IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 59, No. 5, May, 2026, pp. 1357-1362
Journal homepage: http://iieta.org/journals/jesa

Enhance the Communication Network of Electric Vehicles Applications Using Fog Computing

Firas S. Alsharbaty*, Azzam Adnan Mohammed, Ali H. Saeed, Mohammad Tariq Yaseen

Department of Communications and Intelligent Digital Systems Engineering, College of Engineering, University of Mosul, Mosul 41002, Iraq

Corresponding Author Email: alsharbaty@uomosul.edu.iq

https://doi.org/10.18280/jesa.590514

Received: 3 March 2026
Revised: 11 May 2026
Accepted: 21 May 2026
Available online: 31 May 2026

Keywords:
security algorithm, communications network, Electric Vehicle Supply Equipment, fog computing, security

ABSTRACT

The increment of Electric Vehicle Supply Equipment (EVSE) in the world witnesses an exponential rise due to the issues that relate to the traditional energy sources. However, the current unprecedented rise in EVSE has been accompanied by a series of problems in the power grid. The control center of EVSE plays the main role in monitoring and controlling the various activities of such infrastructure. The communications network of the EVSE infrastructure is the cornerstone that transfers the data from the different parts of the EVSE infrastructure into/from control center. This work suggests an enhanced, robust and secure communications network to handle the requirements of the different applications of EVSE by fog computing and the CHACHA20-POLY1305 security algorithm. Three different scenarios are offered in this work. The results of the third scenario that was enhanced using fog computing indicate that the maximum end-to-end delay is less than 0.11 msec and the received data reliability is more than 99.99%. Moreover, the data of the third scenario is secured in terms of confidentiality and integrity using a lightweight algorithm.

1. INTRODUCTION

Electric Vehicle Supply Equipment (EVSE) is one of the landmarks of the transition to clean and renewable energy in the current era [1]. The main function of EVSEs relates to delivering the electric power to the electric vehicles (EV) battery from the smart power grid [2]. Hence, it converts the alternating current of the source into DC current to charge the battery of an EV battery. The role of EVSEs is essential and may have a very significant impact on the stability of the electrical power system, in particular with the widespread use of charging stations [3]. In this context, it is vital to monitor and control the activities of such infrastructure. The control center of EV infrastructure is the entity that receives data from EVSEs and organizes the control and monitoring process [4]. If there is a fault or the power grid suffers from instability, then the control center could make a decision to isolate some of the electrical power lines or power off some of the EVSE stations [5]. This process requires a powerful communications network that could assimilate the various data from the different parts of EVSE infrastructure. Moreover, the candidate communications network of EVSE's infrastructure should guarantee two crucial points. The EVSE includes many services and applications, each one of them has specific requirements. Consequently, the communications network should meet the requirements of such applications. The second point is the capability of communications networks to scalability of EVSEs that leads to a significant rise in the volume of data transferred within the communications network [6, 7]. Another critical point that may form a burden on the communications network is how to secure the transferred data of this vital infrastructure [8]. As a result, another overhead that should be assimilated by the communication networks [9].

Most previous related works regarding the communications network of EVSE infrastructure addressed these issues unilaterally. In terms of the communications network, Kilic [10] proposed a method for reliable communication between EVs and charging stations with respect to the ISO 15118 protocol. Zhang et al. [11] handled one application of EVSE; hence, the authors established a communication system between EVs and charging piles based on power line communication (PLC). The authors exploited transport layer security to protect the data of the International Organization for Standardization's ISO 15118 standard communication between EVs and EVSE after introducing the communication requirements of this standard. Lee [12] targeted the EV charging process and proposed impulse noise cancelation for scooter charging using magnetic in-band communication. Oumaima et al. [13] employed bi-directional communication between EVs and the charging system using the ISO 15118 communication protocol. The authors integrated the mentioned protocol with the electric vehicle communication controller and the supply equipment communication controller. Hence, they established the communication system between EVs and dedicated charging piles based on PLC. Sanjay Moulik et al. [14] introduced a scalable solution for real-time EV routing applications according to Vehicle-to-

Grid incentives. It is noted that previous related work either addressed a specific communication standard, dealt with the intranet of EV, or handled special types of applications in terms of communication networks.

On the other hand, the research [15] proposed a transfer learning framework for cyber-physical attack detection in EV infrastructure to improve both accuracy and scalability. Georgios et al. [16] introduced the concept of blockchain to secure the data of the EV communications network. Mohanty et al. [17] introduced a unitary framework that merges a federated multi-task transformer with a digital twin that is enhanced by reinforcement learning to perform privacy-preserving EV scheduling. Porter et al. [18] developed ISO 15118–20 EV protocol for charging systems. It is clear that previous literature dealt with the security issues without enhancing the performance of such networks. To fill the research gap of the previous related works, this work aims to propose an enhanced and secure communications network for EVSE infrastructure. This work suggests fog computing to improve the performance of the proposed communications network and secure the suggested network using CHACHA20-POLY1305 security algorithm at the application layer.

2. FOG COMPUTING

In general, there are two main approaches relating to processing the data. The first one is in a centralized fashion; hence the data is sent to the data center for the process [19]. The second kind of data processing is a decentralized method. In such a type, the data never waits for a single point for processing. Fog and edge computing are examples of this type. In edge computing, the place of processing nears the source of the data with poor and simple capability regarding the processing. Whilst fog computing is another type of decentralized computing [20]. In this type, the place of computing is located between the source of the data and the destination. The capabilities of fog computing are stronger than edge computing in addition to the capability of assimilation of more data [21].

However, fog computing mitigates the load on the public network that represents the backbone of the global network. Furthermore, it may enhance the privacy of the data if it is combined with suitable procedures to protect the data, see Figure 1 [22].

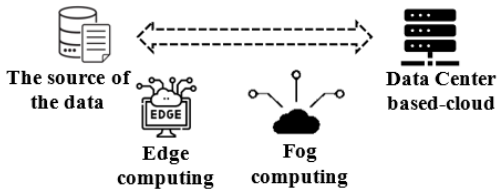

Figure 1. Centralized and decentralized computing

3. CHACHA20-POLY1305

CHACHA20-POLY1305 is a method to protect the confidentiality and the integrity of the data [23]. This security mechanism requires two phases. On the one hand, the first phase includes the CHACHA20 algorithm, hence this algorithm serves as a lightweight stream cipher. The main function of CHACHA20 is encryption. However, it relies on straightforward arithmetic process to generate a keystream (256 bits) [24]. Such simple algorithm could be implemented by software in an efficient way without accelerated hardware, which represents a privilege compared to other algorithms that require acceleration in terms of hardware [25]. On the other hand, the second phase is the algorithm of POLY1305 that represents a code for message authentication. Such algorithm employs to verify the data [26].

4. METHODS AND MATERIALS

4.1 Model assumptions

The adopted model addressing a typical case includes ten EVSEs on a site to charge the EV cars. Each EVSE charges an EV at a nominal time, during this process, the EVSE sends various signals for monitoring and control to the control center. These signals describe the charging process between EV and EVSE, including the current, voltage, frequency, power, status of EV battery, in addition to the signals that relate to protection purposes such as opening and closing the circuit breaker to protect the EVSE [27]. Table 1 describes the signals that are sent from EVSE to the control center in addition to the model assumptions and the main assumptions of the model. Figure 2 explains the layout of the adopted model.

Table 1. Model assumptions

Item	Description
No. of Electric Vehicle Supply Equipment (EVSE)	10
Local network cable	Fast ethernet
Backbone network cable	Fiber optic cable
No. of switches	2
No. of gateway routers	2
EVSE load	Full
Data of the Signals (Bits/sec)	
Current, Voltage	Each one is 5.76 k
Frequency	160
Power	80
Status	16
Circuit breaker	128
Protection	5.12 k
General Status of EVSE	32

In terms of the communications network, each EVSE is connected to the switch of the local site via fast ethernet cable (> 100Mbps). The local switch connects to the public network via a gateway router. EVSE sends the data to the control center through the backbone network via Fiber optic cable (> 1 Gbps). This work assumes that all EVSEs send the data to the control center simultaneously to represent the full load (worst case). It is worth to mention this work employs Riverbed modeler to model the communication network and collect the data, where the simulation time is 10 minutes.

4.2 Threats model

This section aims to discuss the threat model of the adopted system. In terms of cybersecurity, the vulnerabilities of the proposed communication network that serves EVSE can be divided into three parts: confidentiality, integrity, and availability [28]. In the industrial system, the integrity of the

data that is sent from the sender to the receiver is very critical because such data represents the cyber mirror of the physical system and any manipulation in the integrity of the data may lead to a misunderstanding of the suitable actions. As a consequence, the system may break down severely and may break the availability of the system. In this context, any attacker may exploit the weakness of the system at the level of application layer to modify the data of current, voltage, power, status, or protection to intentionally cause serious harm [29]. The current work focuses on the integrity of the system.

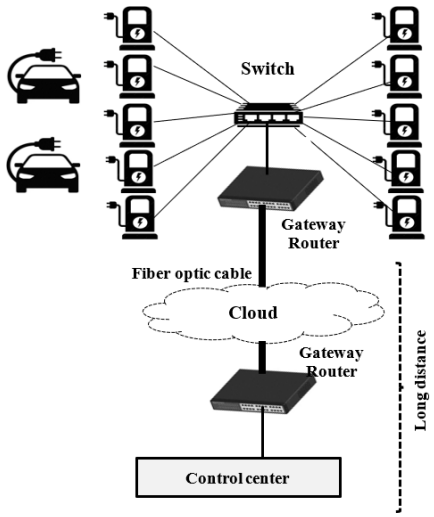

Figure 2. Adopted model architecture layout

4.3 Adopted scenarios

This work introduces three different scenarios to the adopted model.

4.3.1 First scenario

Heavy load based on cloud scenario (S1): In this scenario, each EVSE transmitter sends the data of current, voltage, power, status, circuit breaker, protection, etc., to the control center via a public network, where all EVSE send the data at the same time as the worst case (Full load).

4.3.2 Second scenario

Network based on fog computing (S2): this scenario offers the concept of fog computing to process the data instead of sending the data to the control center directly. The fog computing processes the data in real time, then sends the information to the control center lightly. This mechanism mitigates the data load on the public network, see Figure 3. In this scenario, the middle center of fog computing receives the mentioned data in Table 1 (the data of the EVSE site). Then, the fog computing machine processes the data simultaneously and sends a data log to the control center, including the main information of the received data. For instance, the suggested specifications of fog processing machine are ARM Cortex-M4, 100 MHz. These specifications represent an available solution with a suitable cost with respect to the adopted assumptions [23].

4.3.3 Third scenario

Secured network scenario (S3): This scenario is similar to the second scenario in addition to security level using a security algorithm that mixes between CHACHA20 and poly1305 to protect the data at the level of application layer. The adopted algorithm consists of nonce that represents unique identification, padding, and tags for the purpose of authentication [25]. Such an algorithm is lightweight, and it is suitable to implement in terms of software. The algorithm will add a slight overhead in terms of data and a little delay for processing at the application layer. For instance, the overhead delay of the CHACHA20 and poly1305 per every 1400 bytes is about 400 µsec based on the adopted specifications of the machine of fog computing [23].

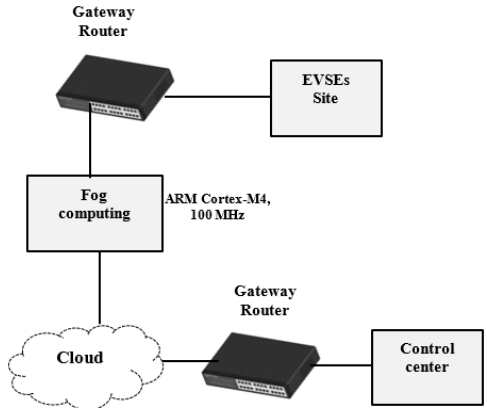

Figure 3. The second scenario, fog computing

5. RESULTS AND DISCUSSION

This section explains the feasibility of the suggested communications network in terms of delay and traffic metrics. In the context of delay, this work states two types of delay, the delay at the level of the datalink layer (ethernet) and the delay of End-to-End delay at the application layer. On the other side, the adopted traffic is the traffic sent and the traffic received. However, the suggested communications network is successful in handling the requirements of the EVSE applications in cases where the traffic sent is equal or very near to the traffic received and the threshold value of delay should be less than or equal to the requirements of the hard real time protection application [28].

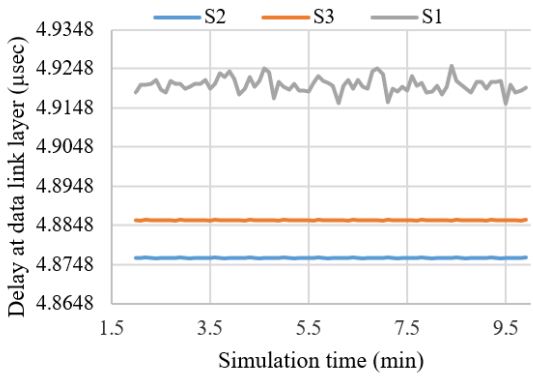

Figure 4. The delay at the data link layer

Figure 4 demonstrates the behavior of the data link layer delay (ethernet delay) with the simulation time (ten minutes). This figure explains the delay from the data link layer at the sender to the data link layer at the receiver. Such delay describes the delay of the wired network for the three scenarios. It is noted the delay of the first scenario (without engaging the fog computing) is bigger than other scenarios due

to the two main factors. The first is the long physical path of the whole data between the senders of the data and the destination (control center). The second is the expected congestion at the cloud network hence the public network is common among many individual networks. While employing the fog computing will reduce the size of transferred data between the main source of the data and the control center. In terms of the third scenario, it is clear that the delay of S3 is bigger than that of S2. This is related to the overhead data of CHACHA20-POLY1305 algorithm.

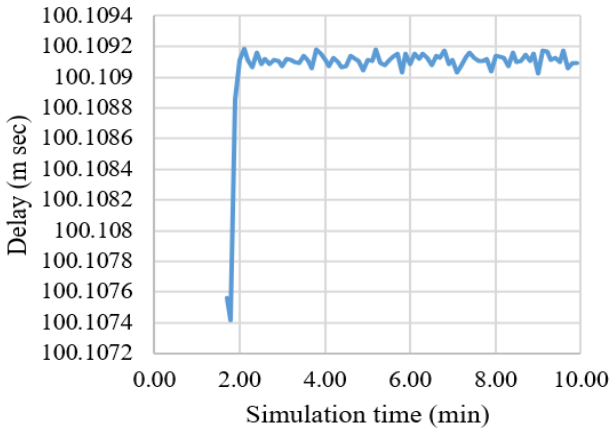

Figure 5. End-to-end delay of S1

Figure 5 addresses another type of delay. End-to-end delay is the delay from the application layer at the sender to the application layer at the destination. This delay describes the behavior of the applications themselves. It is worth to mentioning that Figure 4 combines all adopted scenarios for the case of data link layer delay. However, in the case of End-to-end delay (at the application layer), there is a clear difference between S1 on one hand, with S2 and S3 on the other hand in terms of delay values. For the purpose of explanation, the End-to-End delay of S1 is split into one figure, while the End-to-End delay of S2 and S3 is explained in another figure.

Regarding Figure 5, it is clear that the delay fluctuates between 100.1092 msec to 100.109 msec. In other words, it exceeds the level of 100 msec. Such delay breaks the delay requirements of a specific type of application, in particular the protection application where the hard real-time delay should never exceed 3 msec [29]. Hence, the protection application is responsible for addressing the appropriate action if there is a fault current that may return to the charging station in some cases and will lead to physical damage. Therefore, the protection application (in this case a circuit breaker) should isolate the source of the fault current in 3 msec. Consequently, Figure 5 illustrates that the first scenario fails to handle the requirements of all adopted applications of EVSE in terms of delay.

Figure 6 demonstrates the End-to-End delay of the second (S2) and third scenarios (S3). This figure explains a great improvement in terms of the delay at the level of the application layer compared to the first scenario. In other words, S2 and S3 could meet the requirements of all adopted applications in particular the protection application where the offered delay by these scenarios is less than 3 msec.

It noted that the End-to-End delay of S3 is bigger than S2 by about (0.0126 ms) due to the overhead data of the security algorithm. The main significance of the third scenario is the capability of providing a robust level of security without breaking the requirements of applications in terms of End-to-End delay.

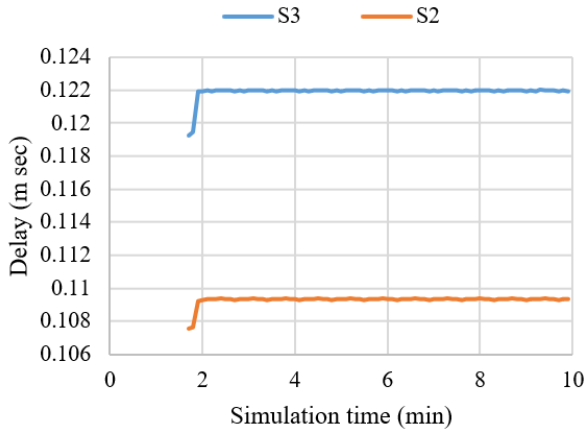

Figure 6. End-to-end delay of S2 and S3 scenarios

Traffic sent and traffic received with the simulation time is illustrated in Figure 7 regarding the first scenario. There is data loss in this scenario of about 1k byte/sec, which means the received data reliability is about 95%.

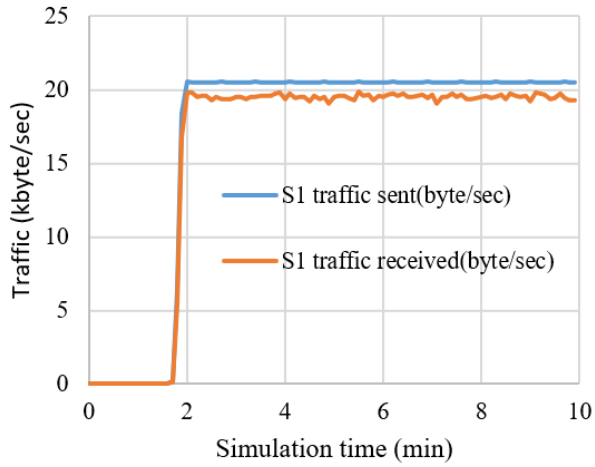

Figure 7. The traffic of the first scenario

Figures 8 and 9 explain the traffic sent and traffic received in the second and third scenarios. The significance of the mentioned figures relates to explaining that suggested scenarios (S2 and S3) never break the received data reliability of the adopted applications of EVSE. Moreover, the suggested scenarios could improve the received data reliability up to 99.99%, while the received data reliability of S1 is about 95%.

It is obvious that the traffic sent is equal to the traffic received, which means the received data reliability is more than 99.99%. Hence, the fog computing could compensate the issue of the received data reliability in the first scenario because the fog computing could process the data in the middle of the path between the source and destination rather than sending the data to the control center for processing. In summarize, the suggested communications network of the third scenario could handle the requirements of EVSE applications in addition to secure the transferred data at the application layer.

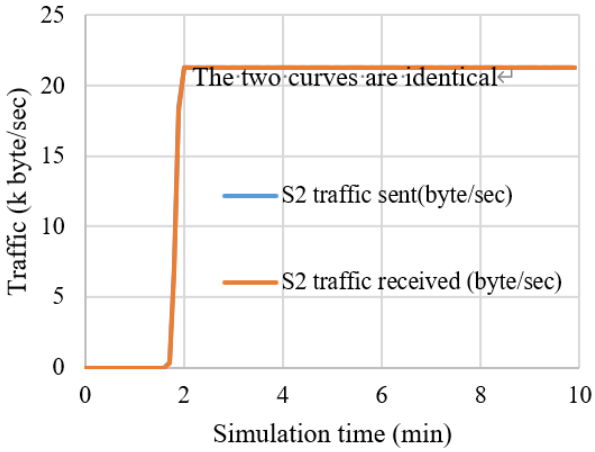

Figure 8. Traffic of the second scenario

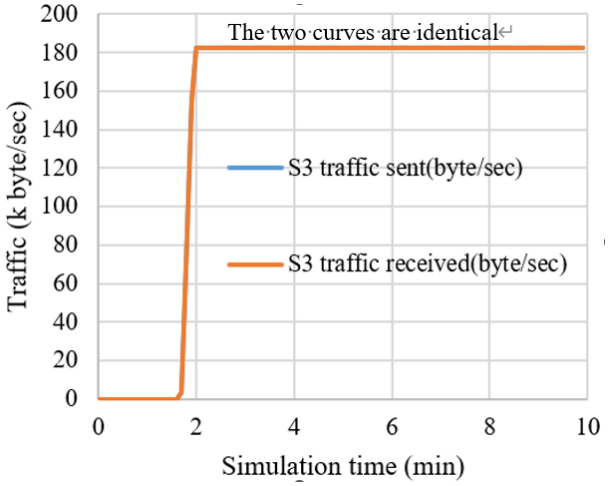

Figure 9. Traffic of the third scenario

6. FEASIBILITY AND POTENTIAL ISSUES

This section discusses the limitations and potential issues regarding this work that aims to offer a secure and enhance communication network to serve EVSE infrastructure.

Firstly, this work discusses a simulation model hence the practical implementation will face real challenges regarding the interoperability issues in the proposed model. In terms of the second scenario, although fog computing could enhance the performance of the adopted model from the delay and reliability points of view. However, it suffers from the physical capabilities in the case of expansion hence, the adopted model serves ten charging stations. Therefore, the expansion phase requires developing the capability of fog computing machine or involving other machines, which leads to an increase in the cost of the model. Furthermore, introducing one machine as a fog computing solution may lead to the issue of one point failure.

On the other hand, employing the algorithms of CHACHA20 and poly1305 offers an attractive choice to protect the data of the adopted model (third scenario) because the proposed model focuses on the application layer threats, but cannot submit one solution to all issues that relate to the threats model of the whole system because this algorithm could protect the application layer partially. A complete countermeasure against EVSE threats model and vulnerabilities may require five-layer hybrid defense.

7. CONCLUSIONS

This research paper offered three scenarios of communication networks to capture the requirements of EVSE infrastructure. The first scenario fails to meet the requirements of EVSE applications in terms of End-to-End delay and received data reliability; hence, the delay exceeds 100 msec while there are 1k bytes as lost bytes in the network because of the congestion at the backbone network. The suggested communications network using fog computing could assimilate the data of EVSE applications from end-to-end delay and received data reliability points of view; hence, the delay is less than 0.123m sec and there is no packet loss. In addition, the employed security algorithm that is used to secure the data of the third scenarios does not break the requirements of EVSE applications in terms of End-to-End delay and packet loss. The future work will concentrate on some points such as involving the mobility of the system, heavy load, expansion, and dealing with deep countermeasures against the issues of cybersecurity.

ACKNOWLEDGMENT

The authors are very grateful to the University of Mosul / College of Engineering for the facilities provided, which helped to improve the quality of this work.

REFERENCES

[1] Tilly, N., Yigitcanlar, T., Degirmenci, K., He, S.Y., Loo, B., Paz, A. (2025). Electric vehicles and sustainable development goals: A multi-level governance analysis. Transport Policy, 171: 239-255. https://doi.org/10.1016/j.tranpol.2025.06.008

[2] Ahmed, A., Shuvo, A.A., Shah, R., Islam, M.R. (2026). Impact of EV charging scheduling and demand side management on overall load profile: An Australian case study. Electric Power Systems Research, 257: 112948. https://doi.org/10.1016/j.epsr.2026.112948

[3] Li, S. (2025). Transportation justice for sustainable cities: An equity review of EV charging infrastructure in China. Sustainable Cities and Society: Advances, 1(1): 100010. https://doi.org/10.1016/j.scsadv.2025.100010

[4] Cordova-Cruzatty, A.C., King, D.A., Kuby, M., Parker, N. (2024). Experiences and perceptions of multi-family housing property managers about electric vehicle charging provision. Transportation Research Interdisciplinary Perspectives, 28: 101263. https://doi.org/10.1016/j.trip.2024.101263

[5] Ghosh, S., Roy, T. (2025). Detection and isolation of battery charging cyberattacks via Koopman operator. Applied Energy, 401: 126695. https://doi.org/10.1016/j.apenergy.2025.126695

[6] Tilly, N., Yigitcanlar, T., Degirmenci, K., Paz, A. (2025). Systems-based approach to public electric vehicle supply equipment expansion: An international policy analysis. Sustainable Cities and Society, 131: 106739. https://doi.org/10.1016/j.scs.2025.106739

[7] Gopinathan, N., Shanmugam, P.K. (2026). Adaptive congestion management for EV charging in synchrophasor enabled ADNs: A decentralised distributed approach with concordance framework.

Energy Reports, 15: 109238. https://doi.org/10.1016/j.egyr.2026.109238
[8] Kilic, A. (2025). A quantitative framework for physical cybersecurity in public EVSE systems. Computers & Security, 159: 104685. https://doi.org/10.1016/j.cose.2025.104685
[9] Mitikiri, S.B., Babu, K.V.S.M., Dwivedi, D., Srinivas, V.L., Chakraborty, P., Yemula, P.K., Pal, M. (2025). Cyber–physical security in EV charging infrastructure: Components, vulnerabilities, and defense strategies. Sustainable Energy Technologies and Assessments, 81: 104435. https://doi.org/10.1016/j.seta.2025.104435
[10] Kilic, A. (2024). TLS-handshake for Plug and Charge in vehicular communications. Computer Networks, 243: 110281. https://doi.org/10.1016/j.comnet.2024.110281
[11] Zhang, L., Chi, S., Hu, Q., Chen, K., Lyu, L. (2020). Reliability oriented modeling and analysis of PLC for EVs to charging piles communication system based on IPA-SAMP impulse noise cancelation. IEEE Access, 8: 4605-4614. https://doi.org/10.1109/ACCESS.2019.2961241
[12] Lee, E.S. (2023). Frequency-modulation-based IPT with magnetic communication for EV wireless charging. IEEE Transactions on Industrial Electronics, 70(2): 1398-1408. https://doi.org/10.1109/TIE.2022.3158027
[13] Oumaima, B., Hassan, E.F., El Jeilani, S., Halima, H., Abdelaziz, K. (2024). Integration of communication between EV and EVSE based on ISO 15118 with an OBD-II system. In Automatic Control and Emerging Technologies, Kenitra, Morocco, pp. 581-588. https://doi.org/10.1007/978-981-97-0126-1_51
[14] Moulik, S., Sindhu, K., Sarma, R. (2026). EV-GREEN: Electric vehicle routing with GreenZone prioritization and vehicle-to-grid incentive integration. Computing, 108(2): 27. https://doi.org/10.1007/s00607-026-01625-0
[15] Almadhor, A., Alsubai, S., Bouazzi, I., Karovic, V., Davidekova, M., Al Hejaili, A., Sampedro, G.A. (2025). Transfer learning for securing electric vehicle charging infrastructure from cyber-physical attacks. Scientific Reports, 15(1): 9331. https://doi.org/10.1038/s41598-025-93135-w
[16] Germanos, G., Lekidis, A., Brotsis, S., Kolokotronis, N. (2026). Blockchain architectures for enhancing EV infrastructure security: A unified framework for addressing sophisticated cyber-attacks. Future Generation Computer Systems, 182: 108426. https://doi.org/10.1016/j.future.2026.108426
[17] Mohanty, P.K., Jena, P., Padhy, N.P. (2026). A federated transformer-based framework for uncertainty-aware and privacy-preserving EV scheduling with digital twin reinforcement learning. Electric Power Systems Research, 258: 113021. https://doi.org/10.1016/j.epsr.2026.113021
[18] Porter, R., Biglari-Abhari, M., Tan, B., Thrimawithana, D. (2025). Enhancing security in the ISO 15118–20 EV charging system. Green Energy and Intelligent Transportation, 4(6): 100262. https://doi.org/10.1016/j.geits.2025.100262
[19] Sun, P., Yu, H., Ren, Y. (2026). Hardware technology evolution for privacy preservation in pervasive cloud computing: A comprehensive review. Neurocomputing, 669: 132544. https://doi.org/10.1016/j.neucom.2025.132544
[20] Cui, Z., Zhang, X., Zhou, S. (2026). Enhancing network monitoring in IoT with an energy-efficient collaborative framework using edge computing and federated learning. Expert Systems with Applications, 318: 132034. https://doi.org/10.1016/j.eswa.2026.132034
[21] Martínez-Sala, A.S., Hernando-Cánovas, L., Sánchez-Aarnoutse, J.C., Alcaraz, J.J. (2025). Resource-efficient fog computing vision system for occupancy monitoring: A real-world deployment in university libraries. Internet of Things, 34: 101748. https://doi.org/10.1016/j.iot.2025.101748
[22] Banik, M., Kumar, S. (2025). Fog computing based public key encryption with multi-keyword search for Internet of vehicles. Journal of Parallel and Distributed Computing, 204: 105131. https://doi.org/10.1016/j.jpdc.2025.105131
[23] Bühler, H., Walz, A., Sikora, A. (2022). Benchmarking of symmetric cryptographic algorithms on a deeply embedded system. IFAC-PapersOnLine, 55(4): 266-271. https://doi.org/10.1016/j.ifacol.2022.06.044
[24] McLaren, P., Buchanan, W.J., Russell, G., Tan, Z. (2019). Deriving CHACHA20 key streams from targeted memory analysis. Journal of Information Security and Applications, 48: 102372. https://doi.org/10.1016/j.jisa.2019.102372
[25] Sohn, E., Lee, S., Kim, S., Sohn, K., Kumar, M., Son, Y. (2025). Phase-level analysis and forecasting of system resources in edge device cryptographic algorithms. CMES-Computer Modeling in Engineering and Sciences, 145(2), 2761-2785. https://doi.org/10.32604/cmes.2025.070888
[26] Wenhua, Z., Hasan, M.K., Jailani, N.B., Islam, S., Safie, N., Albarakati, H.M., Khan, M.A. (2024). A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications. Computers in Human Behavior, 153: 108134. https://doi.org/10.1016/j.chb.2024.108134
[27] Ahmed, M.A., Kim, Y.C. (2017). Performance analysis of communication networks for EV charging stations in residential grid. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Miami, USA, pp. 63-70. https://doi.org/10.1145/3132340.3132352
[28] Alsharbaty, F., Ali, Q. (2022). An enhanced industrial wireless communication network for hard real time performance substation automation purposes. Al-Rafidain Engineering Journal, 27(2): 216-226. https://rengj.uomosul.edu.iq/index.php/rengj/article/view/31071.
[29] Alsharbaty, F., Ali, Q. (2023). A cybersecurity model for the enhancement of wimax-based wirless communications infrastructure to serve smart grid applications. International Journal of Smart Grid, 7(1): 16-22. https://doi.org/10.20508/ijsmartgrid.v7i1.270.g256