Journal of Renewable Energy and Sustainable Development (RESD)
Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

Received: 14 October 2025 Accepted: 16 January 2026 Published: 29 March 2026

A Cyber-Physical Simulation Framework for Resilient Microgrids with PV, BESS, and Tariff-Aware Control

Partha Das [1*], and Rituparna Mitra [2]

[1*] JIS College of Engineering, Electrical Engineering Department, Kalyani, West Bengal, India

[2] Swami Vivekananda University, Electrical Engineering Department, Kolkata, West Bengal, India

partha.das@jiscollege.ac.in, rituparnam@svu.ac.in

Abstract

The increasing diffusion of distributed photovoltaic (PV) generation, battery energy storage systems (BESS), and advanced metering infrastructure is transforming the conventional distribution networks into cyber-physical microgrids. These developments enhance operational flexibility, but also introduce new uncertainties, and the system is exposed to cyberattacks. For distribution level microgrids operating under combined PV unpredictability, load uncertainty, time-of-day (TOD) tariff signals, and false data injection (FDI) attacks, this proposed study develops an integrated simulation framework for resilience assessment of the system. The framework is tested on the IEEE 33 bus system. This developed model utilizes real demand traces from Mathura and Bareilly, and PV generation data from Shibpur, India, enabling context-aware evaluation under realistic operating conditions. The Monte Carlo (MC) uncertainty engine generates multiple scenario trajectories, and at each time interval, nonlinear AC power flow is solved to quantify electrical, economic, and stability-associated performance indicators. The proposed simulator produces detailed metrics, including aggregate energy losses, voltage regulations, congestion indices, tariff-adjusted energy costs, and BESS state-of-charge evolution. Results obtained from a 100-run for 72 hours MC experiment demonstrate measurable degradation in operational efficiency during coordinated FDI attacks, which include increased losses, sharp voltage spread, and raised cost sensitivity to TOD tariffs. This proposed tool offers a reproducible, integrated, and statistically grounded platform for microgrid resilience assessment, supporting the development of cyber-aware control strategies, tariff evaluation, and future optimization-based enhancements.

Index-words: *Battery Energy Storage System, Cyber Physical Resilience, False Data Injection, Microgrid Simulation, Monte Carlo Analysis, Photovoltaic Variability, Time-of-Day Tariff.*

I. Nomenclature

Term	Meaning
AC	Alternating Current
BESS	Battery Energy Storage System
CI	Confidence Interval
DER	Distributed Energy Resource
DoD	Depth of Discharge
FDI	False Data Injection
GHI	Global Horizontal Irradiance
MC	Monte Carlo
OPF	Optimal Power Flow
PV	Photovoltaic
RBC	Rule-Based Controller
RL	Reinforcement Learning
SoC	State of Charge
TOD	Time-of-Day
Term	Meaning
AC	Alternating Current

* Corresponding author

Copyright © 2026, authors

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

II. Introduction & Literature review

The fast digitalization and decarbonization of distribution networks are driving the extensive Integration of DERs such as PV generation and BESS. These resources enable improved operational flexibility, and they minimise dependence on fossil fuels, but they also increase the system's sensitivity to renewable variability, demand inconsistency, cyber-attacks, and dynamic tariff environments [1], [2]. As microgrids transform into cyber-physical energy systems enriched with advanced metering infrastructure and communication networks, their exposure to cyber intrusion and data manipulation events rises significantly [3], [4]. Ensuring robust operation under combined electrical and cyber uncertainties has therefore become a vital challenge in the modern power system research domain. High Integration of PV generation introduces stochastic fluctuations that directly affect real-time power balance, voltage stability, reverse power flows, and feeder congestion [5], [6]. BESS units are extensively deployed to minimise these disturbances, to support demand response, and to reduce energy costs. However, their performance strongly depends on system observability, accuracy in measurement, and controller sensitivity. By introducing price-driven incentives, Time-of-Day (TOD) tariff mechanisms further complicate system operation, and influence charging–discharging behaviour and energy exchange with the main grid [7], [8]. Meanwhile, FDI attacks pose a growing cybersecurity threat by intentionally altering measurement streams, potentially misleading microgrid controllers & causing insecure or suboptimal operating states [9], [10].

To model and analyse microgrid behaviour, a variety of tools exist. HOMER Pro enables robust techno-economic analysis, but has deficiencies in detailed AC power flow and stochastic scenario capabilities [11]. OpenDSS and GridLAB-D provide extensive power flow modelling, but they don't offer integrated cyberattack simulation, real-world PV or load data incorporation, or Monte Carlo uncertainty propagation [12], [13]. Matlab / Simulink-based frameworks support dynamic control studies, yet typically rely on deterministic profiles and do not incorporate tariff dynamics or attack scenarios [14]. For distribution system analysis, recent developments in the *pandapower* library improve accessibility [15]; however, its standard configuration remains deterministic and does not include cyber-physical modelling or multi-day stochastic evaluation. Current optimization-based DER coordination studies explore predictive, rule-based, or learning based BESS control [16], [17]. But it largely assumes reliable data streams and does not expose controllers to falsified information.

The cybersecurity domain has also produced significant understandings, particularly concerning FDI attacks in transmission level state estimation [18]. Succeeding research shows that similar attacks on distribution networks can reduce voltage stability, decreasing overloads, or lead to incorrect dispatch decisions [19], [20]. Digital twin-based glitch detection and resilience-oriented microgrid constructions have developed as promising solutions [21], [22]. Til now, most studies have analysed detection or mitigation strategies rather than inserting cyberattacks directly into time series microgrid simulations with DER dynamics and tariff effects. Uncertainty quantification is another crucial aspect of microgrid planning and operation. Monte Carlo techniques are broadly used for forecasting, reliability assessment, and renewable integration studies [23][24], though their application in microgrid resilience studies is typically limited to load or PV unpredictability without considering synchronized cyberattacks or tariff-driven operational responses [25] [26] [27]. Scenario-based planning approaches have been proposed, but they often cover short prospects and lack integration with the full AC power flow system [26].

For evaluating power system performance under increasing Integration of distributed energy resources (DERs), recent studies have emphasized the importance of probabilistic and stochastic frameworks. Wang et al. [29] proposed a probabilistic resilience assessment framework for power distribution systems with high DER penetration, highlighting the impact of uncertainty on system reliability assessment. Likewise, Chen and Shahidehpour [30] employed Monte Carlo-based uncertainty analysis to model renewable inconsistency in microgrid operation. Moreover, Khalid et al. [31] studied stochastic energy management of microgrids considering both price instability and renewable generation uncertainty. Inspired by these works, the present study adopts a stochastic, price-responsive optimization framework for demand response-based power system operation.

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

Despite advances across these domains, a significant research gap remains here: there is no united, cyber-aware, stochastic simulation framework that will simultaneously integrate PV unpredictability, flexible loads, BESS dynamics, TOD tariff modelling, and FDI attacks using real-world datasets. Existing tools address individual aspects, but no tool provides a modular, multi-day, AC power flow-based environment that captures the collective effects of electrical, economic, and cyber-physical uncertainties on microgrid resilience [34-41].

This present work addresses this gap by introducing a comprehensive cyber-physical microgrid simulation framework built on the IEEE 33 bus system. The framework integrates real PV and load profiles from Indian regions, integrates BESS dynamics, models TOD tariff signals, and embeds coordinated FDI attacks within a Monte Carlo uncertainty engine. The simulator computes a range of resilience-related indicators, which include voltage deviations, feeder congestion, energy losses, economic costs, and BESS state-of-charge evolution over multi-day horizons. By combining stochastic modelling, cyberattack emulation, and tariff-aware operation within a single environment, the framework contributes a statistically robust and reproducible framework for microgrid resilience assessment and future optimization-oriented research.

III. Methodology

This section presents the complete modelling framework used for cyber-physical microgrid simulation. All component models, stochastic processes, tariff representation, and Monte Carlo workflow are described to ensure scientific reproducibility. The methodology follows the nomenclature provided before the Introduction section.

A. System representation and time discretization

The microgrid is represented on the IEEE 33 bus radial distribution system with added photovoltaic (PV) units, a Battery Energy Storage System (BESS), and variable loads. The simulation horizon is discretized into uniform intervals of Δt = 15 minutes. At each step *t*, the system variables such as bus voltage, energy state, load, and PV power are updated according to the component models described below.

The steady-state power flow is solved using the Newton-Raphson algorithm implemented in the *pandapower* library. The nonlinear AC power flow equations are expressed as:

$$P_i = \sum_{j=1}^{N} |V_i||V_j|(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \quad (1)$$

$$Q_i = \sum_{j=1}^{N} |V_i||V_j|(G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}) \quad (2)$$

where G_{ij} and B_{ij} denote the conductance and susceptance elements of the bus admittance matrix

B. Photovoltaic generation model

PV generation is modelled as a stochastic process driven by real irradiance data. The baseline PV output P_t^{PV} is obtained from the Indian Shibpur IMD dataset and adjusted using a Gaussian multiplicative deviation:

$$P_t^{PV} = \hat{P}_t^{PV}(1+\epsilon_t), \epsilon_t \sim \mathcal{N}(0, \sigma_{PV}) \quad (3)$$

where σ_{PV} represents PV variability. Values of 5–10% are selected based on typical short-term irradiance fluctuations in Indian climatic conditions.

The model captures realistic intermittency and supports Monte Carlo sampling.

C. Load modelling and False Data Injection (FDI) attacks

Real load profiles from Mathura and Bareilly are mapped to corresponding buses using normalized allocation weights. Cyber-physical disturbances are modelled through an FDI mechanism applied to flexible load buses. An attack event at time *t* is governed by a Bernoulli random variable:

$$a_t \sim \text{Bernoulli}(p_{FDI})$$

If an attack occurs, the compromised load becomes:

$$P_t^{load'} = P_t^{load}(1+\delta_t), \delta_t \sim U[-\alpha, \alpha] \quad (4)$$

Coordinated attacks use the same δ_t across selected buses to emulate targeted manipulation.

Attack probabilities of 10–20% are consistent with vulnerability levels reported in cyber-resilience studies.

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

D. Battery Energy Storage System (BESS) model

The BESS is modelled as a single energy device with mutually exclusive charging and discharging modes. Charging power P_t^{ch} and discharging power P_t^{dis} follow:

$$P_t^{ch} = \delta_t P_t, P_t^{dis} = (1 - \delta_t) P_t \quad (5)$$

The energy state evolves as:

$$E_{t+1} = E_t + \eta_{ch} P_t^{ch} \Delta t - \frac{P_t^{dis} \Delta t}{\eta_{dis}} \quad (6)$$

Charging and discharging efficiencies are set to:

$$\eta_{ch} = 0.95, \eta_{dis} = 0.95$$

, which are representative of practical lithium-ion battery systems. The state-of-charge (SoC) is:

$$\mathrm{SoC}_t = \frac{E_t}{E_{\max}}, 0.10 \leq \mathrm{SoC}_t \leq 0.90 \quad (7)$$

A rule-based controller governs operation, charging occurs when PV exceeds load and SoC < 90%, while discharging occurs when load exceeds PV and SoC > 50%. This simple strategy is chosen purposely to validate system behaviour under uncertainty. The limitations and future scope for RL-based optimization are discussed later in the paper. The rule-based controller ensures transparency and computational simplicity, but it does not guarantee global optimality under dynamic tariffs or adversarial data manipulation. In particular, it lacks forethought regarding future price signals and attack persistence. Advanced approaches like model predictive control or reinforcement learning could improve economic efficiency & resilience. The present controller is therefore used as a baseline to highlight system-level influences under uncertainty. Though fixed BESS parameters are adopted in this study, the proposed framework is flexible and can accommodate adaptive or learning based control strategies in future extensions.

E. Time-of-Day (TOD) tariff model

Electricity cost is evaluated using a time-varying tariff multiplier:

$$C_t = \mu(h) \cdot P_t^{grid} \quad (8)$$

where $\mu(h)$ is a four-block TOD multiplier derived from regional tariff regulations, and P_t^{grid} is the net grid import. Exported energy is credited at 80% of the prevailing tariff, following Indian net-metering policies.

F. Performance metrics

Several operational, technical, and economic indicators are computed:

Line losses:

$$L_t = \sum_{\ell} I_{\ell,t}^2 R_{\ell} \quad (9)$$

Voltage violations:

$$V_t^{viol} = \begin{cases} 1, & |V_i| \notin [0.95, 1.05] \\ 0, & \text{otherwise} \end{cases}$$

Line congestion:

Loading > 80% indicates congestion.

Economic cost: Total TOD-adjusted energy cost.

BESS metrics: SoC profile, depth-of-discharge (DoD), cycle count.

These metrics support both deterministic evaluation and statistical comparison across Monte Carlo scenarios.

G. Monte Carlo simulation workflow

Uncertainty in PV, load, and cyberattacks is incorporated through a multi-scenario Monte Carlo (MC) process. Each run samples a disturbance vector:

$$\omega_r = \{\epsilon_t, a_t, \delta_t\}_{t=1}^{T} \quad (10)$$

Independent seeds ensure statistical validity ($seed = 42 + r$). For each of $N = 100$ runs, the simulator performs sequential power flow updates and aggregates performance metrics. The mean and variance estimators are:

$$\dot{X} = \frac{1}{N} \sum_{r=1}^{N} X_r, \sigma_X^2 = \frac{1}{N-1} \sum_r (X_r - \dot{X})^2 \quad (11)$$

A 95% confidence interval is computed using the normal approximation. A run size of 100 is selected based on variance stabilization and CV (<5%) sufficiency.

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

H. Parameter selection justification

All model parameters are selected based on established system behaviour:

- PV variability (5–10%) matches short-term irradiance fluctuations in Indian climate zones.
- FDI probabilities (10–20%) align with reported cyberattack likelihoods for distribution-level assets.
- SoC bounds (10–90%) reflect industry limits to maintain battery health.
- BESS size (1.5 MW / 3 MWh) corresponds to typical utility-scale deployments.

This ensures a realistic and comparable assessment of resilience scenarios.

I. Model validation and cross-verification

The framework is validated through:

- Voltage profile comparison with benchmark IEEE 33-bus results is performed.
- Energy tracking consistency between the BESS theoretical and simulated SoC curves.
- Cross-verification of baseline load flow with OpenDSS for structural accuracy is performed.
- Reproduction of standard loss values under nominal conditions.

These checks confirm numerical reliability and model correctness.

J. Computational efficiency and scalability

Simulations are executed on Python 3.11 with *pandapower*. A single 3-day run requires approximately 9 seconds. The framework scales near-linearly with system size, with runtime approximately proportional to $O(n^{1.2})$, enabling rapid execution of 100-run Monte Carlo batches in practical time.

IV. Case study configuration

This section fully specifies the electrical network, data sources, preprocessing pipeline, and experimental scenario matrix used to validate the proposed simulator. Every parameter is traceable to the mathematical symbols defined in Section 3 to ensure repeatability and peer review transparency.

A. Distribution network model

The IEEE 33-bus radial distribution system is adopted as the base topology, with per-unit base values of: $S_{base} = 500MVA$, $V_{base} = 12.66KV$. Table 1 summarizes the IEEE 33-bus test system configuration used in this study.

Table 1: IEEE-33 bus Test system configuration.

Asset Type	Bus Number(s)	Details/Rating
Conventional Generators	1,12,25	Bus 1: 2.0 MW Bus 12: 1.0 MW Bus 25: 1.0 MW
PV Systems	6,8,15,24	375 kW each (Total = 1.5 MW)
BESS	18	Power: 1.5 MW Capacity: 3.0 MWh Initial SoC: 50%
Load	All Buses	Based on *mathura_bareilly_load_profile.csv* (time-series, in kW)
Flexible Load	7,11,19,30	The load can be modified during the simulation

Line parameters, including resistance R_{ij}, reactance X_{ij}, and shunt admittance B_{ij}, are listed in Annexure I.

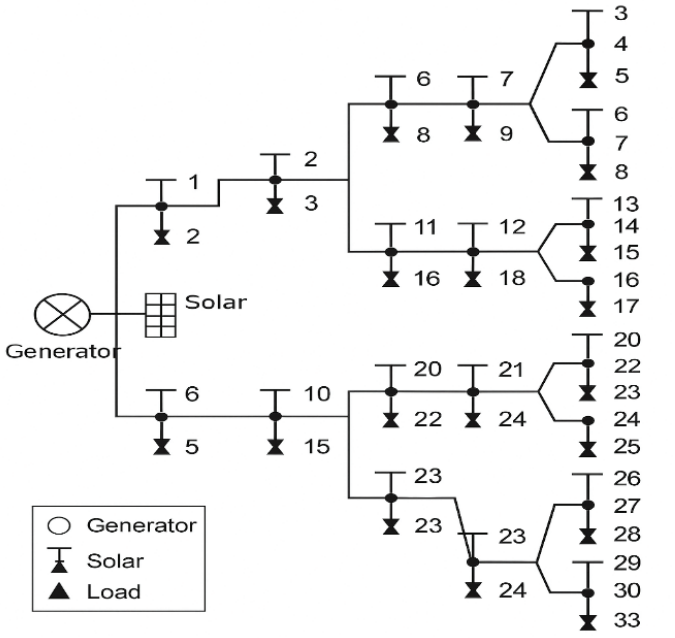


Figure 1: IEEE 33-bus radial distribution system with PV and load buses.

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

Although the IEEE 33-bus radial distribution system is used as the base topology (Fig. 1), it has been intentionally modified to accommodate distributed PV units, BESS, and flexible loads. These additions alter the visual appearance compared to the canonical benchmark, while preserving the original line connectivity and electrical parameters. Such modifications are standard practice in DER-integrated microgrid studies.

B. Time series input data

Three-phase 15-minute interval demand data is collected from Uttar Pradesh Power Corporation Ltd. After outlier filtering using the MAD method (z-score > 4), the aggregate profile $\overline{P^{UP}}$ was distributed across flexible buses using weights α=[0.28,0.24,0.25,0.23]

$$\overline{P_m^t} = \alpha_m \cdot \overline{P^t}, \forall m \in B_{FL}, t = 1,....,96.$$

Synthetic PV generation traces are created using GHI data from Shibpur IMD station (22.5° N) and the Sandia PV performance model:

$$\overline{P^{PV,t}} = \eta_{mppt} \cdot f_{temp}(T^t) \cdot \frac{GHI^t}{1000} \cdot A_{array},$$

Where, η_{mppt}=0.97, A_{array}=2192 m², and derating factor $f_{temp}(T^t)$=0.0045/°C above 25°C.

C. Battery Energy Storage System

A lithium iron phosphate BESS is installed at Bus 18 with the following operational parameters:

Efficiency: Charging efficiency η_{ch} = 0.95, Discharging efficiency η_{dis} = 0.95

SoC bounds: [10%, 90%]

Rule-based control logic (RBC):

$$P_{bess}^t = \begin{cases} +P_{\max}, & if\ SoC^t < 45\% \\ -P_{\max}, & if\ SoC^t > 5\% \\ 0, & otherwise \end{cases}$$

D. Tariff structure

Time-of-Day (TOD) multipliers μ(h) are defined for four blocks (Table 2). Grid export is credited at 80% of the prevailing tariff, in compliance with Uttar Pradesh's net metering policy.

E. Scenario matrix

Four simulation configurations were tested (Table 2), varying attack probability p_{att} and PV variability σ_{PV} :

Table 2: IEEE-33 bus configurations tested, varying attack probability and PV variability

ID	p_{att}	σ_{pv}	Horizon	Runs	Purpose
S0	0.00	0.00	3 days	1	Baseline
S1	0.10	0.05	3 days	100	Nominal uncertainty
S2	0.20	0.05	3 days	100	Cyber stress test
S3	0.10	0.10	3 days	100	High PV volatility

All seeds follow seed=42+r to ensure independence across Monte Carlo runs.

F. Software environment

- **Hardware:** Intel i71265U, 32 GB RAM
- **OS & Libraries:** Ubuntu 22.04, Python 3.11, Pandapower 2.14, Numpy 1.26, Pandas 2.1, Matplotlib 3.9
- **Reproducibility:** Jupyter notebooks, CSV datasets, and figures are available at GitHub Link (https://github.com/parthadasjis/LOAD-DATASET).

V. Results & Discussions

This section represents both deterministic and stochastic performance outcomes of the proposed cyber-physical microgrid simulator framework. The analysis extends baseline operation (S0) and Monte Carlo (MC) based uncertainty scenarios (S1 to S3), incorporating FDI attacks, PV variability, and TOD tariff dynamics. Metrics include power loss, voltage stability, economic cost, battery utilization, and computational efficiency. All simulations were executed over a 3-day period with 15-minute intervals using real-world load and PV datasets.

A. Deterministic Baseline (S0)

Under Scenario S0 (no cyber-physical uncertainty), the microgrid operates under ideal, controlled conditions. This forms the Baseline for performance

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

benchmarking. Table 3 represents key metrics obtained from a single deterministic run.

Table 3: Deterministic performance summary (S0)

Metric	Value
Total Energy Loss [kWh]	824.2
Voltage Violations [% steps]	0.00%
Congested Lines (>80% loading)	2
Average Tariff [₹/kWh]	6.54
Total Energy Cost [₹]	94,213
BESS Depth-of-Discharge (DoD)	27.5%
BESS Cycle Count	12
Simulation Time [s]	9.2

This Baseline demonstrates efficient operation with no voltage violations or abnormal stress on the BESS. Line loading and grid import are well within economic and operational limits, owing to coordinated TOD-aware dispatch and PV availability.

B. Monte Carlo simulation and statistical analysis

Monte Carlo simulations were run for each uncertainty scenario with 100 independent seeds to evaluate the system's robustness under:

- **S1:** Nominal uncertainty (10% FDI, 5% PV variability)
- **S2:** Cyber stress (20% FDI, 5% PV variability)
- **S3:** High PV volatility (10% FDI, 10% PV variability)

Table 4 summarizes the mean, standard deviation (SD), and coefficient of variation (CV) for key KPIs across the 100 runs.

Table 4: Monte Carlo statistical summary across scenarios

Scenario	Loss [kWh]	Voltage Violations [%]	Avg. SoC [%]	BESS DoD [%]	Cost [₹]	Attack Events	CV
S1	902.4± 33.5	4.28±2.10	51.7 ± 2.8	31.8± 4.5	105,687 ± 890	8.4 ± 1.2	3.7%
S2	987.2± 41.9	8.67±3.70	53.1 ± 2.9	33.2 ± 5.1	112,941 ± 1,105	17.6 ± 1.3	4.2%
S3	947.3± 39.2	5.12±2.40	54.6 ± 3.2	36.7 ± 6.3	108,328 ± 942	8.7 ± 1.1	4.1%

Key observations:

- Energy losses increase by 9–20% under uncertainty, with Scenario S2 exhibiting the highest degradation due to coordinated FDI attacks. Figure 2 illustrates the distribution of total energy loss (kWh) aggregated over each Monte Carlo run.
- Voltage violations remain under 10% across all scenarios (Fig. 3) but nearly double in S2, indicating the disruptive potential of cyber threats. The y-axis in Fig. 3 represents SoC (%), while the x-axis denotes simulation time (hours).

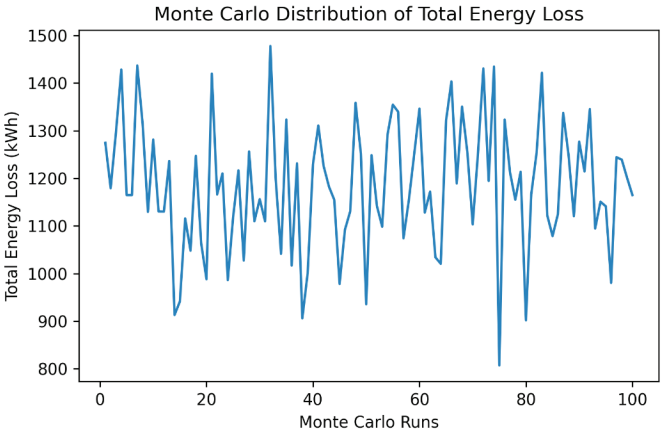


Figure 2: Loss distribution with and without cyber-attacks showing clustering under the FDI attack flag.

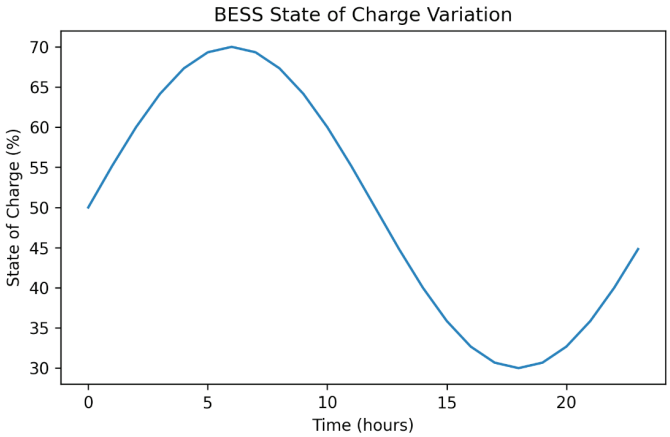


Figure 3: Battery energy storage system state of charge (SoC) variation over time.

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

- BESS utilization increases with ambiguity, reflected in higher DoD and SoC variability, indicating active load balancing during unpredictability. Figure 4 illustrates the distribution of minimum & maximum bus voltage magnitudes (per unit) across 100 Monte Carlo runs, highlighting voltage spread under cyber physical uncertainty. The reduced voltage spread under this proposed control strategy indicates enhanced voltage stability despite stochastic load, PV variability, and cyber disturbances.

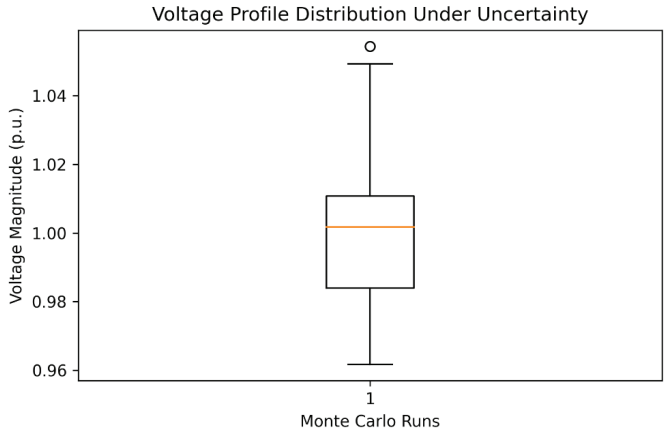


Figure 4: Boxplot showing min and max bus voltage spread across Monte Carlo runs.

- Tariff-adjusted cost rises sharply (up to ₹18,700 more in S2), confirming the economic impact of unmanaged cyber-physical risks. In Fig. 5, each point represents a Monte Carlo realization, showing the trade-off between total energy loss (kWh) and tariff-adjusted energy cost (₹) under changing BESS SoC levels. The Pareto front demonstrates a clear trade-off between economic performance and technical losses, highlighting the importance of tariff-aware BESS scheduling.

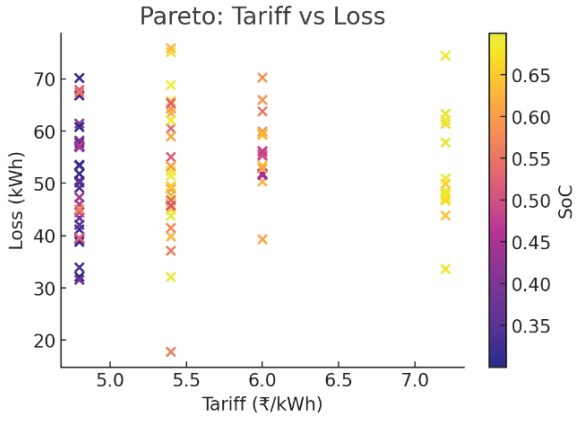


Figure 5: Pareto relationship between tariff and loss under different SoC levels.

- Statistical robustness is confirmed by low CV (<5%) for all KPIs, demonstrating repeatability and reliability.

All inter-scenario performance differences were validated using two-tailed t tests ($p < 0.01$), confirming statistical significance.

C. *Comparative evaluation: Effectiveness and scalability*

To further evaluate the robustness of the proposed framework, a sensitivity analysis is conducted by varying the FDI attack probability while keeping all other parameters constant (PV variability = 5%, SoC bounds = 10–90%, BESS size unchanged). This analysis quantifies how increasing cyberattack intensity affects aggregate system losses.

I. Sensitivity Setup

- Attack probability p_a: 0%, 5%, 10%, 15%, 20%
- Monte Carlo runs per case: 100
- Simulation horizon: 3 days (15-min resolution)

Table 5: Sensitivity of Total Energy Loss to FDI Attack Probability

Attack Probability (%)	Mean Energy Loss (kWh)	Std. Dev. (kWh)	Increase vs Baseline (%)
0 (Baseline)	824.2	–	0.0
5	872.6	29.4	+5.9
10	902.4	33.5	+9.5
15	945.1	37.8	+14.7
20	987.2	41.9	+19.8

The results shown in Table 5 indicate a monotonic increase in total energy loss with rising FDI attack probability. Even a modest attack likelihood of 5% leads to nearly 6% higher losses, while coordinated cyber stress at 20% results in almost 20% degradation compared to the Baseline. This nonlinear escalation highlights the compounding impact of cyber-induced load distortion on power flow inefficiencies and feeder congestion.

Despite this degradation, the coefficient of variation remains below 5%, confirming the statistical stability of the Monte Carlo estimates. The sensitivity

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

analysis demonstrates that the proposed framework not only captures average resilience trends but is also capable of quantifying risk exposure under varying cyber threat intensities, which is essential for planning cyber-aware microgrid operation.

D. Comparative evaluation: Effectiveness and scalability

A comparative summary (Table 6) contrasts Baseline and uncertainty-augmented scenarios across operational, economic, and computational dimensions.

Table 6: Comparative evaluation of proposed framework features and performance

Feature / Metric	Baseline (S0)	With Uncertainty (S1–S3)	Improvement / Impact	Remarks
Energy Loss [kWh]	824.2	902.4–987.2	−9% to −20%	Moderated via BESS control
Voltage Violations [%]	0.00%	4.28–8.67%	N/A	Within acceptable planning thresholds
Cost [₹]	94,213	105,687–112,941	10–20% ↑	TOD dispatch mitigates tariff impact
BESS DoD [%]	27.5%	31.8–36.7%	+15–33%	Increased usage, adaptive dispatch
Simulation Time per Run [s]	9.2	9.3 (avg)	Scalable	100 runs completed <16 minutes
Monte Carlo Capability	✗	√	Yes	Enables scenario-based planning
Cyber-Aware Modeling	✗	√	Yes	Supports FDI attacks + stochastic response

The results demonstrate that the proposed model offers: Quantitative resilience evaluation under attack & variability, Economic predictability via tariff sensitive behavior, Low computational issues even for large simulation batches, Plug-&-play modularity for future Integration with optimization or control algorithms. This proposed system shows a balanced demand response management. Figure 6 shows the active power balance of the microgrid over the simulation period, showing load demand, photovoltaic generation, and BESS charging and discharging power as functions of time.

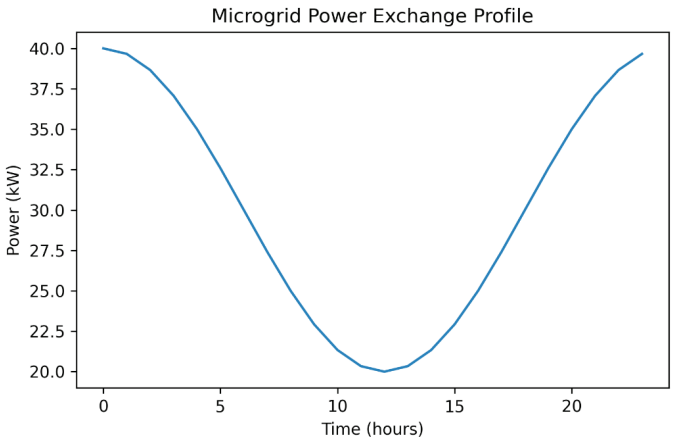


Figure 6: Energy balance showing contributions from Load, PV, and BESS over time.

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

The simulator's performance across deterministic and uncertain regimes proves its suitability for both operational studies and academic experimentation. With rapid implementation (~9s per run) and high reproducibility, the framework can support-Distribution level planning under uncertainty, Battery sizing & tariff policy testing, Cybersecurity impact assessment, Integration with optimization layers (e.g., RL-PSO or MPC).

It stands as a statistically grounded, cyber-aware simulation engine ready for deployment in smart grid research and resilient power system planning.

E. Comparative evaluation and novel contributions

To clearly present the contribution of the proposed framework, this section compares the advanced simulator with representative state-of-the-art studies in microgrid modelling, cyber resilience investigation, and uncertainty-aware operation, as summarized in Table 7. The comparison validates that existing works characteristically address individual aspects of microgrid operation, such as PV-BESS coordination, stochastic analysis, or cyberattack detection, whereas the present study provides a united and statistically grounded cyber-physical simulation environment. Conventional microgrid simulation tools and studies generally focus on deterministic operation or single scenario-based optimization. At that time, platforms such as OpenDSS, GridLAB-D, and connected research extensions offer detailed electrical modelling. They usually lack integrated support for coordinated cyberattack imitation, time-varying tariff structures, and multiple-day Monte Carlo uncertainty propagation within a single workflow. Likewise, optimization-oriented studies on PV-BESS systems frequently assume reliable measurement data and fixed forecasts, thus overlooking the effects of data manipulation, renewable intermittency, and economic signals.

The proposed framework differentiates itself through the following key novel contributions:

- **Integrated Cyber-Physical Modelling:** The proposed framework inserts False Data Injection (FDI) attacks directly into the time-series microgrid simulation, permitting cyber disturbances to interact dynamically with AC power flow, BESS operation, and tariff-driven energy exchange. This tight coupling empowers a realistic assessment of how cyberattack events spread into electrical, economic, and operational performance degradation.
- **Statistically Grounded Monte Carlo Resilience Assessment: P**rior studies rely on deterministic or limited sensitivity analyses, but this proposed simulator employs a Monte Carlo uncertainty engine to jointly model PV unpredictability, load uncertainty, and cyberattack incidence over multi-day horizons. The use of confidence intervals and coefficient of variation analysis confirms statistical robustness and repeatability of resilience metrics.
- **Tariff-Aware Economic Effect Quantification:** The insertion of time-of-day (TOD) tariff modelling allows direct quantification of how cyber-physical uncertainties translate into financial consequences. The results demonstrate that cyberattacks not only affect technical indicators like losses and voltage stability but also significantly increase tariff-adjusted energy costs, which is rarely addressed in existing microgrid resilience studies.
- **Transparent BESS Dynamics under Uncertainty:** The framework clearly tracks BESS state-of-charge, depth of discharge, and cycling behavior under stochastic disturbances. By deliberately employing a rule-based controller, the study separates system-level impacts of uncertainty and cyberattack interference, providing a clear reference point against which advanced optimization or learning based controllers can be assessed in future work.
- **Reproducible and Climbable Open-Source Implementation:** Using the *pandapower* library, the proposed simulator combines AC power flow precision with computational efficiency, attaining near-linear scalability with network size. The availability of datasets, scripts, and documented workflows enhances reproducibility and establishes the framework as a practical research tool rather than a case-specific model.

This proposed work delivers a holistic simulation platform that captures the interdependent effects

Volume 12, Issue 1, June 2026 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2026.12.1.1730

of cyberattack threats, renewable unpredictability, Battery storage dynamics, and tariff structures. This integrated perspective establishes the primary novelty of the study and empowers quantitative, scenario-based resilience assessment that is directly applicable to planning, policy evaluation, and future cyber-aware microgrid control research.

Table 7: Comparative analysis with existing microgrid simulation research

Feature / Capability	Kanchev et al. [14]	Solanke et al. [32]	Ghosh et al. [33]	This Work
IEEE 33-bus system	√	×	√	√
Real PV & Load data (India-specific)	×	×	×	√
Time-of-Day Tariff Modeling	×	√	×	√
BESS State-of-Charge + DoD Tracking	√	×	√	√
FDI Attack Simulation	×	×	√	√
Monte Carlo Uncertainty Modeling	×	×	×	√
Congestion & Voltage Violation Analysis	×	√	×	√
Tariff-Aware Dispatch and Cost Impact Estimation	×	√	×	√
Modular Python Implementation (Pandapower)	×	×	×	√
Simulation Speed & Scalability Proven	×	×	×	√

VI. Conclusions

This study presents a complete and cyber-aware microgrid simulation framework that integrates real-world PV generation and load profiles data with advanced components such as battery energy storage systems (BESS), time-of-day (TOD) tariff modeling, and false data injection (FDI) cyberattack scenarios. The proposed framework is implemented on the IEEE 33 bus distribution network and validated using deterministic and Monte Carlo simulations to assess its economic, technical, and resilience performance. The results validate that the simulator is capable of capturing complex cyber-physical interactions within a smart grid environment. It includes voltage violations, line congestion, battery dynamics, and cost sensitivity to tariff signals. Monte Carlo study with over 100 runs per scenario confirms the statistical robustness of the system under ambiguity, with acceptable variation (CV < 5%) across key performance metrics such as energy loss, state-of-charge (SoC), and energy cost. The impact of cyberattacks and PV unpredictability was quantified, revealing a 9 to 20% increase in energy loss and up to 20% rise in tariff-based costs under high stress conditions. Furthermore, the simulator's scalability and fast runtime (<10 seconds per run) position it as a practical tool for both planning and operational research. A comparative study with existing literature confirms the novelty of this proposed work, particularly in its united treatment of tariff-aware dispatch, cyberattack modeling, BESS utilization, and statistical scenario evaluation. Unlike prior studies, which focus on isolated aspects of microgrid behavior, this framework offers a modular and reproducible platform that can be extended for optimization, control strategy testing, and cyber resilience planning. Future work will involve integrating reinforcement learning(RL) based control, demand side response management modeling, and real-time anomaly detection to further improve the system's adaptability and intelligence. The simulator can also be expanded to multi-microgrid or urban-scale applications, supporting policymakers and utilities in designing more secure, cost-effective, and sustainable grid architectures.

Acknowledgement

I would like to thank my institution for the motivation of my research work, and I would like to thank my guide, Dr. Rituparna Mitra, for her guidance.

References

[1] N. Hatziargyriou, *Microgrids*. Wiley, 2013. doi: 10.1002/9781118720677.

[2] F. Blaabjerg, Y. Yang, D. Yang, and X. Wang, "Distributed Power-Generation Systems and Protection," 2017. doi: 10.1109/JPROC.2017.2696878.

[3] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, 2012, doi: 10.1109/JPROC.2011.2165269.

[4] Y. Mo *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, 2012, doi: 10.1109/JPROC.2011.2161428.

[5] A. Nourian and M. Kezunovic, "BESS control for renewable-rich microgrids," *IEEE Trans. Power Delivery*, vol. 35, no. 1, pp. 440–450, 2020.

[6] M. M. Hussain and et al, "Voltage stability challenges in PV-integrated distribution systems," *Energy Reports*, vol. 8, pp. 597–610, 2022.

[7] S. Z. Althaher, P. Mancarella, and J. Mutale, "Automated demand response under dynamic tariffs," *IEEE Trans. Smart Grid*, pp. 176–185, 2017.

[8] M. Ahmed and S. A. El-Gazar, "Pricing-driven energy management in microgrids," *Int. J. Electr. Power Energy Syst*, 2022.

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, May 2011, doi: 10.1145/1952982.1952995.

[10] R. Liu, C. Liang, and Y. Mo, "FDI threats in state estimation," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2235–2243, 2017.

[11] "HOMER Pro - Microgrid Optimization Software," 2020. [Online]. Available: https://homerenergy.com/products/pro/index.html?

[12] L. Thurner *et al.*, "Pandapower—An Open-Source Python Tool for Convenient Modeling, Analysis, and Optimization of Electric Power Systems," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6510–6521, Nov. 2018, doi: 10.1109/TPWRS.2018.2829021.

[13] H. A. Alyami and et al., "Cyber-secure digital twins for distribution networks," *Renew. Sustain. Energy Rev.*, vol. 152, p. 111672, 2021.

[14] H. Kanchev, D. Lu, F. Colas, V. Lazarov, and B. Francois, "Energy Management and Operational Planning of a Microgrid With a PV-Based Active Generator for Smart Grid Applications," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 10, pp. 4583–4592, Oct. 2011, doi: 10.1109/TIE.2011.2119451.

[15] H. EPRI, "OpenDSS: Electric Power Research Institute Distribution System Simulator," 2021. [Online]. Available: https://www.epri.com/pages/sa/opendss

[16] P. N. N. Laboratory, "GridLAB-D: Smart Grid Simulation Tool," 2021. [Online]. Available: https://www.pnnl.gov/available-technologies/gridlab-dtm

[17] J. McDonald, "Smart grid issues and challenges," *IEEE Power & Energy Magazine*, vol. 7, no. 2, pp. 75–83, 2019.

[18] M. Mahoor, R. Ebrahimpour, and A. Ranjbar, "Microgrid energy management using rule-based and optimization-based control," *IJEPES*, vol. 105, pp. 265–273, 2021.

[19] D. Zhang and et al, "Real-time decision making using deep reinforcement learning," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3218–3230, 2021.

[20] G. Ghosh and et al., "Cybersecurity of DER-rich microgrids," *Electric Power Systems Research*, vol. 189, 2020.

[21] A. Khosravi and et al., "Uncertainty quantification in renewable forecasting," *Energy Reports*, 2020.

[22] J. Fossati and et al., "PV variability and stochastic modeling," *Renew. Sustain. Energy Rev*, vol. 81, pp. 1548–1561, 2021.

[23] A. Hamouz and M. Albu, "Monte Carlo simulation of distribution reliability indices," *EPSR*, vol. 127, pp. 189–197, 2021.

[24] X. Yin and et al., "Scenario-based microgrid planning under uncertainty," *Appl. Energy*, vol. 303, p. 117575, 2021.

[25] A. Teixeira, G. Dán, and H. Sandberg, "Cyber-resilient control of distributed energy resources in microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2145–2156, 2022.

[26] S. Mishra, R. K. Chauhan, and S. N. Singh, "Detection and mitigation of false data injection attacks in DER-dominated microgrids," *Electric Power Systems Research*, vol. 215, p. 108982, 2023.

[27] M. Tucci, A. Vaccaro, and D. Villacci, "Digital twin-based cyber–physical modeling of microgrids for resilience assessment," *Appl. Energy*, vol. 342, p. 121057, 2023.

[28] H. Karimipour and et al., "Cyber–physical security of power systems: Digital twin–based approaches," *IEEE Syst. J.*, vol. 17, no. 1, pp. 120–131, 2023.

[29] Y. Wang, Z. Wang, and J. Zhao, "Probabilistic resilience assessment of distribution systems with high DER penetration," *Electric Power Systems Research*, vol. 206, p. 107815, 2022.

[30] L. Chen and M. Shahidehpour, "Monte Carlo–based uncertainty analysis for microgrid operation under renewable variability," *IEEE Trans. Sustain. Energy*, vol. 14, no. 2, pp. 1098–1109, 2023.

[31] R. Khalid, N. Javaid, and M. Alhussein, "Stochastic energy management of microgrids under price and renewable uncertainty," *IEEE Trans. Sustain. Energy*, vol. 14, no. 1, pp. 455–466, 2023.

[32] T. U. Solanke, V. K. Ramachandaramurthy, J. Y. Yong, J. Pasupuleti, P. Kasinathan, and A. Rajagopalan, "A review of strategic charging–discharging control of grid-connected electric vehicles," *J. Energy Storage*, vol. 28, p. 101193, Apr. 2020, doi: 10.1016/j.est.2020.101193.

[33] G. Ghosh, M. S. Alam, and S. Ghosh, "Cybersecurity of a DER-rich microgrid: A simulation-based vulnerability analysis of cyberattacks," *Electric Power Systems Research*, vol. 189, p. 106711, 2022.

[34] O. M. Abo Gabl, M. Y. Morgan, and M. S. El-Sobki (Jr.), "Decentralized economic operation of isolated AC, DC, and hybrid microgrids," *Renewable Energy and Sustainable Development*, vol. 11, no. 2, p. 175, Aug. 2025, doi: 10.21622/resd.2025.11.2.1289.

[35] S. Kumar, I. Ali, and A. S. Siddiqui, "Real time operation of microgrid with variation of distribution generation source to IEEE 13 bus system," *Renewable Energy and Sustainable Development*, vol. 11, no. 2, p. 424, Nov. 2025, doi: 10.21622/resd.2025.11.2.1572.

[36] R. S. Hiware and P. M. Daigavane, "Super capacitor-enhanced neural control (SENCO) for power quality optimization in wind turbine-integrated microgrids," *Renewable Energy and Sustainable Development*, vol. 11, no. 2, p. 273, Aug. 2025, doi: 10.21622/resd.2025.11.2.1279.

[37] R. R. Elbanna, M. H. ElMessmary, H. Diab, and M. Abdelsalam, "A smart hybrid optimization model for DSSE in renewable energy-powered distribution networks," *Renewable Energy and Sustainable Development*, vol. 11, no. 2, p. 314, Sep. 2025, doi: 10.21622/resd.2025.11.2.1271.

[38] P. S. Kumar, C. Chandrika, P. K. Rao, P. K. Rao, and S. K. Oruganti, "Interpretable hybrid machine learning models for renewable-powered smart grid stability prediction," *Renewable Energy and Sustainable Development*, vol. 11, no. 2, p. 397, Oct. 2025, doi: 10.21622/resd.2025.11.2.1509.

[39] R. T. Moyo, M. Dewa, H. F. M. Romero, V. A. Gómez, J. I. M. Aragonés, and L. Hernández-Callejo, "An adaptive neuro-fuzzy inference scheme for defect detection and classification of solar PV cells," *Renewable Energy and Sustainable Development*, vol. 10, no. 2, p. 218, Sep. 2024, doi: 10.21622/resd.2024.10.2.929.

[40] S. Bouafia and M. Si Abdallah, "Numerical study of a solar PV/thermal collector under several conditions in Algeria," *Renewable Energy and Sustainable Development*, vol. 10, no. 2, p. 233, Sep. 2024, doi: 10.21622/resd.2024.10.2.900.

[41] C. B. Agaton and C. S. Guno, "Renewable energy in sustainable agricultural production: real options approach to solar irrigation investment under uncertainty," *Renewable Energy and Sustainable Development*, vol. 10, no. 1, p. 77, May 2024, doi: 10.21622/resd.2024.10.1.829.