Cybersecurity Management of Power System Data: An Agent-Based Simulation Approach

Daniil Hulak[1, *,†], Maryna Petchenko[3,†], Oleksandr Yakushev[1, 2,†] and Ruslan Naboka[1,†]

[1] *Kherson National Technical University, Institutska 11, 29016, Khmelnitsky, Ukraine*

[2] *Cherkasy State Technological University, Shevchenka 460, 18006, Cherkasy, Ukraine*

[3] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract

The rapid digitalisation of the power sector has increased both the availability of operational data and the vulnerability of critical infrastructures to cyberattacks. Lessons learnt from the Ukrainian case, where insufficient protection of open system data facilitated targeted strikes on energy assets, this paper explores how access-control and data-sanitisation measures can mitigate such risks. We develop an agent-based simulation framework to model interactions of benign users and attackers across 16 scenarios combining different authentication policies and data-masking strategies. Results reveal a clear trade-off between security and usability: open access maximises data utility but exposes the system to high risks, while restrictive policies achieve near-complete protection at the cost of user experience. The most effective outcomes are found along the Pareto frontier, where moderate access controls combined with balanced sanitisation deliver a practical compromise. These findings provide guidance for regulators and system operators in designing secure and functional data-sharing frameworks for power systems.

Keywords

access control, cybersecurity, power systems, open data

1. Introduction

At present, we are living in a world where the volume of data is rapidly growing, creating significant opportunities for innovation, collaboration, and decision-making. However, this growth is also accompanied by an increasing number of security issues, as sensitive data becomes a more attractive target for malicious actors. The need for robust and resilient cybersecurity measures has therefore never been greater, particularly in critical and vulnerable sectors of the economy, where improper data use can have severe societal, financial, and even national security consequences. The electric power sector [1], traditionally seen as a conservative industry, has no exceptions to particular trends, as it faces digitalisation challenges with a rapidly growing volume of data.

Before February 2022, the National Energy and Utilities Regulatory Commission of Ukraine implemented transparent policies for power market operators, ensuring broad access to power system infrastructure data in line with European Union (EU) directives, such as the Third Energy Package, Regulation on Wholesale Energy Market Integrity and Transparency [2], and the ENTSO-E Transparency Regulation [3]. However, insufficient cybersecurity measures led to unintended data leaks, which in turn facilitated the targeting and destruction of generators, substations, and other critical power system equipment. As a result, Ukraine has lost nearly 10 GW of generation capacity [4], representing around one-sixth of its total installed capacity. The destruction of these facilities has destabilised the energy system, resulting in widespread power outages.

Currently, Ukraine has severely limited access to all power system-related data in response to the security threats arising from the war conflict. By contrast, many EU countries, such as Germany and France, as well as past EU members like the United Kingdom, continue to provide broad public access to power market data, including grid availability, generation capacity, outage data, etc., in line with EU transparency regulations requirements. While such an approach is essential for market efficiency,

[1] *SMICS'25: Workshop on Cryptology and Data Security, October 16-18, 2025, Lviv, Ukraine*

[*] Corresponding author

[†] These authors contributed equally.

d.hulak@chdtu.edu.ua (D. Hulak), marinapetcenko@gmail.com (M. Petchenko), aleksandro@i.ua (O. Yakushev), rusnaboka@gmail.com (R. Naboka)

0000-0001-8840-3557 (D.Hulak) 0000-0003-1104-5717 (M. Petchenko), 0000-0002-0699-1795 (O. Yakushev), 0000-0002-3417-8216 (R. Naboka)

it is often implemented without cybersecurity protection measures. Although these countries are not currently involved in any direct military conflicts, the Ukrainian case demonstrates that their cybersecurity practices require careful reconsideration to prevent threats based on available infrastructure data.

Accordingly, this research paper presents a novel, simulation-based study that evaluates how different access-control measures and data sanitisation approaches influence both the security and the utility of power system data for users. By analysing cybersecurity policy measures, we identify trade-offs between cybersecurity and transparency and identify configurations that achieve the most effective balance. The findings aim to support regulators and power system operators in designing access frameworks for data that will safeguard critical infrastructure while maintaining market functionality.

The remainder of the paper is structured as follows. Section 2 reviews the state-of-the-art literature on cybersecurity measures and data transparency in power systems. Section 3 introduces the methods applied in our simulation framework, while Section 4 presents and discusses the results. Finally, Section 5 concludes the paper and outlines implications for future policy and research.

2. Review of state-of-the-art

To establish the background for this study, we began with an analysis of publications indexed in the Scopus database on the topic of cybersecurity. A detailed overview of this analysis is presented in Figure 1. The left part of the figure illustrates the considerable growth in the overall number of papers published on cybersecurity in recent years. In contrast, research specifically addressing cybersecurity in power systems remains comparatively limited. Furthermore, the publications tagged with both ‘cybersecurity’ and ‘simulation’ reveal a clear lack of contributions involving practical applications or experimental validation, reflecting mostly the theoretical character of existing studies.

The right side of Figure 1 presents the results of a textual analysis of abstracts from papers related to power system cybersecurity, conducted using the Text Analytics Toolbox of MATLAB [5]. This analysis highlights the most frequently occurring terms, such as attack, power system/grid security, reserve, control, etc. However, the absence of the term simulation in this analysis reinforces the observation that current research in the cybersecurity domain largely lacks simulation-based approaches and real-world experimental investigations.

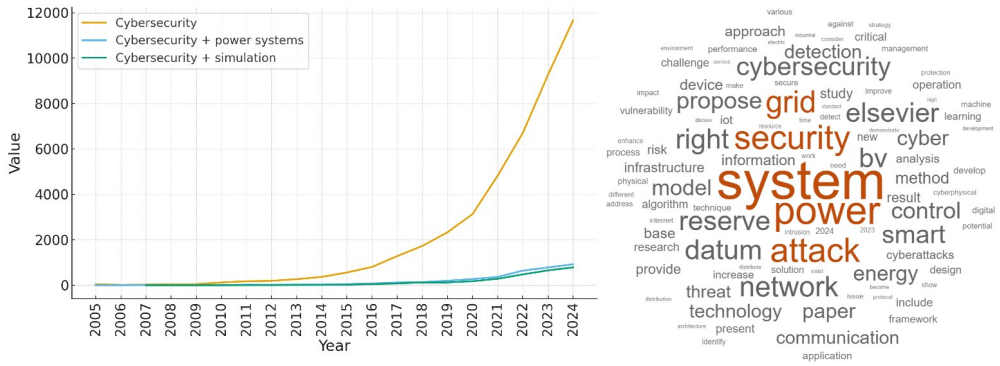

Figure 1: Analysis of the publications on cybersecurity-related topics

Narrowing the research to particular points, we identify that recently published papers on cybersecurity simulations in power systems show both progress and constant gaps. For instance, authors of [6] provide a comprehensive review of simulation, detection, and mitigation approaches, noting that most contributions remain theoretical and that few practical simulation frameworks are available to validate effectiveness in realistic conditions. Paper [7] attempts to bridge this gap through a co-simulation environment that integrates power system and communication network simulators to replicate data attacks on Energy Management Systems (EMS). While this represents an important advance in modelling cyber-physical threats, it remains technically complex and narrowly

focused on operational EMS vulnerabilities.

By contrast, the study presented integrates a higher-level simulation approach that evaluates cybersecurity–utility trade-offs in open data portals of power system operators. Rather than modelling low-level network attacks, we assess how combinations of access-control measures and data-sanitisation strategies affect both attacker success rates and the usability of information for users.

3. Methods

To evaluate the trade-offs between security and usability in power system open data portals, we developed a simulation framework that models the interactions of benign users and attackers under different access-control and data-sanitisation settings. The experiment was designed to replicate realistic user behavior, where users seek reliable data access while hackers attempt to extract sensitive information. The framework proposed enables a systematic comparison of how various policies influence both cybersecurity resilience and data utility.

The scenarios in Table 1 represent the framework and are denoted as Px/Dy, where P refers to the access-control policy and D to the level of data sanitisation. Policies include: P0 - open access with only minimal protection; P1 – combination of Application Programming Interface (API) and Web Application Firewall (WAF), filters traffic and basic rate-limiting is applied; P2 - requires user verification and two-factor authentication (2FA) with stronger rate-limiting; and P3 - combines 2FA with mutual Transport Layer Security (mTLS), the strongest authentication method considered. Data sanitisation levels include: D0 - information is published without masking; D1 - slightly displaces geospatial data to the level of ±0.5–1.5 km; D2 - provides data at a coarser resolution of 1–2 km with hexagonal aggregation; and D3 - blurred data is available to the public and exact data only to verified users. The concept of data utility reflects how useful the released data remains for legitimate (benign) users. Exact data (D0) offers maximum utility, while geomasking and aggregation (D1, D2) reduce precision and thus lower utility. Tiered access (D3) strikes a balance, maintaining relatively high utility for trusted users while reducing exposure to potential attackers.

Table 1
Experimental scenarios combining access-control policies (P0–P3) and data-sanitisation strategies (D0–D3)

Policy	Sanitisation			
	D0 -exact data	D1 - geomask-ing	D2 - hexagonal aggrega-tion	D3 - tiered access
P0 - open access, minimal WAF	P0/ D0	P0/D1	P0/D2	P0/D3
P1 - API + stronger WAF, basic rate-limit	P1/ D0	P1/D1	P1/D2	P1/D3
P2 - verified users + 2FA + strong rate-limit	P2/ D0	P2/D1	P2/D2	P2/D3
P3 - 2FA + mTLS, highest block rate	P3/ D0	P3/D1	P3/D2	P3/D3

For each scenario, we simulated 2000 user sessions, with users randomly assigned as benign ($p_b = 0.85$) or attackers ($p_a = 0.15$). The number of requests per session was drawn from a Poisson distribution [8] $\lambda = 5$ for benign users, $\lambda = 8$ for attackers. At each request step, the probability of blocking was defined as:

$$p_{\text{block}}(t) = min\left(p_{\text{base}} + \text{ratelimit} \cdot t/R - 1, 0.99\right)(1), \text{with the base value}$$

$$p_{\text{base}} = 1 - (1 - p_{\text{WAF}})(1 - p_{\text{2FA}})(1 - p_{\text{mTLS}})(2),$$

where R - number of requests in a session, t - index of the request within a session, $p_{\text{block}}(t)$ - probability that the request t is blocked, p_{base} - base blocking probability depending on WAF, 2FA, and mTLS, $p_{\text{WAF}}, p_{\text{2FA}}, p_{\text{mTLS}}$ - blocking strengths of WAF, 2FA, and mTLS certificates.

A uniform random draw determined whether the request was blocked and possibly ended by cooldown (with the probability of 0.0 for P0 up to 0.6 for P3) or allowed. If allowed, benign users accessed data with a session utility:

$$U_{\text{session}} = U_{\text{base}} \cdot (1 - \text{blocks}/R)(3),$$

where U_{session} - utility of a benign session after sanitisation and blocking, U_{base} - reflected sanitisation (1.0 for D0, 0.85 for D1, 0.75 for D2, 0.88 for D3). Attackers, on the other hand, had a 25% chance per request of hitting sensitive content, which was useful with probability p_{useful} (1.0, 0.7, 0.45, 0.4 for D0–D3 respectively). A successful hit marked the session as compromised and recorded the time to first exfiltration (TFE).

Scenario outcomes were then aggregated into four main metrics: attacker success rate (P_{success}), TFE, benign utility, and average blocks per session and security. Mathematical representation of some of the evaluation metrics is as follows:

$$P_{\text{success}} = \frac{\text{Successful attacker sessions}}{\text{Total attacker sessions}} \ (4),$$

$$\text{Security} = 1 - P_{\text{success}} \ (5),$$

Finally, each scenario was mapped in the Security–Utility space, and Pareto frontier analysis was applied to identify the most effective trade-offs between resilience and usability by comparing all scenarios and selecting those for which no other configuration performed strictly better in both dimensions.

4. Results and Discussion

The results of the simulation are shown, and the trade-off between security and utility across all scenarios is illustrated in Figure 2.

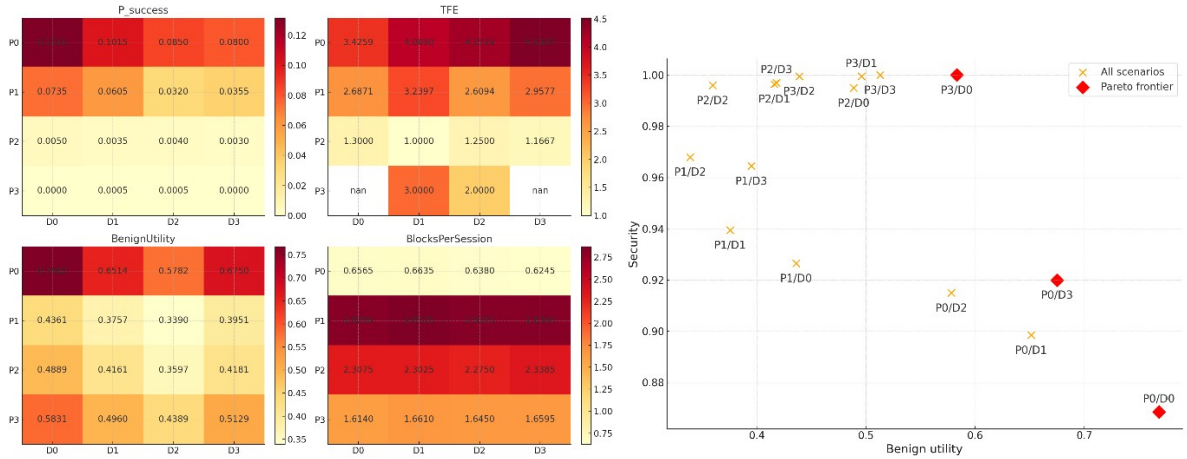

Figure 2: Analysis of the publications on cybersecurity-related topics

The results show a clear trade-off between security and data usability across the 16 simulated scenarios. For clarity the results are presented as a heatmap diagram, where each metric is shown across all policies (P0–P3) and sanitisation strategies (D0–D3). Open access with exact data (P0/D0) provides the highest utility but the weakest security, while stricter measures such as mTLS with strong sanitisation (P3/D2–D3) result in near-zero attacker success rates at the cost of reduced usability for benign users. Intermediate configurations, particularly P1/D2 and P2/D3, appear on the Pareto frontier, shown in Figure 2, demonstrating that combining moderate access controls with balanced sanitisation can significantly reduce attacker success without excessively insulting user experience. These findings highlight that neither extreme openness nor excessive restriction is optimal, but instead, hybrid approaches deliver the most effective balance for securing critical power system data.

5. Conclusions

This study demonstrated how different combinations of access-control policies and data-sanitisation strategies influence both the resilience of power system data portals against cyberattacks and the usability of information for users. Based on 16 simulation scenarios, we showed that extreme openness maximises utility but exposes infrastructure to high risks, while overly restrictive measures protect security at the expense of usability. The most effective outcomes lie along the Pareto frontier, where moderate controls and balanced sanitisation achieve a favourable compromise. These insights provide practical guidance for power system operators and policy makers in designing secure and functional data-sharing frameworks for critical energy infrastructures.

Declaration on Generative AI

During the preparation of this work, the authors used GPT-5 and Grammarly in order to check English grammar and spelling. References in the paper are automatically generated by the Word embedded Mendeley Cite tool. No concepts or ideas were generated by AI. After using these tools, the authors reviewed the content as needed and took full responsibility for the publication's content.

References

[1] O. Yakushev, D. Hulak, O. Zakharova, Y. Kovalenko, O. Yakusheva, and O. Chernyshov, "Management of the modern electric-vehicle market," Polityka Energetyczna – Energy Policy Journal, vol. 25, no. 2, pp. 85–108, 2022.

[2] "I OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2011 on wholesale energy market integrity and transparency (Text with EEA relevance)".

[3] "II of 14 June 2013 on submission and publication of data in electricity markets and amending Annex I to *Regulation* (EC) No 714/2009 of the European Parliament and of the Council (Text

with EEA relevance)".
[4] T. Kurbatova, R. Sidortsov, G. Trypolska, D. Hulak, and I. Sotnyk, "Maintaining Ukraine's Grid Reliability under Rapid Growth of Renewable Electricity Share: Challenges in the Pre-War, War-Time, and Post-War Periods," *International Journal of Sustainable Energy Planning and Management*, vol. 40, pp. 39–51, 2024.
[5] R. E. Banchs, "Text Mining with MATLAB®: Second Edition," *Text Mining with MATLAB®: Second Edition*, pp. 1–475, Jan. 2021.
[6] M. Beikbabaei, A. Mehrizi-Sani, C.-C. Liu, M. Correspondence, and B. Beikbabaei, "State-of-the-art of cybersecurity in the power system: Simulation, detection, mitigation, and research gaps," *IET Generation, Transmission & Distribution*, vol. 19, no. 1, p. e70006, Jan. 2025.
[7] K. Pan, A. Teixeira, C. D. Lopez, and P. Palensky, "Co-simulation for cyber security analysis: Data attacks against energy management system," *2017 IEEE International Conference on Smart Grid Communications, SmartGridComm 2017*, vol. 2018-January, pp. 253–258, Jul. 2017.
[8] D. I. Inouye, E. Yang, G. I. Allen, and P. Ravikumar, "A review of multivariate distributions for count data derived from the Poisson distribution," *Wiley Interdiscip Rev Comput Stat*, vol. 9, no. 3, p. e1398, May 2017.