An Efficient Physically Unclonable Function based Authentication Scheme for V2G Network

Giriraj Sharma
Dept. of Electronics & communication
Malaviya National Institute of Technology
Jaipur, India
2019rec9564@mnit.ac.in

Amit M. Joshi
Dept. of Electronics & communication
Malaviya National Institute of Technology
Jaipur, India
amjoshi.ece@mnit.ac.in

Saraju P. Mohanty
Dept. of comp science & Engg
University of North Texas
Texas, USA
Saraju.Mohanty@unt.edu

Abstract- With the advancement of ICT, the Electrical vehicles (EVs) are connected to the smart grid and this type of network known as Vehicle to Grid (V2G). During the Energy trading process, EV consumers also receives an economic benefit where they buy energy at low cost during slack hours and sell same to grid during higher traffic. However, the V2G network faces various security challenges like hardware security, integrity, identity preservation, mutual authentication, etc. Since EVs and CSs (charging stations) are generally unmanned hence physical security is also an important concern. In this paper, we proposed a secure, lightweight, and hardware-based key agreement scheme using Physical Unclonable Function (PUF). The proposed scheme uses the PUF concept to perform mutual authentication (MA) among EV, CS, and the GS. The formal security analysis has been performed using AVISPA tool. Further, the performance evaluation results show that overhead costs in communication and computation are less compared to the existing schemes.

***Index Terms*—Challenge Response Pair; Hardware Security; Smart Grid; Mutual Authentication; lightweight.**

I. INTRODUCTION

With the advancement of Information Communication Technologies (ICT) in Smart Grid (SG), the Vehicle to Grid (V2G) network has attained immense popularity from the last few years [1], [2]. The ICT has enabled the smart grid with efficient production and distribution of the energy using intelligent algorithm with Energy Cyber Physical System (E-CPS). Vehicle to Grid (V2G) is an integral part of the smart grid for bidirectional communication among EV, Charging Station (CS), and Grid Sever (GS). The charged EV batteries may become an energy source for the grid and other energy deficiency EVs. The energy stored in the EVs' batteries could be useful to transmit power back into the grid during the peak load. On the other hand, during slack hours, the surplus energy in the grid is used to charge the EV batteries. The major advantage of using V2G technology is that it transfers power from EVs to the grid during peak hours and grid to charge EVs during slack hours, hence it prevents loss of generated electricity. In the energy trading process, EVs can buy the power during low price and sell electricity when the price is high [3] [4]. V2G networks can be used for electricity regulation [5] or for storing electricity produced from renewal energy sources like a solar cell, Wind, etc. [6]. Hence, V2G provides a great practical solution for smart grid. One of the important advantages of the V2G Network is that EV owners can trade electricity without building their own transmission and distribution system [7], [8].

In a conventional smart grid, energy flow is one way i.e from GS to customer premises. Generating stations have to be always ready to administer peak load demand. Hence generation capacity has to be kept high for short duration, lead to carbon emission and wastage of infrastructure. V2G Network uses information and communication technologies for bidirectional communication between EV and CS as well as CS and GS. EV takes part in energy trading where it charges when there is surplus power and low tariff is available. Then discharges when demand is very high and high tariff is available hence reduce peak loads. EV gets some reward points. In Fig.1 the system model is shown. Proposed model consists of three entities: EVs, CSs and the GS. Besides the advantages of using

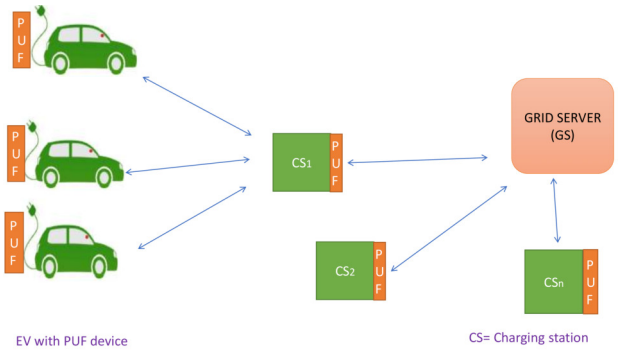

Fig. 1. PUF Based V2G Network

advanced communication technologies, V2G has to face some challenges. Security is the major challenge face by the smart grid to become the next generation power network. When the EV, CS, and the GS are exchanging data and information, an adversary can intrude the confidential data and access the secret information about the power consumption and therefore availability of person at home. Furthermore, the intruder can

modify or replay the electricity consumption report or insert a false message and then steer the Grid server to make wrong decisions. Furthermore, an intruder can physically access an EV or CS and may retrieve important data in the absence of hardware security from its nonvolatile memory (NVM).

In our scheme, we propose a lightweight and secure authenticated key exchange protocol for secure communication that can prevent such attacks. We have considered that the Physically Unclonable Function (PUF) are equipped with EV and CS hence demising the need of storing any cryptographic key. PUF helps to extract the fingerprint from hardware to verify the unique identity [9], [10]. The implementation of such V2G network has been studied and validated in the proposed scheme. The paper is organized as follows: Section II covers the related previous work in the field of V2G network. The system model has been presented in section III. The proposed scheme has been covered in section IV. Section V elaborates security analysis along with comparison whereas the performance evaluation and comparison have been discussed in section VI. The final conclusion is derived in section VII.

II. Related Prior Research

Secure and reliable communication and transmission of electricity and data is a major challenge in V2G Network. Many security schemes have been proposed in the past few years to address security and privacy concerns in V2G network. The idea of secure key exchange scheme for V2G was proposed in [11] that prevents the MITM attack and security in V2G networks was introduced in [12]. Two exchange key schemes based on the ECC and symmetric key algorithm was suggested by Nicanfar and Leung [13]. The scheme was provided for scalability and security for the exchange of secret keys in V2G smart grids. Although, it is unsafe to false data injection attacks. Furthermore, these schemes generate considerable computational overhead for resource-constrained entities in V2G network which makes them incompatible to adapt in the network. The various role played by an individual EV, i.e, consumer, electricity storage, or supplier was proposed by Liu et al. [14]. For V2G networks where EV travel from their own network to other networks was proposed by Saxena and Choi [15]. The paper presented mutual authentication protocol against impersonation attacks. However, it fails against the physical attacks.

A lightweight mutual authentication scheme was suggested by shen et al [3] in 2017, but it suffered from the deficiency of session key integrity and location secrecy. A secure and lightweight MA scheme for energy internet-based V2G network was suggested by Gope and Sikdar in [19]. Their proposed protocol ensures EV location privacy and could combat various cyber-attacks with a less computational overhead cost at the EV side. However, it was not supported by hardware security. A mutual authentication scheme for V2G utilizing physical unclonable functions (PUFs) suggested by Bansal et al. [18] in 2020. As per best knowledge, the suggested scheme could prevent a physical attack. Although, this protocol does not provide EVs location privacy against CS and suffers high computational overheads [17]. After it, protocol which prevents the location identity of the EVs against internal devices was proposed in [17]. However, the paper was not included the security at EV hence suffers a physical attack. In scheme [20]– [21], authors proposed a secure authentication and privacy-preserving scheme that ensures reliable communication in V2G networks. In the research paper [20], the authors claimed that their authentication scheme ensures less delay, computational and communication overhead.

We have discussed different authentication schemes. But no authentication scheme provides complete solution for hardware security for EV. The proposed scheme is able to mitigate all the issues and provides the security in all the attacks as shown in Table II. We have proposed a hardware secure mutual authentication scheme which provides hardware security using PUF at CS and EV along with scheduling for EV. In scheduling distance from CS, waiting time at CS, comprehensive cost and time cost parameters are considered. As per best of our knowledge, no other scheme provides complete hardware security for CS and EV using PUF with scheduling features.

TABLE I
COMPARISON OF SECURITY FEATURES

Security features	[16]	[15]	[17]	[12]	[18]	Our Scheme
Mutual Authentication	Y	Y	Y	Y	Y	Y
DOS Attack	N	Y	Y	Y	Y	Y
MITM (Man in the Middle)	N	Y	Y	Y	Y	Y
Perfect forward secrecy	N	Y	Y	Y	N	Y
Support Anonymity	N	N	Y	N	Y	Y
Physical security	N	N	N	N	Y	Y

III. SYSTEM MODEL

In the proposed system model CS acts as an intermediate between the EVs and the GS. EVs and CS are resources constrained, while the GS has sufficient resources. CSs and EVs have similar capabilities, but GSs have larger memory and computation power. Multiple EVs may connect to CS and multiple CS may connect to GS. The objective is to develop a mutual authentication (MA) protocol between EVs and the GS via CS. Each EV and CS are equipped with PUF. The mutual authentication process may be divided in two stages as in first stage between EV and CS and in second stage between CS and GS. Whenever any EV wishes to register on the network its challenge and response pairs are stored in GS and GS is a trusted authority [2]. The assumptions made in this research paper are as follows:

(a) PUF is small hardware and equipped with each EV and CS and is unique.

(b) The communication between an EV/CS and its PUF is secure and fool-proof [22].

(C) The GS is a trusted authority and has sufficient resources. In opposite to this, EVs and CSs have limited resources [23].

IV. PROPOSED SCHEME

The PUF based hierarchical mutual authentication scheme in V2G can be classified into the following 3 phases: 1) System Initialization and Registration 2) Scheduling and, 3) Mutual Authentication. The complete information about these phases is as below:

Phase 1: For EVs' registrations, EV first generates its identity (IDev) and sends it to GS. After it, GS generates a challenge (Cev) and sends it to EV. Then, EV produces a response (Rev) by providing the challenge (Cev) to its PUF and its response (Rev) to GS. After it, EV removes the challenge-response pair from its NVM. As EVs may park the open area without hardware protection, hence it is necessary for EVs to not store any secret information in its memory to prevent any type of physical attacks. Finally, GS stores Cev, Rev, and IDev in a row of databases that belongs to the corresponding CS.

TABLE II
LIST OF SYMBOLS

Symbols	Descriptions
h	one way hash function
IDev, IDcs	ID EV, CS
Tev, Tcs	Time stamp EV, CS
Rcs, Ccs	CS PUF challenge, response
Rev, Cev	EV PUF challenge, response
A1, A2	Intermediate authentication Message
PIDev	shadow ID of EV

For CSs' registrations, similar process adopted as EV. As CSs are exposed in the open area without hardware protection, hence it advisable not to store any secret data in its memory to prevent physical attacks. Finally, GS stores Ccs, Rcs, LOCcs, and IDcs in a row of database that belongs to the corresponding CS.

Phase 2: In this phase, the scheduling is considered where EV sends charging requests to GS by sending corresponding IDs. The GS checks the IDs and sends schedule requests to the corresponding CS with location details of EV. Schedules are made as per the policy of operator and demand of EV driver (smart contract) which may include the parameters: i) Distance of EV from CS ii) Waiting time at CS iii) Comprehensive cost which includes consumption and time cost where time cost is the expected time of EV to arrive at CS.

Phase 3: Mutual authentication process. Mutual authentication among EV, CS and GS as shown below two stages

(a) Stage-1 :Mutual authentication between CS and GS

EV reaches at charging station and plug in the CS.

Step-1: Initially EV sends it's ID (IDev) and current timestamp Tev to CS. CS checks the freshness of time stamp Tev. After it CS generates a message M1=IDev$\oplus$ LOCev and transmits M1, Timestamp Tcs and IDev to grid server.

Step-2: Grid server first checks the freshness of CS time stamp Tcs and verifies the belongingness of IDcs in the GS database. If either of the conditions fails, the authentication request initiated by CS is terminated. For the next round of validation, it selects the corresponding CRP of CS and computes the verifier v1=h(Rcs$\|$Ccs$\|$IDcs) using hash operation. Along with this, it also generates the current time-stamp Tgs. it sends V1 and Ccs toward CS.

Step-3: The CS generates Rev=PUF(Cev) using Cev received from GS. After it calculates V1'=h(Rcs$\|$Ccs$\|$IDcs). If Calculated V1' is equal to received v1 then CS authenticate the GS. Now Cs calculates new CRP Ccs+1=h(Rcs$\|$ Ccs) and Rcs+1=PUF(Ccs+1). After it calculates verifiable V2=h(Rcs+1$\|$ Ccs+1$\|$ IDcs$\|$ Tcs) using hash function. It also calculates A2= Rcs+1$\oplus$Rcs $\oplus$Tcs. Then CS calculates session key SKcs=kdf(Ccs+1 $\|$Tcs $\|$Tgs). After it Sends A2 and V2.

Step-4: After receiving A2 and V2, GS calculates Ccs+1=h(Rcs$\|$ Ccs) and computes Rcs+1=A2$\oplus$Rcs$\oplus$Tcs. After calculating new response it calculates V2'=(Rcs+1$\|$ Ccs+1$\|$ IDcs$\|$ Tcs). If calculated V2' is equal to received V2 then CS is authenticated. Further it calculates session key SKcs= kdf(Ccs+1 $\|$Tcs $\|$Tgs). GS stores new CRP in its data base. Now CS and GS are authenticated and share data using the session key.

(b) Stage-2: Mutual authentication between EV and CS

Similarly, as above EV and CS are mutually authenticated. New Shadow ID of EV generated in each transaction so its actual identity is not known to anybody including CS.

V. SECURITY ANALYSIS AND COMPARISON

Our proposed protocol provides the following important security features required for smart grid energy trading. We have compared our researches with the latest proposed scheme [17], [18] and also demonstrated the features as defined below.

(A) Mutual Authentication: The proposed protocol supports mutual authentication among the EVs, CSs, and the GS. Two messages V1 and V2 are generated. These messages cannot be generated without knowledge of the challenge and response of PUF. Hence only the authentic and legitimate parties are capable of generating the authentication messages and establishing their trust in each other.

(B) Support Anonymity: The proposed scheme supports the anonymity of EVs against CS. CRP (Cev,Rev) and timestamps (Tev and Tcs) are used in all the message exchanges. Due to this randomness, the authentication token (V1 and V2) gets new values in each session.

(C) Message Integrity: When a EV communicates with CS or CS communicates with GS, it holds own sessions keys. CS and EV generate new CRP and fresh timestamp for each session. The authentication and integrity of the message transmission is ensured by the freshness of the CRP.

(D) MITM (Man in the Middle): Suppose that an adversary intercepts the relayed messages on the communication channel and tries to change the intermediate messages (V1,V2 or V3), pretending to be a legal entity in front of the other. But, this is not possible until the adversary gets the CRP of the EV/CS. Thus, the adversary cannot execute the MITM attack under the considered situations.

(E) DDoS Attack (Malicious Registration): GS maintains a database about the EV and CS. when invader CS/EV try to

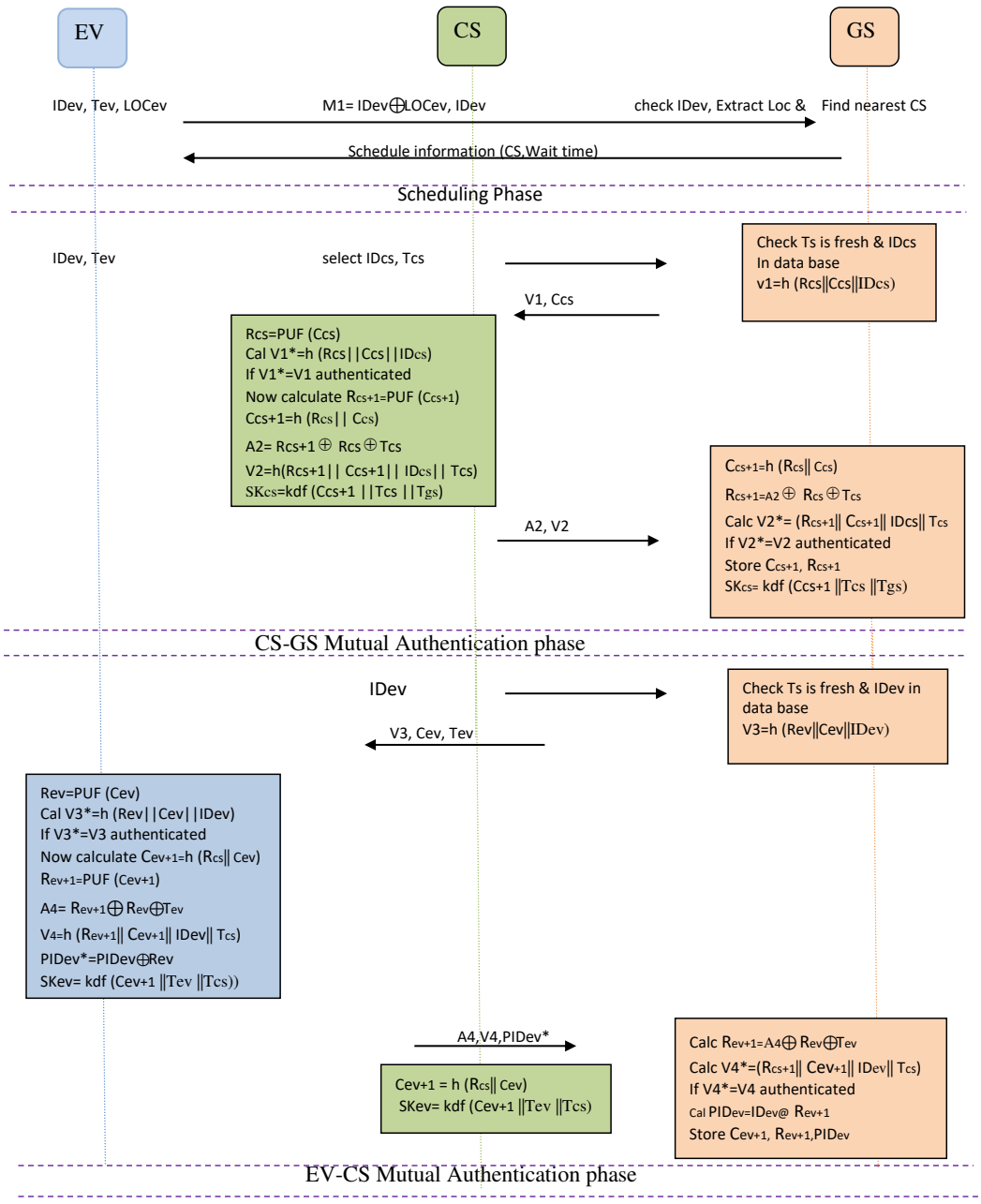

Fig. 2. Mutual Authentication

register, GS checks its database and refuses to register. Also, the intermediate authentication tokens acquire fresh values in each session, since they involve the freshly generated time-stamps and CRP for their computation.

(F) Perfect forward secrecy: It is supported as the session keys involved in the key agreement are not compromised even if the CRP of either the EV or the CSs are compromised. Session key usages combination of CRP(C,R), timestamp (Tev,Tcs,Tgs) which are fresh in each session.

VI. Performance Evaluation and Comparison

A. Formal verification using AVISPA Tool

Security of proposed model is verified by widely used and accepted automated verification of Internet Security Protocol (AVISPA) tool. These protocols have been written in the High-Level Protocol Specification Language (HLPSL). This tool is used to verify and validate the security attacks of any designed model by providing the AVISPA's back-ends.

B. Computational overhead analysis

The computational overhead of the proposed PUF based scheme has been evaluated and compared with other schemes in this section. The comparison of the computational overhead of our scheme with other recent schemes having similar models is shown in Table III. We have made a comparison for the EV is authenticating with the grid. We compared the different schemes based on different operations like XOR, Addition, Hash, MAC, PUF operation, etc. Our scheme uses only 4 cryptographic operations compared to 33 in [18] and 37 in [15]. Our scheme has 12 hash function computations while [15] has 16 and scheme [17] has 14. Scheme [15] has no MAC/HMAC or PUF operations but it has 16 hash and 37 XOR operations while our scheme has only 12 hash and 4 operations. While there is no physical security in [15], our scheme is physically secured due to PUF concept. Hence it is demonstrated that computational overhead of the proposed scheme is superior in comparison to related prior work.

TABLE III
COMPARISON OF COMPUTATION OVERHEAD

Operations	Saxena et al. [15]	Kaveh et al. [17]	Gaur ang B. et al [18]	Our scheme
XOR, Addition	37	8	33	4
Hash	16	14	-	12
MAC/HMAC	-	-	8	-
PUF	-	4	2	4

VII. CONCLUSION

The paper presents a PUF-based secure mutual authenticated scheme for V2G network. PUF is used at CS and EV to have the physical security with unique CRP where no secret information is stored in the NVM. One pair of CRP is stored for EV and CS respectively which changes after each transition. Session key established between CS and GS and another for EV and CS for secure exchange of information. We demonstrated that our scheme provides seurity against most of the attacks. Our scheme is proven formally secure by widely accepted AVISPA tool and computations overhead simulated using python 2.7. The simple computation algorithm is used hence our scheme is efficient and fast. Hence, our designed scheme is a feasible solution for the next-generation V2G network.

REFERENCES

[1] J. Rifkin, M. Carvalho, A. Consoli, and M. Bonifacio, "Leading the way to the third industrial revolution," *European Energ Rev*, vol. 1, 2008.

[2] H. Jain, M. Kumar, and A. Joshi, "Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection," *Electrical Engineering*, pp. 1–16, 2021.

[3] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things," *IEEE Internet of things Journal*, vol. 5, no. 4, pp. 2526–2536, 2017.

[4] P. W. Khan and Y.-C. Byun, "Smart contract centric inference engine for intelligent electric vehicle transportation system," *Sensors*, vol. 20, no. 15, pp. 42–52, 2020.

[5] H. Liu, Z. Hu, Y. Song, and J. Lin, "Decentralized vehicle-to-grid control for primary frequency regulation considering charging demands," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3480–3489, 2013.

[6] H. Lund and W. Kempton, "Integration of renewable energy into the transport and electricity sectors through V2G," *Energy policy*, vol. 36, no. 9, pp. 3578–3587, 2008.

[7] K. Zhou, S. Yang, and Z. Shao, "Energy internet: the business perspective," *Applied Energy*, vol. 178, pp. 212–222, 2016.

[8] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8–16, 2020.

[9] A. Jain and A. M. Joshi, "Device authentication in iot using reconfigurable PUF," in *2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*. IEEE, 2019, pp. 1–4.

[10] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[11] M. Yilmaz and P. T. Krein, "Review of benefits and challenges of vehicle-to-grid technology," in *2012 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2012, pp. 3082–3089.

[12] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012.

[13] H. Nicanfar and V. C. Leung, "Multilayer consensus ecc-based password authenticated key-exchange (MCEPAK) protocol for smart grid system," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 253–264, 2013.

[14] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. T. Yang, "Role-dependent privacy preservation for secure V2G networks in the Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 208–220, 2013.

[15] N. Saxena and B. J. Choi, "Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1438–1452, 2016.

[16] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE transactions on smart grid*, vol. 7, no. 2, pp. 906–914, 2015.

[17] M. Kaveh, D. Martín, and M. R. Mosavi, "A lightweight authentication scheme for V2G communications: A PUF-based approach ensuring cyber/physical security and identity/location privacy," *Electronics*, vol. 9, no. 9, p. 1479, 2020.

[18] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7234–7246, 2020.

[19] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6607–6618, 2019.

[20] H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, "UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 707–714, 2011.

[21] Z. Yang, S. Yu, W. Lou, and C. Liu, "Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[22] A. M. Joshi, P. Jain, and S. P. Mohanty, "Secure-iGLU: A secure device for noninvasive glucose measurement and automatic insulin delivery in iomt framework," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 440–445.

[23] J. Zhang and G. Qu, "Physical Unclonable Function-based key sharing via machine learning for IoT security," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 7025–7033, 2019.