Checker. The Zero Round-Trip Time (0-RTT) mode was applied to reduce the bandwidth overhead by 193 bytes, making it suitable for IoT. However, because of the lack of dependency on power constraints such as IoT, a different lightweight approach is required for EV charging systems.

Received 15 February 2024, **Revised** 23 April 2024, **Accepted** 13 May 2024
***Corresponding Author** Ki-Il Kim (E-mail: kikim@cnu.ac.kr, Tel: +82-42-821-6856)
Department of Computer Science and Engineering, Chungnam National University, Daejeon 34134, Republic of Korea

Open Access https://doi.org/10.56977/jicce.2024.22.3.199 print ISSN: 2234-8255 online ISSN: 2234-8883

To address the TLS lightweight, as a second approach, differential authentication based on user trust has been proposed by our research group in [5]. In our previous work, we evaluated the trust of EV users and reduced the communication overhead for user authentication between the CS and server by applying a simpler authentication method than TLS. Trusted users are authenticated using a simpler method than existing TLS authentication methods, such as Open Authorization (OAuth) [6] and One-Time Password (OTP). EV-Auth [7] is not considered when reducing the overhead associated with TLS authentication. Therefore, we chose OTP as a simple authentication method. This approach contributes to reducing the communication overhead. However, previous studies have simply made decisions regarding user evaluations using arithmetic and numerical approaches. Moreover, no performance evaluation was conducted. Therefore, it is necessary to replace the threshold-based scheme as well as provide performance evaluation. For this purpose, we introduced machine learning schemes for user evaluation using user data. In particular, we focus on user-charging patterns, which have been extensively studied.

Previous studies that utilized user-charging patterns were categorized into classifying user groups and deriving charging patterns. In [8-10], EV users were categorized based on their charging behaviors, preferred locations, and charger types. In [8], Dutch EV users were clustered into daytime and nighttime charging types. [9] classified Korean electric vehicle users based on charging stations and charger types, and identified their charging habits. [10] studied California plug-in electric vehicle users and differentiated their charging behavior based on charger type and location. These studies used regular charging times, charger types, and charging details to classify users and suggested that users prefer specific locations and charger types. In [11-15], machine learning was used for the predictive modeling of EV charging behavior. Several predictive modeling and machine learning techniques have been proposed to analyze and recommend current and future EV charging infrastructures. These models include power demand prediction, charging demand prediction, and diverse charging-pattern analyses.

Despite previous studies on user-charging patterns, none have explored the use of these data to evaluate trust in user authentication. Although previous studies have focused on predicting charging demand and efficient energy management, this study aims to explore a new approach for evaluating trust to reduce the overhead of TLS authentication by reducing the number of TLS user authentications.

The remainder of this paper is organized as follows. Section II summarizes previous studies on EV user-charging patterns and describes machine learning approaches. Section III describes the simulation settings used in this study and the performance metrics for each scenario. Section IV summarizes our findings and suggests avenues for future research.

II. DIFFERENTIAL AUTHENTICATION SCHEME THROUGH ML APPROACHES

In the previous section, various studies that used EV charging patterns were described. In this section, we analyze the algorithms proposed in existing studies and propose an improved trust-evaluation algorithm by extending the study by adding threshold settings through machine learning using user-charging data.

A. Previous Numeric-based Differential Authentication

A trust evaluation of both charging stations and users was performed using a previously proposed algorithm [5]. This section focuses on the CS and user trust evaluation parameters outlined in Table 1.

1) CS trust-evaluation parameters

For the trust-evaluation items of the charging station, we checked and compared the number of incorrect payments made at the charging station using a directly set threshold. If it is higher than the threshold, we evaluate it as having low trust. If it is lower than the threshold, we evaluate it as having high trust. First, if trust in the charging station visited by the user is high, the user's trust-evaluation algorithm is executed. The payment error rate of the CS_i is used as a trust-evaluation item, as expressed in (1).

$$payment\_error\_rate\_CS_i = \frac{\Sigma_{i=1}^{N}(1-S_i)}{N} \quad (1)$$

The payment error rate of the charging station is used as a trust-evaluation item for the charging station, and the calculation method is as follows: First, find the sum of i datasets from 1 to N, S_i is the i-th payment status of the i-th CS and is 0 (abnormal) and S_i is 1 (normal). Calculate 1-S_i and in

Table 1. List of symbols

Symbol	Description
i	CS index
j	User index
CS_i	The i-th CS (i.e., evaluation target)
S_i	Payment error rate vector of CS_i
P_i	Charging-power rate vector of CS_i
U_j	The j-th EV user (i.e., evaluation target)
T_{ij}	Charging time vector of U_j for CS_i
P_{ij}	Charging-power rate vector of U_j for CS_i
S_{ij}	Payment error rate vector of U_j for CS_i
$\overline{T}_{ij}$	Average charging time of U_j for CS_i
$\overline{P}_{ij}$	Average charging-power rate of U_j for CS_i
$\overline{S}_{ij}$	Average payment error rate of U_j for CS_i

the case of payment errors, 1 can be obtained. The sum of the abnormal payment states for all datasets is then divided by the total number of datasets to calculate the average payment error rate of the CS. By comparing the payment error rate to a numerical threshold, user trust is evaluated only if it is below the threshold.

2) User trust-evaluation parameters

To evaluate user trust, P_{ij}, T_{ij} and S_{ij} are used. First, the user's charging frequency uses the charging date of charging station C_i to check the gap between the visit date and the next visit date, and calculates it as an average value. Next, we calculate the user's average payment error rate using (1). The calculation method for the user's average charging-power rate is shown in (2).

$$\overline{P}_{ij} = \frac{\Sigma_{j=1}^{N} P_{ij}}{N} \tag{2}$$

N refers to the total data size and P_{ij} refers to the j-th charging amount. The value calculated in this way is substituted into $\overline{P}_{ij}$, which means the average charge amount and the corresponding value is calculated with the weight value ω to determine whether it is located in the center:

① Subtract the weight ω value calculated on the left side from the average charge amount.

② Add the weight ω value calculated on the right side to the average charge amount.

③ Check whether the user's average charge amount $\overline{P}_{ij}$ satisfies this condition.

The calculation that satisfies the above conditions is as in (3).

$$\overline{P}_i - \omega \le \overline{P}_{ij} \le \overline{P}_i + \omega \tag{3}$$

The average charging-power rate was calculated using (2). In addition, the average charging-power rate of CS_i can be calculated by entering P_i into the element. If the average charging-power rate of U_j, which is the subject of trust evaluation, is within the allowable range of the average charge amount of CS_i, this indicates that the trust of U_j is high. If the charging station meets the trust-evaluation criteria outlined in the previous section and U_j satisfies the conditions of constant charging frequency, charging time, charging amount, and low-error payment, OTP authentication is performed. If any of these conditions are not met, the existing TLS authentication is used.

The proposed algorithm applies a differentiated authentication to EV users with specific charging patterns. The proposed algorithm replaces TLS authentication with OTP authentication, resulting in a reduction in the number of TLS authentication attempts, which decreases the overhead.

B. New ML-based Differential Authentication

The arbitrarily set threshold (i.e., 1.95), although a convenient starting point, revealed its limitations in providing an accurate evaluation of the trust of the user-charging pattern through our algorithm. In this section, our objective is to delve deeper into this issue by comparing and elaborating on the thresholds derived using various machine learning models. The models employed for this comparative analysis include linear regression, decision-tree regression, random forest regression, and k-nearest neighbors (k-NN) regression.

We used a dataset of EV charging data encompassing 50 users, 11,683 rows, and ACN-Data [15]. Each piece of data within the set provides valuable insights into the charging patterns and behaviors. The model was trained and tested to assess its predictive accuracy by comparing the set threshold with actual charging patterns. These experiments serve as a foundation for exploring the effectiveness and performance of various machine learning techniques in determining the threshold indicating trust in charging patterns. When we trained the model at the beginning of our study, we obtained results similar to those of the k-NN in Table 2.

Initially, we confirmed that it is difficult to set the predicted value using machine learning as the threshold value. This is because the amount of power, charging type, and user ID are used as input data to obtain the charging time as the output data, and each user has a different charging pattern. At the beginning of the study, the performance evaluation results were poor. However, the addition of charging duration improved the results. When conducting machine learning model training with a test size of 25-30%, it is possible to compare the performance of the four models. The decision-tree model was found to be the most suitable.

This is done by substituting the calculation result of the charging end date-charging start date, and the charging time prediction result is calculated. Therefore, the threshold calculation through machine learning training compares the average value for each item with the average value of the threshold. This is determined by the user characteristics and requires further study because it can be regular or irregular.

In the previous sections, we confirmed the previously proposed algorithm and explained the machine learning thresh-

Table 2. Charging time threshold performance results

Model	MSE	MAE	SMAPE	Process time
Linear Regression	2.428s	4.309s	5.590 %	0.031s
Decision Tree	2.010s	0.597s	0.036 %	0.044s
Random Forest	1.092s	0.451s	0.029 %	1.319s
k-NN	401.1s	8.907s	0.621 %	0.049s

old-setting method, which is a change from the existing numerical-based threshold-setting method. This section describes the improved differential authentication method. The problem with existing algorithms is the lack of numerical threshold-setting methods and trust-evaluation items. To solve this problem, we reviewed a recent study on the analysis of EV user-charging behavior using machine learning models. We used a suitable model to calculate the predicted threshold value from the user-charging data, which was then compared with the average user value.

In [16-18], decision-tree methods were shown to be the most effective in predicting EV user behavior. Random Forest [16] and Gradient Boosted Decision Tree (GBDT) methods, such as eXtreme Gradient Boosting (XGBoost) [17] and Light Gradient Boosting Machine (LGBM) [18], are tree-based methods used for EV charging behavior prediction. Among the models mentioned, the LGBM was faster than the GBDT. However, its application should consider the size of the EV charging data as it may overfit small-scale data.

This study evaluated trust indicators for both charging stations and users. The CS trust index was assessed using the CS payment error and return rates of electric vehicle users. If the station's trust is high, user trust is evaluated using the peak-hour visit rate, payment error rate, average EV charging amount, and average EV charging time. The values predicted by training the LGBM were averaged and compared.

Algorithm 1 Trust Level Evaluation Algorithm at CS_i

Input: Charging data set
Output: Trust level
Initialization:
i : index of charging station
j : index of electric vehicle user
$model \leftarrow$ LGBM

1: $\overline{T}_{ij} \leftarrow$ Average charging time of U_j
2: $\overline{P}_{ij} \leftarrow$ Average charging power rate of U_j
3: $\overline{S}_{ij} \leftarrow$ Average payment error rate of U_j
4: $\overline{T}_{ij}^{pred} \leftarrow$ Average charging time of U_j by prediction $model$
5: $\overline{P}_{ij}^{pred} \leftarrow$ Average charging power rate of U_j by prediction $model$
6: $\overline{S}_{ij}^{pred} \leftarrow$ Average payment error rate of U_j by prediction $model$
7: //After evaluating CS_i reliability, proceed with U_j trust level evaluation
8: **if** payment error rate of $CS_i <$ Avg payment error rate of all CS **&&** return rate of $CS_i >$ Avg return rate of all CS **then**
9: **if** peak hour visit rate of $U_i <$ Avg peak hour visit rate of CS_i **then**
10: **if** $\overline{T}_{ij} > \overline{T}_{ij}^{pred}$ **&&** $\overline{P}_{ij} > \overline{P}_{ij}^{pred}$ **&&** $\overline{S}_{ij} < \overline{S}_{ij}^{pred}$ **then**
11: //All elements in U_i greater than elements in $pred$
12: Trust_level_$U_j \leftarrow$ **high**
13: **else**
14: Trust_level_$U_j \leftarrow$ **low**
15: **end if**
16: **else**
17: Trust_level_$U_j \leftarrow$ **low**
18: **end if**
19: **else**
20: Trust_level_$CS_i \leftarrow$ **low**
21: **end if**

To implement the proposed differential authentication, we evaluated the trust of both the CS and user in the following steps.

- Step 1 (lines 1-6): The user trust is evaluated by comparing their evaluation items with the machine learning threshold value. To calculate the average value, (2) was used with only the corresponding elements changed. The average charging time of U_j, which is the target of the trust evaluation of the current charging station CS_i is calculated and substituted into $\overline{T}_{ij}$. Similarly, the average charging amount of U is calculated and substituted into $\overline{P}_{ij}$. The average error payment rate of U_j is calculated and substituted into $\overline{S}_{ij}$. Predict and calculate U_j's charging time, charging amount, and payment error rate using the machine learning model LGBM, and substitute the average values into $\overline{T}_{ij}^{pred}$ and $\overline{P}_{ij}^{pred}$. Finally, the average payment error rate of the model's predicted value is substituted into $\overline{S}_{ij}^{pred}$.
- Step 2 (lines 7-8): The assessment of charging station trust involves comparing payment error and user return rates. For CS_i to be deemed very reliable, its payment error rate must be lower than the average payment error rate of all the charging stations and its user return rate must be higher than the average return rate of all the charging stations. The user return rate is determined by dividing the number of visits by the total number of visits during each period. This calculation provides the average return rate for all users in each period. Reliable charging stations offer seamless services to EV users, encouraging them to return to the CS. In simpler terms, if both the average return rate of all charging stations and the return rate of the CS corresponding to CS_i are high, then the CS_i is considered to have high trust.
- Step 3 (lines 9-12): The user trust-evaluation item checks the peak-hour visit rate of CS_i. To calculate the peak-hour visit rate, increase the counter count when U_j visits during the time when the power consumption of the CS_i charging station is the highest and divide it by the total visit period. To ensure a high trust in U_j, the average user value entered in Step 1 is compared with the average threshold value set by machine learning. The average charging time and amount of charging U_j must be greater than the threshold values. Additionally, the U_j average payment error rate must be lower than the threshold value.

As a result, the charging station user must have a lower payment error rate, higher average charging-power rate, and higher average charging time than the prediction data generated by model learning. The peak-hour visit rate for the user must be lower than the average peak-hour visit rate for charging station users. Thresholds using machine learning learn from the user data in the model and predict each indi-

cator. These were then reprocessed into the user's average payment error rate, average charging-power rate, and average charging time. The LGBM [19] is much better than Gaussian Mixture Model-based models and similar sessions. This highlights the effectiveness of data-driven models in predicting the behaviors of EV users.

If the trust in the charging station visited by the user is evaluated as high, we perform a trust evaluation using the user's EV charging data. The results of the trust evaluation are expressed as high or low levels of user trust. This reduces the communication overhead that occurs during the authentication of existing TLS users. This is because, when user trust is rated high, the number of TLS authentications is reduced using a simple authentication method instead of the existing TLS authentication. In other words, in the case of a charging station with many highly trusted users, the number of TLS authentications is reduced, thereby reducing the overhead of the charging station. Although this approach is performed on a server, the trust-assessment cycle and time must be considered depending on the server environment.

III. PERFORMANCE EVALUATION

A. Simulation Tool & Settings

We conduct the simulation using Python version 3.9 in both a Windows environment and Ubuntu 20.04. First, we illustrate our simulation settings (Table 3), followed by simulation results and discussions to evaluate the obtained results.

Simulation results were obtained across various scenarios based on the findings. The second-scenario simulation results were replicated in 1,000 parallel instances using four processes to generate a busy waiting state for the CPU. The third simulation result included three sleep commands of 0.333s each to stop and restart the process.

Table 3. Simulation parameters

Parameters	Value/ Range
Simulation set count	1 set of 100 repeat for each load count
User authentication	Basic, TLS, OTP
CPU busy waiting (s)	Parallel execution repeat 1,000 times with 4 processes
Process sleep (s)	3 times for 0.333 seconds

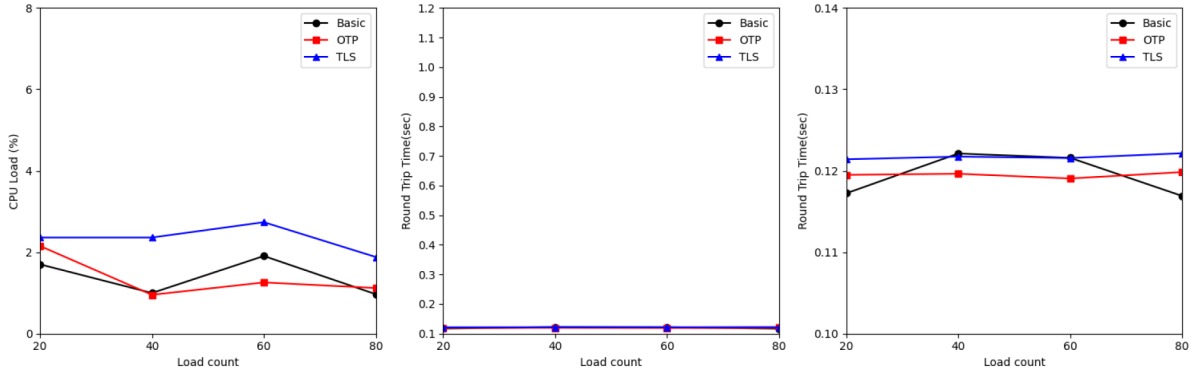
Table 4. Results by scenario

Scenario	Min (a)	Max (a)	Min (b)	Max (b)
Fig. 1 Basic	0.96 %	1.90 %	0.11s	0.12s
Fig. 1 OTP	0.95 %	2.15 %	0.11s	0.11s
Fig. 1 TLS	1.88 %	2.73 %	0.12s	0.12s
Fig. 2 Basic	2.84 %	5.56 %	0.52s	0.53s
Fig. 2 OTP	3.45 %	3.69 %	0.51s	0.53s
Fig. 2 TLS	4.19 %	6.6 %	0.87s	0.91s
Fig. 3 Basic	3.13 %	3.13 %	1.03s	1.03s
Fig. 3 OTP	3.71 %	4.32 %	1.03s	1.04s
Fig. 3 TLS	5.10 %	6.62 %	1.12s	1.14s

B. Analysis of Results

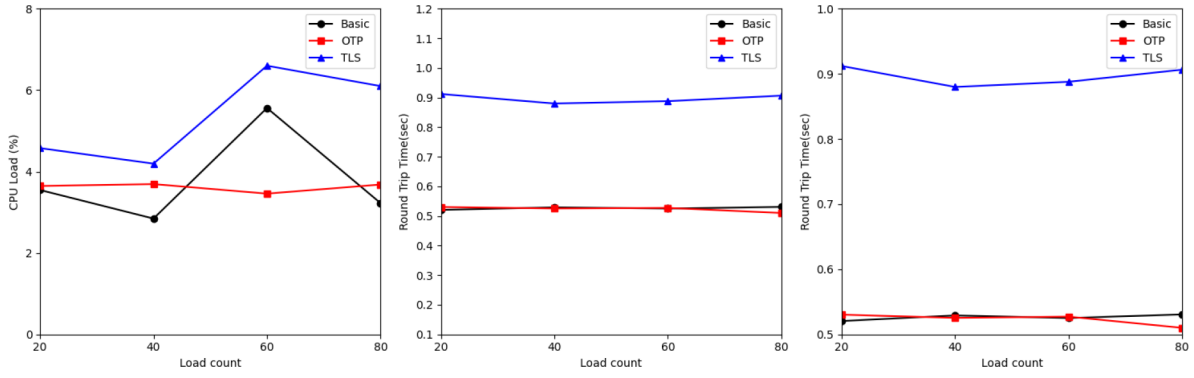
Figs. 1-3 show the performance ranking of Basic and OTP, followed by that of TLS. In Fig. 1, the CPU status for the three authentication methods can be observed in (a) without any scenarios. OTP authentication gradually stabilizes, whereas basic authentication exhibits a relatively fast processing speed. As a result, the CPU load increases slightly up to a load count of 60 on the x-axis of the graph and then decreases again. The basic authentication pattern is confirmed in (c) by a slight increase and subsequent decrease in the RTT. In contrast, the TLS completes 3-way handshaking sequentially, resulting in a slight increase in the load count to 60, followed by stabilization.

Fig. 2 illustrates a busy waiting-state scenario by assigning weights to the CPU during the authentication stage. Fig. 2



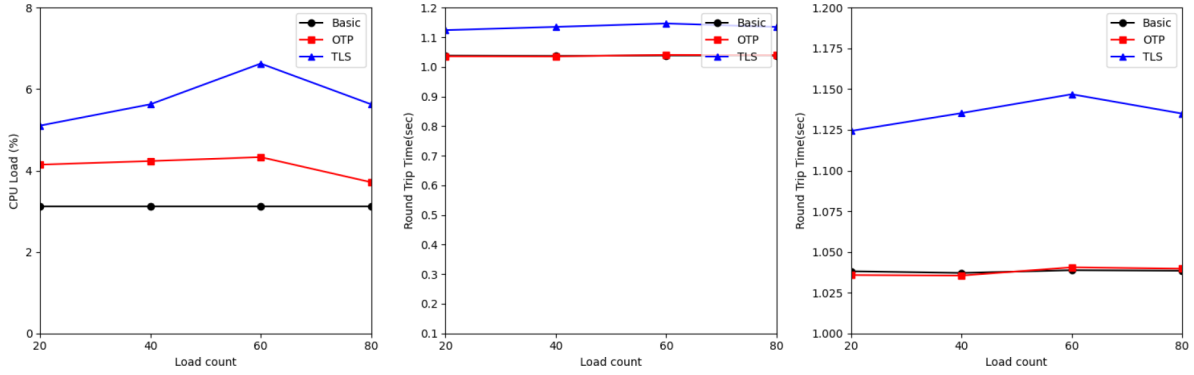
(a) Normal state CPU Load. (b) Normal state RTT. (c) Detail: Normal state RTT.

Fig. 1. Normal state: during user authentication.



(a) Busy waiting state CPU Load. (b) Busy waiting state RTT. (c) Detail: Busy waiting state RTT.

Fig. 2. Weighted busy for CPU: during user authentication.



(a) Process sleep state CPU Load. (b) Process sleep state RTT. (c) Detail: Process sleep state RTT.

Fig. 3. Process sleep 3 times for 0.333 sec: during user authentication.

(a) shows a pattern similar to that shown in Fig. 1(a), the CPU load remains stable at less than 4% during OTP authentication. This is further supported by (b) and (c), which show that RTT is not different from basic authentication. However, for TLS authentication, the RTT increased significantly to 0.9 compared to the normal state. During TLS authentication, a 3-way handshake is used between the server and client while exchanging messages. This imposes a significant burden on each recipient waiting for a response, resulting in a considerable increase in the round-trip time. In (b) and (c), OTP outperformed TLS by 37% in terms of RTT.

Fig. 3 illustrates a scenario in which the authentication process is interrupted three times for 0.333 s before restarting. As shown in Fig. 3(a), the CPU load for basic authentication remains stable at approximately 3%. Figs. 1 and 2 demonstrate that OTP authentication is more stable than other methods; however, the sleep state during the OTP encryption process is a disadvantage. However, both (b) and (c) exhibit RTT levels similar to those of basic authentication. Additionally, Fig. 3 shows that when the load count confirmed in Figs. 1 and 2 reaches 60, the increase in RTT for TLS authentication is significantly higher than that of the other authentication methods. This is evident in (c), the detailed screen of RTT, where TLS authentication in the scenarios depicted in Fig. 2(c) and Fig. 3(c) displays a highly unstable RTT compared to the other two authentication types. As shown in Figs. 1-3, when various charging patterns of EV perform TLS authentication, there is a significant difference in the actual server.

We evaluated user trust based on EV charging data and proposed an algorithm that replaces complex TLS authentication with simpler OTP authentication. As shown in Table 4, the proposed algorithm is used to replace highly trusted users with OTP authentication. In Fig. 2(c) RTT performance, calculated using the minimum value in Table 4, decreased by 0.36s from 0.87s to 0.51s, which indicates an improvement of 41.36%. If calculated using the maximum value in Table 4, it decreased by 0.38s from 0.91s to 0.53s, which is an improvement of up to 41.76%. It becomes more sensitive when users whose trust evaluations have been completed are processed simultaneously. Because TLS authentication is not performed on M users, who are highly trusted users, rather than performing TLS authentication on all N users, the performance can be improved by M-N.

In this paper, we explain the replacement of TLS authentication, which is performed in the transport layer, with OTP authentication, which is performed in the application layer. In other words, the communication overhead is also reduced by performing a user trust evaluation and then reducing the number of TLS authentications using a differential authentication method.

IV. CONCLUSION AND FUTURE WORK

In this study, we propose a new scheme to evaluate the trust of users and apply simpler authentication instead of TLS authentication if the trust is high. To evaluate trust in the CS, we add the user's return rate and the peak-hour visitation rate for user evaluation. We demonstrated that replacing TLS authentication with a simpler authentication method such as OTP authentication for high-trust users is more efficient when the server is busy waiting. In a future study, we plan to minimize the error range of the trust-evaluation items. We also plan to analyze alternative, simpler authentication methods more clearly.

ACKNOWLEDGMENTS

This work was supported by the Chungnam National University.

REFERENCES

[1] ISO, "15118-2: 2014-Road vehicles: Vehicle to grid communication interface part 2: Network and application protocol requirements," *ISO Standard.*, 2014.

[2] C. Shen, E. Nahum, H. Schulzrinne, and C. Wright, "The impact of TLS on SIP server performance," in *Proceeding of the Principles, Systems and Applications of IP Telecommunications*, Munich, Germany, pp. 59-70, 2010. DOI: 10.1145/1941530.1941540.

[3] P. Li, J. Su, and X. Wang, "iTLS: Lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy," *IEEE Internet Things Journal*, vol. 7, no. 8, pp. 6828-6841, 2020. DOI: 10.1109/JIOT.2020.2988126.

[4] K. Tange, S. Modersheim, A. Lalos, X. Fafoutis, and N. Dragoni, "rTLS: Secure and efficient TLS session resumption for the Internet of Things," *Sensors*, vol. 21, no. 19, pp. 6524, 2021. DOI: 10.3390/s21196524.

[5] B. Lim and K. Kim, "Differential authentication methods based on electric vehicle charging patterns," in *Proceeding of the 2023 Korea Internet and Information Society Spring Conference Papers,* Gwanggyo, Korea, pp. 89-90, 2023.

[6] D. Hardt, The OAuth 2.0 authorization framework, Internet Engineering Task Force [Internet], Available: https://www.rfc-editor.org/rfc/rfc6749.

[7] P. B. Babu, A. G. Reddy, B. Palaniswamy, and S. K. Kommuri, "EV-Auth: Lightweight authentication protocol suite for dynamic charging system of electric vehicles with seamless handover," in *Proceeding of the IEEE Transactions on Intelligent Vehicles,* vol. 7, no. 3, pp. 734-747, 2022. DOI: 10.1109/TIV.2022.3153658.

[8] J. Helmus, M. Lees, and R. Hoed, "A data driven typology of electric vehicle user types and charging sessions," *Transportation Research Part C: Emerging Technologies*, vol. 115, pp. 102637, 2020. DOI: 10.1016/j.trc.2020.102637.

[9] J. Y. Park and C. S. Kim, "Charging pattern of electric vehicle user and affecting factors: latent class analysis approach," *The Transactions of the Korean Institute of Electrical Engineers*, vol. 71, no. 11, pp. 1639-1645, 2022. DOI: 10.5370/KIEE.2022.71.11.1639.

[10] J. H. Lee, D. Chakraborty, S. J. Hardman, and G. Tal, "Exploring electric vehicle charging patterns: Mixed usage of charging infrastructure," *Transportation Research Part D: Transport and Environment*, vol. 79, pp. 102249, 2020. DOI: 10.1016/j.trd.2020.102249.

[11] S. Baghali, S. Hasan, and Z. Guo. "Analyzing the travel and charging behavior of electric vehicles a data-driven approach," in *Proceeding of the IEEE Kansas Power and Energy Conference*, Manhattan, USA, pp. 1-5, 2021. DOI: 10.1109/KPEC51835.2021.9446240.

[12] T. Mazhar, R. N. Asif, M. A. Malik, M. A. Nadeem, I. Haq, M. Iqbal, M. Kamran, and S. Ashraf, "Electric vehicle charging system in the smart grid using different machine learning methods," *Sustainability*, vol. 15, no. 3, pp. 2603, 2023. DOI: 10.3390/su15032603.

[13] S. Shahriar, A. R. Al-Ali, A. H. Osman, S. Dhou, and M. Nijim, "Machine learning approaches for EV charging behavior: A review," *IEEE Access*, vol. 8, pp. 168980-168993, 2020. DOI: 10.1109/ACCESS.2020.3023388.

[14] Y. W. Chung, B. Khaki, T. Li, C. Chu, and R. Gadh, "Ensemble machine learning-based algorithm for electric vehicle user behavior prediction," *Applied Energy*, vol. 254, pp. 113732, 2019. DOI: 10.1016/j.apenergy.2019.113732.

[15] Z. J. Lee, T. Li, and S. H. Low, "ACN-data: Analysis and applications of an open EV charging dataset," in *Proceeding of the tenth ACM international conference on future energy systems*, Phoenix, USA pp. 139-149, 2019. DOI: 10.1145/3307772.3328313.

[16] Y. Lu, Y. Li, D. Xie, E. Wei, X. Bao, H. Chen, and X. Zhong, "The application of improved random forest algorithm on the prediction of electric vehicle charging load," *Energies*, vol. 11, no. 11, 2018. DOI: 10.3390/en11113207.

[17] O. Frendo, N. Gaertner, and H. Stuckenschmidt, "Improving smart charging prioritization by predicting electric vehicle departure time," in *proceeding of the IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 10, pp. 6646-6653, 2021. DOI: 10.1109/TITS.2020.2988648.

[18] Y. Chen, K. S. S. Alamin, D. J. Pagliari, S. Vinco, E. Macii, and M. Poncino, "Electric vehicles plug-in duration forecasting using machine learning for battery optimization," *Energies*, vol. 13, no. 16, pp. 4208, 2020. DOI: 10.3390/en13164208.

[19] E. Genov, C. D. Cauwer, G. V. Kriekinge, T. Coorsemans, and M. Messagie, "Forecasting flexibility of charging of electric vehicles: tree and cluster-based methods," *Applied Energy*, vol. 353, pp. 121969, 2024. DOI: 10.1016/j.apenergy.2023.121969.

Byung-Hyun Lim

He is currently working toward M.S degree at Department of Computer Science and Engineering, Chungnam National University. His research interests are EV charging pattern, IoT security and Machine Learning.

Ismatov Akobir

He is currently working toward M.S degree at Department of Computer Science and Engineering, Chungnam National University. His research interests are AI for Network and IoT security.

Ki-Il Kim

He received the M.S. and Ph.D. degrees in computer science from the Chungnam National University, received the M.S. and Ph.D. degrees in computer science from Chungnam National University, Daejeon, South Korea, in 2002 and 2005, respectively. He has been with the Department of Informatics, Gyeongsang National University since 2006. He is currently affiliated with the Department of Computer Science and Engineering, Chungnam National University. His current research interests include machine learning for networks, wireless/mobile networks, fog computing, MANET, QoS for wireless, and wireless sensor networks.