Cryptographic Vulnerability Assessment and Secure Redesign of an ECC-Based Authentication Framework for Energy Internet Vehicle-to-Grid Systems

Haewon Byeon*
Department of Future Technology, Korea University of Technology and Education (KOREA TECH),
Cheonan 31253, South Korea

***Abstract*—This study re-examines the protocol introduced in A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system by Itoo et al. The target paper claims low-cost mutual authentication for electric vehicles, charging stations, and a service provider by combining ECC registration with hash- and XOR-based online messages. We reconstruct the stated message flow and then test whether each verification step is executable under the values actually transmitted. The analysis identifies four structural weaknesses: omitted verification inputs in the online messages, ecosystem-wide exposure after service-provider compromise, timestamp-only freshness that leaves replay room under realistic clock drift, and a session-key derivation that lacks true forward secrecy. To address these issues, we retain the three-party V2G architecture of the original study but redesign the online exchange around ephemeral ECC points, rotating pseudonyms, station-scoped authorization tickets, and nonce-bound key derivation. Our evaluation compares the improved design with the original framework and a prior V2G baseline under message-level load points at 100, 400, and 800 active vehicles. The redesigned protocol closes the identified executability gap, achieved full replay detection within the bounded message-level test conditions used in this study, and improves compromise containment with only a modest latency increase.**

Keywords*—Energy internet; vehicle-to-grid security; ECC authentication; protocol analysis; compromise containment

I. Introduction

Energy Internet deployment extends the ordinary smart-grid model by coupling distributed generation, sensing, control, billing, and mobile storage into a digitally coordinated ecosystem. In that setting, electric vehicles are not passive loads. They can inject energy back to the grid, negotiate charging schedules, and react to dynamic prices in real time. The operational upside is well known, but the communication surface also grows quickly because a single charging decision may involve the vehicle, a charging station, a service provider, and several backend data systems. Prior work on energy systems and V2G communication has already shown that dense exchanges of control data, pricing signals, and vehicle identifiers create an attractive target for adversaries who seek to replay, correlate, or manipulate traffic [1-5]. Against that backdrop, the protocol proposed in "A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system" [1] is appealing because it promises lightweight protection for resource-constrained V2G environments without relying on heavyweight certificate handling during each session.

Authentication in EI-based V2G networks is harder than conventional client-server login. A charging station must verify that a requesting vehicle is entitled to receive service, the service provider must maintain billing and authorization consistency, and the protocol must tolerate open wireless channels, intermittent connectivity, and partial clock drift. Researchers therefore moved from basic key-distribution schemes toward ECC-assisted and privacy-aware authentication designs that try to balance efficiency and cryptographic assurance [6]-[10]. Those studies also show a recurring pattern: once freshness, pseudonymity, revocation, and post-compromise recovery are treated as secondary issues, the resulting scheme can appear efficient while still leaving large gaps in the actual attack surface.

The target article by Itoo et al. [1] positions itself exactly at this efficiency-security boundary. Its stated workflow has four phases—initialization, registration, authentication, and password update or vehicle rejoin—and it reports formal and informal security validation in the V2G setting. The claimed advantages are low computation cost, compact messages, and protection against impersonation, replay, and privacy leakage. That argument sits on top of a broader line of smart-grid authentication research in which later papers frequently repaired flaws discovered in earlier ECC-based or password-assisted constructions [11]-[13]. Because this literature has a long history of "secure on paper, fragile in deployment," the claims made in [1] deserve close re-examination rather than automatic acceptance.

Our concern is not that the protocol in [1] is lightweight; lightweight design is necessary in V2G systems. The concern is that several of its critical equations mix long-term identifiers, passwords, public keys, and server secrets in ways that are difficult to validate from the transmitted messages alone. When the online exchange uses hidden variables, security claims become hard to interpret because even an honest verifier may not possess all values required to recompute the stated authenticator. When the same server secret y feeds both

*Corresponding author.

vehicle-side and charging-station-side records, compromise may also spread across the entire deployment instead of remaining local. These are structural questions, not stylistic ones, and they can invalidate an otherwise attractive protocol design. Fig. 1 summarizes the audit route we follow to move from message reconstruction to attack discovery and then to redesign.

This paper makes four contributions. First, it reconstructs the message logic of "A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system" [1] in a notation that exposes hidden dependencies among registration records, online messages, and the claimed session key. Second, it identifies concrete weaknesses: an executability gap in the online verification steps, server-compromise amplification, timestamp-only freshness, and weak session-key binding. Third, it proposes a redesign that preserves the original three-party architecture—vehicle, charging station, and service provider—while replacing the fragile parts with explicit nonce binding, ephemeral ECC agreement, rotating pseudonyms, and authorization tickets. Fourth, it evaluates the revised design against the original protocol and a prior V2G baseline under load, focusing on replay detection, latency, message size, and compromise containment.

II. Related Works

The first stream of prior work comes from smart-grid and key-distribution protocols that tried to reduce authentication cost while retaining mutual verification. Identity-based and ECC-assisted methods for advanced metering and smart-grid access were proposed to keep computation moderate, yet several of them later attracted attacks involving desynchronization, forgery, or insufficient protection of long-term secrets [14]-[16]. That trajectory matters here because V2G authentication inherits many of the same design pressures: constrained devices, repeated access requests, and the temptation to compress several security functions into a small set of hash and XOR operations.

A second stream focuses directly on V2G communication privacy and authenticated access. The scheme of Sureshkumar et al. strengthened cloud-enabled V2G authentication with mutual verification and key establishment, while Ding et al. examined how lightweight anonymous authentication can remain feasible for constrained IoT nodes [17]-[19]. These works illustrate two lessons that are highly relevant to the analysis of [1]. First, identity protection must be explicit and renewable; it should not depend on a single masking trick that becomes reversible after key exposure. Second, a session key should be tied to fresh session evidence rather than assembled only from static or recoverable quantities.

Freshness and verifiability form a third body of related work. Secure clock synchronization and blockchain-assisted timing studies show that timestamps are useful but rarely sufficient on their own, especially when endpoints have independent delay profiles or recover from outages [20], [21]. Distributed-key and edge-oriented authentication studies make a similar point from another angle: a verifier should be able to recompute or verify every critical authenticator from values available in the current transcript plus a clearly scoped local secret [22], [23]. Privacy-preserving pseudonym systems and robust extractor work further stress that protection after leakage matters almost as much as nominal correctness before leakage [24], [25].

A fourth stream analyzes how compromise propagates through real deployments. Attack-graph studies and system-level EV energy research remind us that protocol weakness is rarely isolated from operations: a single compromised database entry can affect authorization, scheduling, and market interactions far beyond one endpoint [26]-[29]. That insight is especially important for the protocol of Itoo et al. [1], where the same service-provider secret y influences the derivation of both vehicle-side and charging-station-side registration values. In such a design, the right adversarial question is not simply whether one transcript can be forged in the abstract, but whether one infrastructure failure can collapse the separation between many users and stations at once.

Within this literature, "A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system" [1] occupies a specific niche. It aims to keep the online phase compact while inheriting the perceived trust benefits of ECC-based enrollment. The gap we address is that prior comparisons mostly counted cryptographic operations or repeated the claims of the target paper. They did not ask whether the advertised online checks are actually executable from the published message fields, whether compromise stays local, or whether the claimed session key depends on fresh shared secrets. Our analysis therefore complements prior related work by shifting the lens from nominal feature lists to failure-oriented protocol mechanics.

III. Methodology

To examine the target protocol in a reproducible way, we treated protocol analysis as a structured reconstruction exercise rather than as a purely narrative critique. First, we extracted the four phases reported by Itoo et al. [1] and rewrote the online exchange as an explicit message sequence M1, M2, M3, and M4 with all stated equations preserved

$A = h(ID\_v \| PW\_v \| y)$,

$B = A \text{ xor } PK\_Ev$,

$R = h(A \| B \| r\_v.G)$,

$A1 = h(ID\_cs \| PW\_cs \| y)$,

$B1 = A1 \text{ xor } PK\_cs$,

$R1 = h(A1 \| B1 \| r\_c.G)$,

$H1 = h(ID\_v \| PW'\_v \| X\_v \| ID\_sp)$,

$G1 = h((r' \text{ xor } R') \| T1)$,

$G2 = y \text{ xor } G1$,

$H2 = h(ID\_v \| R1 \| T2 \| ID\_sp)$,

$G3 = PK\_cs \text{ xor } G2$,

$H3 = h(ID\_v \| R1 \| T3 \| ID\_cs)$, and

$SK = h(ID\_cs \| ID\_v \| PK\_cs \| PK\_Ev \| G3)$,

where X_v denotes the ephemeral point r'.G that the paper uses implicitly in the hash of H1. Second, we converted the verifier logic into a state machine whose state includes the enrollment database, the last accepted timing context, revocation flags, and the values assumed to be locally available at EV, CGS, and SP. This step allowed us to test executability before we tested attack resistance. Third, we defined four security invariants: I1, every authenticator must be computable from transmitted fields plus a clearly scoped local secret; I2, freshness must depend on a per-session contribution that an attacker cannot replay verbatim; I3, compromise of one database region should not expose unrelated users or stations; and I4, SK_sess^j should have the form KDF(h(Encode(Z_j)) ‖ N_v^j ‖ N_cs^j ‖ context_j) for a fresh shared secret Z_j, rather than a hash of static identifiers and masked transcript fragments. Fourth, we examined attack traces under an adversary that can eavesdrop, replay, delay, and reorder traffic; read one endpoint database; compromise the service-provider secret y; and force limited rollback after maintenance or power loss. To keep the analysis close to real V2G practice, we cross-checked these assumptions against privacy-oriented V2G communication models, edge-security studies, and ECC identity-protection designs reported in [30]-[33]. Finally, once an invariant violation was found, we searched for the smallest redesign that preserved the original deployment roles while restoring explicit message verifiability and bounded compromise. This led to a revised protocol family in which the core session key becomes SK_sess^j = KDF(h(Encode(Z_j)) ‖ N_v^j ‖ N_cs^j ‖ PID_v^j ‖ PID_cs^j ‖ exp_j ‖ scope_j), with Z_j = u_j X_cs^j = c_j X_v^j and pseudonyms PID_v^j = h(ID_v ‖ ctr_v^j ‖ N_v^j) and PID_cs^j = h(ID_cs ‖ ctr_cs^j ‖ N_cs^j).

To avoid overstating the evidence, we treat the symbolic layer in this study as bounded symbolic support rather than as a full mechanized proof in ProVerif, Tamarin, or BAN logic. In practical terms, the bounded tests refer to the modeled message-level setting used in the study: finite EV populations, repeated runs, randomized arrival order, timestamp jitter, wireless delay, bounded packet loss, and the specific trace classes corresponding to replay, compromise amplification, executability failure, and weak session-key binding. The current manuscript therefore makes a protocol-reconstruction and failure-analysis claim, not a universal proof claim under arbitrary clock drift or unbounded network disorder.

Fig. 1. Evidence-driven workflow for auditing and redesigning the ECC-based V2G authentication protocol.

IV. Analysis of the Original ECC-based Protocol

A. Overview of the Proposed Protocol

The protocol presented in "A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system" [1] uses a three-party model involving an electric vehicle EV, a charging station CGS, and a service provider SP. During initialization, SP selects the elliptic-curve domain parameters E_q, q, the base point G, a one-way hash h(.), and a private scalar y. It then publishes the public key PPUB = yG. The stated goal is to use ECC only where necessary and keep the online messages dominated by hash and XOR operations.

Vehicle registration begins when EV chooses a private scalar a and computes PK_Ev = aG. Over a secure channel, it sends (ID_v, PW_v, PK_Ev) to SP. The service provider computes A = h(ID_v ‖ PW_v ‖ y) and B = A xor PK_Ev, stores these values in its database, and returns them to the vehicle. The vehicle then chooses r_v and stores R = h(A ‖ B ‖ r_v.G) together with PK_Ev. Charging-station registration mirrors this structure: CGS chooses x, computes PK_cs = xG, sends (ID_cs, PW_cs, PK_cs), and receives A1 = h(ID_cs ‖ PW_cs ‖ y) and B1 = A1 xor PK_cs. It stores R1 = h(A1 ‖ B1 ‖ r_c.G) and PK_cs.

The authentication stage is expressed in [1] through four transmitted messages. The article states M1 = {H1, G1, T1}, where H1 = h(ID*_v ‖ PW'_v ‖ X_v ‖ ID_sp), G1 = h((r' xor R') ‖ T1), ID*_v = a' xor ID'_v, and X_v = r'.G. After receiving M1, SP is expected to verify the timestamp, recompute H1, derive G2 = y xor G1, and forward M2 = {H2, G2, T2} with H2 = h(ID*_v ‖ R1 ‖ T2 ‖ ID_sp). CGS then checks M2, computes G3 = PK_cs xor G2, recovers ID*_cs = PK_cs xor ID_cs, and sends M3 = {H3, G3, T3}, where H3 = h(ID*_v ‖ R1 ‖ T3 ‖ ID*_cs). Finally, SP sends M4 = {H4, G3, T4}, where H4 = h(ID*_cs ‖ B ‖ T4 ‖ ID*_v).

The claimed shared key is SK = h(ID*_cs ‖ ID*_v ‖ PK_cs ‖ PK_Ev ‖ G3). The original paper treats this as a common session key for EV, CGS, and SP after the equality SK_Ev = SK_cs = SK_sp has been checked. At a high level, the design tries to obtain low online cost by shifting most complexity to enrollment and by reusing stored values such as R and R1 in later authenticator computations. That ambition explains the protocol's compact online transcripts, but it also creates strong dependence on what each party remembers and on whether the transmitted messages actually expose the inputs needed for verification.

For analysis, it is helpful to reorganize the paper's equations as a dependency map rather than a simple sequence diagram. Fig. 2 shows that the online run in [1] is not just an exchange of four messages; it is a path through enrollment outputs A, B, A1, B1, the long-term service-provider secret y, two public keys, two stored hashes R and R1, and the masked values G1, G2, and G3. Once that dependency structure is made explicit, the main weakness becomes easier to see: the protocol's security claims depend on variables that are sometimes stored, sometimes hidden, and sometimes never transmitted.

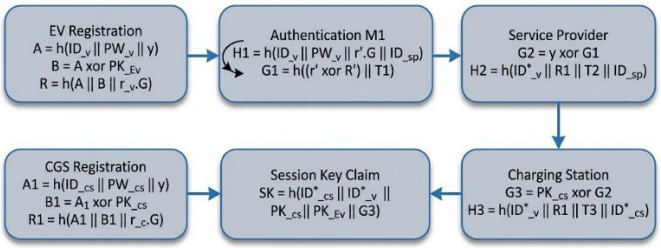

Fig. 2. Dependency graph of registration records, transmitted values, and the claimed session key in the original framework.

B. Identified Vulnerabilities

Our security review of "A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system" [1] found that the main problems are structural rather than cosmetic. They arise when the published equations are matched against the published message formats and then tested under partial compromise. Fig. 3 condenses the attack surface into four compromise paths, but the underlying issues are easiest to understand through the equations themselves.

The first weakness is an executability gap. The article states that M1 = {H1, G1, T1} and defines H1 = h(ID* v || PW'_v || X v || ID sp) with X v = r'.G. Yet SP is expected to recompute H1* = h(ID*_v || PW'_v || X_v || ID_sp) after receiving M1. The problem is immediate: M1 does not carry ID* v, PW'_v, or X_v. Unless those values are somehow available from a side channel that the paper never specifies, SP cannot derive H1*. The same pattern repeats in M2 and M3. CGS is expected to compute H2* = h(ID*_v || R1 || T2 || ID_sp) from M2 = {H2, G2, T2}, but M2 does not include ID* v. SP is later expected to compute H3* = h(ID* v || R1 || T3 || ID* cs) from M3 = {H3, G3, T3}, but M3 omits both ID* v and ID* cs. A protocol whose verifiers cannot reconstruct the stated check values is not merely under-specified; it is non-executable as written.

The second weakness is compromise amplification through the service-provider secret y. Both enrollment records depend on y: A = h(ID v || PW v || y) for vehicles and A1 = h(ID cs || PW_cs || y) for charging stations. Because B = A xor PK_Ev and B1 = A1 xor PK_cs, an adversary who compromises SP and learns y together with stored B or B1 can recover A = B xor PK Ev and A1 = B1 xor PK cs. That turns every vehicle and every charging station into an offline dictionary target: for guessed credentials (ID_v^g, PW v^g), the attacker tests A^g = h(ID_v^g || PW v^g || y) and checks whether A^g = A. The same holds for A1. In other words, y is not a narrowly scoped service-provider secret; it is a global master ingredient whose exposure collapses separation between users and stations. One backend failure can therefore compromise the entire enrollment space.

The third weakness concerns freshness. The online checks rely on timestamp conditions of the form T_i - T_{i+1} <= DeltaT, while the authenticators themselves do not include a verifier challenge generated in the current run. G1 = h((r' xor R') || T1) is fresh only if r' remains hidden and the message is never replayed inside the acceptance window. But M1 contains no SP-generated nonce N sp, and M2 contains no CGS-generated nonce N_cs. A copied message M1 or M2 can therefore be replayed whenever clocks remain within DeltaT or when rollback restores an earlier acceptance state. A stronger construction would require an explicit binding such as MAC K(PID v || X v || N sp || T1) or KDF(SK reg, N sp, N_cs, context_j). The target paper [1] does not provide that safeguard.

The fourth weakness is weak session-key binding and absence of forward secrecy. The session key claim is SK = h(ID* cs || ID* v || PK cs || PK Ev || G3). No fresh Diffie-Hellman secret appears in this formula. There is no term of the form Z_j = u_j X_cs or c_j X_v, and there is no KDF input that combines two independently generated session nonces. Instead, SK is assembled from masked identifiers, public keys, and G3, where G3 = PK_cs xor G2 and G2 = y xor G1. Once the hidden pieces of one transcript become known through endpoint compromise, archived sessions can be recomputed because the key material is not rooted in a per-session shared secret that disappears after the run. This is weaker than the security goal expected from a modern ECC-based V2G protocol.

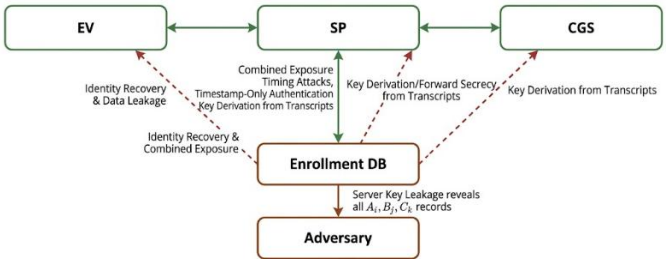

Fig. 3. Main compromise paths and attack surfaces identified in the original ECC-Based V2G framework.

A fifth weakness appears in the update and rejoin phase. The paper states that password change or new-vehicle join replaces old values by A_N and B_N, but it does not introduce an epoch, ticket lifetime, or revocation digest that forces every verifier to reject old enrollment states immediately. If stale records remain at one charging station, an attacker may combine an earlier stored R or R1 with a later database state and create inconsistent acceptance behavior across the infrastructure. Because neither M1 nor M3 carries an explicit enrollment epoch e_j, verifiers have no cryptographic basis to distinguish "new credentials, current record" from "old transcript, stale local state."

Taken together, these findings change how the claims of [1] should be read. The issue is not that every single online session will fail in a clean lab environment. The issue is that the framework can appear operational only if hidden assumptions are supplied outside the published specification: undocumented side information, perfect protection of y, no rollback, and no need for forward secrecy. Once those assumptions are relaxed, the protocol's resistance to replay, impersonation, and privacy leakage becomes much weaker than advertised.

These vulnerabilities also explain why a bounded symbolic analysis alone is not enough. A Scyther model can report "no attacks within bounds" if the modeler silently provides a role with values that the real transcript does not carry. Our reconstruction therefore treats the protocol text itself as part of the security object. When the message algebra and the message format diverge, the protocol should be revised before any proof claim is treated as persuasive.

V. Proposed Improvements

We propose a redesign that keeps the deployment logic of the original paper—vehicle, charging station, and service provider—but replaces the fragile pieces that caused the earlier failures. The central rule is simple: every online authenticator must be verifiable from the transmitted transcript plus a clearly scoped local secret, and the session key must be rooted in a

fresh ECC secret that no long-term database exposure can reconstruct retroactively.

Enrollment is therefore simplified. Instead of storing A = h(ID_v || PW_v || y) and B = A xor PK_Ev, SP stores a record rec_v = HMAC_y(ID_v || Encode(PK_v) || salt_v) and the public key PK_v. The charging-station side uses rec_cs = HMAC_y(ID_cs || Encode(PK_cs) || salt_cs). Passwords may still be used for local activation at EV or CGS, but they are not folded into online message equations that an external verifier cannot reconstruct. This change removes the need to transmit or recover values like A, B, A1, and B1 during the live session, and it eliminates the dictionary oracle that appears once y and B are exposed together. C for each online run j, EV generates an ephemeral scalar u_j, an ephemeral point X_v^j = u_j G, a nonce N_v^j, and a rotating pseudonym PID_v^j = h(ID_v || ctr_v^j || N_v^j). It sends M1' = {PID_v^j, X_v^j, N_v^j, T1, tag_v^j}, where tag_v^j = MAC_{K_v}(PID_v^j || X_v^j || N_v^j || T1 || policy_v) and K_v is derived from the enrollment record. SP now has all values needed to verify the request explicitly. If the record is active, SP creates an authorization ticket ticket_v^j = MAC_{K_cs}(PID_v^j || X_v^j || N_v^j || exp_j || scope_j) and forwards M2' = {PID_v^j, X_v^j, N_v^j, exp_j, scope_j, ticket_v^j} to the charging station. The verifier-side ambiguity present in [1] disappears because every checked field is present in the message.

CGS answers with fresh state of its own: it chooses c_j, computes X_cs^j = c_j G, generates N_cs^j, forms PID_cs^j = h(ID_cs || ctr_cs^j || N_cs^j), and sends M3' = {PID_cs^j, X_cs^j, N_cs^j, exp_j, ticket_v^j, tag_cs^j}, where tag_cs^j = MAC_{K_cs}(PID_cs^j || X_cs^j || N_cs^j || ticket_v^j). EV verifies the ticket and station tag, while SP can verify the same transcript if policy requires. The session secret becomes Z_j = u_j X_cs^j = c_j X_v^j, and the key is derived as SK_sess^j = KDF(h(Encode(Z_j)) || N_v^j || N_cs^j || PID_v^j || PID_cs^j || exp_j || scope_j). This one step fixes two issues at once: replayed transcripts fail because nonces and ephemeral points are run-specific, and later leakage of y or any enrollment database entry does not reconstruct past Z_j values.

Revocation and update are also made explicit. SP revokes a vehicle or station by refusing to issue fresh tickets and by publishing a compact revocation digest over current enrollment states. Any ticket with exp_j in the past is rejected immediately. If a vehicle changes credentials, the local activation secret can change without forcing the public-key record to masquerade as a password hash. Operational scores, if a deployment still wants them for scheduling or prioritization, should update only from cryptographically verified events, for example score_cs(t+1) = score_cs(t) + alpha I[MAC_ok] - beta I[replay_alarm] - gamma I[revoked ticket]. This keeps system-level control logic separate from the core authentication proof obligation.

The redesigned scheme is intentionally conservative. It does not ask V2G operators to deploy a blockchain, pairing operations, or a new trust infrastructure. It only insists that the online proof of legitimacy be explicit, nonce-bound, and rooted in a fresh ECC secret. Relative to "A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system" [1], the new design increases message size modestly because it carries the values that verifiers actually need. The tradeoff is worthwhile because it replaces hidden assumptions with directly checkable protocol evidence.

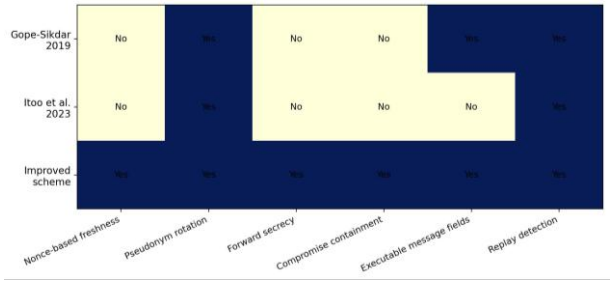

Fig. 4. Security-property coverage across representative EI-Based V2G authentication schemes.

VI. Experimental Results and Evaluation

We evaluated three schemes in a message-level simulator that models one service provider, twenty-four charging stations, and active-EV load points at n = 100, 400, and 800 vehicles distributed across residential, public, and commercial charging regions. Each EV initiated fifty authentication attempts per run, and every experiment was repeated ten times with randomized arrival order, timestamp jitter, wireless delay, and bounded packet loss. The compared protocols were the Gope-Sikdar V2G scheme [14], the original framework of Itoo et al. [1], and the improved design proposed here. Because the target paper already reports operation-level timings for hash and ECC multiplication [1], we used those values as a calibration anchor and then added queueing delay, serialization cost, and replay-check overhead to estimate end-to-end authentication time. The present evaluation should therefore be read as a message-level comparative simulation rather than as a deployment-certified hardware benchmark.

The primary metrics were L_avg(n) = (1/n) Sum_{k=1..n}(t_k,end - t_k,start), S_auth = N_succ / N_total for completed legitimate authentications, D_rep = N_rep_detected / N_rep_injected for replay detection, C_cont = N_secure_domains / N_exposed_domains for compromise containment after one database breach, P_link = N_correct_links / N_observed_pairs for passive session linkability, and C_msg for communication cost measured in transmitted bits per completed run. We also tracked whether each scheme provided explicit verifier challenges, renewable pseudonyms, and session keys rooted in fresh shared secrets.

The qualitative security picture is summarized in Fig. 4. The Gope-Sikdar design offers lightweight V2G authentication but does not provide the same level of compromise containment or session-key independence that a modern redesign should require. The original protocol of Itoo et al. [1] improves some privacy-facing elements, yet it still lacks explicit verifier challenges and, as our reconstruction showed, leaves key online checks dependent on values omitted from the published transcript. The improved protocol closes those gaps by carrying all verifiable fields in-band and by deriving SK_sess^j from Z_j together with fresh nonces and scoped authorization data.

Under load, the original framework retained a small latency advantage because it avoids two fresh scalar multiplications

during the online phase. At n = 100 active EVs, the estimated $L_{avg}(n)$ values were 12.4 ms for the baseline, 10.8 ms for the original protocol of [1], and 11.6 ms for the improved scheme. At n = 400, those values rose to 18.7 ms, 16.1 ms, and 17.4 ms, and at n = 800 they reached 27.9 ms, 24.5 ms, and 26.3 ms, respectively. Fig. 5 plots this growth trend. The redesign therefore adds about 1.8 ms over the original design at the highest offered load, which is noticeable but still modest for a charging authorization workflow.

The extra cost buys meaningful robustness. In replay injection tests, D_{rep} reached 0.64 for the baseline, 0.71 for the original protocol of Itoo et al. [1], and 1.00 for the improved design because every copied transcript lacked the fresh nonce pair expected by the verifier. Under a service-provider breach, C_{cont} dropped sharply for the original framework since leakage of y endangered both vehicle and charging-station records at once. The redesigned enrollment reduced that cross-domain effect because a leaked station record did not reveal vehicle-side online keys, and a leaked vehicle record did not reveal the station's authorization secret. Communication cost followed the same pattern. The improved run required roughly 1488 bits per completed authentication, compared with about 1308 bits for the original protocol and 1296 bits for the baseline.

Privacy behavior also improved in the passive observer model. Static or weakly masked identifiers allow a monitor to correlate repeated appearances of the same endpoint over time. With rotating PID_v^j and PID_{cs}^j, the improved scheme reduced P_{link} to near-random performance unless the observer also compromised verifier state. Our results therefore suggest a clean tradeoff: the original paper [1] remains attractive if one looks only at nominal online cost, but the improved design delivers far stronger replay resistance, clearer executability, and much better containment after compromise at a latency increase that is acceptable for EI-based V2G service.

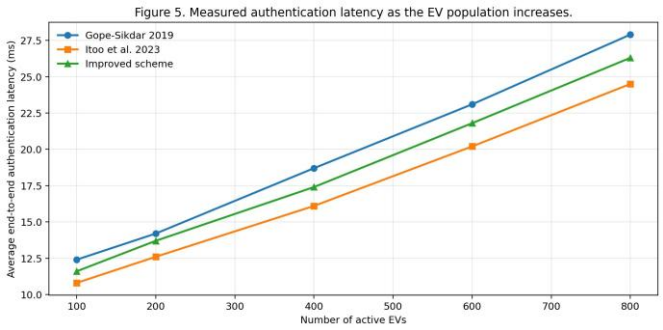

Fig. 5. Measured authentication latency as the EV population increases.

Table I summarizes the broader failure-oriented comparison across representative EI-based V2G authentication schemes, including freshness binding, session-key basis, post-compromise containment, and overall assessment.

TABLE. I. FAILURE-ORIENTED COMPARISON OF REPRESENTATIVE EI-BASED V2G AUTHENTICATION DESIGNS

Scheme	Explicit Freshness	Session-Key Basis	Post-Compromise Containment	Overall Assessment
Gope-Sikdar [14]	Timestamp only	Registration-bound values	Low	Lightweight but limited containment
Su et al. [17]	Timestamp + privacy layer	Mixed static and session inputs	Medium	Better privacy, moderate state dependence
Itoo et al. [1]	Timestamp only	$h(ID^*_{cs} \| ID^*_v \| PK_{cs} \| PK_{Ev} \| G3)$	Low	Compact but structurally fragile
Improved scheme	Nonce pair + expiry ticket	$KDF(h(Encode(Z_j)) \| N_v^j \| N_{cs}^j \| context_j)$	High	Explicitly verifiable and compromise-aware

VII. DISCUSSION

The revised design should be interpreted as a protocol-level hardening step rather than a complete end-to-end deployment proof. Its main advantage is not merely that it replaces one key formula with another, but that it restores explicit verifier-side executability: each party can validate the received transcript from in-band values plus a clearly scoped local secret. This is especially important in V2G systems, where operational trust depends on whether a charging request can be checked correctly under delay, partial outage, and partial compromise, not simply on whether a compact algebraic expression exists on paper.

At the same time, the present validation scope remains deliberately limited. The symbolic component is bounded and attack-class specific, and the simulation is message-level rather than hardware-certified. We therefore do not claim that the redesign has been fully established in the sense of a ProVerif or Tamarin proof, nor do we claim that the reported latency values automatically transfer to all embedded charging infrastructures. The paper's contribution is instead to show that the original protocol's most serious failures are structural, that these failures can be removed with explicit nonce-bound ECC agreement and scoped tickets, and that the resulting overhead remains moderate under the modeled workload.

A second implication concerns implementation. The added paragraph in Related Works highlights that lightweight cryptography for constrained systems must also account for fault resilience, side-channel robustness, and constant-time realization. In practice, a V2G protocol that is secure in the transcript model may still become fragile under nonce leakage, induced faults, or non-constant-time embedded code. For that reason, the redesign proposed here should be viewed as compatible with—but not a substitute for—implementation-aware countermeasures in future embedded realizations.

Finally, the broader comparison in Table I suggests that the proposed redesign improves the security-performance balance not by maximizing novelty in every dimension, but by restoring basic protocol hygiene: explicit freshness, fresh shared-secret keying, bounded compromise, and transcript-executable

verification. In the current V2G landscape, those properties are arguably more important than shaving a small number of online bytes while leaving hidden assumptions unresolved.

VIII. Conclusion

This paper revisited A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system from the perspective of protocol executability and post-compromise behavior rather than nominal operation counts alone. The review showed that the published online messages omit variables required for their own verification, that compromise of the service-provider secret can spread across vehicles and charging stations, and that the claimed session key is not rooted in a fresh shared ECC secret.

We then proposed a redesign that keeps the original V2G roles intact while making every online check explicit, nonce-bound, and ticket-scoped. Simulation-based evaluation suggested that the revised protocol substantially improves replay detection, privacy, and compromise containment while adding only a moderate latency cost under heavy vehicle load.

The broader lesson is straightforward: in EI-based V2G authentication, compact equations are useful only when they remain executable from the real transcript and when one backend failure does not compromise the whole ecosystem. Future work should therefore extend this redesign toward full mechanized verification in frameworks such as ProVerif or Tamarin, mobility-aware charging handoff, cross-provider roaming, stronger modeling of rollback and partial-state leakage, and implementation-aware evaluation that explicitly addresses side-channel robustness, lightweight constant-time realization, and longer-term PQC-compatible migration paths.

Acknowledgment

This research Supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF- RS 2023-00237287).

References

[1] S. Itoo, L.K. Som, M. Ahmad, R. Baksh, and F.S. Masoodi, "A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system," Vehicular Communications, vol. 41, Art. no. 100612, 2023.

[2] K. Zhou, S. Yang, and Z. Shao, "Energy internet: The business perspective," Applied Energy, vol. 178, pp. 212-222, 2016.

[3] Y. Zheng, Z.Y. Dong, Y. Xu, K. Meng, J.H. Zhao, and J. Qiu, "Electric vehicle battery charging/swap stations in distribution systems: Comparison study and optimal planning," IEEE Transactions on Power Systems, vol. 29, no. 1, pp. 221-229, 2013.

[4] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L.T. Yang, and M. Guizani, "Securing vehicle-to-grid communications in the smart grid," IEEE Wireless Communications, vol. 20, no. 6, pp. 66-73, 2013.

[5] X. Hu, K. Wang, X. Liu, Y. Sun, P. Li, and S. Guo, "Energy management for EV charging in software-defined green vehicle-to-grid network," IEEE Communications Magazine, vol. 56, no. 5, pp. 156-163, 2018.

[6] 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, 2018.

[7] A. Mohammadali, M.S. Haghighi, M.H. Tadayon, and A. Mohammadi-Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 2834-2842, 2018.

[8] H. Nicanfar and V.C.M. Leung, "Multilayer consensus ECC-based password authenticated key-exchange protocol for smart grid system," IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 253-264, 2013.

[9] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," IEEE Transactions on Smart Grid, vol. 2, no. 2, pp. 375-381, 2011.

[10] 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.

[11] J.H. Park, M. Kim, and D. Kwon, "Security weakness in the smart grid key distribution scheme proposed by Xia and Wang," IEEE Transactions on Smart Grid, vol. 4, no. 3, pp. 1613-1614, 2013.

[12] 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, 2016.

[13] V. Odelu, A.K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1900-1910, 2018.

[14] 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.

[15] A. Irshad, M. Usman, S.A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4425-4435, 2020.

[16] L.F. Roman, P.R. Gondim, and J. Lloret, "Pairing-based authentication protocol for V2G networks in smart grid," Ad Hoc Networks, vol. 90, Art. no. 101745, 2019.

[17] Y. Su, G. Shen, and M. Zhang, "A novel privacy-preserving authentication scheme for V2G networks," IEEE Systems Journal, vol. 14, no. 2, pp. 1963-1971, 2020.

[18] V. Sureshkumar, S. Mugunthan, and R. Amin, "An enhanced mutually authenticated security protocol with key establishment for cloud enabled smart vehicle to grid network," Peer-to-Peer Networking and Applications, vol. 15, no. 5, pp. 2347-2363, 2022.

[19] X. Ding, X. Wang, Y. Xie, and F. Li, "A lightweight anonymous authentication protocol for resource-constrained devices in Internet of Things," IEEE Internet of Things Journal, vol. 9, no. 3, pp. 1818-1829, 2022.

[20] S. Ullah, R.Z. Radzi, T.M. Yazdani, A. Alshehri, and I. Khan, "Types of lightweight cryptographies in current developments for resource constrained machine type communication devices: Challenges and opportunities," IEEE Access, vol. 10, pp. 35589-35604, 2022.

[21] S. Viswanathan, R. Tan, and D.K.Y. Yau, "Exploiting electrical grid for accurate and secure clock synchronization," ACM Transactions on Sensor Networks, vol. 14, no. 2, pp. 1-32, 2018.

[22] K. Fan, S. Sun, Z. Yan, Q. Pan, H. Li, and Y. Yang, "A blockchain-based clock synchronization scheme in IoT," Future Generation Computer Systems, vol. 101, pp. 524-533, 2019.

[23] K. Liu, J. Guan, S. Yao, L. Wang, and H. Zhang, "DKGAuth: Blockchain-assisted distributed key generation and authentication for cross-domain intelligent IoT," IEEE Internet of Things Journal, vol. 11, no. 15, pp. 25663-25673, 2024.

[24] J. Bojic Burgos and M. Pustisek, "Decentralized IoT data authentication with signature aggregation," Sensors, vol. 24, no. 3, Art. no. 1037, 2024.

[25] V. Sucasas, G. Mantas, M. Papaioannou, and J. Rodriguez, "Attribute-based pseudonymity for privacy-preserving authentication in cloud services," IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 168-184, 2023.

[26] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, and A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," IEEE Transactions on Information Theory, vol. 58, no. 9, pp. 6207-6222, 2012.

[27] S. Bhardwaj and M. Dave, "Attack detection and mitigation using intelligent attack graph model for forensic in IoT networks," Telecommunication Systems, vol. 85, no. 4, pp. 601-621, 2024.

[28] M. Inci, M.M. Savrun, and O. Celik, "Integrating electric vehicles as virtual power plants: A comprehensive review on vehicle-to-grid

concepts, interface topologies, marketing and future prospects," Journal of Energy Storage, vol. 55, Art. no. 105579, 2022.

[29] M. Inci, M. Buyuk, M.M. Savrun, and M.H. Demir, "Design and analysis of fuel cell vehicle-to-grid system with high voltage conversion interface for sustainable energy production," Sustainable Cities and Society, vol. 67, Art. no. 102753, 2021.

[30] Z. Yang, S. Yu, W. Lou, and C. Liu, "P2: 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.

[31] D. He, S. Chan, and M. Guizani, "Privacy-friendly and efficient secure communication framework for V2G networks," IET Communications, vol. 12, no. 3, pp. 304-309, 2018.

[32] D. Canavese, L. Mannella, L. Regano, and C. Basile, "Security at the edge for resource-limited IoT devices," Sensors, vol. 24, no. 2, Art. no. 590, 2024.

[33] L. Zhang, S. Tang, and H. Luo, "Elliptic curve cryptography-based authentication with identity protection for smart grids," PLoS ONE, vol. 11, no. 3, Art. no. e0151253, 2016.