Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Smart Grid Security Through Cyber Threat Intelligence

[1]Pradnya Kawade, [2]Dr. Ashwini Dalvi
[1]*Department of IT (Information Security), K. J. Somaiya College of Engineering, Mumbai, India*
Email: pdnykawade12@gmail.com
[2]*Assistant Professor, Department of IT (Information Security), K. J. Somaiya College of Engineering, Mumbai, India*
Email: ashwinidalvi@somaiya.edu

ARTICLE INFO

Received: 24 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Energy sector digitization is rapidly increasing through technologies such as smart grid deployment and cyber physical power systems (CPPSs). It has enhanced the efficiency and sustainability of energy infrastructure. However, this transformation has also increased the attack surface for smart energy systems. There are several cases related to cyber-attacks and security breaches of smart grids reported. Cyber criminals release breached data on different platforms like dark web, hacker forums. This case study evaluates how the breached data can be misused by cyber criminals to further disrupt smart grid operations. The definite goal of this work is to create cyber threat intelligence for smart grids from breached dataset. Synthetic dataset of power grid available on the Dark-Net market archive is used in the proposed work. An intelligent model for smart grids is developed to identify confidential information exposed in the data breaches. Threat modelling is done to analyse potential threats to the compromised power grid. In real world, this study gives energy sector a proactive approach to analyse breached dataset. By understanding impact of threats, energy providers can strengthen the security posture of smart grid. This work highlights the importance of cyber threat intelligence for smart grid's security.

Keywords: Smart Grid, Cyber Threat Intelligence, Threat Modeling, Cyber Physical Power Systems

1. INTRODUCTION

The transformation in global energy sector have developed an efficient power infrastructure. Smart grids are advanced electrical power systems which combines both the traditional power grid infrastructure with advanced information and communication technology. It is one of the critical infrastructures which provides real time monitoring and control of power flow from generation to consumption. Smart grids are built on cyber physical systems (CPSs) also known as cyber physical power systems (CPPSs). CPSs integrate the functions such as networking, sensing, computation and control into physical infrastructure. Interconnecting cyber and physical worlds can give rise to new security challenges and they currently become one of the main targets for hackers. Thus, securing smart grid is most important factor for efficient, reliable and sustainable energy infrastructure. Understanding the threat landscape and implementing security measures is important for smart grid industries. There are several cases related to cyber-attacks on power grids reported. Cyber criminals release this breached data on different platforms like dark web, hacker forums. This confidential data can be leveraged by attackers to further infiltrate and disrupt the functionality of power grid.

The proposed work aims to enhance the security of smart grid through cyber threat intelligence. An intelligent analytical model for smart grids is developed to identify confidential information exposed in the data breaches. Energy providers can use this model after data breach to analyse confidential and high-risk components included in a compromised data. Cyber-attacks on smart grid can cause power supply disruption, huge financial loss, reputation damage and can create negative economic impact. If energy providers are successful to analyse the risk associated, they can initiate implementing proactive security controls.

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In this work we have used the synthetic data like the breached dataset of smart grid available on the Dark-Net market archive. The dataset contains CAD files of power substation's network layouts from multiple locations. It includes various substations, control centre layouts, substation-interconnections, power parameters etc. A thorough analysis of the dataset is done to understand cyber threats to the system. All CAD files from the dataset are converted into high resolution images. Optical character recognition model is used to extract texts from all the network layout images. The extracted raw texts are analysed by using Named Entity Recognition (NER) model specifically trained for smart grids. The model can analyse the various entities present in dataset. The recognized entities can be then used for threat modelling of the compromised power grid to analyse potential threats. Potential threats need to be analysed on an emergency basis for the compromised resources so that energy providers can implement proactive defence measures. Implementing proactive defences will reduce the risk of further potential attacks.

2. LITERATURE REVIEW

2.1.Threat Intelligence for Power Systems

There are many cyber-attacks reported on smart grid around the world like slammer worm of the David-besse nuclear plant in ohio, USA on 2003, SCADA system in the nuclear power plant attacked by Stuxnet worm in Iran on 2009 & 2010, Ukraine cyber attack in December 2015 leading to the loss of power for about 225,000 customers which were considered as the worst blackout caused by cyber-attack in power system history discussed in Alomari et.al [1]. There are various studies done previously for understanding cyber security challenges of power grids and implementing security controls discussed in S. Amanlou et al., [11]. The study in [1, 9] explores potential cyber attacks and threats to power systems. Cyber criminals steal this smart grid confidential data and release it on dark web which can be misused by anyone. The study in Sangher et al.,[12] has developed a cyber threat intelligence system for dark web forum content to identify cyber crimes. A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid is done in Yohanandhan et al.,[14]. There are different approaches for securing the power grid presented in previous studies Krause et al., Zhang Y et al., [8,15]. Deep learning and hybrid security models are discussed in Dayarathne et al., [3] that will help mitigating various cyber attacks like false data injection, Man-in-the-Middle Attack, Replay attack etc. The proposed work here is focused on creating cyber threat intelligence for smart grid using the breached data. This threat intelligence data can be used to analyse high risk areas and sensitive components in a data breach. It is important for smart grid to understand the associated threats and mitigation strategies to prevent from future attacks.

2.2. Threat Modelling for Smart Grids

Threat modelling is used to highlight high risk threats for the targeted power grid. Various studies done on the risk assessment strategies for power grids Rahim f. a. et al., [10], but these techniques provide limited inputs for risk analysis. The researchers have used STRIDE and DREAD based model approach for threat modelling in study proposed by Bhaskar N. et al., [2]. The research in Ghadi Y. Y. et al., [5] proposed a security risks models by using big data and artificial intelligence for various attack scenarios in smart grid. All these threat modelling techniques uses previous attack scenarios and power grid's present condition. In this research work threat modelling of compromised power grid is done based on its analysed sensitive interconnected components.

3. CYBER THREAT INTELLIGENCE FOR SMART GRID

3.1.Synthetic Data Discussion

The synthetic breached dataset contains CAD files of power grid's substations located in overall Mumbai, India. The dataset includes 66 files, and all of these are in AutoCAD drawing file i.e. .dwg file format. The layouts of various power generation and receiving stations are present in the dataset. It contains power system's control centre (PSCC) floor plan and supply layouts of energy provider. The power grid's operations are centrally controlled from Power System Control Centre (PSCC) through SCADA system. The layouts also include network connections of various power companies, electrical equipment and their power parameters etc. Unauthorized access to power grid data could potentially lead to disruptions in the supply of electricity, manipulation of control systems leading to power outages.

3.2. Proposed Methodology

The work focuses on creating cyber threat intelligence for smart grid from breached dataset. The CAD files (.dwg) from dataset are converted into image (.jpg) format for analysis. The vital information from these images is extracted

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

by using Optical Character Recognition (OCR) model. OCR is used for text recognition from digital image and convert it into machine readable data. In this work Tesseract is used for text extraction from the images which is an open-source OCR engine developed by Google. The text extracted from images are in raw format. These texts are first pre-processed to correct the word in case if there are some issues in OCR and to remove unwanted characters or spaces. As OCR is not able to extract each and every word, Levenshtein Distance is used to check the closest match as per the entities and to correct the word. Figure 1 describes the detailed methodology.

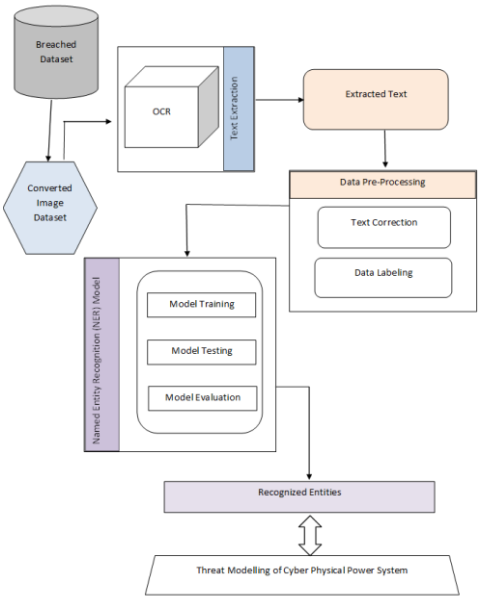

Figure 1: Proposed Methodology

The raw texts are recognised by using Named Entity Recognition (NER) model. NER model is a type of Natural Language Processing (NLP) model designed to recognize and categorize entities defined in the dataset. Entities defined in this work are Sub-Station, Sub-Station Interconnection, Power Company, Organization, Receiving Station (R/S), Generating Station, Control Centre, Power Parameter, Electrical Equipment, Railway Feeder, Busbar Section. NER requires a dataset labelled in a specific format to specify what type of entity it represents. The custom trained NER model for smart grid is built by using spaCy library in Python. The entity annotations in spaCy is done as {Image ID, [(start index, end index, entity type)]},

For e.g., Format: {1 POWER NETWORK LAYOUT - Temp-Model.jpg, [(11, 18, SUBSTATION), (50, 54, POWER COMPANY), (56,60, SUBSTATION INTERCONNECTION)]},

Figure 2: Entity Annotations

Figure 2 shows some of the entity annotations for network images in labelled dataset. This labelled dataset is used to train the NER model. The NER model is trained with 200 epochs and during each epoch the model try to capture

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

different patterns in the data and the model's parameters gets updated. The model's evaluation is done by testing it on the synthetic power grid's dataset. This test data is similar to breached data on which the model is trained and substations from different regions of India are included. The test data on which model's performance is tested is shown in figure 3. The model has been tested on 3 test datasets for the better analysis.

Figure 3: Test Data

4. RESULTS

The NER model predicts entity labels for each word in a sequence, and the loss is calculated based on the dissimilarity between these predictions and the true labels. During training, the model improves its ability to recognize named entities in text and minimize the loss. Figure 4, NER model output shows the detailed recognised entities by the NER model w.r.t their labels. These recognised entities can be used to analyse high risk areas of which the security needs to be enhanced.

{'POWER PARAMETER': ['MVA', 'A', 'KV', 'AO', 'MW', 'MVAR'], 'ELECTRICAL EQUIPMENT': ['PT', 'DT', 'ICT', 'TRF', 'AT'],
'POWER VALUES': ['33KV', '145KV', '110KV', '220KV', '22KV', '400KV'], 'POWER COMPANY': ['BEST','AEML', 'TPC', 'MSEB','NTPC','MSEDCL', 'TATA POWER', 'MSETCL'],
'CONTROL CENTER': ['ANAAPARKING SIDE','DC SYSTEM','LOUNGE ENTRANCE','SPARE COLORCHEM BAPGAON PUNE','AC ROOM ROOM','ENGG. ROOM','CHILLER PLANT','SERVER','DRAWING NO', 'LOCKERS CONFERENCE DMS ROOM','OFFICE', 'EMERGENCYY EXIT','RAW MENS','PANTRY','DIVEAGAR', 'OLD KARVENAGAR', 'AHU ROOM', 'SERVER ROOM', 'AC MAIN UNIT', 'IT COMMUN', 'PASHAN', 'PANEL', 'UPS ROOM', '~IANKHURD', 'CENTRAL OFFICE CONFERENCE OFFICE CCTV-2', 'GANDHINAGAR DABHOI', 'EMERGENCY', 'ARE HERE', 'STAIR SN\\- FIRE CASE TO ROOM', 'SERVER DESK', 'GOA PANAJI', 'SW ROOM', 'EMERGENCY EXIT', 'SPARE ALD CCTV-2', 'CONTROL ROOM', 'RIGHT MOST CUPBOARD', 'LAYOUT', 'CENTRAL ELSTER', 'GR FLOOR', 'OFFICE AREA', 'AHU', 'EXTINGUISHER ASSEMBLY AREA', 'UPS ROOM BACK SIDE', 'LADIES REST ROOM', 'AC ROOM', 'TERRACE', 'EXTINGUISHER I ASSEMBLY AREA', 'PSCC', 'SPARE'],
'SUBSTATION INTERCONNECTION': ['KHRD-VAGH', 'MANGAON-GOREGAON', 'KALYANINAGAR-VAGHOLI', 'KARJAT-AHMEDNAGAR', 'CASE N', 'VARSOVA-POWTRANSFER', 'KOREGAON-SHIVAJINAGAR', 'VAGHOLI-KARVENAGAR', 'MAHAD-RAIGAD', 'SAL-POWAI', 'MHD-RGD', 'TR-CAR', 'DH-TR', 'KARVENAGAR-VAGHOLI', 'KOREGAON-VAGHOLI', 'PASHAN-BANER'],
'ORGANIZATION': ['MLG', 'BPCL', 'RCSHPCL', 'HPCL', 'PRG', 'TVK', 'DSM', 'KVD', 'NPT', 'RVS', 'SSB'],
'SUBSTATION': ['GARBADA', 'MATITHON', 'KANPUR', 'VRINDAVAN', 'SAKHAR', 'KOLSHET', 'KALYANINAGAR', 'SHIVPURI', 'AGRA', 'KARVENAGAR', 'KOCHI', 'KHIRA', 'BACKBAY', 'SAGAR', 'CARNAC', 'TROMBAY', 'MALAVALI', 'KANDVALI', 'VRDN', 'KOPARGAON', 'AMRITSAR', 'PANSHET', 'MAHAD', 'MCZMW', 'ASNAA', 'KHOPOLI', 'DAPOLI', 'KOTA', 'S/S'],
'RECEIVING STATION': ['R/S', 'MRSS'],
'GENERATING STATION': ['UAT', 'G/S', 'GT', 'GEN'],
'RAILWAY FEEDER': ['W.RLY', 'C.RLY', 'RLY', 'WARLY'],
'BUSBAR SECTION': ['BS II', 'BS I']}

Figure 4: NER Output

NER model has successfully identified defined entities from the test data. Model is tested on 3 test datasets related to power grid, and it has given approximately 94% accuracy. The accuracy is calculated manually w.r.t. all the test data outputs.

Even though NER models are not able to detect completely unknown data, which is out of vocabulary, unknown substations, interconnections, power companies included in test data are recognized by trained NER model. By using this model, the compromised power grid can analyse their breached data to determine the sensitive components and high-risk areas. Threat modelling can be done to implement pro-active security defence against the identified threats to be secure from the future attacks.

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. THREAT MODELING

Threat modelling is a step-by-step process which include defining scope and sensitive assets in the system, identifying potential threats and vulnerabilities. In the proposed work, threat modelling of compromised smart grid is done which can clarify the potential threats and vulnerabilities in the system. This will help to implement security measures based on each entity. STRIDE threat modelling is used in this work to identity threats based on categories like Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. The detailed threats and vulnerabilities associated with each entity is described in Table 1.

Assets	Potential Threats	Potential Vulnerabilities
Substation	Unauthorised Access, Remote Attacks, Delayed detection of security incidents.	Insufficient physical, network security, Inadequate monitoring
Substation Interconnection	Unauthorized access to the internal system, Data tampering during transmission	Lack of Encryption, Weak authentication and access control, Inadequate validation of data, Insecure communication channel
Power Company	Disruption of functionality, Alteration of configurations, interconnections and control system data.	Data integrity and confidentiality failure, Lack of encryption and access control
Receiving Station	Unauthorized access, Increased risk of disruption	Insufficient physical security
Control Centre	Manipulation of control systems and operations, Unauthorized access to control centre room, systems or databases, Injection of malicious data, data tampering, interception of communication, manipulating the transmitted data, DoS attack	Weak physical security, Weak access controls, Inadequate data validation, Insufficient security logging and monitoring, Security misconfigurations
Generating Station	Unauthorized modifications, Operational failures	Lack of control, Insufficient redundancy in critical systems, Vulnerable and outdated components
Power parameters	Unauthorized alterations of power parameters, Inadequate monitoring of user activities.	Inadequate data validation, Malicious insiders
Electrical equipment	Manipulation of equipment setting and configuration	Weak access controls and monitoring
Railway feeders	Unauthorized access to railway feeders and network connections enables attackers to perform data modifications	Insufficient authentication mechanism

Busbar section	Overload specific sections, leading to equipment failures, damage, or the need for emergency shutdowns	Lack of access and authentication controls

Table 1: Assets and Potential Threats

Energy providers need to implement strong security controls as cyber-attack on power systems can cause adverse impacts like power outages, operational disruption, reputation and infrastructure damage, financial loss etc. The development of mitigation strategies for each high-risk threat is important to protect the compromised power grid from further potential cyber-attacks. Threat modelling is an iterative process, and it should be revisited periodically to adapt to changes in the threat landscape and the power grid environment.

DISCUSSION

This case study proposes an approach for enhancing the smart grid security. NER model is developed which can efficiently recognize predefined entities. Even though with the small amount of data, the model training and evaluation has been done successfully with 94% accuracy. With the help of this model, the raw power grid data is converted into threat intelligence, that could be used to analyse the high risk and sensitive components included in a data breach. Threat modelling of the compromised data is done to identify potential threats and their impacts on system environment. This threat intelligence data can be used by energy providers to implement proactive defences against potential threats identified with the help of proposed model. Thus, in real world, this work can be used to analyse any breached dataset of smart grid to understand impact of the attack and further potential threats to the system.

REFRENCES

[1] Alomari, M. A., Al-Andoli, M. N., Ghaleb, M., Thabit, R., Alkawsi, G., Alsayaydeh, J. A. J., & Gaid, A. S. A. (2025). Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. Energies, 18(1), 141. https://doi.org/10.3390/en18010141

[2] Bhaskar, N., Ahmed, J., Masood, R., Ahmed, N., Kerr, S., & Jha, S. K. (2024). A Comprehensive Threat Modelling Analysis for Distributed Energy Resources. ACM Transactions on Cyber-Physical Systems, 8(4), 1-32. https://dl.acm.org/doi/abs/10.1145/3678260

[3] Dayarathne, M. A. S. P., Jayathilaka, M. S. M., Bandara, R. M. V. A., Logeeshan, V., Kumarawadu, S., & Wanigasekara, C. (2025). Mitigating Cyber Risks in Smart Cyber-Physical Power Systems through Deep Learning and Hybrid Security Models. IEEE Access. https://ieeexplore.ieee.org/abstract/document/10902404/

[4] Du, D. (2024). Smart Grid and Cyber Security Technologies. Springer Nature. https://books.google.com/books?hl=en&lr=&id=b_U6EQAAQBAJ&oi=fnd&pg=PR6&dq=cyber+attacks+on+smart+grid+2023,2024,2025&ots=ZZBQ-Pq34k&sig=UDQMkvMvCUXL-tM-MhgU7Sij-NE

[5] Ghadi, Y. Y., Mazhar, T., Aurangzeb, K., Haq, I., Shahzad, T., Laghari, A. A., & Anwar, M. S. (2024). Security risk models against attacks in smart grid using big data and artificial intelligence. PeerJ Computer Science, 10, e1840. https://peerj.com/articles/cs-1840/

[6] Harish, V. S. K. V., Gupta, S., Bhatt, J. G., & Bansal, M. (2025). International standards, regulations, and best practices for cyber security of smart grid. In Cyber Security Solutions for Protecting and Building the Future Smart Grid (pp. 321-348). Elsevier. https://www.sciencedirect.com/science/article/pii/B9780443140662000104

[7] Klauzer, A., Maier, M., Abart-Heriszt, L., & Ullrich, J. (2024). Fostering security research in the energy sector: A validation of open source intelligence for power grid model data. Computers & Security, 146, 104042. https://www.sciencedirect.com/science/article/pii/S016740482400347X

[8] Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. Sensors, 21(18), 6225. https://doi.org/10.3390/s21186225

[9] Nguyen, L. H., Nguyen, V. L., Hwang, R. H., Kuo, J. J., Chen, Y. W., Huang, C. C., & Pan, P. I. (2024). Towards Secured Smart Grid 2.0: Exploring Security Threats, Protection Models, and Challenges. IEEE Communications Surveys & Tutorials. https://ieeexplore.ieee.org/abstract/document/10746402/

[10] Rahim, F. A., Ahmad, N. A., Magalingam, P., Jamil, N., Cob, Z. C., & Salahudin, L. (2023). Cybersecurity vulnerabilities in smart grids with solar photovoltaic: A threat modelling and risk assessment approach. International Journal of Sustainable Construction Engineering and Technology, 14(3), 210-220. https://publisher.uthm.edu.my/ojs/index.php/IJSCET/article/view/15287

[11] S. Amanlou et al., (2025). Cybersecurity Challenges in Smart Grid Systems: Current and Emerging Attacks, Opportunities, and Recommendations. IEEE Open Journal of the Communications Society. 6(1965-1997). https://ieeexplore.ieee.org/abstract/document/10902093/

[12] Sangher, Kanti Singh, Archana Singh, Hari Pandey, and Vivek Kumar. (2023) Towards Safe Cyber Practices: Developing a Proactive Cyber-Threat Intelligence System for Dark Web Forum Content by Identifying Cybercrimes. Information 14(6), 349. https://doi.org/10.3390/info14060349

[13] Shahinzadeh, H., Azani, S., Baghernezhad, A., Mehrabani-Najafabadi, S., Gharehpetian, G. B., & Jurado, F. (2024, October). Cyber Threats and Resilience in Smart Grids and Microgrids: A Cybersecurity Perspective on Challenges and Innovations. In 2024 19th Iranian Conference on Intelligent Systems (ICIS) (pp. 299-308). IEEE. https://ieeexplore.ieee.org/abstract/document/10887512/

[14] Yohanandhan, R. V., Elavarasan, R. M., Pugazhendhi, R., Premkumar, M., Mihet-Popa, L., Zhao, J., & Terzija, V. (2022). A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid. International Journal of Electrical Power & Energy Systems, 136, 107720. https://www.sciencedirect.com/science/article/pii/S0142061521009467

[15] Zhang, Y., & Zhao, X. (2020, September). Key technologies of data security protection system for power grid. In Journal of Physics: Conference Series (Vol. 1656, No. 1, p. 012024). IOP Publishing. https://iopscience.iop.org/article/10.1088/1742-6596/1656/1/012024/meta