Integration of digital twin, blockchain, artificial intelligence in an IoT Metaverse environment for mitigation and assessment of cascading failure events in smart grids: Recent advancement and future research challenges

Kinza Fida[1], Usman Abbasi[1], Muhammad Adnan[2], Muhammad Sajid Iqbal[2], Irfan Ishaq[2], and Salah Eldeen Gasim Mohamed[3]

[1]Department of Electrical Engineering, National University of Computer and Emerging Sciences (FAST), Peshawar Campus, Peshawar, Pakistan; kinzamalik934@gmail.com, usman.abbasi@nu.edu.pk

[2]Department of Electrical Engineering, National University of Computer and Emerging Sciences (FAST), Chiniot-Faisalabad Campus, Chiniot 38000, Pakistan; m.adnan@nu.edu.pk, iqbal.sajid@nu.edu.pk, irfan.ishaq@nu.edu.pk

[3]Department of Electrical Power and Machines, Sudan University of Science and Technology, Sudan; salahedingasim@sustech.edu

*Correspondence Authors: m.adnan@nu.edu.pk

Abstract:

Among several disturbances in power systems, cascading failures (CF) are considered extreme and serious hazards to grid procedures, possibly prominent to substantial stability problems or regular power blackouts. The growing smart grid (SG) complexity and their correlation to distinct infrastructure structures have enhanced their vulnerability to CF incidents. These challenges require innovative techniques that integrate developed technologies. This survey studies the incorporation of artificial intelligence (AI), blockchain (BC), digital twin (DT), and within an IoT-permitted Metaverse (MV) environment to mitigate and assess CF in SGs. The technology of DT facilitates dynamic simulations, predictive analysis, and real-time monitoring, enabling resolution and proactive identification of structure irregularities. Blockchain (BC) presents a decentralized framework, secure for data management, and develops transparency in smart contracts, while artificial intelligence (AI) forces decision support approaches, predictive analytics, and autonomous mitigation policies. The IoT proposes immersive, real-time simulation, collaboration, and visualization of failure situations, enabling stakeholders to test and design effective results. Despite recent innovations, considerable challenges remain. These involve standardization and interoperability across varied policies, scalability to manage energy efficiency, cybersecurity threats, vast datasets, and the solutions of cost-effective integration. Adopting these challenges demands innovative design and interdisciplinary research to ensure a sustainable, resilient, robust SG network. This research survey delivers a comprehensive review of recent advancements, outlines future directions, identifies serious research gaps, and leverages these technologies to increase the SG resilience against CF.

Keywords: Metaverse; Blockchain; Digital Twin, IoT, Smart Grid, Cascading Failures

Nomenclature:

CF	Cascading failure
MAN	Multi-agent Network
ABGP	Algorithm Based on Greedy Partition
CLMILB	Critical-Line with Maximum-Impact through Limited Budget
ADBHE	Algorithm of Defense-Based Homogeneous-Equality
INB	IoTs concerned with node betweenness
TNSOE-E	Transmission Network System Operator by European Electricity
IoT	Internet of thing
WoS	Web of Science
PoP	Proof-of-Picket
GD	Grid digitalization
STS	Success tree structure
CA	Cyber attack
SN	Sensing node
RN	Relay node
BS	Base station

I. Introduction:

The power grid is a standard manufactured multifaceted structure that has enhanced a crucial infrastructure in advanced organizations. CF initiated by primary small-scale disasters has been established to happen, often indicating power outages at large-scale [1]. Because of the catastrophic outcomes of power outages, system engineers and complication scientists have allocated considerable determination to examining cascading failure in power networks and have presented substantial progress lately [2]. A variation of models with fluctuating amounts of real-world details has been established [3], [4], from which self-organized cruciality [5], profiles of failure spread [6], and further statistical structures [7] in real power, schemes have been effectively repeated [8].

CF begins with the power component's failure and distribution across the network. The interdependences between cyber elements and the system’s power imply that an early failure can spread throughout the structure and main to blackouts and power outages [9]. The load is repeatedly redistributed across the structure when a power component fails [10]. Therefore, power components and transmission lines can become disconnected and overloaded from the structure [11]. Several studies have explored how to lessen the impact of cyberattacks on CF. For example, [12], [13], [14] projected algorithms to classify the greatest vulnerable components and power lines in terms of their weakness to occurrences of CF to brace the power network by defending these exposed resources [15]. These struggles show the status of focusing on the issue of the attacks of CF on SG and the significance of weakening to do so. Several simulations have been projected to examine CF in CPS and smart grids [16], [17], [18]. Physics, statistics, and probability methods are commonly utilized in modeling diverse network phenomena [19]. Yet, some examines did not

reflect the function of CF or cyber-attacks in failures of communication factors. Others did not reflect the interdependences between communication networks and power or only developed the power grid [20]. However, some articles modeled both interdependencies and the networks between their several components, the power component's role, and the power capacity limitations [21], [22]. This model's problem is that they underrated the scope to which the power components [23].

CF in the power grid (PG) with huge numbers of components is complex and the interactions and dynamics of diverse time scales have made analysis and modeling and make events of blackout extremely complex. Focused research on the modeling of CF precisely is still ongoing. Cascading failures vulnerability analysis, load-dependent, and complex dynamics models respectively are given in ref [24], [25], [26]. Failures assessment with the use of phenomena of time-dependent, centrality measure and suppressed failure model [27], [28], [29], [30], [31], [32], [33], [34]. The methods offered comprise either the load shedding utilized to avoid the application of CF or defense procedures that are designed to lower the probability of CF circumstance. Load shedding produces losses to all participants of the power network. This research avoids the CF occurrence when a contingency incident without the load shedding usage. The explanation projected to CF occupies as capabilities of a Multi-Agent Network (MAN). An agent is an object with carries out and sets objectives and actions of self-governing in a world to meet the purposes. An agent has capabilities, goals, and knowledge; it suffers logical analysis and takes and makes conclusions. Some of the elementary assets of an agent are proactivity, reactivity, sociability, and sovereignty. MAN is an agent network connected to attain a global objective while each agent may have local or single targets. A thorough summary of MAN and various of its purposes in power networks can be given in [35], [36], [37], [38]. MAN was utilized to command the agents of an SG system to interact successfully to avoid the CF occurrence after a contingency occurrence [39].

The metaverse (MV) describes a progressive immersive technology of the internet that supports an interface between virtual and physical environments [40]. Metaverse is inspired by numerous modern technologies, such as the blockchain, digital twins (DTs), artificial intelligence (AI), and the Internet of Things (IoT) [41]. These collective technologies enable cognitive metaverse help by proposing capabilities of diverse connectivity [42]. The convergence of DT, AI, and BC, in the metaverse is explored in [43].

The survey has a flowchart that represents the main contribution of this paper is given in Figure 1.

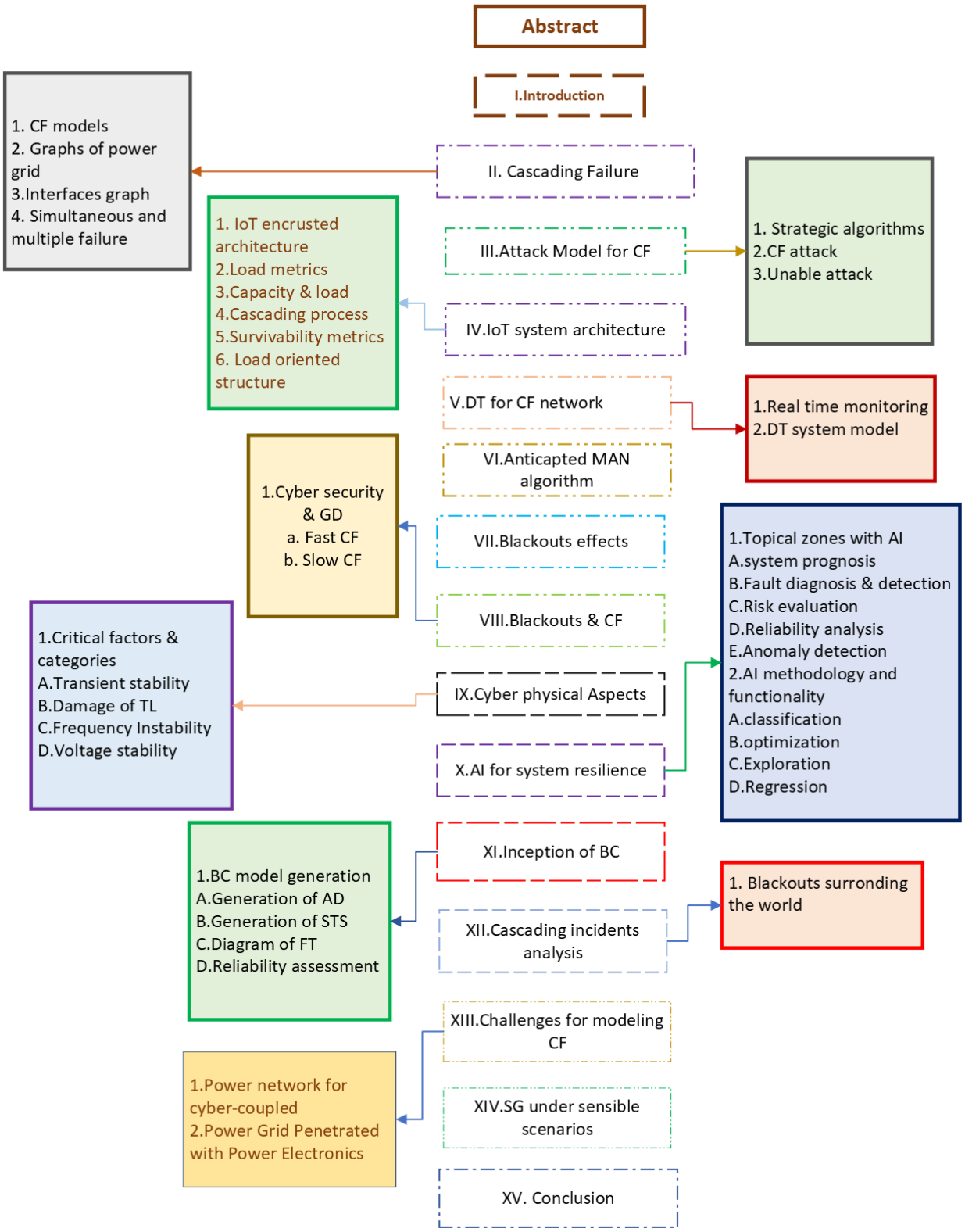

Figure 1. Flowchart of this survey paper.

1. Contributions:

Section II explained the introduction of cascading failure (CF) with models of CF, physical topological power grid graphs, and interface and simultaneous graphs. CF attack models with a strategic algorithm, load distribution unable attack is described in section III. Section IV and Section V define the architecture of the IoT structure and digital twin with models. Anticipated MAN algorithm with their flowchart, optimality, and combinations are explained in section VI. Blackout effects and Cascading failure, cyber security, and grid digitalization with fast and slow CF are given in section VIII. Section IX explains the cyber-physical aspects with critical factors and categories and damage of transmission lines. Artificial intelligence for system resilience is described in section X. Inceptions of BC with a generation model for reliability are explained in section XI. Cascading incidents with analysis and modeling of blackouts surrounding the world are described in section XII. Challenges for CF analysis are explained in XIII and the conclusion is given in XV. The main contributions of previously discussed technologies are given in Table 1.

Table 1. Main contributions of this survey.

Reference	Year	Contribution
[44]	2023	Discuss the systematic review for cascading failure models
[45]	2024	Evaluate the dynamic updated CF with digital twin hierarchically.
[46]	2022	Discuss the cascading reliability of the Internet of Things.
[47]	2021	Evaluate the models of CF for IoT.
[48]	2023	Describe the CF scenarios under extreme conditions of rainfall.
[49]	2023	Discuss the approaches of fast CF in dynamic power systems.
[50]	2014	Evaluate the stochastic analysis of CF dynamics.
[51]	2017	Discuss the critical review for analysis and modeling of CF.
[52]	2024	Mitigation and assessment of cascading failure.
[53]	2018	Predict the propagation of CF based on machine learning.
Our survey		Our survey includes the assessment of CF with different technologies in the metaverse.

II. What are Cascading Failures?

Cascading failures (CF) is the indicating source of wide region blackouts [54], [55]. Though large blackouts are irregular, the power law manners demonstrated by the size of blackout distribution (e.g., number of tripped transmission lines, records of clients with no service, and calculation of the unserved energy terms) permit the require studying such occurrences [56], [57], [58]. Adnan et al. suggested the transmission planning structure in [59]. Overload failure like CF in renewable smart grids is suggested in [60] and multiple fault contingencies in [61]. A CF can be identified as a classification of mutually dependent outage events, admitted by limited disturbances or outages [62], [63]. The originating events can be recognized by various aspects such as errors of software/hardware, human errors, vegetation disorder (e.g., tree contact), natural disasters, and so

on. For some years, attacks of physical/cyber on power grids, like the incident of the cyber-attack on the Ukrainian in 2015 [64], are also predecessors to CF. After the incidence of the originating events, the reliant outages outcomes sequence from numerous inner events such as hidden failures, line overloads, angular and voltage instabilities, produced due to the misconduct of protection equipment as well as errors linked to human factors, operation, and maintenance [59]. Further, several operating situations of the power grid, such as the primary loading situations of the apparatuses, also pretend the performance of the complete power grid through cascade procedures [65], [66]. Signal stability with aperiodic for CF detection is given in ref [67].

1. Cascading Failures Models:

Studying and modeling CF involves an assorted field of approaches and techniques [68], [69]. They comprise interdependent patterns with other organizations (e.g., a communication network), hybrid models, simulation-founded models for exploring the dynamic and quasi-steady performance of the system, topological models, probabilistic and deterministic models, models of high-level statistics, and so on [70].

These techniques have been cross-validated, validated, and bench-marked [71], [72]. Since this evaluation is mainly dedicated on methods of graph-based, graphs of physical topology-founded power grids and their restrictions during CF, are discussed below [73], [74].

2. Graphs of Physical Topology-Founded Power Grids:

studies of initial graph-founded power grids, in [75], [76], [77], [78], were founded on the power grid's physical topology. Usually, a power grid can naturally be characterized by a graph, G = (V, E), where V signifies the set of load buses, substations, transmission, or generator, and E signifies the conventional power lines [79], [80] is given in Figure 2. This displays the physical relationship among the network components. Several reviews have been completed on the power grid's physical topology by evaluating the properties of the global structure [77], [78], such as degree distribution, clustering coefficient, and length of the average path, and for evaluating power grids concerning standard complex systems such as graphs of scale-free, random, and small-world [81].

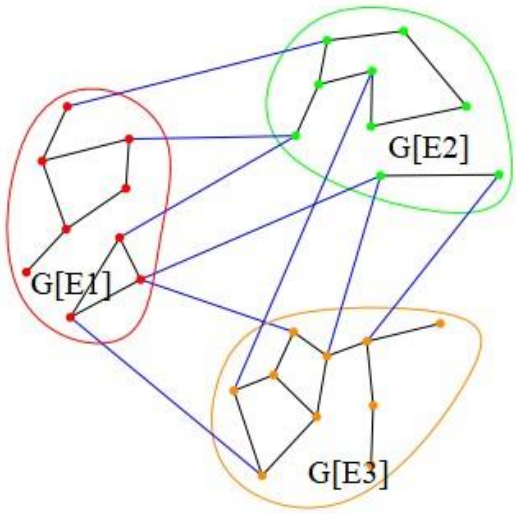

Figure 2. The physical topological graph on the power grid.

3. Graph of Interfaces:

The modeling power network method by interface graphs is examined in two definite categories: method of electric distance-based and the data-driven [82], [83]. These procedures build an interface graph for the network, denoted by $G_I = (V_I, E_I)$ in which the properties of vertices V_I are the network components whose interfaces are of interest, such as the combination of transmission lines or buses. Further, the properties of E_I signify the rest of influences/interactions among the components, that are undirected, directed, unweighted, or weighted (indicating the intensity of influences or interactions), or varying on the study of interest [84], [85], [86].

i. Methods of Data-Driven for Interfaces Graphs (IG):

Several data-driven techniques have been projected for modeling and inferring interfaces among the power grid elements [87]. These methods are based on information from outages of historical or simulation datasets. As the limited historical datasets, most findings handle simulation information. However, the attention of this study is not on revising the structure for creating cascade information, for example, from simulations of power systems. Significantly, the aim is to model the cascade information into graphs of interface and the successive reliability consideration presented on such interface graphs.

The datasets of cascade treated in the several methods will be declared. Data-driven approaches have five classes that have been reviewed and identified for modeling interface graphs for examining CF in power grids as given in Table 2. Next, each method class is reviewed in detail.

Table 2. Subclasses of the data-driven graph.

Ref	class	Subclass	Further class
[87]	Data-driven Interface graph	Correlation-based	
[105], [88], [89], [90], [91], [92], [93]		Risk-graph	
[94], [95], [96], [97], [98], [99], [100], [101]		Sequence of outages	Influence based
[102], [103], [104], [105], [106], [107], [108]			Consecutive failure
[109], [110], [111], [112], [113], [114], [115]			Simultaneous and multiple failure
			Failure relied on the generation

ii. Interfaces Graphs Relied on Outage Sequences in CF:

This method relies on CF data as a chain of failures in every cascade. For order, the sequence $T_3 \rightarrow T_5 \rightarrow T_7 \rightarrow T_2$ signifies the sequence example of failures in transmission lines (TL) in a cascading scenario, where T_i signifies transmission lines outages and the sign signifies the direction in which the failed lines during cascading. These methods rely on failure sequence analysis for focus and obtaining interactions on the effect and cause interactions between components failure. Techniques in this classification use several statistics and techniques to study such data.

iii. Interfaces Graph Relied on Sequential Failures:

In this outage classification analysis category, only failures of direct sequential in a chain are utilized for getting the interaction connections among the sections of the network. We also say that network two components have an interaction connection, $e_{l,k} \in E_l$, only if they happen as sequential outages in the series $T_l \rightarrow T_k$ in the dataset of cascading scenarios. The arrangement of the outages signifies the way the links in the interfaces graph, e.g., outage sequence $T_3 \rightarrow T_2$ indicating an outgoing linkage from the node T_3 to node T_2. The intensity of interfaces among the components in this event can be described using the occurrences statistics of pairs of sequential outages in dataset cascading circumstances. For order, the work in 13] gives weight to the interface's sides by statistical exploration of the total of records that a sets of outages in successive lines happens in the dataset of the cascade. For example, the interaction link weight from the node T_a to node T_b can be denoted as $|T_a \rightarrow T_b|/$ (overall number of sequential sets in the dataset of the complete cascade), where $|T_a \rightarrow T_b|$ is the failure number of times T_a and T_b happened

successively in the dataset of the cascade. These consequences can be clarified as the occurrence probability of outages of each set sequential line. Studies examples operating this process to happen the interaction graph of comprise [94], [95], [96], [97], [98], [99], [100], where the network of transmission lines is the vertices V_l of the interfaces graph G_l. In this analysis presented in [116], the consecutive failure sequences are called fault chains.

iv. Generation-Based Failures Analysis by Interaction Graph:

The method relied on successive failures and focused on one effect that the line outage had on the other line outage. Yet, in CF, instead of interfaces pairwise including sequential failures, a failures group may cause other component failures [117]. Therefore, it is focal to study the effects of failure groups and illustrate interfaces amongst the components relying on the impact among component groups. The works are shown in [109], [110], [111], [112], [113] describe such groups as the failures of generation within a process of cascade, which are failures that happen within a short temporal distance. In these workings, the cascade failure sequence is split into a generation sequence, and the failure-induced effect and cause connections are measured between successive generations. Particularly, outages happening in generation n+1 are imagined to be affected by generation outages 'n' [118], [119].

v. Influence-Based Interfaces Graph:

In this process, the interfaces between the components are drawn relying on consecutive cascade generations; though, the interface weights are described relying on the model influence and the framework of the process of branching probabilistic. The model influence is the framework of the Markov chain network, formerly informed in [120] and was key functional to a dataset of cascade in the effort given in [121]. It also analyses the findings that utilize the influence template in the framework of power grids to create the interface graph. In these revisions, the TL in the network is measured as the vertices V_l of the interfaces graph G_l and the interactions/influences linking the edges lines as the E_l [78], [122], [123].

It combines the information from a matrix of single influence S (indicating the connections of the interfaces graph and their weights). The matrix elements are outlined built on the restricted probability that a specific component 'w' stops in the next group n + 1, assuming that component 'l' has stopped in group 'n' and that group n+1 contains exact failures of 'x'. This probability can be distinct as

$$P(w|l,x) = 1 - (1 - g[w|l])^x \qquad (1)$$

Then, the uncertain probability $s_{l,j,n}$ that element 'w' stops in generation 'n + 1', assumed that component 'l' stopped in a generation 'n', overall probable 'x' values signify the real elements of 'S' and originate by multiplying $P(w|l,x)$ with the 'x' failures probability happening as follows:

$$s_{l,j,n} = \sum_{x=0}^{\infty} 1 - (1 - g[w|l])^x \frac{\lambda_{l.n}^x}{x!} e^{-\lambda_{l,n}} \qquad (2)$$

$$s_{l,j,n} = \sum_{x=0}^{\infty} 1 - (1 - g[w|l])^x \frac{\lambda_{l.n}^x}{x!} e^{-\lambda_{l,n}} \quad (3)$$

Founded on the influence graph, CF can begin with a line outage at a graph node and generate probabilistically near the graph-directed links. Patterns of extra works that have utilized the approach of influence founded to originate the interfaces power grids graph [91], [92], [93].

4. Simultaneous and Multiple Failures Interfaces Graph:

This method uses the failure sequence to show interactions among network components. Though, they study the interfaces with multiple simultaneous failures. In the learning existing in [102], a graph with Markovian was established to address the issue of taking the outcome of simultaneous multiple outages within groups on the interaction's representation among the components of the succeeding cascade generations. In this problem, the graph nodes denote the conditions of the Markov chain specified as the regulated line outages in a cascade generation, and the links signify the transition. Hence, each graph node may denote the outage of a multiple line or single lines. Graphs of Markovian interface vary from influence-founded and generation-based interface graphs as interactions of edges are between succeeding generations of line outage sets in place of the individual interfaces between succeeding generations of line outages. Graphs of Markovian interaction also think of a null state node, which signifies the state that stops the cascade. This condition appears at the end of scenarios of all cascades. The probabilities of transition among the states from state 'l' to state 'w' can be anticipated by holding the consecutive state's number in which state 'l' and state 'w' happen in all the cascades and splitting by the number of state circumstances 'l' [121].

III. Attack Model (AM) for Cascading Failures (CF):

Study the network from the attacker's viewpoint to model an algorithm of effective attacking. A satisfactory knowledge of the structural susceptibility of smart grids (SG) is expected to benefit the protection of better structures. In ref [124], the author explained the SG load flow balancing and its future trends. In this phase, we expect to construct an attacking process that can increase smart grid damage. It can interpret the destruction as the total users (consumers) impact. This aim effects our practical work but also challenging. Future navigation of unleashing energy efficiency of the smart grid is given in the ref [125]. To extend the damages to SG, we plan to initially solve the highest critical clients (the impact on clients in the 6). Consequently, a specified number of relations correlated with the serious clients that their failure can cause an effect of CF, are chosen as target relations to be attacked to detach the clients. Since the CF [126], [127], [128], [129], is the focus of this function, we give the CF as follows. Data-driven integration in sustainable and resilient smart grid is explained in [130]

Because of the interdependency of the SGs, an early line failure in the network (for example, by attack injection of wrong data) can generate a redistribution progression [131]. Prevention and instability detection with asymmetric faults of the smart grid are given in [132].

The cracked line's power flow is redistributed and expressed by extra lines utilizing the redistribution elements. Analysis of transient stability and balancing of load flow is given in [133]. The failure signals are transmitted in time phases [134]. The transition of socio-technical with the super smart grid is given in ref [135]. Adnan et al. [136] suggested the smart grid network stability with a probabilistic approach and stabilizing the smart grid in [137]. Our purpose in this effort again is to method the SG employing the near-real-world or at least the practical simulation. Hence, study the subsequent elements in this investigation:

To attain the correlation between the system and the attackers, we believe the attacking funds are expressed by a set of attacks (B_{ATK}) for the aggressors. From the viewpoint of SG, line (w,x) has a total cost τ (w,x) that indicates the line's robustness [138], [139]. This is the attacker's cost for if they choose to line fail. In the network of SG, some areas are more valuable than others. Thus, put the significance element to every representing user how the operator is essential in the SGs. Let g(w) represent the weight (significant element) of an operator w.

1. Strategic Algorithm:

First, propose an attack algorithm, explicitly Algorithm Based on Greedy Partition (ABGP) for explaining the Critical-Line with Maximum-Impact through Limited Budget (CLMILB) issues. Then, a proper defense algorithm, explicitly the Algorithm of Defense Based Homogeneous-Equality (ADBHE) is proposed.

A. Algorithm Based on Greedy Partition (ABGP):

SG vulnerability assessment terms, focus on present works on the lines or nodes with advanced load to introduce attacks. The reason behind the purpose is that the lines or nodes with greater load may trigger a heavier effect of CF [140], [141], [142]. Then additional failures can be completed (cogitated from the perspective of the attacker). However, the lines or nodes with greater load do not indicate they are the highest decisive ones. In other talks, the nodes or lines failure may not conduct to a CF, or even if it occurs, no assurance maximized the whole impact. In calculation, the CF does not constantly occur in the SG. To give a complete evaluation, we will study both normal attacks and CF attacks [143], [144].

2. CF Attack:

Primarily, try to determine if the impact of CF happens in the SG. The CF is activated by one or more primary failures because of the redistribution procedure. This failure could be a mix-up with the links or node failure with a great load that may indicate a greater failure of its next nationals but does not affect a CF effect [145], [146], [147]. Then concentrate on determining analytical nodes that can initiate a large CF effect. We organize the components of SG as develops:

- Non-critical connection: Let UC signify the establish of non-critical connections A non-critical link $(w, x) \in UC$ is a connection whose failure does not happen to any clients. This

occurs caused of the network instability or impact of previous attacks, or the connection is not indirectly (or directly) linked to any clients.

- Ranking factor's citation: There is an approach to construct a prominent collapse that is stopping off all retiring power surges from producers. But remember that there is a constrained budget for attacks, so deciding the best target limits selects the destruction scale from the viewpoint of the attacker. Broadly, the process of redistribution is that the flow of power is transmitted by locations (nodes), we will focus on concluding the highest critical outgoing connections involving numerous outgoing connections of several nodes [148], [149].

Reflecting the interdependency between links and nodes, we must regulate the greatly vulnerable nodes, to establish the highest critical relations. Remember that a node 'w' that is a client $(O(w) - I(w) < 0)$,

is weighted by its value g(w). Providing splendid assistance to these essential clients is the significance of the contributor since they are potential and critical clients. Let $\beta(w)$ represent the inadequate feature of the customer 'u'. The inadequate feature is assessed relying on overall, delivered power in the consumer's demand and incoming connections.

$$\beta(w) = \frac{d_w - |I(w) - O(w)|}{d_w} \tag{4}$$

Eq 5 specifies that the greater $\beta(w)$ is, the less consumer 'w' satisfaction will be. Spontaneously, those nodes with an advanced unsatisfactory feature and greater weight will possibly be aimed at attackers. This is for the users with the greater $\beta(w)$ are deficient supply and, thus, possibly are exposed to attacks. Hence, we initiate a metric demonstrating the consumer impact $(\forall w \in U)$, denoted by $\gamma(w)$.

$$\gamma(w) = \beta(w) \times g(w) \tag{5}$$

Nonetheless, from the point of view of attackers, choosing an attack target to rely on only the consumer impression (γ) may need a greater cost, which may raise significantly developed entire applying costs but improve little overall affect. To prevent this development, we classify every consumer's new metric $(w \in U)$, represented as the ordinary impact amount per incremental cost of w, signified by $M(w)$.

$$M(w) = \frac{\gamma(w)}{O(w) \Big/ \lambda(\mathrm{w})} \tag{6}$$

Where λ(w) is the entire desired cost to cause a CF at node w. Apparently, in the defective problem, all outgoing connections of 'w' required to be taken set down:

$$\lambda(\mathrm{w}) = \sum_{t \in N_w^+} \tau(w, x) \tag{7}$$

However, we must study the effect of primary attacked connections to initiate a substantial failure. Hence, the collapse of limited outward connections of node 'w' is limited to taking down all of its outgoing connections. This occurs if the overall load of previously attacked connections is greater than the part of the left connection.

$$\delta(\mathrm{w}, \mathrm{x}) \leq \sum_{t \in N_w^+ \setminus \{\mathrm{x}\}} \tau(w, x) \tag{8}$$

We consider these eq as a sample. In the sample, we have

$$f(w, x_1) + f(w, x_2) \geq \delta(w, x_3) \tag{9}$$

Then, the failures of (w, x_1) and (w, x_2) affect the overload at (w, x_3), causing the failure of (w, x_3). This indicates that here is no requirement to outbreak all outgoing connections to detach a node. If there happens the co-impact can initiate a substantial failure to entirely detach a node w, then the entire cost λ(w) can be lowered as below:

$$\lambda(\mathrm{w}) = \sum_{t \in N_w^+} \tau(w, x) - \sum \tau(w, t) \tag{10}$$

$$\sum \delta(w, t) and (u, t) \notin UC < \forall\, v, t \in N_w^+ / \sum f(w, x) \tag{11}$$

Hence, the ordinary impact worth per incremental node cost is estimated. After assessing the ordinary impact value, we can establish the target connections for an attack of CF.

3. Unstable Attack on Load Distribution:

The influence on clients can support regulating the serious clients and the ordinary impact value per incremental node cost can support target links selection (correlated with the critical nodes) to attack with an effect of CF [150], [151]. However, it is not feasible if the budget of the attack is not adequate to raise the effect of cascading failure. As stated, when the resources are adequate, to separate a node we can tackle a guaranteed number of its exiting connections to prompt a CF effect and accomplish an enormous blackout. In contrast, when the attacking budget and resources are inadequate, a complicated crisis behind the connection's relationship is subjected. Let's cogitate a power grid. The failure of $f(w, x_1)$ causes the redistributed power flow to happen at 'w'. It appears

that $f(w, x_1)$'s failure impacts on the clients $g_4, g_5 \, and \, g_6$, but it is not. Since (w, x_1)'s redistributed power flow to $x_1 and \, x_2$, and keeps operating $g_4, g_5 \, and \, g_6$. Then neglect the failure impact. Call this happening as the restored flow. To conquer this contest, we plan the attack approach as given [152], [153]. Because of the absence of a budget for attacking, we first categorize power grid sub-sections into unsatisfied sections and satisfied sections. Let $T(x)$ be the tree-rooted Depth-First Search (DFS) at x. Also, let $S_{E(w)}$ and $D_{E(w)}$ indicate the entire power supply and the entire node demands for all nodes in $E(w)$, respectively.

- Satisfied Section: is the section without the absence of power supplies ($S_{E(w)} \geq D_{E(w)}$)
- Unsatisfied Section: is the region with an absence of power supplies ($S_{E(w)} \leq D_{E(w)}$)

The objective behind the category is to target the attacks on unsatisfied sections that initially outage suffered. Then, the initial outage effect is intensified by the subsequent attacks.

A. Algorithm of Defense Based Homogeneous-Equality (ADBHE):

The ABGP is suggested to obtain an ordered connection set of ATK such that the effect (whole weights) on clients from failures of connections in ATK is extended. To defend the network, we plan a defense algorithm to support determining the connections that are required to be safe against ABGP, described as the Algorithm of Defense Based Homogeneous-Equality (ADBHE). Since there is a restricted attacking resource B_{ATK}, we also deliberate a restricted shielding budget, namely B_{RDF}. To manage the budget economically, we propose a measured, implied to as homogeneous impartiality.

$$HE = [\frac{B_{ATK} + \sum_{(w,x)\in ATK} \tau(w, x)}{|ATK|}] \qquad (11)$$

Our objective is basic estimate HE value for entirely connections. Then, we will initiate the damages to collapse individually connection based on its HE. Further, appraise the network with the residual links and nodes (once every F.C collection) modernized. The theory behind ADBHE is to save critical connections in ATK with additional charges. Later, the connection budget is improved, it is further strong and develops difficulty to be carried down below attacks. But, because of the restricted defense budget, importance is shared on the best perilous connections to be safe [154].

IV. IoT system architecture for elaborate the CF:

CF is elaborated with the help of the Internet of Things (IoT) system architecture.

1. The encrusted architecture of IoTs:

The Internet of Things (IoT) system usually comprises many networked apparatuses sited in a wide region, the aim of which is to gather and upload environmental data to the Internet [155], [156]. To attain this objective, the IoTs need three sorts of networked nodes: base stations, relay nodes,

and sensing nodes. Its design can be split down into three layers: aggregation layer, relay layer, and sensing layer, as illustrated in Figure 3.

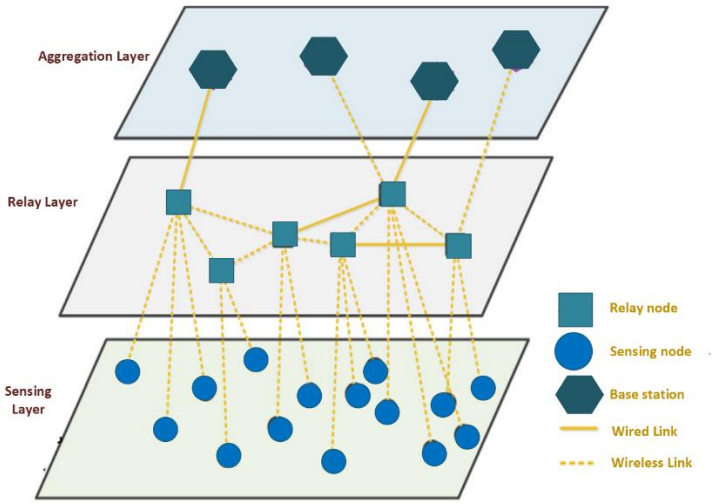

Figure 3. IoT architecture with three layers.

The bottom layer is the sensing layer, compiled with many sensing nodes. These nodes are armed with sorts of sensors, and the idea of this node is to gather environmental data. These nodes do not connect, and this node is first admitted to establishing a wireless bond with one node of the relay on the other layer which is the relay layer. Wireless or wired connections are used in relay nodes for communication. Through the transmission of the multi-hop relay, relay nodes can accomplish delivery of data in long-distance. A specified relay node's number on the relay layer can determine wireless or wired joining on the aggregation layer with base stations [157]. Base stations use Internet access, and they are networked devices. from the bottom to the top delivery of IoT data: collected data of the sensing node is sent to its relay node; this data is transferred by the relay node to the adjoining base station using a multi-hop relay; this data is uploaded by the base station to the Internet. According to the IoT layered manner, since the grid apparatuses on the aggregation layer and relay layer want other network apparatuses to relay the load, their disasters will origin the load of the network to be reorganized, which can cause CF triggers. In distinction, since the system apparatuses on the sensing layer do not require to take tasks of data-advancing from other nodes, the load distribution of the network cannot renew from their failures and therefore cannot CF trigger [158].

2. Load metrics:

In the previous section, the network modules on the aggregation layer and relay layer have an essential effect on the IoTs CF activity, so in this section, suggest three load system of measurement (i.e., IoTs-concerned with aggregation degree, IoTs-leaning link betweenness, and IoTs-concerned

with node betweenness) to indicate the relay nodes with load distributions, base stations and links on the aggregation layer and relay layer, correspondingly [159].

At the time 't', the IoTs concerned with node betweenness (INB) of relay node 'k' may be stated as:

$$T_k(t) = \sum_{m \in N_R} \sum_{j \in C_m} \frac{\frac{p_{m,j,k}(t) b_m(t)}{p_{m,j}(t)}}{N_e N_{U_{i(t)}}}, \quad (12)$$

$$U_{i(t)} = \{ | \ h_{m,w}(t) = \min [h_{m,w}(t), w \in N_B] \} \quad (13)$$

'$b_m(t)$' is the SN attached to the RN 'm'; '$U_{i(t)}$' is the BS set next to the RN 'm', and $h_{m,w}(t)$ is the least hop number between the BS 'w' and RN 'm'. N_B and N_R signify the set of BS and RN in the network, correspondingly. 'N_e' signifies SN in the system. $p_{m,j,k}(t)$ is the number of the smallest paths from the RN 'm' to its closest BS 'j' which passes around the RN 'k' at time 't'. $p_{m,j}(t)$ is the smallest path from the RN 'm' to its closest BS 'j'. $N_{U_{i(t)}}$ is the closest RN 'm' BS. All of the smallest paths from some SN to their closest BS to relay node 'k'; $T_k(t)$ brings the 1 maximum value. On the basis that SN are not required to pass through relay nodes 'k' to accomplish their closest base stations, $T_k(t)$ gets the 0 minimum value [160].

At time 't', the IoTs-concerned with link betweenness (ILB) of link $f_{k,j}$ can be classified as:

$$T_{f_{k,j}}(t) = \sum_{m \in N_R} \sum_{j \in C_m} \frac{\frac{p_{m,j,f_{k,j}}(t) b_m(t)}{p_{m,j}(t)}}{N_e N_{U_{i(t)}}}, \quad (14)$$

$p_{m,j,f_{k,j}}(t)$ are the quickest tracks from the RN 'm' to its closest BS 'j' which passes via a link $f_{k,j}$ at time 't'. In the scenario that each of the smallest paths from some SN to their closest link of BS $f_{k,j}$; $T_{f_{k,j}}(t)$ takes the 1 maximum value. SN are not required to pass through the link $f_{k,j}$ to access their closest BS, $T_{f_{k,j}}(t)$ takes the 0 minimum value [161].

At time 't', the IoTs-leaning aggregation degree (IAD) of BS 'j' can be stated as:

$$M_k(t) = \sum_{m \in N_R} b_m(t) \varphi_{m,j}(t) \Big/ N_e N_{U_{i(t)}} \quad (15)$$

$$\varphi_{m,j}(t) = \begin{cases} 0\ j \notin C_m(t) \\ 1\ j \in C_m(t) \end{cases}$$

where $\varphi_{m,j}(t)$ indicates BS 'j' is one of the closest RN 'm' BS. According to above eq 14 and eq 15 if all the SN created data in the structure is accumulated at BS 'j'; $M_k(t)$ brings the 1 concentrated quantity. Sensing facts is not collected at base station 'j'; $M_k(t)$ brings the 0 minimum quantity. To validate the logic of the recommended metrics IAD, ILB, and INB, we suggest two classified topological arrangements (i.e., multiple BS topology and one BS topology) [162].

Figure 4 shows a topology example of the two BS IoTs. In this regional anatomy, it simply obtained that RN no 3 and link $f_{1,3}$ want to data of relay starting SN (i.e., nodes 5 and node 6); link $f_{2,4}$ and RN 4 required to transfer data since SN (i.e., nodes 7 to 9); links $f_{3,5}$, $f_{3,6}$, $f_{4,7}$, $f_{4,8}$ and $f_{4,9}$ only required from one SN to RN data; there is no activity of data-advancing among nodes 3 and 4, it load-free the link $f_{1,3}$; Facts from SN 5 and 6 are gathered at 1 BS; in SN 7, 8, and 9, data are gathered at 2 BS . By evaluating the quantities given in Table 1 with the real load distribution, the logic of the intended load system of measur validated.

Table 3.Real load distribution values.

Links	ILB	Base Stations	IAD	Relay nodes	INB
$f_{1,3}$	0.4	2	0.6	3	0.4
$f_{2,4}$	0.6	1	0.4	C4	0.6
$f_{3,4}$	0				

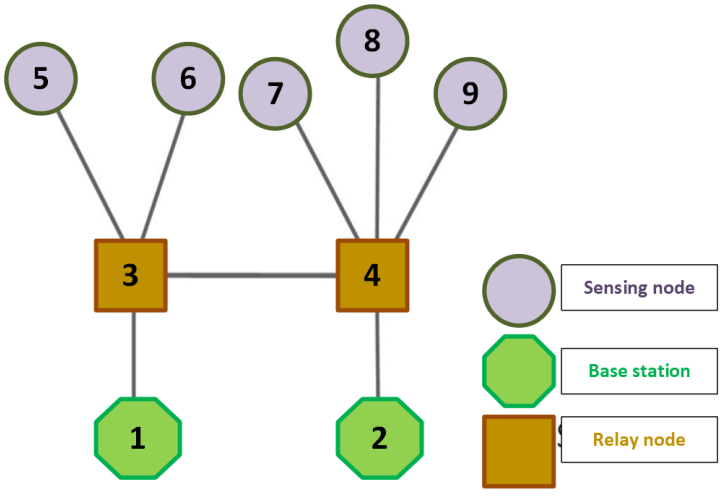

Figure 4. Topology example of two base stations.

3. Capacity and Load:

Existing models generally pretend that the network component's capacity is confidently associated to their starting load, but this theory does not concern the IoTs [163]. In some instances, system elements in the IoTs of the identical type generally have a similar capacity. Hence, in this representation, we explain the relay node 'm' load functions, base station 'j', and link $f_{m,k}$ at time 't' as:

$$\begin{aligned} H_m(t) &= T_m(t)^{\alpha}, \\ H_{f_{m,k}}(t) &= T_{f_{m,k}}(t)^{\alpha}, \\ B_j(t) &= M_j(t)^{\alpha}, \end{aligned} \tag{16}$$

where $\propto \geq 0$ is the load-exponential factor to modify the load supply of the system. In the example of $\propto \geq 0$, the network components' load is linearly associated with their values of load measured. In the real IoTs, the link capability is restricted by bandwidth [164]. Define the link $f_{m,k}$ capacity in this model as:

$$W_{f_{m,k}} = (1 + \lambda_H)(1 + \omega_{f_{m,k}})H_F(0), \tag{17}$$

$$L_F(0) = \max\{H_{f_{b,g}}(0), f_{b,g} \in F_{RA}\}, \tag{18}$$

where $0 \leq \lambda_H$ is the link-acceptance measurement to imply the bandwidth suppliers held by every link. $\omega_{f_{m,k}}$ is the wired links gain coefficient. When link $f_{m,k}$ is a wireless link, $\omega_{f_{m,k}} = 0$ and when link $f_{m,k}$ is a installed link, $\omega_{f_{m,k}}$ is a 0 greater quantity. By advancing the acquire coefficient $\omega_{f_{m,k}}$, the wired links compensations in capacity terms can be revealed. $H_F(0)$ is the largest load including all network links at t = 0. F_{RA} indicates to the links set between links and relay nodes between base stations and relay nodes. We can make certain that all initial network links will not be overfull [165]. $W_{f_{m,k}}$ can be deemed as the largest load that transferred by link $f_{m,k}$. If the existing load on link $f_{m,k}$ is larger than its size, it will stop at the subsequent instant due to crowding of bandwidth.

In the real IoTs, the node components' capacity (i.e., base stations and relay nodes) are restricted by the store gap. In this sort, we describe the relay node size of H_R and the base capacity H_G as:

$$P_R = (1 + \lambda_R)H_R(0), \tag{19}$$

$$H_R(0) = \max\{H_m(0), m \in N_R\}, \tag{20}$$

$$P_G = (1 + \lambda_G)H_G(0), \tag{21}$$

$$H_G(0) = \max\{B_k(0), k \in N_G\}, \quad (22)$$

Here the tolerance coefficients are λ_G and λ_R for base stations and relay nodes, correspondingly, to distinguish the cache sources they have. $B_k(0)$ and $H_m(0)$ indicate to the load on the base station 'k' and relay node 'm' at t = 0, correspondingly. $H_G(0)$ and $H_R(0)$ are the largest network load among all base stations and all relay nodes at t = 0, correspondingly. By introducing $H_G(0)$ and $H_R(0)$, we can make sure that all network base stations and relay nodes will not be burdened at t = 0. If the base stations and relay nodes' current load is limited to their ability, at the next moment they will collapse due to overflow of cache.

4. Cascading process:

The starting load on entire links and nodes on the aggregation layer (AL) and relay layer (RL) is fewer than their capability. When nearly links or nodes fail, it renews the system load distribution, which fails nearly links and nodes due to burden. This process of CF will resume until no fresh links or nodes fail. If a relay node or a SN fails all the lines to BS in the real IoTs, it will crash from an operational point of opinion since it cannot resume delivering data. In this instance, we think this node type is called an isolated node.

The next figures explain the process of CF in the IoTs with an example. This system has BS on 1 and 6 RN, and RN are 2, 3, 4, 5, 7, and 8. RN 3, 4, 8, and 7 are linked to SN. We suppose that the coefficient of load-exponential $\alpha = 1$, 0.8 links, BS, and the RN capacity. In Figure *5* it does not overload all the network components. As is given in Figure *6*, it renewed the load distribution of the network and attacked RN 5. As all the lines to BS 6 are separate, the network load has to pass through a link $f_{1,2}$ and RN 2 to grasp BS 1, which enhances these structure load components to 1. The load enhancement will cause them to be burdened. In Figure 7, because all the paths and BS stopped, the lasting SN and RN are inaccessible, and the structure is incapacitated due to CF.

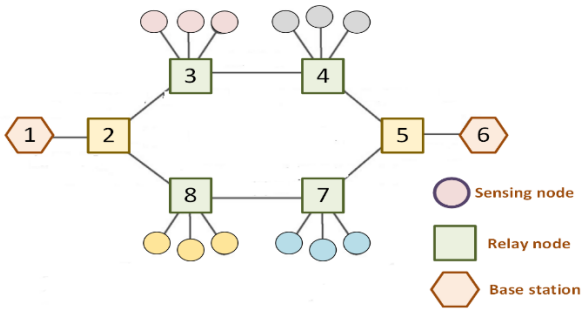

Figure 5. The IoT CF process with network components is not overloaded.

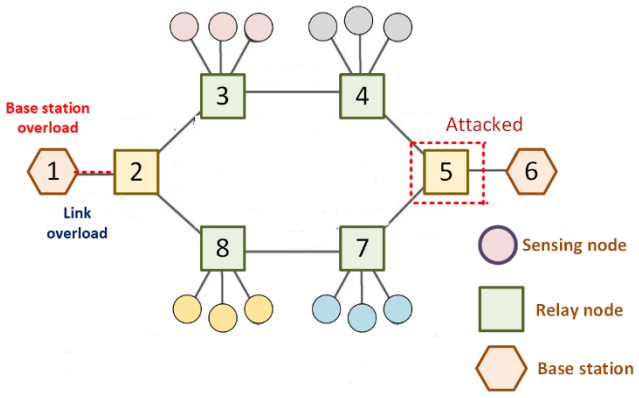

Figure 6. Network load distribution is renewed.

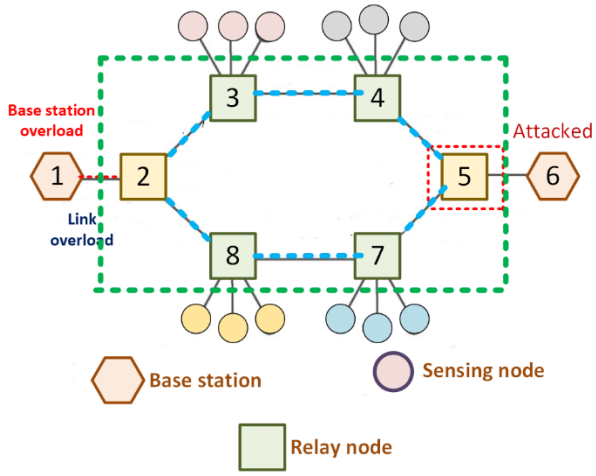

Figure 7. Paths and stations have failed.

5. Survivability metrics:

In ref [166], [167], [168], they applied the giant component comparative size after deleting certain links or node numbers to evaluate the network survivability versus CF. This measure is enough sensible in peer-to-peer structures, but not appropriate for the IoTs. The figure of RN and SN is more concerned that can motionlessly connect with BS with CF in the real IoTs. Hence, the new theory of 'IoTs-oriented efficient component" involves RN and SN that claim at minimum one logical line to BS. A model of the IoTs-oriented efficient element and the giant element is given in Figure 8. In this model, the giant component is completed with 10 SN and 5 RN, though the IoTs-oriented efficient component is completed with 6 SN and 3 RN that have as a minimum one line to BS.

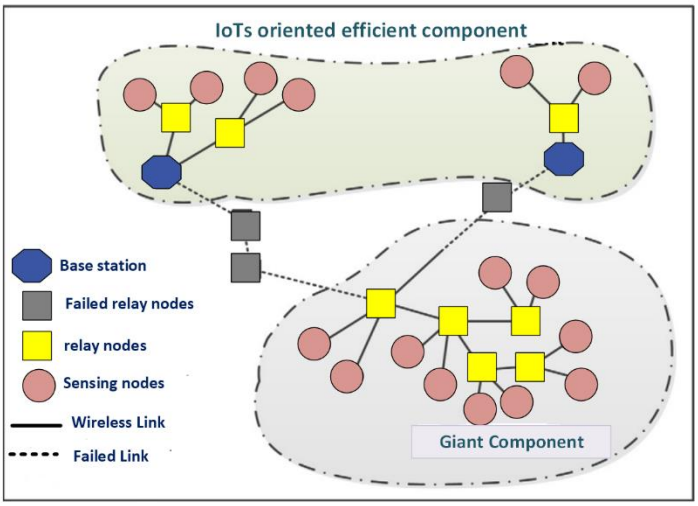

Figure 8. IoTs oriented efficient components.

Thus, to relatively exhibit the IoTs network survivability, we outline three systems of measurement built on the IoTs-oriented efficient element to estimate the system survivability beneath three assorted attack approaches (i.e., sole attack approach for relay links, solo attack approach for RN and solo attack approach for BS), separately. It must be observed that in this effort we generally estimate the system survivability in the failure of a single element. Because in some circumstances, the failure prospect of a single module is much greater than the failure possibility of a multi-module [169], [170].

In the solo attack approach for relay nodes (SARN), firstly delete a RN 'm' from the primary structure casually and examine the magnitude of the IoTs-oriented efficient element E_m [171]. In this method, we can acquire the effective element size after eliminating the left relay nodes. Under SARN estimate the network survivability, we apply the normalized effective element size,

$$E_R = \frac{\sum_{m \in V_R} E_j}{N_R(N_e + N_R - 1)} \tag{23}$$

by eliminating every RN, it is the sum of the normalized efficient elements. N_R indicates the number of network RN. $E_m = 0$ specifies that any RN failure can incapacitate the intact structure and $E_m = 0$ signifies that any RN failure cannot activate CF.

In the solo attack approach for relay links (SARL), firstly delete a link $f_{m,k}$ from the primary complex casually and examine the extent of the IoTs-oriented efficient element $E_{f_{m,k}}$. It must be stated that the SARL attack aim did not imply the links relating SN and RN since these link failures cannot start CF. Similarly, we can obtain the effective component size after eliminating the lasting links. Under SARN to estimate the network survivability, we apply the effective component normalized size,

$$E_H = \frac{\sum_{f_{m,k} \in F_{RA}} E_{f_{m,k}}}{N_{RA}(N_e + N_R)} \quad (24)$$

by eliminating each link, it is the sum of the standardized effective elements. F_{RA} is the set containing all links among BS and RN. N_{RA} is the magnitude of the link set F_{RA}. $E_H = 0$ specifies that any link failure can incapacitate the whole network and $E_H = 1$ shows that any link failure cannot initiation CFs.

In the solo attack approach for base stations (SABS), firstly delete a base station 'j' from the primary network casually and examine the magnitude of the IoTs-oriented efficient element E_j. Similarly, we can obtain the effective element size after deleting lasting base stations. Under SABS to estimate the network survivability, we apply the effective component normalized size,

$$E_G = \frac{\sum_{j \in V_G} E_j}{N_G(N_e + N_R)} \quad (25)$$

which is the quantity of standardized efficient elements by eliminating each base station. NB signifies the number of BS in the structure. It is calm to recognize that CB = 0 specifies that any BS failure can petrify the entire structure. CB = 1 specifies that failure of any BS cannot initiate CF.

6. Load-oriented outline structure:

We suggest a load-oriented outline structure (LOS) for BS to optimize the BS outline. Apply the outline structure, initially split the evenly network zone into grids. Every grid has at utmost one BS. The offered load-oriented outline structure has two stages. The first stage is to choose a grid for the primary organized BS. We choose the grid with the greatest next relay node number as the primary BS location. Then each network grid is allocated a load assessment. The other BS in the grid will be adopted with the greatest load consequence. When a BS is organized, each grid load assessment will be reorganized, and the subsequent BS will be employed conferring to the newest load value. Each grid load value is depressingly connected to the load of its adjacent RN, and absolutely associated to the amount of its adjacent RN is considered by:

$$Y(x_m, z_m) = |V_{(x_m,z_m)}| \sum_{m \in V_{(x_m,z_m)}} [1 - H_m(t)], \quad (26)$$

where $Y(x_m, z_m)$ signifies the grid load value whose center synchronizes are (x_m, z_m); $V_{(x_m,z_m)}$ signifies relay nodes set protected by a circle d_{TR} as the radius with (x_m, z_m) as the center d_{TR} is the wireless statement sort of node component; $|V_{(x_m,z_m)}|$ is the size of the set (x_m, z_m), is also reflected in the amount of adjacent relay nodes. The fundamental idea in eq 26 is to enhance structure load harmonizing by adopting new base stations in zones [172].

V. Digital Twin (DT) for elaborate the network:

A DT is outlined as a simulated demonstration of a network or ability that assesses network situations and built info availability in a system, through data and integrated models, to specify its life cycle decision support. The overview of DT model usage dates to NASA's Apollo sequencer in the 1970s during the mission when similar dual space automobiles were developed to mirror the requirements of the space automobile [173], [174].

Technology DT has acquired widespread purposes across numerous industries, involving industries, smart city [175], manufacturing [176], healthcare [177], automotive [178], and aerospace [179], etc. DT's early applications are obvious in jet fighters of the US Air Force and NASA's spacecraft [180], [181]. Main sellers like Dassault Systems, PTC, and Siemens have combined DT models into their PLM schemes. The DT scheme has also been recommended to establish the durable application of the (IoT) [182]. Corporations like TESLA are dynamically pursuing the advancement of DTs for all built cars, permitting synchronous information transmission between the production facility and the vehicles [183].

While the idea of DT is not initially novel, it lacked auxiliary and largely descriptive technologies in its initial stages [184], [185]. Figure 9 demonstrates the pitch in investigative activity in the DT idea, which is obvious from the spreading number of discoveries gained through examining the subject 'DT' in the Web of Science (WoS) database. Notably, from 2019, there is a significant rush in pursuit from academia and industry, as exposed in the soaring number of found outcomes. Permitting to information from WoS, China develops as the ahead country publications of DT, tracked by South Korea, the UK, Italy, Germany, and the USA, among others, demonstrating engagement and global recognition in this advancing field [186].

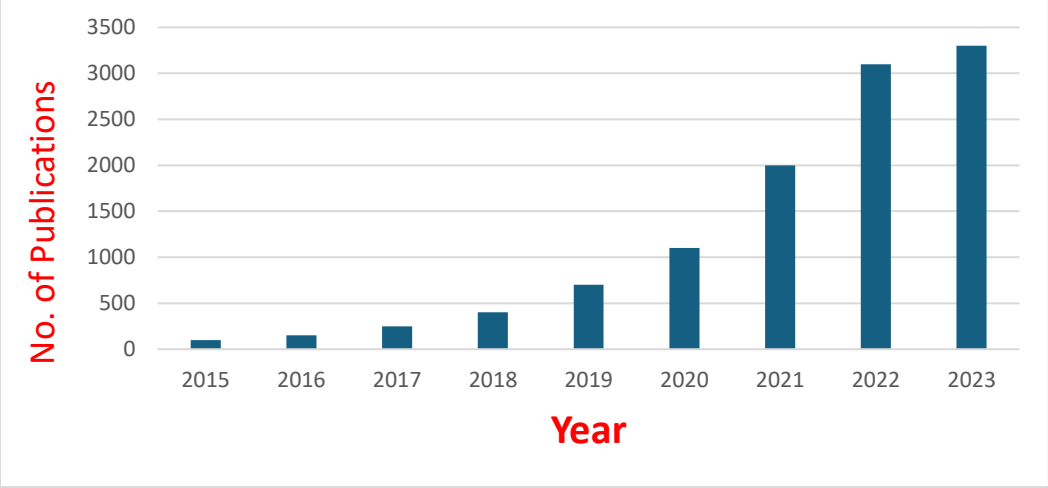

Figure 9. Research activities of DT.

1. Real-Time Examining and Predictive Analytics:

Monitoring in real-time is a foundation of DT skill, allowing operators to analyze and capture live information from instruments fixed during resources. Some sensors gather a piece of data,

involving performance statistics, structural parameters, environmental situations, and operative health metrics [187]. By adding these real-time records into the DT structure, operatives acquire instant perceptions into ability routine, enabling them to identify anomalies, detect latent problems, and select practical portions to guarantee reliability and safety. By employing the energy of DT technology, workers advance unprecedented awareness into optimizing energy output, maximizing reliability, allowing proactive maintenance interferences, and performance and operational health [188], [189], [190].

DTs permit operators with capabilities of decision-making data-driven, qualifying them to command informed selections concerning strategies of risk mitigation, optimization, and asset maintenance [191], [192]. By requiring operators with illegal insights to come from progressed operational efficiency, extensive asset lifespans, predictive analytics, and real-time monitoring, DTs enable enhanced asset performance. A probabilistic structure was presented in [193] Improve the structural reliability of infrastructures by leveraging data from DTs. The acquired information from DTs participated in a critical task in revising and quantifying the vagueness associated with parameters of load modeling and structural dynamics relating to fatigue harm accumulation. This structure was operated done two numerical scenarios starring a distinctive OWT [194], operating data from determined DTs [195], [196], as displayed in Figure 10 [197].

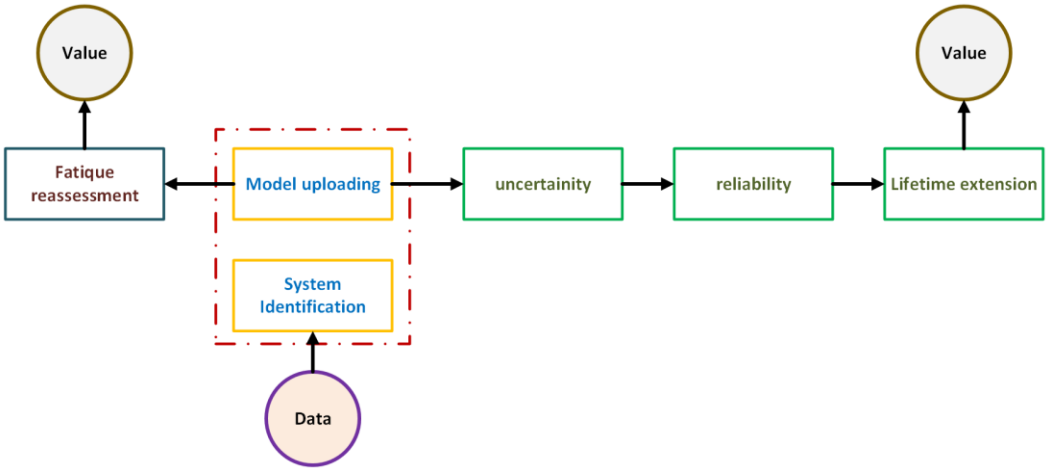

Figure 10. The numerical scenario of the model.

2. System Model of DT:

propose a DT-permitted metaverse occupied edge intelligence and communication for low-latency and ultra-reliable (CLLUR), which contains the virtual domain and physical domain as presented in Figure 11. In the virtual domain, DT facilitates devices' full replication of the physical domain involving the present working states, resource budget, and device configuration to cooperate with the physical matters in real-time. In the physical domain, there is a device set of Q Internet of Things in Industries (IoTI) (UEs), $\Upsilon = \{1,2, \ldots \ldots, Q\}$ which are casually allocated in an industrial section such as a smart factory. These devices of IoTI relate to a retrieve point (RP) via links of

CLLUR. There is an edge attendant (EA) linked to the RP to present both services of edge caching and edge computing to decrease the latency in end-to-end (e2e) tasks of offloaded computation-intensive from the UEs. In the control edge, metaverse service sources jointly adjust storage resources, computation, and communication, and make rapid decisions to effectively manage the whole system [198], [199].

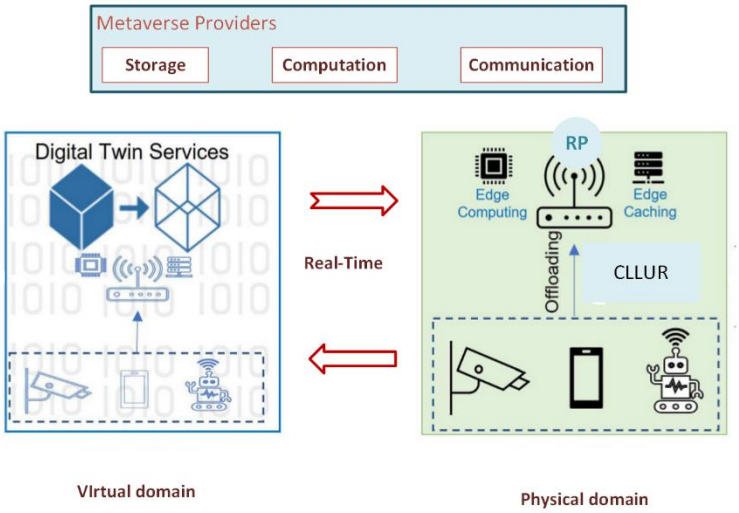

Figure 11. Physical & virtual domain of DT.

A. DT-Enabled Communication Model with Metaverse:

The RP is trained with H antennas to help Q single-antenna UEs.

$$l_i = \sqrt{ji}\,\overline{l_i} \in \mathbb{C}^{H\times 1} \tag{27}$$

Let be the station vector between the RP and the q-th UE, where l_i represents the coefficient of the large-scale station, and l_i is the small-scale vanishing obeying the distribution of $\mathbb{C}\mathcal{R}(0,1)$.

$$L = [l_1, l_2, \dots, l_Q] \in \mathbb{C}^{H\times Q} \tag{28}$$

Let be the station matrix from devices of Q to the RP. The coefficient of shared bandwidth of the q-th UE is represented by S_q. The sign-to-noise (SNR) of the q-th UE is provided by:

$$\gamma_q(s_q, z_q) = \frac{Z_q \|L_Q\|^2}{S_q S \mathcal{R}_0} \tag{29}$$

where S is the structure bandwidth, Z_q is the spread power of the q-th UE, and $\mathcal{R}_0$ is the spectral density of the single-side noise. Then, the transmission rate (bit/s) of uplink CLLUR is stated as follows [200], [201], [202] [203].

$$R_q(S_q, Z_q) \approx \frac{S}{\ln 2}\left[s_q \ln\left(1+\gamma_q(s_q, z_q)\right) - \sqrt{\frac{S_q X_q(s_q, z_q)}{\emptyset S}} M^{-1}(\varepsilon_q)\right], \quad (30)$$

Here, the transmission time period is the $\emptyset$, decoding error probability is the ε_q, $\gamma_q(s_q, z_q)$ represents the q-th UE SNR, $M^{-1}(.)$ is the inverse function of:

$$Q(w) = \frac{1}{\sqrt{2\pi}} \int_w^{\infty} e^{\frac{-t^2}{2}} dt \quad (31)$$

$$X_q(s_q, z_q) = 1 - [1+\gamma_q(s_q, z_q)]^{-2} \quad (32)$$

X_q is the channel distribution. As an outcome, the latency of uplink transmission is given by:

$$T_q^{co}(\alpha_q, s_q, z_q) = \frac{C_q}{R(s_q, z_q)} \quad (33)$$

where $C_q$is the size of data in (bits).

B. Estimation Model with DT-Permitted Metaverse (Mv):

A tuple illustrates a task that happens from the q-th UE:

$$K_q = (C_q, D_q, T_q^{max}) \quad (34)$$

where $D_q$is the required estimation source (cycles) and T_q^{max}) is the task maximum requirement of latency [9]. Let $\alpha \triangleq \{\alpha_q\}_{\forall q}$ be the tasks part of which is accomplished nearby at the UEs. Then, from the q-th UE, the offloaded share affected by the ES is $(1-\alpha_q)$. The service of DT for local q-th UE processing is represented as DT_q^{ue}, which can be demonstrated as:

$$DT_q^{ue} = (g_q^{ue}, \widehat{g_q^{ue}}), \quad (35)$$

where $g_q^{ue}$is the projected q-th UE processing rate, and $\widehat{g_q^{ue}}$ is the difference between the real worth and the processing rate projected value. The deviation can be negative or positive to model the simulated DT processing rate [204], [205]. Subsequently, the local q-th latency processing for executing a locally task is given by:

$$T_q^{ue}(\alpha_q, g_q^{ue}) = \frac{\alpha_q D_q}{(g_q^{ue} - \widehat{g_q^{ue}})} \quad (36)$$

It comes from

$$T_q^{ue} = \widehat{T_q^{ue}} + \Delta T_q^{ue} \quad (37)$$

with the estimated processing latency

$$\widehat{T_q^{ue}} = \frac{\alpha_q D_q}{g_q^{ue}} \quad (38)$$

and deviation latency is

$$\Delta T_q^{ue} = \frac{\alpha_q D_q \widehat{g_q^{ue}}}{[g_q^{ue}(g_q^{ue} - \widehat{g_q^{ue}})]} \quad (39)$$

Correspondingly, the ES processing latency to execute the q-th UE offloaded task can be determined as follows:

$$T_q^{es}(\alpha_q, g_q^{es}) = \frac{(1-\alpha_q)D_q}{(g_q^{es} - \widehat{g_q^{es}})} \quad (40)$$

where $\widehat{g_q^{es}}$and g_q^{es} are the deviation value and projected processing rate in DT. As we can see from these eq, the deviation between the projected processing rate and the real has altered the performance of the system. Then, it is essential for the DT to all the parameters exactly estimate the physical domain to prevent loss of performance [201], [202].

C. Energy and Latency Model with Edge Caching:

Modeling the strategies of task caching by operating variables of integer decision,

$$b \triangleq \{b_q\} | b_q \in \{0,1\}, \forall q \quad (41)$$

which specifies whether the task K_q is cached ($b_q = 0$) at the ES or not ($b_q = 1$). At the ES the task is cached, and only calculated the processing of edge latency [7], [8]. On the other side, when the task is not caught, it is generally handled with the model of offloading computing tasks. The outcomes restored from the RP to UEs are typically less (controlled messages) and the RP transfers the messages with additional power in the UEs, so we only believe the latency of uplink transmission [206], [207], [208]. As an answer, the edge caching latency model is stated as:

$$T_q^{e2e}(\alpha_q, g_q^{es}, g_q^{eu}, b_q, s_q, z_q) \quad (42)$$
$$= \frac{b_q D_q}{(g_q^{es} - \widehat{g_q^{es}})} + (1 - b_q) \times [T_q^{es}(\alpha_q, g_q^{es})$$
$$+ T_q^{co}(\alpha_q, s_q, z_q) + T_q^{ue}(\alpha_q, g_q^{ue})]$$

The whole consumed energy in the q-th UE, containing the energy for estimation U_q^{cp} and communication U_q^{cm} is given by:

$$U_q^{wh}\left(\alpha_q, g_q^{eu}, b_q, s_q, z_q\right) = (1-b_q)(U_q^{cp} + U_q^{cm}) \qquad (43)$$
$$= (1-b_q)[\alpha_q \frac{\theta}{2}(g_q^{eu} - \widehat{g_q^{eu}})^2 + \frac{\left(1-\alpha_q\right)z_q C_q}{R_q\left(s_q, z_q\right)},$$

where the constant 'θ' is the estimation power constraint for UE energy consumption 2], 8]. This model is proposed as a DT basis to permit metaverse functions by jointly studying the storage, computing, and communication, to minimize the latency implementation [209], [210], [211]. Adnan et al. examine the policy imperatives and impacts of socio-economic and emerging computing techniques in ref [212].

VI. Anticipated MAN Algorithm:

CF can be started by several events. Some of these actions are deprived voltage management and reactive power, main outages of TL, poor human reaction to power network procedures [213], and unprotected power networks with extremely loaded connection lines [37]. The MAN is initiated by the incidence of a contingency in the right network; we treated the N-1-1 and N-1 contingency TL [214]. The benefit of this procedure is that it does not need load shedding (LS) to avoid CF. Behind these contingencies, there is a superior possibility of the loaded line(s) in the structure; if this is the argument, eq 44 consider the loaded line(s):

$$I_{max} \leq I_m \qquad (44)$$

where I_{max} is the transmission line (m) current and I_g is the line's current maximum limit [215], [216]. Once the MAN proves there is no less than one overloaded line, the procedure initiates the main sequence of power dispatch for the conferred loaded line. Utilizing the initiated sequence, the MAN succeeds in power dispatching from the producers till that loaded TL is carried under the bound. The procedure then confirms if there is yet a loaded line; if there is a loaded line, the algorithm duplicates the procedure immediately expressed till all lines are caused beneath the control so the CF incidence and prevented the blackout procedures [217]. Each time the MAN tries each sequence, it guarantees that the power shipped constraint by every generator as assured in eq 45 is not abused:

$$P_{d_u max} \geq P_{d_u} \geq P_{d_u min} \qquad (45)$$

where P_{d_u} is the dispatched power by generator 'u'. $P_{d_u max}$ and $P_{d_u min}$ the maximum and minimum power restricts that generator 'u' can notice. There are constraints 'f 'numbers for a power network with 'f' numbers of producers.

The combination whole number T_c present for every transmission line dispatching power is:

$$T_c = (C_1^n)^f \tag{46}$$

where 'n' is the potentials for every system generator. The MAN remains on a transmission line solution if an individual combination instantaneously suits the constraints, where (47) concerns to the transmission line current:

$$I_{max} \geq I_m \tag{47}$$

There are 'q' constraint numbers (49) for a power network with 'q' transmission line numbers. The experimental procedure has to follow the equations of load flow which are:

$$P_{d_u} - P_{q_u} - \sum_{v=1}^{n_a} |V_u||V_v||Y_{uv}| \cos(\theta_{uv} - \delta_u + \delta_v) = 0 \tag{48}$$

$$Q_{d_u} - Q_{q_u} - \sum_{v=1}^{n_a} |V_u||V_v||Y_{uv}| \sin(\theta_{uv} - \delta_u + \delta_v) = 0 \tag{49}$$

where P_{d_u} and Q_{d_u} are the wholly real and reactive dispatched power by producers attached to bus 'u'. P_{q_u} and Q_{q_u} are the wholly real and reactive loads of power attached to bus 'u'. δ_u and $|V_u|$ are the voltage angle and magnitude at Bus 'u' correspondingly. δ_u and $|V_v|$ are the voltage angle and magnitude at Bus 'v' correspondingly; n_a is the network bus number. δ_v and $|Y_{uv}|$ are the angle and magnitude of the admittance on row 'u' and column 'v' of the Y-bus matrix or admittance of the network [218], [219]. There are n_a numbers of each of eq 50 and eq 51, Consequently, the whole constraint numbers that the MAN must fulfill instantaneously before it can avoid the CF occurrence:

$$f + 1 + 2n_a - 1 \tag{50}$$

in the problem of N-1 contingency and

$$f + 1 + 2n_a - 2 \tag{51}$$

in the problem of N-1-1 contingency [217], [218].

1. Collection of MAN Flowchart, Combinations, and Optimality:

The applicable combination(s) is heuristically preferred from the overall of combinations figure for every line no concern about how big the network is by utilizing the studies of power flow and

history of economic dispatch (i.e., ramping of generators and their impact on TL). For systems of real power, services have substantial information on the history of the economic report of these networks. Any modifications in the arrangement of economic dispatch affiliate with one of the arrangements. If such alteration makes the line 'm' current drive above the size edge, the sensitivity increase S_i of the agreeing combination for line 'm' is disciplined; but if such modification varieties the overloaded line current of a drive underneath the boundary, S_i of the consistent combination for line 'm' is satisfie,

$$S_{i_{mx}}(p+\Delta p) = \begin{cases} S_{i_{mx}}(p) - S_c \\ S_{i_{mx}}(p) + S_r \end{cases} \quad (52)$$

where $S_{i_{mx}}(p+\Delta p)$ is the sensitivity increase for combination 'x' of line 'm' at period $p+\Delta p$; while $S_c$and S_r are the sensitivity discipline and reward values correspondingly. The last sensitivity value for every pattern for every line is determined utilizing the squashing work.

$$S_{mx}(p) = \frac{1}{1+\exp\left(0.5 - S_{i_{mx}}(p)\right)} \quad (53)$$

where $S_{mx}(p)$ is the sensitivity of combination 'x' for line 'm' at period 'p'. Choice of the primary quantities of $S_{i_{mx}}$ varies on the clients, though the identical value S_{int} relates to all combinations. Hence,

$$S_{i_{mx}}(0) = I_{1\times N} \times S_{int} \quad (54)$$

Eq 54 confirms at all-time $0 \le S_{mx}(p) \le 1$. The suitable combination(s) for every row is heuristically chosen from the patterns with the maximum values of understanding [220].

The sensitivities support the MAN in the process of decision-making as transferring the network from one position to alternative [221]. This method will permit the algorithm completion on substantial networks wherever the combination number is too great to finish if directed in a fashion ad-hoc. It was learned from the outcomes, that the huge generator numbers in large networks support the algorithm quicker than it does for tiny networks which have controlled combinations and resources [222].

In optimality terms, two modes of MAN are applied. In the initial mode which has a limited optimality, when the procedure is determining the overload of a link 'm', it does not examine if other lines that were not initially burdened shoot over the size edge. The procedure only examines for the other lines municipal after it has resolved effectively the overload of line 'm'. In global optimality, the procedure examines the condition of all lines by dynamically solving the overload of line 'm'. If the procedure determines that the initiated grouping is about to enhance the overloaded line number, it finishes the practice of the mixture and repeals its moves and effects to

try the lines' next grouping [223], [224]. A flowchart gives the MAN operation in Figure 12. In the flowchart, damaged lines indicate that the box input receives/sends over the line. During every implementation of a combination iteration, adequate time delays are inserted in the procedure to guarantee the network is briefly secure to each variation and prevent disrupting either network synchronism or solidity [225], [226].

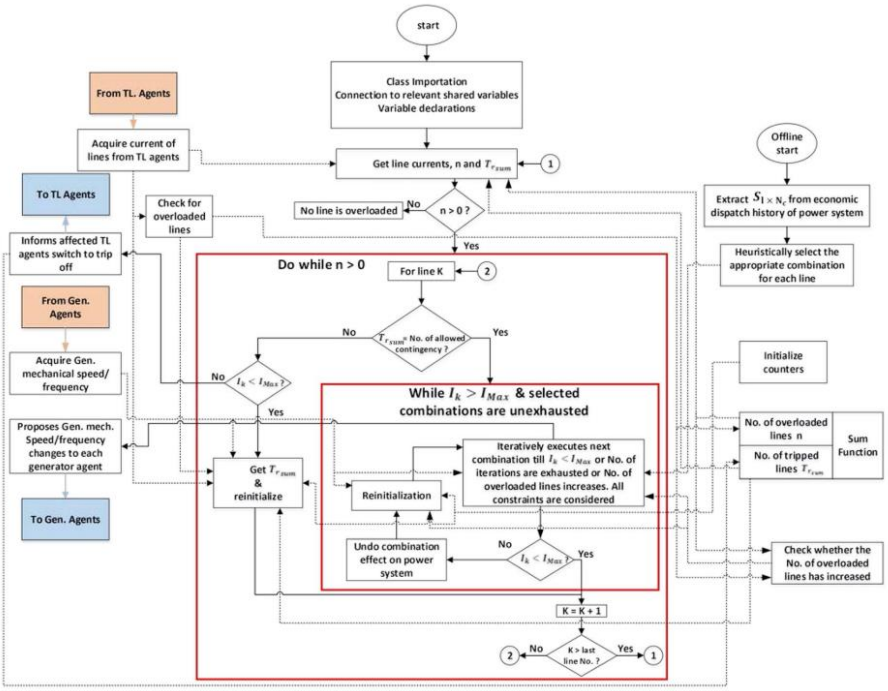

Figure 12. Flowchart of MAN algorithm from ref. [39].

2. MAN, Requirements and Assumptions:

The initial established of constraints is the main condition of hardware for any MAN comprehension in the real creation. This hardware necessity has shared pro programmability and communication competence. The second requirement set is the network assumption or state requirement which is needed for the restricted MAN applied to successfully halt the CF occurrence without load shedding usage. The first of these constraints is the presence of an adequate study of power flow and the history of economic dispatch needed to determine each combination's sensitivity. This is mostly present with the effectiveness or can be produced over studies of intricate simulation. The procedure must fulfill the constraints entire number performed relying on the contingency deemed as it stops CF [227]. If the generator loss is contingency, then there is a requirement for a reasonable equilibrium between the remaining generator's dispatchable power in the networks and the loads attached to the network. In this condition, none of the power organization constraints will be destroyed as the procedure attempts to avoid CF; else, the procedure will barely locate a resolution fact for avoiding CF in the network [39].

VII. Blackouts Effects (BE):

Unintended power blackouts and outages have noteworthy effects on industries working in the involved zones [228], [229], [230]. Human actions worldwide are substantially determined by power source to a level that, when a power network downfall, several impacts are suffered. In Figure 13, power blackouts have political, economic, and social effects on today's human actions [231].

Informally, when experiencing a blackout, road and rail traffic schemes, and medical systems, are heavily disturbed [232], [233]. Facilities in towns and big cities, like water source, relied on electricity to pump and treat water for industrial and domestic usage. The power loss effects in such advantages basis to an end. Water damage for big cities puts a giant health danger—for instance, in specific nations, disease outbursts appear, which can gross lives. Drugs and vaccines that make refrigeration are in danger in the experience of a lengthy blackout [234], [235].

In business, massive economic victims appear due to downtime of production and manufacturing industries, closure of payment networks, and internet breakdown [236]. Industries, although having reserve generators, can immobile drop generation hours ensuing in failures in revenue from declining to encounter targets or demand [237]. Entry ports (rail/road/air/sea) push economies and heavily rely on control tower electricity to handle vessels that make winches to transport goods. The wait in offloading/loading of cargo at seaports can have CF impacts i.e., essential goods like food, medicines, and oil. Unpreserved goods at ports are in danger due to a failure of refrigeration and delay in delivery or shipping [238].

21st-century Agriculture has become broadly determined by mechanization to extend the appropriate yield needed to forage the extending residents. Significant apparatus such as irrigation meets the usage of pumps to obtain water from rivers and boreholes for animals and crops to treat the yield. The power damage can produce farmer overwhelming loss to a in the farm line of making. The blackouts have major effects on the utility corporations that are needed to compact with the blackouts [239], [240].

Through a blackout, the safety techniques are halted, and, if there are rejection backup power resources, this can be a radical warning to a state [241], [242].

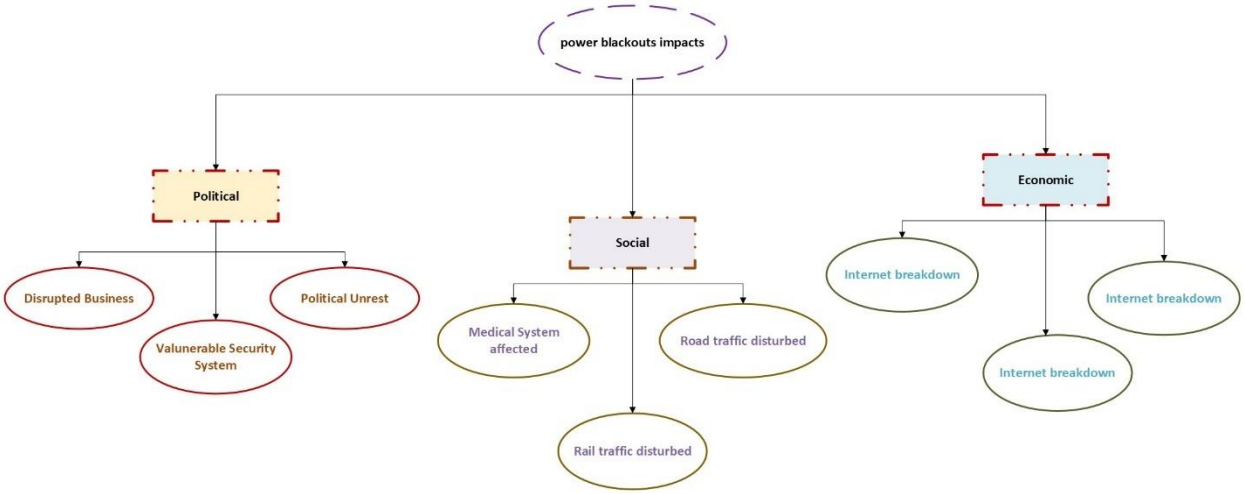

Figure 13. Effects of power blackouts.

VIII. Blackouts and Cascading Failures:

Mostly blackout is demarcated by the Transmission Network System Operator by European Electricity (TNSOE-E) as, ‘‘the processes of electricity interruption in transmission, generation, consumption, and distribution when transmission network operation or a portion thence is finished.’’ The effects of blackouts are well known, with socioeconomic ramifications and simple technological [243], [244], affecting all societal effectiveness. In ref [245]The author explained the electric power infrastructure and resilient network implementation to avoid blackouts. It is viewed that outages of power are a persistent issue, affected by various reasons. most general reasons involve, but are not constrained to, poor network planning, high demand of load, extreme weather, etc. Hence, a blackout is affected by an order of jointly exclusive, multiple, low-probability actions. This creates into the process play of CF. A CF is ‘‘the unrestrained sequential system loss triggered quantities by an event at any situation [246]. Some blackouts are instructed by some power grid general disorder, indicating propagation of CF across the whole system [247], [248]. The affected user's number, occurrence year, and origin country, of some main global blackouts from the 2003-2022. The heaviest blackout, in conditions of affected users in 2012 appeared in India during a critical blackout of 15 hours, involving an alternating 620 million humans. Other important blackouts occurred in 2015 in Turkey for about 8 hours, involving 70 million, and in 2021 in Pakistan (affecting 200 million humans, 9 hours). The most general details of these blackouts were poor weather requirements, extremely strained networks, or a mixture thereof. The rising combination of RES and the rapid power system digitalization has substantial inferences on power system CF. This builds a combination of complicated interactions between aspects of cyber-physical and physical power structure. The faith in interdependent and interconnected networks may increase the potential impact of CF. A failure or localized disturbance in one portion of the network can spread through physical components and networks of digital communication, leading to disruptions and widespread outages [249].

1. Cyber Security and Grid Digitalization (GD):

The outcome of enhanced power grid digitalization is the convergence between systems of Operational Technology (OT) and Information Technology (IT). While presenting control capabilities and greater monitoring, this has carried forth severe concerns about cyber security. CF accelerates and is triggered by power grids with mean cyber-attacks, indicating harmful concerns. A coordinated and sophisticated cyber-attack through numerous places may fail the entire organized power grid of continents or nations. This is a threat of real modern-day, as proven by the Ukrainian power grid CA in 2015 and 2016 [250]. It is the power outages cyber-attacks results.

Figure 14 describes the past 5-6 years of incidents of cyber-attacks in power systems. There is an enhancing cyber-attack threat on the power network. In 2015, the Ukraine attack initiated intermittent power outages, concerning above than 225,000 individuals. In 2016, complicated malware was applied which managed to be a distraction in the distribution network. In the end, over 200 MW of power outage and load is lost. However, on March 9, 2020, it was informed that the IT association of TNSOE-E was cooperated in a cyber interference. A current study has exposed that the outage was associated with 'RedEcho', a group of active hackers. The sophisticated malware is used by attackers to object a center of regional controller, in an operation taking over 6 months [251]. Thus, power systems cyber protocol has occurred as a critical and dynamic research area [252], [253].

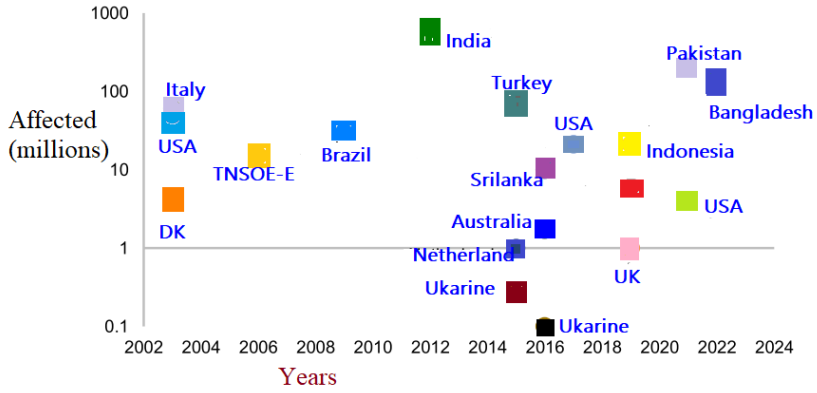

Figure 14. History of Cyber-attacks.

2. The power network blackout anatomy is summarized as given:

i. Prerequisites: describe the underlying vulnerabilities or conditions in the power network that may occur earlier to a blackout. These can involve operational limitations, ineffective maintenance, or deficient infrastructure.

ii. Triggers: factors or events that originate the blackout. They can be exterior incidents such as human errors, equipment failures, natural disasters, or severe weather circumstances. Initiates can also be core factors like voltage instability or network overloads.

iii. Remedial procedures and Emergency disorder: once the triggers begin, the power organization states an crisis. At this phase, several remedial events must be agreed upon to prevent a concluded blackout and stabilize the network. This program may involve redirecting power flows, generation alterations, or load shedding.

iv. Additional triggers: In addition to the primary triggers, additional causes can add to the blackout rise. These can add a lack of contingency plans, or ineffective actions by the system operator.

v. Fast and slow CF: refers to the interconnected and progressive failures that happen in a power network. They can be classified as fast or slow relying on the pace at which they generate.

a. Fast CF:

On the other side, exhibits a simultaneous and rapid multiple elements collapse, leading to a severe and sudden blackout.

b. Slow CF:

It is depicted by a power system's steady deterioration, where one failure of an element leads to enhanced stress on others, ultimately resulting in disruptions system-wide.

The Point of No Return (PNR) is reached sometime among these two levels. This signifies an inflection stage between the results and stages in a blackout, i.e., deficiency of power resources to a substantial portion of the whole power network. This process can also be imagined through the arising Figure 15. All power grids are proposed to fulfill the N-1 principle, i.e., a failure of one element/component does not affect the entire system ruin. However, a single failure combination can cause an effect of CF through the link [254], [255]. Impacts like operational errors and relays Hidden Failures (HF) [256], [257] can increase the effects and worsen network conditions of a specific failure.

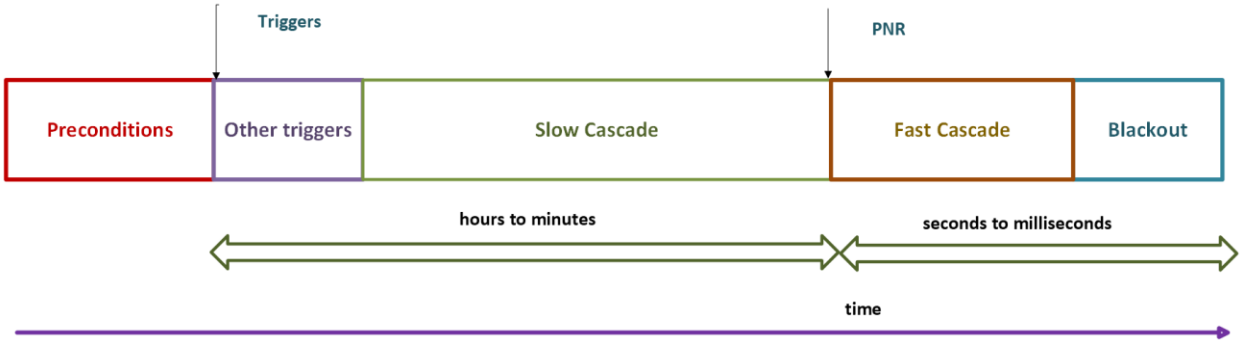

Figure 15. Two stages of blackouts.

IX. Cyber-Physical Aspects:

Operations in a power system have large disturbances that can be caused by a chain of incidents. If these incidents are not controlled or managed, they can start to blackout similar a CF. For a certain power network with ‘l’ successive failures and ‘n’ components, the component's successive failure is presented by ‘nl’ combinations [258]. Thus, it is unworkable to verify all combinations. However, CF-induced blackouts reveal some continual properties, such as:

- failures at system-level,
- Hidden Failures [259],
- Human errors,
- natural disasters and Extreme weather.

A sequence of CF, power network dynamics cooperates a crucial role [260], [261]. A critical event or major disturbance in the power grid begins a divergence between demand and power generation, primary to the system's unsafe operation. Accordingly, transmission lines and generators can become overloaded, triggering the voltages and system frequency to decline. To maintain the voltage and frequency within acceptable constraints, load shedding is frequently assumed. Still, if the curbed load is not enough or if the activity is suspended, extra generators and transmission lines may trip, indicating a domino CF effect. A whole CF can require everywhere between minutes to hours, containing two discrete stages, i.e., ‘fast’ and ‘slow’ [262], [263]. This can be visualized in Figure 16 which explains the two stages for the blackout in Canada USA 2003. The maximum harm is affected in the ‘fast’ stage, causing a domino impact that implies interruption of components and rapid tripping. This stage typically happens at the end of a structure of CF, with an end of no revert. It comprises dynamic phenomena and highly non-linear, such as:

- frequency variations,
- overloading of transmission line,
- synchronism loss,
- voltage instabilities,
- generator disconnections,

It plays a major physical phenomena function in the spread of CF. Power network subtleties can also be substantially altered by ICT organizations [264], [265]. This contains protective relays, generator controls, protection systems, substation automation, etc. With the cyber-attacks looming threat on power structure, the effect evaluation of Cas on the dynamics of power systems is a fundamental subject.

Hence, a complete assessment of the key phenomena and dynamic factors influencing CF is granted in the following subsection in the Figure 17.

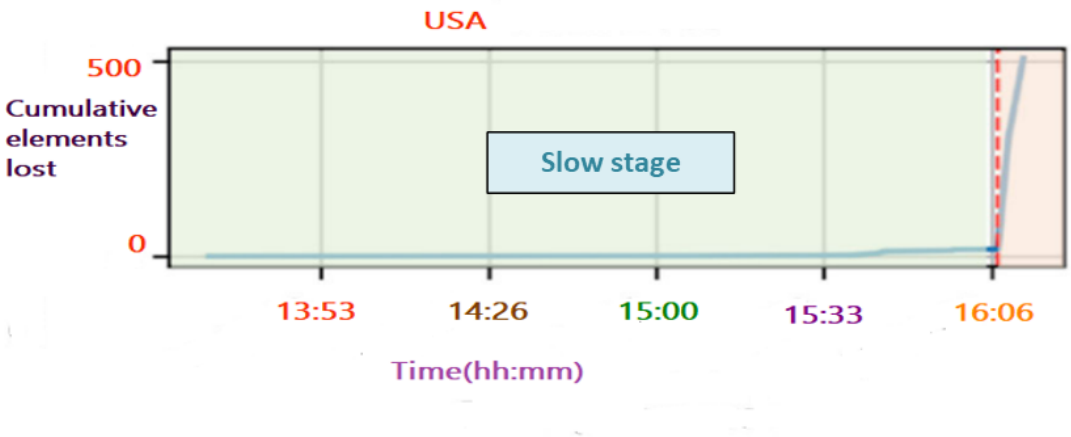

Figure 16. Damage of elements in blackout.

1. Critical Factors and Categories:

A. Transient Stability:

CF's most impactful incident is the synchronism loss and generator units' disconnection. Lacking adequate power manufacture destabilizes the power grid promptly. The main contributing reasons to transient instabilities in CF are the arising:

(i) Time required for Fault-clearing:

The main transient stability necessity is the approval of the identical-area condition, i.e., the generator rotor absorbed kinetic energy (KE) during fault or acceleration situation must be equivalent the dissipated KE throughout post-fault, deceleration. Therefore, faults must disappear as fast as possible to stop synchronism loss. Hence, a cyberattack that controls their linked communications and protection schemes to cause enhanced times of fault-clearing can result in a synchronism loss. This may be feasible via attacks of Denial-of-Service (DoS) which pause the transmission of essential limit orders, as examined in [266], [267].

(ii) Demise of generation:

In CF incidents, angular variabilities may appear due to abrupt system changes or components' significant disconnections, leading to rotor angle variabilities. The quick harm of a line switch or substantial generator can generate transient instabilities. As argued in [268], [269], pursuing the wave rapidly switching and generator controlling them out of period can end in transient variabilities. Thus, the generator can get disconnected and consume synchronism or even be harmed.

(iii) Generator Restraints:

The decisive view to confirm transient stability is the generator's fatal voltage, AVR is used for controlling finished-field excitation. Therefore, a CA modifying the parameters of field excitation

can pretend system transient stability. This is particularly confirmed in a synchronized attack, indicating multiple components loss. Usually, generators are supplied with various interface schemes and protection relays, to protect them in the case of a major fault situation. While confirming the generator safety that can cooperate the rest of the network with similar protection relays, during the process of CF. This directly degrades the CF process of the system [270].

Generators have switching attacks that are significantly discussed in [271]. This study proves how CA can initiate CF and separate generators. Furthermore, ref [272] reveals the substantial effects of such Cas on the power system and machine. Thus, a CA to cooperate with transient variability can promptly disconnect and link the primary circuit breaker of generators. Such an enhanced attack can disrupt the whole power structure in an issue of a few seconds [273]. This can outcome in a synchronism shortfall in the system's remaining functions. Successively, other units of the generator may be tripped, causing a blackout on a large scale, and probably involving significant quantities of restorative forces.

B. Damage of Transmission Lines (TL):

Approximately all blackouts and damage to TL have performed a general part [274], [275]. The major IEs beforehand the CF involve interaction with vegetation, extreme weather terms, unplanned or excessive power transfers, etc. Several critical causes within this sort have given to real-world CF.

(i) Protection operation in the distance of Zone 3:

A fundamental aspect that is constantly examined in numerous critical CF outages is the inaccurate protection strategy of zone 3 TL distance. Extreme loading, linked with comparatively low network voltage, confuses the distance relay with the overloading circumstances for an uncleared fault in zone 3 as the impedance competes in the protection 3rd zone. Such an occurrence has been described in the sources [276] and signed in real-world blackouts and CF such as Turkey 2015 and in 2003 USA-Canada [277]. Such severe aspects can be guided by cyber-attacks that trick communication dimensions with schemes of supported protection [278]. Modifying the measurements of current or voltage suspected by relays may make it feasible to trip them wickedly. Furthermore, this aspect can be indirectly initiated in the incident of multiple line loss and switching attacks.

(ii) Overloaded Lines:

When overloaded transmission lines are outside their nominal parameters, due to enhanced I2R losses, they turn to dissipate and sag substantial heat. This concerns both electrical and thermal facts. If left unimpeded beyond a particular period, by using overload protection they are tripped automatically. In adverse incidents, it can sag the overhead lines, encounter vegetation, and due to flashover trips happen. Hence, overloading resolved off a chain of CF; systems with additional parallel lines may get trip as well and overloaded [279], thereby strictly cooperating network

integrity. It is observed that the overloading of the overhead line is a ‘slow’ incident, in association with other categories and dynamic parameters argued subsequently.

Flashovers and line sags can take place everywhere from minutes to hours. Remarkably, the propagation of CF non-locally, i.e., the beginning incident might be a substantial distance away from following trips the line [280]. This line loss disconnects equipment and indicates system constraints such as frequency and voltage cross their limits. By obtaining access at once to the opening of several circuit breakers and substation controls, lines can be put out of examination, as observed during the attack on Ukraine in 2015 [281]. Therefore, it overloaded the parallel lines. If the primary lines are not put back into maintenance promptly, the parallel lines that are overloaded can also trip, starting a domino impact and probably a voltage failure. This can have a specifically damaging impact on the whole power network, as noted in Canada and Italy in 2003 [282]

C. Frequency Instability:

The frequency instability root cause is an inequality between demand and supply. This can be exhibited in multiple ways, as follows:

(i) Supply-demand inequality:

To initiate an inequality between demand and supply, multiple strategies of cyber-attack are feasible. In [283], tells how botnets may be required to quickly enhance power needs before it can answer to the mechanisms of frequency control. Using an example of continental Europe, they explain how this can indicate generation and load loss. Likewise, [284] presents a scenario of a cyber-attack to unnaturally control the demand for power through a signal of the spoofed market estimate.

(ii) Islanding:

CF affects connected generators tripping and overloading of transmission lines. This may outcome in islanding, i.e., the area's formation with a large inequality between demand and power supply. In the end, the islanded system's frequency can change greatly. This can also happen due to quick disconnections of large loads. In the system, relying on the synchronous generator inertia such a variance can initiate a Changing of Frequency Rate (CFR) protection to defend the generator units.

Expected the system inertias to reduce further, With the arrival of more generation from RES power [285]. Hence, CFR protection is a crucial parameter concerning CF and analysis of frequency stability. A cyber-attack resonance targeting load frequency and ROCOF generator control is discussed in [286]. In this class of attack, the opponent changes to modify the generator controllers from input signals founded on a significance basis, e.g., CFR. This outcome is a minus response to control of load frequency, such that the stability is lost from the targeted generator. Moreover, it concludes that the modified mean inputs remain within the common performing limit, thereby yielding the attack substantially cautious.

(iii) Loadshedding (LS):

To avoid cases such as corrective trial, islanding techniques such as Load Shedding in Under Frequency (LSUF) are accepted. These techniques lead to a load loss, thereby designing a power inequity. These techniques should be fast sufficient to avoid dropping the frequency; else, the network can be more disrupted. Persistent over-frequency or under-frequency situations can initiate automatic trips of the generators [287].

Hence, a cyber-attack DoS which affects a pause in load shedding command communication can ruin frequency strength, as given in [288], [289]. It is to be directed that all of the discussed things as mentioned earlier, and categories are not equally complete but intertwined [290]. For example, instabilities of voltage and transient usually happen together and are strongly linked. Likewise, transient instability and frequency unpredictability also affect each other. It is significant that exploiting cyber-attacks even one of the essential groups may cause CF due to the intense interaction connecting all the occurrences. Delaying this thought line, an organized cyber-attack can accelerate the structure of CF. A recent experiment has proven this mechanism of acceleration being monitored in main chronological CF outages [286]. In the incident of a corresponding cyber-attack, the power grid reached a point where a revert is not possible, initiating a substantial failure.

D. Voltage Stability:

System voltage is maintained at nominal principles and is vital to confirm and guarantee network control. The elementary justification for the volatility of voltage is the failure to satisfy the demand for reactivity. Therefore, losses of reactive power can rise, indicating voltage sags. Through a CF activity, due to rapid and sudden elements falling, it drastically changes the bus voltages, causing serious voltage instabilities. Reactive or active power output changes can cause issues in reactive power and power swings, respectively. Hence, either backup or primary protection relays can fall, causing a voltage collapse. This usually activates protection schemes or LSUVs that remove sections due to particularly down voltage points. The deficiency of adequate voltage points collapses the whole power structure, causing a blackout. The voltage stability concerning critical factors during a CF is as follows:

(i) Excitation of generator:

for every synchronous generator grid-tied, Var/voltage control is presented by the Regulator of Automatic Voltage (RAV) by modifying current on-field excitement. Hence, generators can be over or under-excited, relying on the requirements of voltage adopt. In the incident of over or under-excitation, can trip the generator's AVRs for safety purposes. This can hypothetically initiate issues of voltage stability in the other contingencies case. In such a superior scenario of cyber-attack, AVRs targeting generator is considered [284]

(ii) Line overloading:

Due to the risen flow of reactive power, it can heavily load the transmission lines, affecting voltage drops. Consequently, due to distance or overload protection, they can be tripped, combining further issues. The cyber security influence of this reason is discussed earlier.

(iii) Compensation of reactive function:

The root of voltage variability is the unacceptable compensation of reactive. Reactive power defense devices such as Static Compensators (STATCOMs) and Static VAr Compensators (SVCs) can be affected by attacks of data modification to modify injections of reactive power [282]. In the worst situation, this can cause critical instabilities in voltage and direct a voltage collapse.

(iv) Voltage regulation:

Voltage-regulating tap changer mechanisms are used for compromise to affect voltage stability. Resources of Distributed Energy (RDE) with increased presence give a further attack area in the future. These DERs are estimated to interact with grid edge, via the Internet of thing (IoT) that are also at risk. Ref [274] examine the vulnerability exploitation in photovoltaic (PV) inverters to connect remedial processes and initiate unusual voltages to prevent this situation.

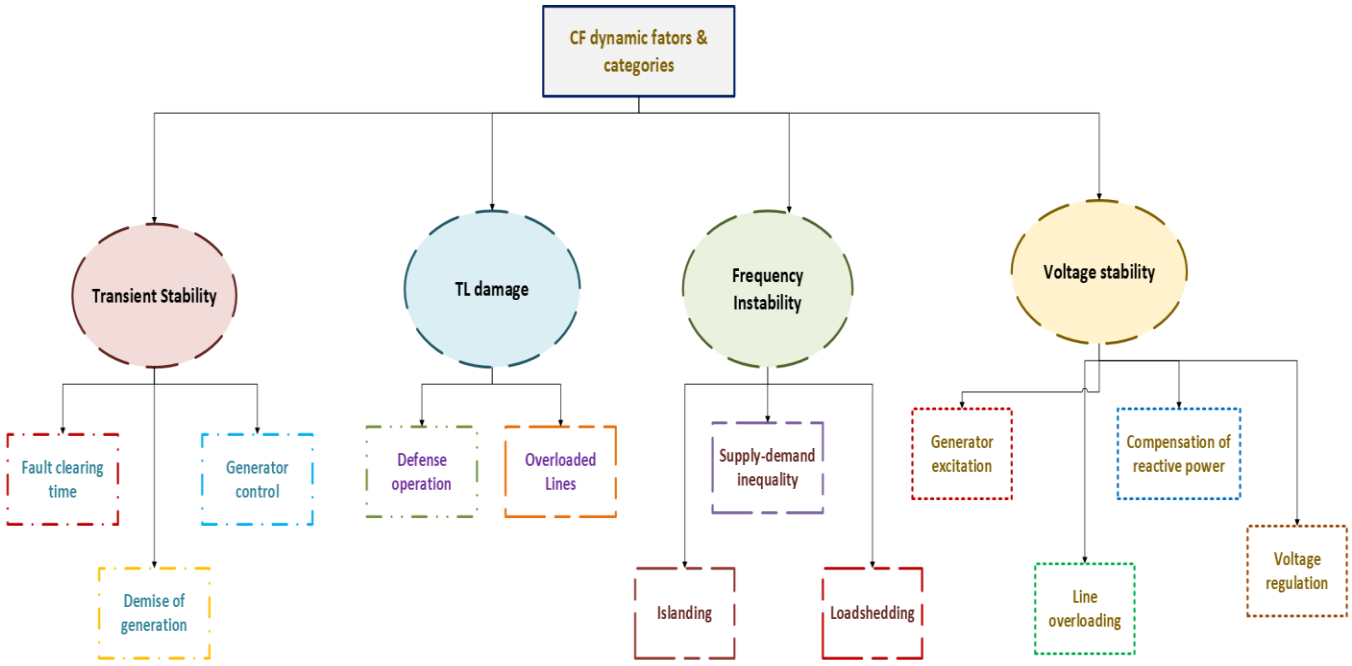

Figure 17. Dynamic categories and factors of CF.

X. Artificial Intelligence (AI) for system resilience:

AI incorporates various approaches, algorithms, and techniques to permit computers to achieve tasks that classically require language translation, visual perception, speech recognition, human intelligence, decision-making, problem-solving, and further. Although its general integration throughout several phases of human existence, AI rests a moderately evolving and nascent domain, requiring a formal definition and universally acknowledged [291]. Ref [292], the author suggested the network instability situations, transformation for

The AI landscape constantly evolves, incorporating numerous methods and technologies that track the common intention of evolving AI systems [293]. Amongst the divisions of AI, here is Machine Learning (ML), which states “the determined procedures that can repeatedly detect data patterns, and then utilize the exposed designs to expect forecast information, or to achieve another choice assembly type below uncertainty” [294]. Then, while the two phrases are often swapped, ML is studied as an AI subset directed at procedures that can study information and utilize the acquired facts to make predictions or take action. Phrases are frequently swapped, and ML is deemed a subgroup of AI-fixing procedures that can discover information and usage the obtained learning to take actions or make estimates.

1. Topical zones with AI in reliability and safety:

A. System prognosis (SP):

SP states the procedure of assessing the system's future health state, which usually includes components or predicting the system's Remaining Suitable Life (RSL), given its present condition and running history [295]. The target of SP is to provide caution against failures of potential tackle and allow state-based schemes of predictive protection. These methods can upgrade overall network reliability, lower maintenance costs, and minimize downtime. There are main primary methodologies to SP, which are generally grouped as data-driven and non-data-driven [296]. The end directs on analytical, physical models, or developed models across expert data. In the earlier, data is utilized to create a model that can forecast the status of the forecast health of a scheme; here, past facts from other sources or sensors are utilized to progress a model that forecasts the other health displays or RSL of a network. Together methods have their disadvantages and compensations, and the selection of methodology relies on circumstances such as the expertise of the specialists, the complication of the technique, and the availability of information. Data-driven methods are repeatedly utilized when a huge data extent is accessible, and when the structure is extremely complicated for physics-based or analytical forms [297].

B. Fault diagnosis and detection (FDD):

FDD is a critical procedure in various industries, such as chemical, energy, aerospace, and manufacturing [298]. Fault detection engrosses detecting when a fault happens in a equipment or system. It usually involves monitoring several data streams, signals, or sensors or detecting any variations from the supposed behavior of the method [299]. Previously a fault is identified, an alarm may be produced to notify the applicable workforce to examine more. Fault detection's main goal is to primarily trap problems before they become more substantial concerns. In distinction, fault diagnosis implies establishing the fault root cause has been discovered. This route relates to evaluating facts from numerous causes to verify the inherent reason [300]. FDD can be a time-consuming and complex manner that forces the proficiency of technicians or engineers who are intimate with the system or equipment. The focal target of fault diagnosis is to dismiss repair costs and downtime by instantly fixing and identifying the trouble. In short, FDD is the procedure of

detecting when a fault appears, but the process of FDD is of concluding the fundamental fault cause [301].

C. Risk Evaluation:

Risk estimation is essential in several power plants, incorporating chemical trades, projects of civil manufacturing, nuclear facilities, and industrial sectors [302]. In these manufacturing, networks are frequently compound and have sharp hazards, where redundant consequences may end in substantial values, such as injury, financial losses, environmental destruction, or regular harm to existence [303]. Risk estimation extends to an organized method to evaluate and identify potential risks, and ultimately reckon their potential and likelihood outcomes. Risk estimation approaches point to measuring the incidence of discarded events (e.g., damage of physical reliability, loss of containment) and the difficulty of the effects (e.g., financial loss, number of accidents), which are ultimately gathered to make widespread risk facts. Lastly, risk stages are associated with risk-getting standards to appraise if the lasting hazard is needed or acceptable to be declined by executing risk-dropping procedures [304]. By accompanying risk evaluation, engineers can style learned conclusions concerning the operation, structure, and design of serious structures to lessen the impact and likelihood of dangers, confirming the sustainability, consistency, and safety, of these structures [305].

D. Reliability analysis (RA):

RA implies a process, element, or system's capacity to steadily execute its anticipated performance over indicated and below-described settings. It is a determination of how trustworthy and dependable a structure is and is frequently extracted as the network probability without failure will perform appropriately. Consistency determines influences such as operational conditions, maintenance, construction, and design, and can be evaluated via several techniques, involving analysis, demonstrating, and testing. Despite its significance, the assessment of reliability poses various tasks that must be defeated to confirm a perfect evaluation of network functioning. Including the others, there is difficulty. It develops progressively challenging to estimate method RA as interconnectedness and complexity improve. Also, uncertainty performances a critical part in RA as it can substantially bearing the accuracy of decisions and predictions. Particularly, it is hard to model uncertainty in different bases, such as material properties, assembly errors, manufacturing, and uncertain operating restrictions [306].

E. Anomaly detection (AD):

AD involves recognizing observations or data stages that divert radically from the sample expected or behavior in each approach [307]. Unlike fault diagnosis and detection, which identify the objective for the existence of a diagnosed burden or specific fault that has previously happened, [308] the designated “anomaly” specifies that the structure is different from standard operational circumstances, so further info is unavailable. Anomalies can be initiated by numerous causes, such as disturbances of several nature, incorrect operations, and equipment disasters, and can have

substantial concerns if left hidden [309]. Hence, anomaly finding shows a desperate function in arguing the efficiency, reliability, and safety of several industrial methods [310][311].

2. AI Methodologies and Functionalities for Reliability:

This elaborates on methodologies and functions of AI for reliability-adjusted maintenance. In ref [312], the author explained the artificial intelligence in navigating hybrid models in load forecasting. As a capable, practical point and the purpose relating to AI, the scholars categorized the vital resolves of AI as [313], [314], [315]:

- Classification,
- Optimization,
- Exploration of Data structure (DS),
- Regression

These are valuable means for progressing attributes of database evaluation, such as planning prospects, logic, and database analysis, as given in Figure 18.

A. Classification:

Scholars have recognized that fault diagnostics and abnormality findings identifiable arrangement task maintenance can choose fault tags with monitoring data condition. Yet, the reliable database might contain noise labeled in [316], including non-logical errors [317]. Scholars have also broadly studied methodologies of ML and deep learning and observed that they precisely deal with delivering input data essentials with a tag indicating the modules of k discrete [318], [319], [320].

B. Optimization:

Scholars have recognized that the optimization purpose offers a consideration of the most appropriate solution by diminishing or exploiting the unbiased purposes, comprising a particular set of available substitutes that are given disproportions, independence, or limits to please the results [321].

C. Exploration of Data Structure:

The scholars proposed that data structure includes gathering of the database. It regulates clusters of comparable information within a dataset, density calculation that directs the dataset supply within the planetary of input, and density of database those strategies of higher-measurement dataset down to a dataset of lesser-dimension for the futuristic failure [322].

D. Regression:

Historical databases spread much data to users. Furthermore, the precision of the forecasted approach is essential [323]. Then, effectiveness and accuracy interchange are essential for the methodologies of forecasted dataset-triggered energy [324], [325]. The investigators in [326] noticed that the shorter-term memory (STM) and more extensive and convolutional neural network

(CNN)-unified method [327] fails the discrete method in failing the error while seeking to integrate. This approach acknowledges the association between output parameters and erratic input to approximate the inference of extra active constraints on the estimated input limits. The professors in learned that among the SVM [328], and procedures of random forest (RF), polynomials predicted a small daily error at 0.58%. However, the algorithm's RF methods are unacceptable for long-term prediction. For example, in [329] the researchers discovered that the regression model (RM) could enable an intellectual controller among the modifying parameters of electrical output and input regulated [330].

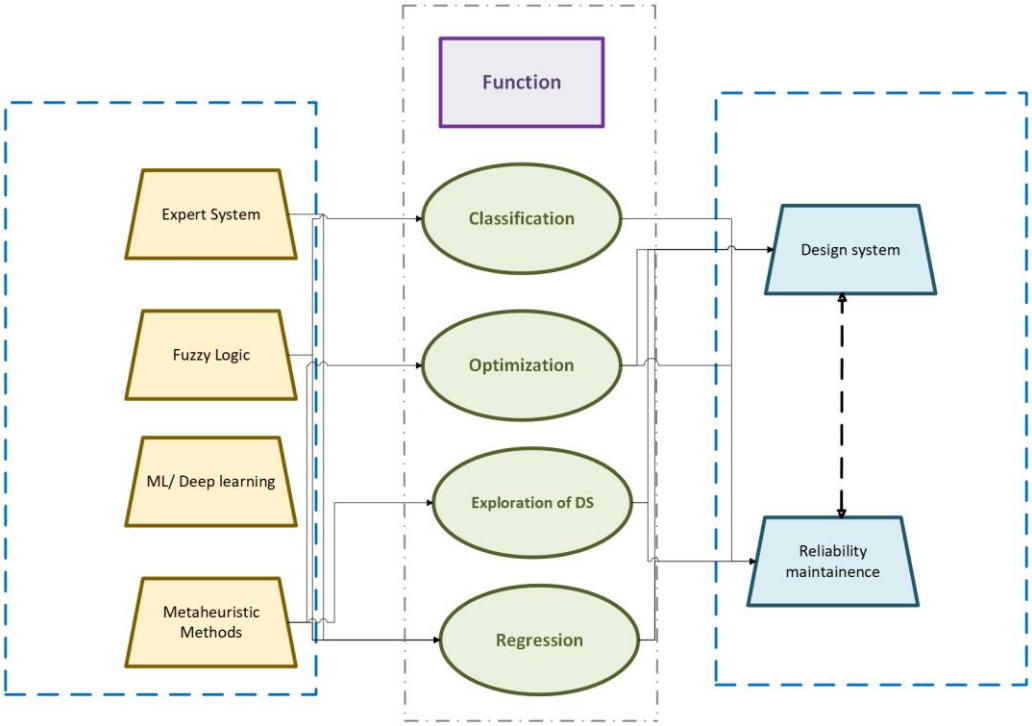

Figure 18. Database analysis of AI.

XI. Inceptions of Blockchain (BC):

The formation of BC began starting a white document printed in 2008 by Nakamoto Satoshi [331]. BC, also named spread ledger, admits sequential blocks, which relate to each other finished earlier block header with the hash value. The other timestamp-fated cryptographic hash, transaction data, and nonce are also comprised of a block [332]. The block timestamp is judged acceptable only if its estimate is greater than the two hours' time plus network-adjusted and more than the prior eleven blocks' median timestamp, which blocks challenger to affect the possible BC. Note that time refers to network-adjusted timestamps median from whole joined nodes. The blockchain's smooth execution is not just preserved by one or many nodes, as an alternative, each network blockchain node should obey a widespread consent protocol to validate and generate novel blocks. The consent procedure is the blockchain pillar where the legitimate actions and controlling laws are all structured [333].

The recognized bitcoin embraces the Proof of Work (PoW) method, which claims sappers supply a famous computing power number to guess out a solution for casual mathematical issues [334]. To prevent centralization of the difficulty, computing power, also entitled nonce of generation of the following block, is energetically modified based on per block in 10 minutes. While incredible computation power delays the mass of aggressors, PoW also directs to extreme energy consumption and a high rate of inefficient transactions. Proof-of-Picket (PoP) alleviates the difficulties carried by PoW, so the collier who suits the decisive success varies on their holding's extent in the consistent cryptocurrency more readily than computation supremacy [335]. The recent promising System of Interplanetary Folder (SIPF) spreads consensus of Proof of Space (Po Space), which makes applicants supply some space of storage to evidence a trial declared by the facility source [336]. The operation information is arranged according to the method used for each block Merkle tree, which develops the verification competence. Merkle tree allows clients to move any section for verification without completing documents of transactions. The overall blockchain parts and the handling of the transaction in a BC are illustrated in Figure 19 and Figure 20 correspondingly [337].

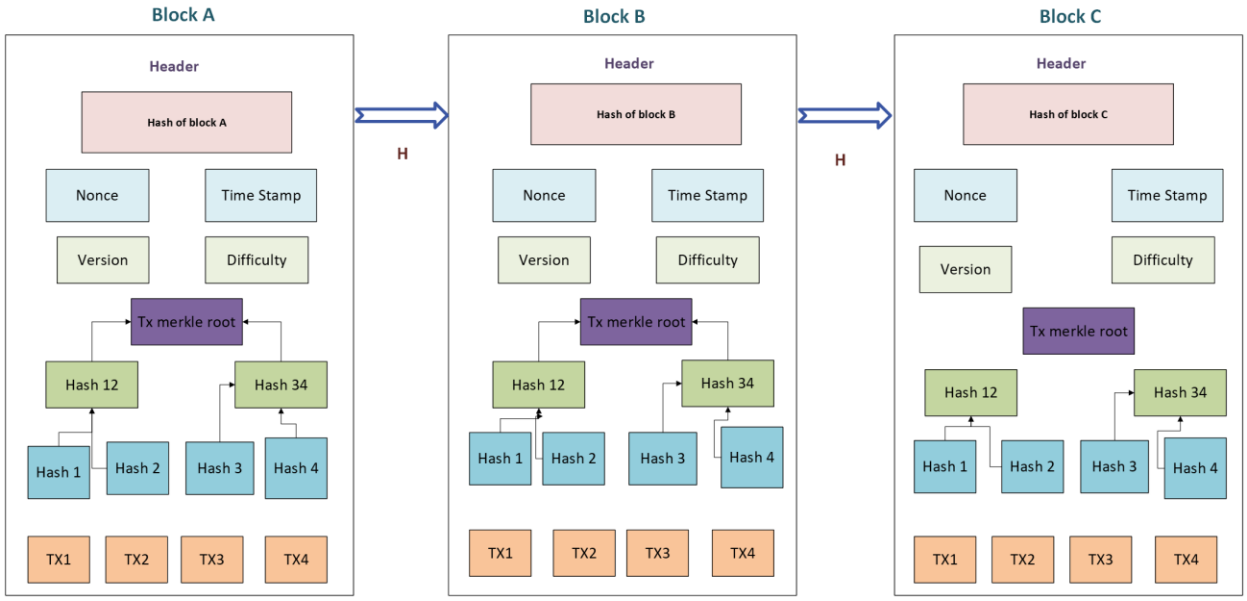

Figure 19. The general parts of blockchain.

BC is a capable key in this esteem due to its evident characteristics of transparency, immutableness, and decentralization. To improved recognize the role of BC in the MV, try to give massive research on the functions of BC for the MV [338]. Extensively review blockchain-based techniques for the metaverse (MV) from expert perceptions, such as privacy preservation of information, facts interoperability, data distribution, data storage, and facts acquisition [339].

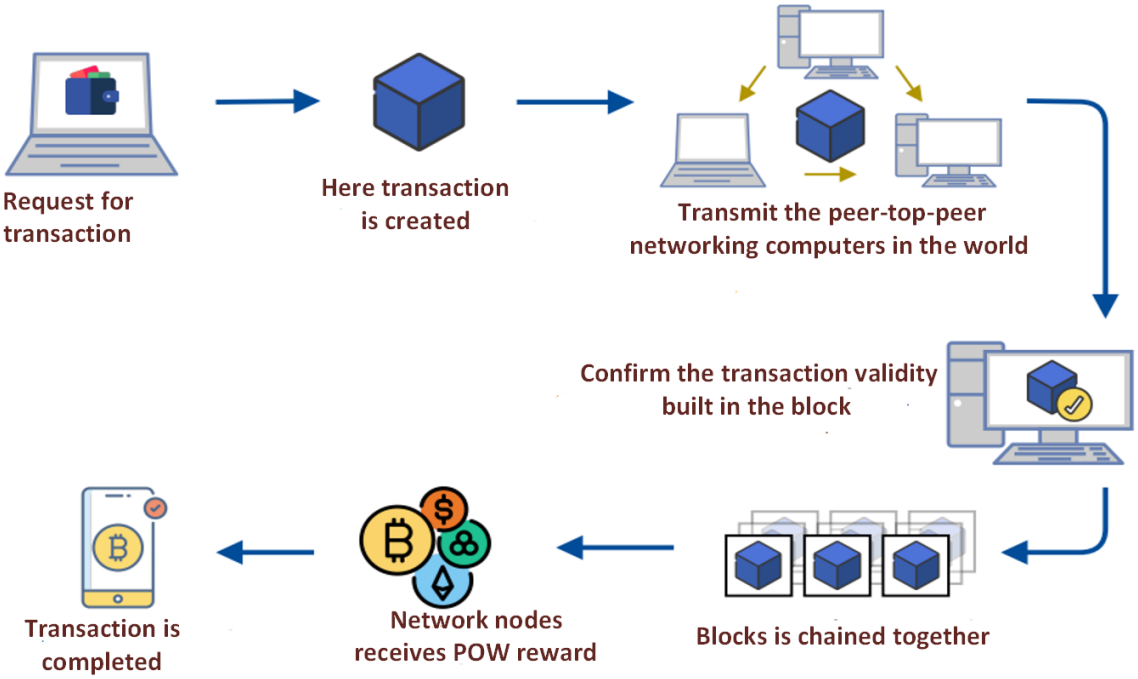

Figure 20. Transaction process of blockchain.

1. BC Model Generation for Reliability Framework:

A. Generation of Activity diagram (AD):

ADs symbolize the operation logic, the business logic flow or the use case. An AD can be exploited to imagine the dynamic actions of an approach through the unique flows of actions, such as concurrent and parallel activities [340]. An AD is applied here to characterize the oracle processes flow from demand to objection for external data, to the oracle carrying data off-chain, through to suggesting the data back to the BC. The description in these processes modeling was held at the equal level for all mechanisms of oracle to admit comparable evaluation of the processes of oracle. Centralized oracle schemes have an easier AD than decentralized oracle schemes. The generated AD for chain-link.

B. Generation of Success Tree Structure (STS):

The next stage in the approach engages the AD for the generation of an STS [341]. An STS is a tree structure that is used to identify and analyze the required components to accomplish the proposed success. The STS exhibits the elements and conditions to accomplish the top incident through a sequence of basic actions and several logic gates. An STS can be transformed into a risk analysis and FTD for reliability. The AD illustrated in Figure 21, examines that five actions are

essential for the oracle Chain-link to accomplish in asking for external data. Transforming gave us an STS with five procedures required to inquire about the external data [342].

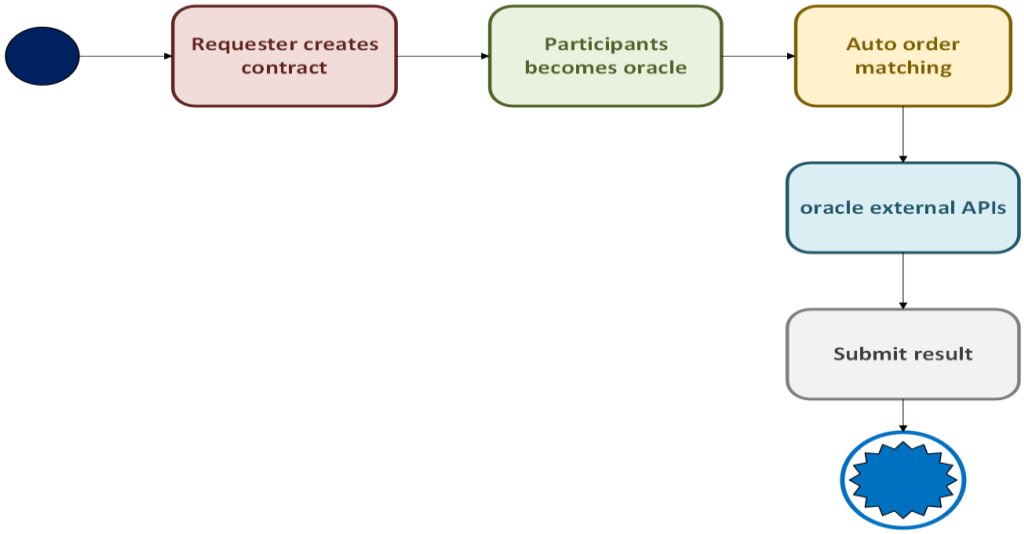

Figure 21. Five actions of oracle chain-link in blockchain.

C. Diagram of Fault Tree (DFT):

DFT is the set of an STS. DFTs are regularly used to investigate the hazards to economically critical and safe assets. It's widely applied in recognizing the risks of a system or software. DFTs are usually guided acyclic diagrams, where faults of components are developed at the leaves of the diagram. Logic gates embody how the faults reproduce. The DFT actions are the set from the STS, and gates are also switched, e.g. an AND gate from the STS is altered into an OR gate in the DFT [343]. From an AD it is the restriction of creating a tree structure that might not protect all lower-level sections isolated from publications, GitHub, and forums that impact the top incident. These lower-level sections are drawn onto the produced DFT to form the entire DFT, as displayed in Figure 22.

D. Reliability Assessment:

Reliability assessment is essential to operating, constructing, and designing economically essential technical procedures [344]. Numerous models and methods have been found to confirm systematic assessment of the risk and reliability of a scheme and DFTs are one of the most used models. A DFT created in the earlier step can be applied to conduct both quantitative and qualitative assessments for the reliability of the BC oracle approach. A cut set (CS) is an exceptional set of outcomes attained from a DFT that is enough to base the top event to occur. It gives a procedure for probability estimates and also shows the decisive links in the method design [344]. The lowest CS (MCS) is the CS with less events number that can basis the happening of the top event. By applying the complete DFT chain link in Figure 22 as an example, we can create the MCS equation (Eq.) for the DFT as below:

$$Z = \frac{Q1 + Q2 + Q3 + Q4 + Q5 + J}{M[Q6 + Q7 + Q8 + Q9 + Q10]} \tag{55}$$

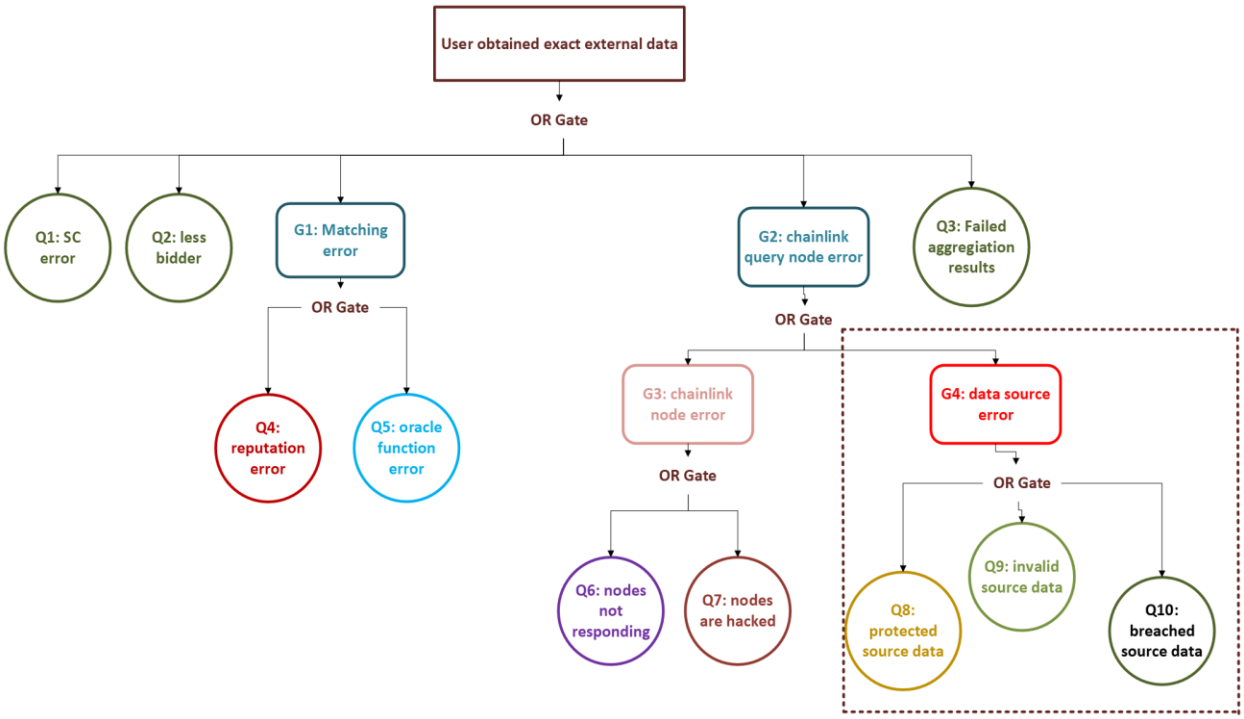

Figure 22. Procedure of DFT.

Chain-link includes 10 single-factor lowest cut sets [345], [346]. Any of the smaller incidents from $Q1$ to $Q10$ is enough to produce the top incident $'Z'$ to happen. Lower actions from $Q6$ to $Q10$ are limited by the gate, later we operated the reliability Eq. for J-out-of-M to lower actions $Q6$ to $Q10$. To estimate the reliability of BC oracles using DFT, use the reliability Eq. for a structure and reliability Eq. for the structure of J-out-of-M.

$$F = \sum_{j}^{m} \frac{m!}{j!\,(m-j)!} (e^{-\lambda z})^{j}\,(1 - e^{-\lambda z})^{m-j} \tag{56}$$

Eq 56 is the Eq. for the J-out-of-M system

$$F_{\text{Chain-Link}} = F_{Q1} \times F_{Q2} \times F_{Q3} \ldots \times F_{Q10} \tag{57}$$

Eq 57 below is taken from the MCS for the FTD Chain-link

By replacing the equation of system reliability $F = (e^{-\lambda z})^{j}$ and the complete Eq. can be produced:

$$F_{Q1\ldots\ldots Q5} = e^{-\lambda Q1 z} \times e^{-\lambda Q2 z} \ldots\ldots e^{-\lambda Q5 z} \tag{58}$$

$$F_{Q6.....Q10} = \sum_{j}^{m} \frac{m!}{j!(m-j)!} (e^{-\lambda Q6z})^{j} (1 - e^{-\lambda Q6z})^{m-j} \times \ldots \times \sum_{j}^{m} \frac{m!}{j!\,(m-j)!} (e^{-\lambda Q10z})^{j} (1 - e^{-\lambda Q10z})^{m-j} \quad (59)$$

Components failure rates are substituted into the Eq. to determine the overall oracle mechanism reliability [347]. BC oracle services and platforms are too latest to have enough historical information to estimate the component's failure rate empirically. Hence, to display the methodology used for reported failure rates for fixed software components. Some previous research on failure rates of smart contracts. The input values of the model are presented in Table 4. There are three types of general errors, which are human error, server error, and smart contract error. All matters related to infrastructure errors, data sources, and server hacks are gathered under the server failure classification [348], [349].

Table 4.Error types with failure rates.

Errors type		Failure rate	Examples
Human error	Server error	0.001-0.005	Server hacked
			Infrastructure error
	Hard task	0.1-0.25	Update new factors
	Routine task	0.06	Client-side error
			Reporter not reporting
	Smart contract error		Suicidal contract
		0.003678	Prodigal contract
			Greedy contract
	Simple task	0.0005	Close invalid data source

XII. Cascading Incident Analysis and Modeling:

Several serious CFs have been recorded, therefore; it is of major significance to develop proper models that classify the critical primary disturbances and prevent the cascading blackout of power networks in advance [350], [351]. Primarily, the cascading process and cause of blackouts must be experienced. Commonly, a blackout mostly begins as a solo failure of the system, which can, start to CF [352], [353], [354]. These cascading blackouts drop several people and can result in substantial economic losses. Earlier model making, figuring out the process and cause of cascading blackouts in essential power systems. Three main types of models describe power systems CFs.

- The first model type only explains the topological assets of power systems and overlooks the primary physics laws of electrotechnics principles [355], [356], [357].

- The second model type deems the quasi-steady state of power networks and determines the power flow by resolving the power flow equations of the alternate current (AC) or direct current (DC) [358], [359], [360].
- The third model explores the occurrence of CF by modeling the dynamic of power network components [361], [362].

Though, the analysis of complicated network approaches in power grids was examined by [363] and it was gathered that it is required to integrate the electrical and physical belongings. In the last periods, investigators from several domains were involved in the control and coordination of multi-agent networks [364], [365], [366]. Since in-power grid buses can be studied as smart agents competent to interact and communicate with their neighbors, an approach of the multi-agent network can be worked to protect and constraint of power system as in [367]. The research institutions and industry should have a thorough learning about the outages of cascading [368]. Electrical power networks cover considerable geographical regions and comprise numerous types of interlinked equipment together. Owing to this nature and structure, it is tough to understand the direction by which CF outages [353]. In this concern, investigators have dealt with a range of modeling methods of CF [369]. The most familiar technique for examining CF is the quasi-steady state (QSS) with the model of DC power flow [370], [371]. These models are robust and simple in defining overloads of cascading. The general challenge with the power flow of QSS-DC is that they decline to secure nonlinear systems. To model these methods of nonlinear, such as dynamic instability or voltage collapse, power flow QSS-AC models are worked.

In [372], [373], [374], [375], [376], power flow QSS-AC models are managed in cascading analysis effect. Just as they can manage the effects of nonlinear, models of QSS-AC have conjunction difficulties. As a finding, they need selected machine-developing assumptions. In [375], a sequence of together AC and DC models is suggested. This permits the load shedding with under-frequency and scenarios of under voltage to the modeled accurately. These procedures are better for models of DC but do not justify the voltage collapse effects. Some suggested methods based on simulation or historical facts to come up with the general cascading effect types. The procedures are generally proven as statistical approaches. In [377], [378], [379], [380] topological simulations have been projected. However, when employed for vulnerability assessment of power systems, they need adequate grid knowledge; then, the findings will be inadequate [381]. To recognize the mid-to-lasting strength effect on outages of cascading, statistical and dynamic methods have been concerned [382], [383], [384], [385]. It is essential, however, to also do simultaneous modeling of the protection operation and the approach dynamics as in [386].

1. Blackouts surrounding the World:

The power structure's capability to sustain stability and assure customers a constant electrical power supply during a disturbance event is critical [387], [388]. In this happening, when a power structure blackout appears, the outcomes can be widespread. Reasons of power structure blackouts comprise overloading or tripping transmission lines, quick-frequency drops, protection structures

mal-operation and control, cyber-attacks, equipment failure, voltage collapse, human error, poor maintenance, lightning attacks on power system equipment, and others [190].

In 2010, various power network blackouts happened, which exited millions of clients trapped for hours. For example, a power outage happened on 8 September 2011 in the Pacific Southwest, which continued for about 12 hours concerning 2.7 million people in Mexico, Arizona, California, and San Diego [389]. In this incident, the main transmission line tripping through peak load headed to the structure collapse. Throughout this, San Diego suffered a total of simulations and blackout in confirmed that inadequate load shedding conducted to the impacts of cascading. On 4 February 2011, a power network blackout happened in Brazil appropriate to transmission line flaws and it survived for about 16 hours. Almost 53 million clients were completely involved [228], [229]. On 30 July 2012, another blackout, which persisted for about 15 hours, happened, disturbing nearly 620 million people in the east and north of India. The blackout happened due to transmission lines (400 kV Gwali–Binar) overloading [230], [390]. The system collapsed again on the surveying day due to an imbalance of demand generation and almost 700 million residents survived when close to 32 GW of energy was suspended. This blackout is the heaviest power outage ever recorded in which people are affected [391]. In Vietnam, on 22 May 2013, a 500 kV line stumbled, splitting the southern and northern grids of Vietnam's power networks [392]. In the Philippines the same year, 14 power plants were reduced disturbing their center city Manila, and closing 40 % of the Luzon Islands [393]. The affected individuals were probably to be 8 million. The falling of transmission lines and generators is directed to the total voltage collapse in the structure. A lightning bolt affected Thailand's power network in 2013 assuming nearly 8 million people in 14 provinces [394], [395]. Bangladesh Power Network (BPN) suffered an overall network collapse on 1 November 2014, which continued for about 24 hours [396]. According to outcomes in [397], this was due to an unexpected outage of station high voltage direct current (HVDC). The impassive facts and rotating reserve around generators were under maintenance degenerated the condition [398]. After all stages of the load shedding under-frequency (LSUF) were triggered, the total load shed amount was less associated with the qualified disturbance, which controlled the blackout.

The development of the load-shedding BPN method was recommended as a solution of long-lasting in the future with comparable outages cases. The BPN power outage involved about 150 million people. A technical power station fault in Sindh on 26 January 2015 involved almost 140 million residents in Pakistan 10, [399], [400]. In Turkey, on 31 March 2016, approximately 70 million individuals had to survive power outages due to the failure of the power network [401]. Nevertheless, some areas that are combined with the Iran power system such as Van and Hakkari did not suffer the blackout. Approximately 10 million Kenyans on 7 June 2016 had their interrupted power supply for more than 4 hours when the transformer subsequently interrupted and tripped 180 MW of power [402]. Unrestrained events ensuing the power loss of 180 MW get worse the condition and headed to structure collapse. Table 5 illustrates the number of recorded power outages around the world in 2011. Each outage's average duration is assigned in a similar table in hours. From Table 3, it can be observed that of the less number of recorded outages in the

Caribbean and Latin America, during each outage the average period was extended than in the other regions. Almost 1200 power outages with a shorter period were suffered in South Asia. The existence of the wide incidence of power network blackouts across the world shown in Table *5* [403].

Table 5. Number of recorded power outages across the world.

Areas	**Duration of each power outage**	**Power outages**
North Africa and the Middle East	4.00	50
Central Asia and Eastern Europe	6.50	100
Sub Saharan Africa	7.50	210
Pacific and East Asia	6.00	200
Caribbean and Latin America	8.00	40
South Asia	2.50	1200
The rest of the countries	5.00	250

XIII. Challenges for Analysis and Modeling of CF:

This sector examines the tasks of analyzing and modeling CF in upcoming power grids. To address these challenges, feasibility study guidance is also sought.

1. Power Network with Cyber-Coupled:

Contrasting the guidelines of CF in an individual power grid, the combining of cyber directly and ultimately convinces opposing impacts on the standard controlling of a power network with cyber-coupled [404]. Cyber-attacks can indicate the closure of a power substation straightforwardly, though signal measurement attained in cyber approaches can be ultimately ruined [405]. Therefore, system operators are distorted to elect the wrong outcome in running the power organization. At this point, three challenges are declined to further increase the effectiveness and practicality of analysis and modeling of CF power systems with cyber-coupled [406].

- The first task is to understand the interdependence between power networks and cyber. The existing courtesy of the topological belongings of the joined network is other from standing sufficient in forming an exact template for the investigation of CF [407]. As an alternative to consuming some generalized conventions on the means cyber networks offer monitoring jobs to power schemes while the power networks are measured by the cyber fragments, accurate clarifications of the interdependence between power networks and cyber must be appropriately incorporated and considered in the model of failure. This stage will be vital to generating outcomes that are reliable with the substantial power grid [408].

- The next task is to examine the connecting arrangements in power systems with cyber-coupled [409]. The connection method of one-to-one could not be the appropriate interpretation of the correlation between cyber networks and power. Therefore, potential patterns of realistic coupling are found on real incidents of SGs is a fundamental step concerning an interdependent framework of network-based for exploring CF. Additionally, network-based models with multiple layers can be considered [410], [411]. A strategic management roadmap for a smart grid with the next generation is suggested in ref [412].
- The 3rd task is to examine the relations between defense and attack. The transitory of the relations between defense and attack, as explored in the transitory of Tse and Liu [413], is favorable to originating actual protective and defensive tactics for the critical organization and thus to keeping an extreme safety stage of the power grid with cyber-coupled [414].

2. Power Grid Penetrated with Power Electronics:

The superior invasion of power electronics equipment will model two definite topics in the analysis and modeling of CF.

- First, the actions of fast switching may cause new forms of failure of power components.
- Second, the devices of power electronics have less lenient abnormal voltages and currents and are close to zero inertia, as contrasted to traditional power equipment [415].

Such variations would undermine the standard functioning restrictions of the present power grid. Three tasks can be recognized to advance appropriate models in which the complete evaluation in the bottom-up approaches has participated in the top-down methods [416].

- The first task is to recognize new types and causes of failure of power components. The cumulative power electronics equipment use will spread the sources of failure of power components. Thus, a basic task is to classify and identify these new failure categories and have them connected and analytically contained with the presented descriptions of failure events [417].
- Another task is to indicate the crescendos of failure promulgation. The structure that influences the failure events happening (failure actions succession and their ensuing time moments) is the fundamental tread in the analysis and modeling of CF [418]. because of the reorganization of power flows, the mechanism is distant from the overloading tripping, and new dynamic forces of failure spread, carried by the fundamental character of power electronics equipment, should be appropriately comprised [419]. To contract with this task, mutual effects between power networks and power electronics disturbing the failure propagation dynamics must be distinguished [420].
- The 3rd task is to determine the assessment processes of the system’s presentation. The greatest empirical aspect of the analysis and modeling of CF is the power system's strength. Hence, practically applicable indicative methods that permit examination of the influences of raising access to power electronics equipment on coming power grids must be identified and applied for comparison and estimation of performance [421], [8].

XIV: **SG under Sensible Scenarios:**

This survey identifies further tasks when contemplating the SG under sensible scenarios. These tasks are summarized here:

- T1: To recognize the SG vulnerability, not only identify each component's assets but also illustrate the interdependence between components for any component failure can indicate unpredictable successive collapses. In correlated operations, the researchers fail to study the interdependence between elements. It is extremely challenging and involves a multifaceted method to recognize profoundly the SG vulnerability [422], [423], [424], [425].
- T2: From the perspective of attackers, achieving the greatest damage, it needs an effective attack algorithm in the SG. In previous designs, they proposed some efficient procedures for attacks of CF because they studied that the attack budget is infinite. As ever, these expectations are idealistic since the attack's scale varies on the resources of the presented attack [426]. In the system, there is an insufficient attack budget, and a CF does not always succeed. Hence, how to model a full method for defenses and genuine attacks in SG is a challenge [427], [428].
- T3: The 3rd task is how to tentatively examine the structure to plan a real defense and attack algorithm. Because the explored issue Critical-Line with Maximum-Impact through Limited Budget (CLMILB) is NP-wide-ranging, there is no method to acquire precisely the succeeding failures of the entire network, and it is also hard to regulate applicable workings for the direction of occurrences. The inquiry of guaranteeing for largest total effect of attacks on clients becomes tougher. Thus, the operation of the chosen algorithm not only alters a comprehensive assessment but also needs a detailed mechanism and technique for the SG susceptibility assessment [126], [127], [128].

To focus on these tasks, initially plan a unique attack procedure that reflects the partial attack funds, indicated as the Algorithm Based on Greedy Partition (ABGP), to extend the whole effect on clients. We then structure an applicable defence procedure, specifically the Algorithm of Defense Based Homogeneous-Equality (ADBHE) to defend essential components that support and decrease the impact of the ABGP attack on clients [154].

Table 6. Our work novelty with related reviews. Note: CF- Cascading Failure, AM- Attack Model, BE- Blackout Effects, MAN- Multi-agent network, CA- Cyber Attacks, GD- Grid Digitalization, SG- Smart Grid, IG- Interfere Graph, DT- Digital Twin, MV- Metaverse, BC-Blockchain.

Ref	Duration	CF	Reliability	AM	BE	MAN	CA	GD	SG	IG	DT	MV	BC	IoT	AI
[210]	2014-2024	×	√	×	×	×	√	×	×	×	√	×	×	√	√
[121]	2010-2020	√	×	√	√	×	√	×	×	√	×	×	×	×	×

[249]	2003-2022	√	√	√	√	×	√	√	√	×	×	×	×	×	×
[231]	2008-2019	√	×	×	√	√	√	×	√	×	×	×	×	×	√
[41]	2003-2023	×	√	×	×	×	√	×	×	×	√	√	√	√	√
[172]	2010-2020	√	×	√	×	×	×	×	×	×	×	×	×	√	×
[330]	2012-2022	×	√	×	×	×	×	×	√	×	×	×	×	√	√
[70]	2007-2017	√	√	×	√	×	√	×	√	×	×	×	×	×	×
[429]	2012-2021	√	√	×	√	×	√	×	√	×	×	×	×	√	×
[430]	2010-2020	√	√	√	×	×	×	×	√	×	×	×	×	×	×
[431]	2012-2023	√	√	×	√	×	×	×	×	×	×	×	×	×	×
Our work	Up to 2023	√	√	√	√	√	√	√	√	√	√	√	√	√	√

XV. Conclusion:

This survey provides an overview of introduction, causing, and attack models for CF, categorizing them into probabilistic models and physical models. The integration of DT, BC, and AI within an IoT-permitted Metaverse environment signifies a transformative methodology to focus on the challenges of CF incidents in SG. By leveraging DT, SG can complete predictive analytics, advanced simulations, and real-time monitoring, qualifying proactive interventions to avoid failures. BC, with its secure framework and decentralized, enhances automation, transparency, and data integrity through smart contracts, raising efficiency and trust in grid controls. Meanwhile, AI emboldens autonomous decision-making, adaptive control, and predictive modeling, significantly enhancing the grid's resilience. Simultaneously, these technologies establish an immersive MV where stakeholders can simulate, visualize, and collaborate solutions in a risk-free, dynamic virtual space.

Although these promising substantial challenges, advancements endure in realizing the deep capability of this integration. Interoperability among unrelated structures, scalability for managing large datasets, and cybersecurity involvements are pressing concerns that require urgent consideration. Furthermore, attaining energy efficiency for AI algorithms and BC operations through decreasing operational costs is critical for sustainable assumption. The IoT, while innovative, also appears usability encounters that must be addressed to confirm effective and accessible decision-making for all investors. Defeating these barriers imposes interdisciplinary, collaborative research attempts that merge expertise in data science, engineering, and human-

computer interface. Moving forward, the attention should be on user-friendly systems, cost-effective, and scalable, and that evaluate technical sophistication with operative feasibility. By addressing the recognized research gaps and proceeding with our consideration of this network, the integration of these technologies can become a foundation of intelligent, sustainable, and resilient, smart grids, accomplished by mitigating CF and confirming reliable energy sources for the future.

References:

[1] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Phys Rev E*, vol. 66, no. 6, p. 065102, Dec. 2002, doi: 10.1103/PhysRevE.66.065102.

[2] X. Zhang and C. K. Tse, "Assessment of Robustness of Power Systems From a Network Perspective," *IEEE J Emerg Sel Top Circuits Syst*, vol. 5, no. 3, pp. 456–464, Sep. 2015, doi: 10.1109/JETCAS.2015.2462152.

[3] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, "Evidence for self-organized criticality in a time series of electric power system blackouts," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 51, no. 9, pp. 1733–1740, 2004, doi: 10.1109/TCSI.2004.834513.

[4] H. Tu, Y. Xia, H. H. C. Iu, and X. Chen, "Optimal robustness in power grids from a network science perspective," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 1, pp. 126–130, Jan. 2019, doi: 10.1109/TCSII.2018.2832850.

[5] X. Zhang, C. Zhan, and C. K. Tse, "Modeling the Dynamics of Cascading Failures in Power Systems," *IEEE J Emerg Sel Top Circuits Syst*, vol. 7, no. 2, pp. 192–204, Jun. 2017, doi: 10.1109/JETCAS.2017.2671354.

[6] Y. Yang, T. Nishikawa, and A. E. Motter, "Small vulnerable sets determine large network cascades in power grids," *Science (1979)*, vol. 358, no. 6365, Nov. 2017, doi: 10.1126/SCIENCE.AAN3184.

[7] "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," 2016.

[8] D. Liu, X. Zhang, and C. K. Tse, "A Tutorial on Modeling and Analysis of Cascading Failure in Future Power Grids," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 1, pp. 49–55, Jan. 2021, doi: 10.1109/TCSII.2020.3040860.

[9] "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure | CISA." Accessed: Dec. 21, 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a

[10] N. Sharma, A. Acharya, I. Jacob, S. Yamujala, V. Gupta, and R. Bhakar, "Major Blackouts of the Decade: Underlying Causes, Recommendations and Arising Challenges," *ICPS 2021 - 9th IEEE International Conference on Power Systems: Developments towards*

Inclusive Growth for Sustainable and Resilient Grid, 2021, doi: 10.1109/ICPS52420.2021.9670166.

[11] D. Liu, X. Zhang, and C. K. Tse, "A Tutorial on Modeling and Analysis of Cascading Failure in Future Power Grids," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 1, pp. 49–55, Jan. 2021, doi: 10.1109/TCSII.2020.3040860.

[12] T. N. Nguyen, B. H. Liu, N. P. Nguyen, B. Dumba, and J. Te Chou, "Smart Grid Vulnerability and Defense Analysis under Cascading Failure Attacks," *IEEE Transactions on Power Delivery*, vol. 36, no. 4, pp. 2264–2273, Aug. 2021, doi: 10.1109/TPWRD.2021.3061358.

[13] O. Boyaci, M. R. Narimani, K. Davis, M. Ismail, T. J. Overbye, and E. Serpedin, "Joint Detection and Localization of Stealth False Data Injection Attacks in Smart Grids using Graph Neural Networks," *IEEE Trans Smart Grid*, vol. 13, no. 1, pp. 807–819, Apr. 2021, doi: 10.1109/TSG.2021.3117977.

[14] P. Y. Kong, "Optimal Backup Power Deployment for Communication Network with Interdependent Power Network," *IEEE Access*, vol. 10, pp. 17287–17299, 2022, doi: 10.1109/ACCESS.2022.3150318.

[15] C. C. Sun, D. J. Sebastian Cardenas, A. Hahn, and C. C. Liu, "Intrusion Detection for Cybersecurity of Smart Meters," *IEEE Trans Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021, doi: 10.1109/TSG.2020.3010230.

[16] D. Liu and C. K. Tse, "Cascading Failure of Cyber-Coupled Power Systems Considering Interactions between Attack and Defense," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 11, pp. 4323–4336, Nov. 2019, doi: 10.1109/TCSI.2019.2922371.

[17] Y. Ji and J. Yuan, "Overhead Transmission Lines Sag and Voltage Monitoring Method Based on Electrostatic Inverse Calculation," *IEEE Trans Instrum Meas*, vol. 71, 2022, doi: 10.1109/TIM.2022.3157907.

[18] Z. Huang, C. Wang, A. Nayak, and I. Stojmenovic, "Small Cluster in Cyber Physical Systems: Network Topology, Interdependence and Cascading Failures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2340–2351, Aug. 2015, doi: 10.1109/TPDS.2014.2342740.

[19] G. Wu, M. Li, and Z. S. Li, "A Stochastic Modeling Approach for Cascading Failures in Cyberphysical Power Systems," *IEEE Syst J*, vol. 16, no. 1, pp. 723–734, Mar. 2022, doi: 10.1109/JSYST.2021.3070503.

[20] M. Jusup *et al.*, "Social physics," *Phys Rep*, vol. 948, pp. 1–148, Oct. 2021, doi: 10.1016/j.physrep.2021.10.005.

[21] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, “Cascading failure analysis considering interaction between power grids and communication networks,” *IEEE Trans Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016, doi: 10.1109/TSG.2015.2478888.

[22] L. Liu, H. Wu, L. Li, D. Shen, F. Qian, and J. Liu, “Cascading Failure Pattern Identification in Power Systems Based on Sequential Pattern Mining,” *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 1856–1866, May 2021, doi: 10.1109/TPWRS.2020.3028999.

[23] A. Salehpour, I. Al-Anbagi, K. C. Yow, and X. Cheng, “Modeling Cascading Failures in Coupled Smart Grid Networks,” *IEEE Access*, vol. 10, pp. 81054–81070, 2022, doi: 10.1109/ACCESS.2022.3194989.

[24] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, “Complex dynamics of blackouts in power transmission systems,” 2004, doi: 10.1063/1.1781391.

[25] I. Dobson, B. A. Carreras, and D. E. Newman, “A loading-dependent model of probabilistic cascading failure,” *Probab Eng Inf Sci*, vol. 19, no. 1, pp. 15–32, 2005, doi: 10.1017/S0269964805050023.

[26] X. Yu and C. Singh, “A practical approach for integrated power system vulnerability analysis with protection failures,” *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1811–1820, Nov. 2004, doi: 10.1109/TPWRS.2004.835656.

[27] J. Chen, J. S. Thorp, and I. Dobson, “Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model,” *International Journal of Electrical Power & Energy Systems*, vol. 27, no. 4, pp. 318–326, May 2005, doi: 10.1016/J.IJEPES.2004.12.003.

[28] P. Hines and S. Blumsack, “A centrality measure for electrical networks,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2008, doi: 10.1109/HICSS.2008.5.

[29] M. A. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan, “Value of security: Modeling time-dependent phenomena and weather conditions,” *IEEE Transactions on Power Systems*, vol. 17, no. 3, pp. 543–548, Aug. 2002, doi: 10.1109/TPWRS.2002.800872.

[30] A. E. Motter and Y. C. Lai, “Cascade-based attacks on complex networks,” *Phys Rev E Stat Phys Plasmas Fluids Relat Interdiscip Topics*, vol. 66, no. 6, p. 4, Dec. 2002, doi: 10.1103/PHYSREVE.66.065102.

[31] K. Sun and Z. X. Han, “Analysis and comparison on several kinds of models of cascading failure in power system,” *Proceedings of the IEEE Power Engineering Society*

Transmission and Distribution Conference, vol. 2005, pp. 1–7, 2005, doi: 10.1109/TDC.2005.1547073.

[32] I. Dobson, J. Kim, and K. R. Wierzbicki, "Testing branching process estimators of cascading failure with data from a simulation of transmission line outages," *Risk Analysis*, vol. 30, no. 4, pp. 650–662, Apr. 2010, doi: 10.1111/J.1539-6924.2010.01369.X.

[33] Q. Chen and L. Mili, "Composite power system vulnerability evaluation to cascading failures using importance sampling and antithetic variates," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2321–2330, 2013, doi: 10.1109/TPWRS.2013.2238258.

[34] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, "Stochastic analysis of cascading-failure dynamics in power grids," *IEEE Transactions on Power Systems*, vol. 29, no. 4, pp. 1767–1779, 2014, doi: 10.1109/TPWRS.2013.2297276.

[35] A. G. Phadke and J. S. Thorp, "Expose hidden failures to prevent cascading outages," *IEEE Computer Applications in Power*, vol. 9, no. 3, pp. 20–23, Jul. 1996, doi: 10.1109/67.526849.

[36] P. Hines and S. Talukdar, "Reciprocally altruistic agents for the mitigation of cascading failures in electrical power networks," *2008 1st International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future, INFRA 2008*, 2008, doi: 10.1109/INFRA.2008.5439616.

[37] M. Vaiman *et al.*, "Mitigation and prevention of cascading outages: Methodologies and practical applications," *IEEE Power and Energy Society General Meeting*, 2013, doi: 10.1109/PESMG.2013.6672795.

[38] Y. Wang, Y. X. Zhang, and S. X. Xu, "Wide-area protection against chain over-load trip based on multi-agent technology," *Proceedings of the 7th International Conference on Machine Learning and Cybernetics, ICMLC*, vol. 3, pp. 1548–1552, 2008, doi: 10.1109/ICMLC.2008.4620652.

[39] A. A. Babalola, R. Belkacemi, and S. Zarrabian, "Real-time cascading failures prevention for multiple contingencies in smart grids through a multi-agent system," *IEEE Trans Smart Grid*, vol. 9, no. 1, pp. 373–385, Jan. 2018, doi: 10.1109/TSG.2016.2553146.

[40] T. Huynh-The, Q. V. Pham, X. Q. Pham, T. T. Nguyen, Z. Han, and D. S. Kim, "Artificial intelligence for the metaverse," *Eng Appl Artif Intell*, vol. 117, Jan. 2023, doi: 10.1016/J.ENGAPPAI.2022.105581.

[41] V. T. Truong, L. Le, and D. Niyato, "Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey," *IEEE Access*, vol. 11, pp. 26258–26288, 2023, doi: 10.1109/ACCESS.2023.3257029.

[42] A. Zainudin, M. A. P. Putra, R. N. Alief, R. Akter, D. S. Kim, and J. M. Lee, "Blockchain-Inspired Collaborative Cyber-Attacks Detection for Securing Metaverse," *IEEE Internet Things J*, vol. 11, no. 10, pp. 18221–18236, May 2024, doi: 10.1109/JIOT.2024.3364247.

[43] M. Adnan, I. Ahmed, S. Iqbal, M. R. Fazal, S. J. Siddiqi, and M. Tariq, "Exploring the convergence of Metaverse, Blockchain, Artificial Intelligence, and digital twin for pioneering the digitization in the envision smart grid 3.0," *Computers and Electrical Engineering*, vol. 120, p. 109709, Dec. 2024, doi: 10.1016/J.COMPELECENG.2024.109709.

[44] M. Z. Zakariya and J. Teh, "A Systematic Review on Cascading Failures Models in Renewable Power Systems with Dynamics Perspective and Protections Modeling," *Electric Power Systems Research*, vol. 214, p. 108928, Jan. 2023, doi: 10.1016/J.EPSR.2022.108928.

[45] H. Guo, S. Wang, J. Shi, Y. Niu, F. Lizzio, and G. Guglieri, "Dynamically adaptive cascading updates for hierarchical digital twins," *Meas Sci Technol*, vol. 35, no. 12, Dec. 2024, doi: 10.1088/1361-6501/AD7162.

[46] X. Fu and Y. Yang, "Modeling and analyzing cascading failures for Internet of Things," *Inf Sci (N Y)*, vol. 545, pp. 753–770, Feb. 2021, doi: 10.1016/J.INS.2020.09.054.

[47] X. Fu, Y. Wang, Y. Yang, and O. Postolache, "Analysis on cascading reliability of edge-assisted Internet of Things," *Reliab Eng Syst Saf*, vol. 223, p. 108463, Jul. 2022, doi: 10.1016/J.RESS.2022.108463.

[48] Z. Yang, X. Dong, and L. Guo, "Scenario inference model of urban metro system cascading failure under extreme rainfall conditions," *Reliab Eng Syst Saf*, vol. 229, p. 108888, Jan. 2023, doi: 10.1016/J.RESS.2022.108888.

[49] S. Gharebaghi, N. R. Chaudhuri, T. He, and T. La Porta, "An approach for fast cascading failure simulation in dynamic models of power systems," *Appl Energy*, vol. 332, p. 120534, Feb. 2023, doi: 10.1016/J.APENERGY.2022.120534.

[50] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, "Stochastic analysis of cascading-failure dynamics in power grids," *IEEE Transactions on Power Systems*, vol. 29, no. 4, pp. 1767–1779, 2014, doi: 10.1109/TPWRS.2013.2297276.

[51] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9–22, Dec. 2017, doi: 10.1016/J.RSER.2017.05.206.

[52] F. Hayat, M. Adnan, and S. Iqbal, "Expert and Intelligent Systems for Assessment and Mitigation of Cascading Failures in Smart Grids: Research Challenges and Survey," Nov. 2024, doi: 10.31224/4056.

[53] R. Pi, Y. Cai, Y. Li, and Y. Cao, “Machine learning based on bayes networks to predict the cascading failure propagation,” *IEEE Access*, vol. 6, pp. 44815–44823, Jul. 2018, doi: 10.1109/ACCESS.2018.2858838.

[54] P. Hines, K. Balasubramaniam, and E. C. Sanchez, “Cascading failures in power grids,” *IEEE Potentials*, vol. 28, no. 5, pp. 24–30, 2009, doi: 10.1109/MPOT.2009.933498.

[55] A. Berizzi, “The Italian 2003 blackout,” *2004 IEEE Power Engineering Society General Meeting*, vol. 2, pp. 1673–1679, 2004, doi: 10.1109/PES.2004.1373159.

[56] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, “Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization,” *Chaos*, vol. 17, no. 2, Jun. 2007, doi: 10.1063/1.2737822/934765.

[57] L. L. Lai, H. T. Zhang, C. S. Lai, F. Y. Xu, and S. Mishra, “Investigation on July 2012 Indian blackout,” *Proc Int Conf Mach Learn Cybern*, vol. 1, pp. 92–97, 2013, doi: 10.1109/ICMLC.2013.6890450.

[58] M. Noebels, R. Preece, and M. Panteli, “AC Cascading Failure Model for Resilience Analysis in Power Networks,” *IEEE Syst J*, vol. 16, no. 1, pp. 374–385, Mar. 2022, doi: 10.1109/JSYST.2020.3037400.

[59] M. Adnan, Y. Ghadi, I. Ahmed, and M. Ali, “Transmission Network Planning in Super Smart Grids: A Survey,” *IEEE Access*, vol. 11, pp. 77163–77227, 2023, doi: 10.1109/ACCESS.2023.3296152.

[60] M. Adnan and M. Tariq, “Cascading overload failure analysis in renewable integrated power grids,” *Reliab Eng Syst Saf*, vol. 198, p. 106887, Jun. 2020, doi: 10.1016/J.RESS.2020.106887.

[61] M. Adnan, M. G. Khan, A. A. Amin, M. R. Fazal, W. S. Tan, and M. Ali, “Cascading Failures Assessment in Renewable Integrated Power Grids under Multiple Faults Contingencies,” *IEEE Access*, vol. 9, pp. 82272–82287, 2021, doi: 10.1109/ACCESS.2021.3087195.

[62] R. Baldick *et al.*, “Initial review of methods for cascading failure analysis in electric power transmission systems,” *IEEE Power and Energy Society 2008 General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, PES*, 2008, doi: 10.1109/PES.2008.4596430.

[63] M. Vaiman *et al.*, “Risk assessment of cascading outages: Methodologies and challenges,” *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012, doi: 10.1109/TPWRS.2011.2177868.

[64] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine Blackout: Implications for False Data Injection Attacks,” *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017, doi: 10.1109/TPWRS.2016.2631891.

[65] M. Vaiman *et al.*, “Risk assessment of cascading outages: Methodologies and challenges,” *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012, doi: 10.1109/TPWRS.2011.2177868.

[66] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine Blackout: Implications for False Data Injection Attacks,” *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017, doi: 10.1109/TPWRS.2016.2631891.

[67] F. Hayat, M. Adnan, S. Iqbal, and S. E. Gasim Mohamed, “Aperiodic small signal stability method for detection and mitigation of cascading failures in smart grids,” *Results in Engineering*, vol. 23, p. 102661, Sep. 2024, doi: 10.1016/J.RINENG.2024.102661.

[68] P. Henneaux *et al.*, “Benchmarking quasi-steady state cascading outage analysis methodologies,” *2018 International Conference on Probabilistic Methods Applied to Power Systems, PMAPS 2018 - Proceedings*, Aug. 2018, doi: 10.1109/PMAPS.2018.8440212.

[69] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” *Nature 2010 464:7291*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010, doi: 10.1038/nature08932.

[70] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, “A critical review of cascading failure analysis and modeling of power system,” *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9–22, Dec. 2017, doi: 10.1016/J.RSER.2017.05.206.

[71] J. Bialek *et al.*, “Benchmarking and Validation of Cascading Failure Analysis Tools,” *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4887–4900, Nov. 2016, doi: 10.1109/TPWRS.2016.2518660.

[72] P. Henneaux *et al.*, “Benchmarking quasi-steady state cascading outage analysis methodologies,” *2018 International Conference on Probabilistic Methods Applied to Power Systems, PMAPS 2018 - Proceedings*, Aug. 2018, doi: 10.1109/PMAPS.2018.8440212.

[73] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, “A critical review of cascading failure analysis and modeling of power system,” *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9–22, 2017, doi: 10.1016/j.rser.2017.05.206.

[74] J. Bialek *et al.*, “Benchmarking and Validation of Cascading Failure Analysis Tools,” *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4887–4900, Nov. 2016, doi: 10.1109/TPWRS.2016.2518660.

[75] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” *Nature*, vol. 464, no. 7291, pp. 1025–1028, Jul. 2009, doi: 10.1038/nature08932.

[76] P. Crucitti, V. Latora, and M. Marchiori, “A model for cascading failures in complex networks,” *Phys Rev E Stat Phys Plasmas Fluids Relat Interdiscip Topics*, vol. 69, no. 4, p. 4, Sep. 2003, doi: 10.1103/PhysRevE.69.045104.

[77] R. Albert, I. Albert, and G. L. Nakarado, “Structural Vulnerability of the North American Power Grid,” *Phys Rev E Stat Nonlin Soft Matter Phys*, vol. 69, no. 2 2, Jan. 2004, doi: 10.1103/PhysRevE.69.025103.

[78] Å. J. Holmgren, “Using Graph Models to Analyze the Vulnerability of Electric Power Networks,” *Risk Analysis*, vol. 26, no. 4, pp. 955–969, Aug. 2006, doi: 10.1111/J.1539-6924.2006.00791.X.

[79] P. Crucitti, V. Latora, and M. Marchiori, “Model for cascading failures in complex networks,” *Phys Rev E*, vol. 69, no. 4, p. 045104, Apr. 2004, doi: 10.1103/PhysRevE.69.045104.

[80] R. Albert, I. Albert, and G. L. Nakarado, “Structural vulnerability of the North American power grid,” *Phys Rev E*, vol. 69, no. 2, p. 025103, Feb. 2004, doi: 10.1103/PhysRevE.69.025103.

[81] N. Alon, B. Awerbuch, Y. Azar, N. Buchbinder, J. (Seffi, and) Naor, “The Online Set Cover Problem,” 2003.

[82] Å. J. Holmgren, “Using graph models to analyze the vulnerability of electric power networks,” *Risk Anal*, vol. 26, no. 4, pp. 955–969, Aug. 2006, doi: 10.1111/J.1539-6924.2006.00791.X.

[83] S. G. Aksoy, E. Purvine, E. Cotilla-Sanchez, and M. Halappanavar, “A generative graph model for electrical infrastructure networks,” *J Complex Netw*, vol. 7, no. 1, pp. 128–162, Nov. 2017, doi: 10.1093/comnet/cny016.

[84] Yihai Zhu, Jun Yan, Yan Sun, and Haibo He, “Risk-aware vulnerability analysis of electric grids from attacker’s perspective,” pp. 1–6, Jul. 2013, doi: 10.1109/ISGT.2013.6497817.

[85] Y. Zhu, J. Yan, Y. Sun, and H. He, “Revealing cascading failure vulnerability in power grids using risk-graph,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3274–3284, Dec. 2014, doi: 10.1109/TPDS.2013.2295814.

[86] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, “Resilience analysis of power grids under the sequential attack,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2340–2354, Dec. 2014, doi: 10.1109/TIFS.2014.2363786.

[87] P. A. Kaplunovich and K. S. Turitsyn, “Statistical properties and classification of N-2 contingencies in large scale power grids,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 2517–2526, 2014, doi: 10.1109/HICSS.2014.316.

[88] P. D. H. Hines, I. Dobson, and P. Rezaei, “Cascading Power Outages Propagate Locally in an Influence Graph that is not the Actual Grid Topology,” *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 958–967, Aug. 2015, doi: 10.1109/TPWRS.2016.2578259.

[89] C. Luo, J. Yang, Y. Sun, J. Yan, and H. He, “Identify critical branches with cascading failure chain statistics and hypertext-induced topic search algorithm,” *IEEE Power and Energy Society General Meeting*, vol. 2018-January, pp. 1–5, Jan. 2018, doi: 10.1109/PESGM.2017.8274213.

[90] P. D. H. Hines, I. Dobson, and P. Rezaei, “Cascading Power Outages Propagate Locally in an Influence Graph That is Not the Actual Grid Topology,” *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 958–967, Mar. 2017, doi: 10.1109/TPWRS.2016.2578259.

[91] K. Zhou, I. Dobson, P. D. H. Hines, and Z. Wang, “Can an influence graph driven by outage data determine transmission line upgrades that mitigate cascading blackouts?,” *2018 International Conference on Probabilistic Methods Applied to Power Systems, PMAPS 2018 - Proceedings*, Aug. 2018, doi: 10.1109/PMAPS.2018.8440497.

[92] U. Nakarmi and M. Rahnamay-Naeini, “Analyzing Power Grids’ Cascading Failures and Critical Components using Interaction Graphs,” *IEEE Power and Energy Society General Meeting*, vol. 2018-August, Dec. 2018, doi: 10.1109/PESGM.2018.8585812.

[93] U. Nakarmi, M. Rahnamay-Naeini, and H. Khamfroush, “Critical Component Analysis in Cascading Failures for Power Grids Using Community Structures in Interaction Graphs,” *IEEE Trans Netw Sci Eng*, vol. 7, no. 3, pp. 1079–1093, Jul. 2020, doi: 10.1109/TNSE.2019.2904008.

[94] P. D. H. Hines, I. Dobson, E. Cotilla-Sanchez, and M. Eppstein, “‘Dual graph’ and ‘random chemistry’ methods for cascading failure analysis,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 2141–2150, 2013, doi: 10.1109/HICSS.2013.1.

[95] X. Wei, J. Zhao, T. Huang, and E. Bompard, “A Novel Cascading Faults Graph Based Transmission Network Vulnerability Assessment Method,” *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2995–3000, May 2018, doi: 10.1109/TPWRS.2017.2759782.

[96] X. Wei, S. Gao, T. Huang, E. Bompard, R. Pi, and T. Wang, “Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability,” *IEEE Trans Industr Inform*, vol. 15, no. 3, pp. 1265–1276, Mar. 2019, doi: 10.1109/TII.2018.2840429.

[97] X. Wei, S. Gao, T. Huang, T. Wang, and W. Fan, “Identification of Two Vulnerability Features: A New Framework for Electrical Networks Based on the Load Redistribution Mechanism of Complex Networks,” *Complexity*, vol. 2019, pp. 1–14, 2019, doi: 10.1155/2019/3531209.

[98] T. Wang *et al.*, “Modeling Fault Propagation Paths in Power Systems: A New Framework Based on Event SNP Systems With Neurotransmitter Concentration,” *IEEE Access*, vol. 7, pp. 12798–12808, 2019, doi: 10.1109/ACCESS.2019.2892797.

[99] T. Zang *et al.*, “Adjacent Graph Based Vulnerability Assessment for Electrical Networks Considering Fault Adjacent Relationships Among Branches”, doi: 10.1109/ACCESS.2019.2926148.

[100] S. Yang, W. Chen, X. Zhang, C. Liang, H. Wang, and W. Cui, “A Graph-Based Model for Transmission Network Vulnerability Analysis,” *IEEE Syst J*, vol. 14, no. 1, pp. 1447–1456, Mar. 2020, doi: 10.1109/JSYST.2019.2919958.

[101] “Electrical Network Operational Vulnerability Evaluation Based On Small-World and Scale-Free Properties | PDF | Mathematical Relations | Systems Theory.” Accessed: Oct. 12, 2024. [Online]. Available: https://www.scribd.com/document/675473390/Electrical-Network-Operational-Vulnerability-Evaluation-Based-on-Small-World-and-Scale-Free-Properties

[102] K. Zhou, I. Dobson, Z. Wang, A. Roitershtein, and A. P. Ghosh, “A Markovian Influence Graph Formed from Utility Line Outage Data to Mitigate Large Cascades,” *IEEE Transactions on Power Systems*, vol. 35, no. 4, pp. 3224–3235, Jul. 2020, doi: 10.1109/TPWRS.2020.2970406.

[103] Z. G. Wu, Q. Zhong, and Y. Zhang, “State transition graph of cascading electrical power grids,” *2007 IEEE Power Engineering Society General Meeting, PES*, 2007, doi: 10.1109/PES.2007.385867.

[104] L. Chang and Z. Wu, “Performance and reliability of electrical power grids under cascading failures,” *International Journal of Electrical Power & Energy Systems*, vol. 33, no. 8, pp. 1410–1419, Oct. 2011, doi: 10.1016/J.IJEPES.2011.06.021.

[105] L. Li, H. Wu, and Y. Song, “Temporal Difference Learning Based Critical Component Identifying Method with Cascading Failure Data in Power Systems,” *IEEE Power and Energy Society General Meeting*, vol. 2018-August, Dec. 2018, doi: 10.1109/PESGM.2018.8586590.

[106] L. Li, H. Wu, Y. Song, D. Song, and Y. Liu, “Quantify the Impact of Line Capacity Temporary Expansion on Blackout Risk by the State-Failure-Network Method,” *IEEE Access*, vol. 7, pp. 183049–183060, 2019, doi: 10.1109/ACCESS.2019.2960306.

[107] L. Li, H. Wu, Y. Song, and Y. Liu, “A state-failure-network method to identify critical components in power systems,” *Electric Power Systems Research*, vol. 181, p. 106192, Apr. 2020, doi: 10.1016/J.EPSR.2019.106192.

[108] L. Liu, L. Li, and H. Wu, “Identifying Critical Patterns of Cascading Failure in Power Systems Based on Sequential Pattern Mining with Gap Constraints,” *Lecture Notes in Electrical Engineering*, vol. 585, pp. 837–855, 2020, doi: 10.1007/978-981-13-9783-7_69.

[109] J. Qi, K. Sun, and S. Mei, “An interaction model for simulation and mitigation of cascading failures,” *IEEE Transactions on Power Systems*, vol. 30, no. 2, pp. 804–819, Mar. 2015, doi: 10.1109/TPWRS.2014.2337284.

[110] J. Qi, J. Wang, and K. Sun, “Efficient Estimation of Component Interactions for Cascading Failure Analysis by em Algorithm,” *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3153–3161, May 2018, doi: 10.1109/TPWRS.2017.2764041.

[111] W. Ju, J. Qi, and K. Sun, “Simulation and analysis of cascading failures on an NPCC power system test bed,” *IEEE Power and Energy Society General Meeting*, vol. 2015-September, Sep. 2015, doi: 10.1109/PESGM.2015.7286478.

[112] J. Qi, J. Wang, and K. Sun, “Efficient Estimation of Component Interactions for Cascading Failure Analysis by em Algorithm,” *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3153–3161, May 2018, doi: 10.1109/TPWRS.2017.2764041.

[113] W. Ju, J. Qi, and K. Sun, “Simulation and analysis of cascading failures on an NPCC power system test bed,” *IEEE Power & Energy Society General Meeting*, vol. 2015-September, Sep. 2015, doi: 10.1109/PESGM.2015.7286478.

[114] W. Ju, K. Sun, and J. Qi, “Multi-Layer Interaction Graph for Analysis and Mitigation of Cascading Outages,” *IEEE J Emerg Sel Top Circuits Syst*, vol. 7, no. 2, pp. 239–249, Jun. 2017, doi: 10.1109/JETCAS.2017.2703948.

[115] C. Chen, W. Ju, K. Sun, and S. Ma, “Mitigation of cascading outages using a dynamic interaction graph-based optimal power flow model,” *IEEE Access*, vol. 7, pp. 168637–168648, 2019, doi: 10.1109/ACCESS.2019.2953774.

[116] A. Wang, Y. Luo, G. Tu, and P. Liu, “Vulnerability assessment scheme for power system transmission networks based on the fault chain theory,” *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 442–450, Feb. 2011, doi: 10.1109/TPWRS.2010.2052291.

[117] C. Caro-Ruiz and E. Mojica-Nava, “Centrality measures for voltage instability analysis in power networks,” *2015 IEEE 2nd Colombian Conference on Automatic Control, CCAC 2015 - Conference Proceedings*, Dec. 2015, doi: 10.1109/CCAC.2015.7345182.

[118] E. Cotilla-Sanchez, P. D. H. Hines, C. Barrows, and S. Blumsack, “Comparing the topological and electrical structure of the North American electric power infrastructure,” *IEEE Syst J*, vol. 6, no. 4, pp. 616–626, 2012, doi: 10.1109/JSYST.2012.2183033.

[119] E. Cotilla-Sanchez, P. D. H. Hines, C. Barrows, S. Blumsack, and M. Patel, “Multi-attribute partitioning of power networks based on electrical distance,” *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4979–4987, 2013, doi: 10.1109/TPWRS.2013.2263886.

[120] C. Asavathiratham, S. Roy, B. Lesieutre, and G. Verghese, “The influence model,” *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 52–64, 2001, doi: 10.1109/37.969135.

[121] U. Nakarmi, M. R. Naeini, M. J. Hossain, and M. A. Hasnat, “Interaction graphs for cascading failure analysis in power grids: A survey,” *Energies (Basel)*, vol. 13, no. 9, p. 2219, May 2020, doi: 10.3390/en13092219.

[122] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, “Do topological models provide good information about vulnerability in electric power networks?,” *Chaos*, vol. 20, no. 3, Feb. 2010, doi: 10.1063/1.3489887.

[123] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. W. Geem, “A Critical Review of Robustness in Power Grids Using Complex Networks Concepts,” *Energies 2015, Vol. 8, Pages 9211-9265*, vol. 8, no. 9, pp. 9211–9265, Aug. 2015, doi: 10.3390/EN8099211.

[124] M. Adnan, I. Ahmed, and S. Iqbal, “Load flow balancing in super smart grids: A review of technical challenges, possible solutions and future trends from European prospective,” *Computers and Electrical Engineering*, vol. 117, p. 109265, Jul. 2024, doi: 10.1016/J.COMPELECENG.2024.109265.

[125] A. Raza, M. Liaqat, M. Adnan, M. S. Iqbal, L. Jingzhao, and I. Ahmad, “SAARC super smart grid: Navigating the future - unleashing the power of an energy-efficient integration of renewable energy resources in the saarc region,” *Computers and Electrical Engineering*, vol. 118, p. 109405, Sep. 2024, doi: 10.1016/J.COMPELECENG.2024.109405.

[126] W. Ren, J. Wu, X. Zhang, R. Lai, and L. Chen, “A Stochastic Model of Cascading Failure Dynamics in Communication Networks,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 5, pp. 632–636, May 2018, doi: 10.1109/TCSII.2018.2822049.

[127] W. Liao, S. Salinas, M. Li, P. Li, and K. A. Loparo, “Cascading Failure Attacks in the Power System: A Stochastic Game Perspective,” *IEEE Internet Things J*, vol. 4, no. 6, 2017, doi: 10.1109/JIOT.2017.2761353.

[128] A. Azzolin, L. Dueñas-Osorio, F. Cadini, and E. Zio, “Electrical and topological drivers of the cascading failure dynamics in power transmission networks,” *Reliab Eng Syst Saf*, vol. 175, pp. 196–206, Jul. 2018, doi: 10.1016/J.RESS.2018.03.011.

[129] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, “A critical review of cascading failure analysis and modeling of power system,” *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9–22, Dec. 2017, doi: 10.1016/J.RSER.2017.05.206.

[130] M. Ali *et al.*, “Integration of Data Driven Technologies in Smart Grids for Resilient and Sustainable Smart Cities: A Comprehensive Review,” Jan. 2023, Accessed: Dec. 21, 2024. [Online]. Available: https://arxiv.org/abs/2301.08814v2

[131] S. M. Amin and B. F. Wollenberg, “Toward a smart grid,” *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, Sep. 2005, doi: 10.1109/MPAE.2005.1507024.

[132] M. Tariq, M. Adnan, G. Srivastava, and H. Vincent Poor, “Instability Detection and Prevention in Smart Grids under Asymmetric Faults,” *IEEE Trans Ind Appl*, vol. 56, no. 4, pp. 4510–4520, Jul. 2020, doi: 10.1109/TIA.2020.2964594.

[133] M. Adnan, M. Tariq, Z. Zhou, and H. V. Poor, “Load flow balancing and transient stability analysis in renewable integrated power grids,” *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 744–771, Jan. 2019, doi: 10.1016/J.IJEPES.2018.06.037.

[134] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, “Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks,” *IEEE Internet Things J*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019, doi: 10.1109/JIOT.2019.2904303.

[135] H. Zahid, A. Zulfiqar, M. Adnan, S. Iqbal, and S. E. G. Mohamed, “A Review on Socio-technical Transition Pathway to European Super Smart Grid: Trends, Challenges and Way Forward via Enabling Technologies,” Dec. 2024, doi: 10.31224/4068.

[136] M. Adnan, M. Ali, and M. Tariq, “A probabilistic approach for power network stability in smart grids,” *15th International Conference on Emerging Technologies, ICET 2019*, Dec. 2019, doi: 10.1109/ICET48972.2019.8994461.

[137] M. Tariq and M. Adnan, “Stabilizing super smart grids using V2G: A probabilistic analysis,” *IEEE Vehicular Technology Conference*, vol. 2019-April, Apr. 2019, doi: 10.1109/VTCSPRING.2019.8746708.

[138] T. Roth and B. M. McMillin, “Physical Attestation in the Smart Grid for Distributed State Verification,” *Proceedings - International Computer Software and Applications Conference*, vol. 1, pp. 626–627, Sep. 2017, doi: 10.1109/COMPSAC.2017.188.

[139] F. Li, Y. Wei, and S. Adhikari, “Improving an unjustified common practice in ex post LMP calculation: An expanded version,” *IEEE PES General Meeting, PES 2010*, 2010, doi: 10.1109/PES.2010.5590167.

[140] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," *IEEE Trans Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017, doi: 10.1109/TSG.2015.2495133.

[141] Y. Yuan, Z. Li, and K. Ren, "Quantitative Analysis of Load Redistribution Attacks in Power Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012, doi: 10.1109/TPDS.2012.58.

[142] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014, doi: 10.1109/TSG.2013.2291661.

[143] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of Local False Data Injection Attacks With Reduced Network Information," *IEEE Trans Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015, doi: 10.1109/TSG.2015.2394358.

[144] D. H. Choi and L. Xie, "Economic impact assessment of topology data attacks with virtual bids," *IEEE Trans Smart Grid*, vol. 9, no. 2, pp. 512–520, Mar. 2016, doi: 10.1109/TSG.2016.2535246.

[145] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A Stealthy Attack Against Electricity Market Using Independent Component Analysis," *IEEE Syst J*, vol. 12, no. 1, pp. 297–307, Mar. 2018, doi: 10.1109/JSYST.2015.2483742.

[146] X. Liu, Z. Li, S. Member, Z. Li, and S. Member, "Masking Transmission Line Outages via False Data Injection Attacks".

[147] H. Shayan and T. Amraee, "Network Constrained Unit Commitment under Cyber Attacks Driven Overloads," *IEEE Trans Smart Grid*, vol. 10, no. 6, pp. 6449–6460, Nov. 2019, doi: 10.1109/TSG.2019.2904873.

[148] J. Fang, C. Su, Z. Chen, H. Sun, and P. Lund, "Power system structural vulnerability assessment based on an improved maximum flow approach," *IEEE Trans Smart Grid*, vol. 9, no. 2, pp. 777–785, 2018, doi: 10.1109/TSG.2016.2565619.

[149] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014, doi: 10.1109/TSG.2013.2291661.

[150] S. Mishra, X. Li, T. Pan, A. Kuhnle, M. T. Thai, and J. Seo, "Price Modification Attack and Protection Scheme in Smart Grid," *IEEE Trans Smart Grid*, vol. 8, no. 4, pp. 1864–1875, Jul. 2017, doi: 10.1109/TSG.2015.2509945.

[151] D. Van Hertem, "Usefulness of DC power flow for active power flow analysis with flow controlling devices," pp. 58–62, Jul. 2006, doi: 10.1049/CP:20060013.

[152] S. Mishra, X. Li, A. Kuhnle, M. T. Thai, and J. Seo, “Rate alteration attacks in smart grid,” *Proceedings - IEEE INFOCOM*, vol. 26, pp. 2353–2361, Aug. 2015, doi: 10.1109/INFOCOM.2015.7218623.

[153] C. Coffrin, P. Van Hentenryck, and R. Bent, “Approximating line losses and apparent power in AC power flow linearizations,” *IEEE Power and Energy Society General Meeting*, 2012, doi: 10.1109/PESGM.2012.6345342.

[154] T. N. Nguyen, B. H. Liu, N. P. Nguyen, B. Dumba, and J. Te Chou, “Smart Grid Vulnerability and Defense Analysis under Cascading Failure Attacks,” *IEEE Transactions on Power Delivery*, vol. 36, no. 4, pp. 2264–2273, Aug. 2021, doi: 10.1109/TPWRD.2021.3061358.

[155] S. El Kafhali and K. Salah, “Efficient and dynamic scaling of fog nodes for IoT devices,” *Journal of Supercomputing*, vol. 73, no. 12, pp. 5261–5284, Dec. 2017, doi: 10.1007/S11227-017-2083-X/METRICS.

[156] F. Al-Haidari, M. Sqalli, and K. Salah, “Impact of CPU utilization thresholds and scaling size on autoscaling cloud resources,” *Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom*, vol. 2, pp. 256–261, 2013, doi: 10.1109/CLOUDCOM.2013.142.

[157] “Towards interoperable IOT systems with a constraint-aware semantic web of things | Request PDF.” Accessed: Dec. 18, 2024. [Online]. Available: https://www.researchgate.net/publication/332537677_Towards_interoperable_IOT_systems_with_a_constraint-aware_semantic_web_of_things

[158] K. Wang, Y. Wang, Y. Sun, S. Guo, and J. Wu, “Green Industrial Internet of Things Architecture: An Energy-Efficient Perspective,” *IEEE Communications Magazine*, vol. 54, no. 11, pp. 48–54, Dec. 2016, doi: 10.1109/MCOM.2016.1600399CM.

[159] J. Huang, Y. Meng, X. Gong, Y. Liu, and Q. Duan, “A novel deployment scheme for green internet of things,” *IEEE Internet Things J*, vol. 1, no. 2, pp. 196–205, Apr. 2014, doi: 10.1109/JIOT.2014.2301819.

[160] X. Fu, H. Yao, and Y. Yang, “Modeling and analyzing cascading dynamics of the clustered wireless sensor network,” *Reliab Eng Syst Saf*, vol. 186, pp. 1–10, Jun. 2019, doi: 10.1016/J.RESS.2019.02.009.

[161] I. Dobson, B. A. Carreras, and D. E. Newman, “A loading-dependent model of probabilistic cascading failure,” *Probab Eng Inf Sci*, vol. 19, no. 1, pp. 15–32, 2005, doi: 10.1017/S0269964805050023.

[162] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, “Stochastic analysis of cascading-failure dynamics in power grids,” *IEEE Transactions on Power Systems*, vol. 29, no. 4, pp. 1767–1779, 2014, doi: 10.1109/TPWRS.2013.2297276.

[163] I. Dobson, B. A. Carreras, and D. E. Newman, “A loading-dependent model of probabilistic cascading failure,” *Probab Eng Inf Sci*, vol. 19, no. 1, pp. 15–32, 2005, doi: 10.1017/S0269964805050023.

[164] I. Dobson, B. A. Carreras, and D. E. Newman, “A loading-dependent model of probabilistic cascading failure,” *Probab Eng Inf Sci*, vol. 19, no. 1, pp. 15–32, 2005, doi: 10.1017/S0269964805050023.

[165] W. Liao, S. Salinas, M. Li, P. Li, and K. A. Loparo, “Cascading Failure Attacks in the Power System: A Stochastic Game Perspective,” *IEEE Internet Things J*, vol. 4, no. 6, pp. 2247–2259, Dec. 2017, doi: 10.1109/JIOT.2017.2761353.

[166] W. Ren, J. Wu, X. Zhang, R. Lai, and L. Chen, “A Stochastic Model of Cascading Failure Dynamics in Communication Networks,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 5, pp. 632–636, May 2018, doi: 10.1109/TCSII.2018.2822049.

[167] R. Ghanbari, M. Jalili, and X. Yu, “Correlation of cascade failures and centrality measures in complex networks,” *Future Generation Computer Systems*, vol. 83, pp. 390–400, Jun. 2018, doi: 10.1016/J.FUTURE.2017.09.007.

[168] K. Salah, “On the deployment of VoIP in Ethernet networks: methodology and case study,” *Comput Commun*, vol. 29, no. 8, pp. 1039–1054, May 2006, doi: 10.1016/J.COMCOM.2005.06.004.

[169] J. Wang, L. Rong, L. Zhang, and Z. Zhang, “Attack vulnerability of scale-free networks due to cascading failures,” *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 26, pp. 6671–6678, Nov. 2008, doi: 10.1016/J.PHYSA.2008.08.037.

[170] H. Khamfroush, S. L. Iloo, and M. Rahnamay-Naeini, “Vulnerability of Interdependent Infrastructures Under Random Attacks,” *SIGMETRICS Perform. Evaluation Rev.*, vol. 46, no. 2, pp. 67–71, Jan. 2019, doi: 10.1145/3305218.3305242.

[171] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, “Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions,” *IEEE Access*, vol. 7, pp. 62962–63003, 2019, doi: 10.1109/ACCESS.2019.2913984.

[172] X. Fu and Y. Yang, “Modeling and analyzing cascading failures for Internet of Things,” *Inf Sci (N Y)*, vol. 545, pp. 753–770, Feb. 2021, doi: 10.1016/J.INS.2020.09.054.

[173] R. Rosen, G. Von Wichert, G. Lo, and K. D. Bettenhausen, “About The Importance of Autonomy and Digital Twins for the Future of Manufacturing,” *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 567–572, Jan. 2015, doi: 10.1016/J.IFACOL.2015.06.141.

[174] M. Grieves, “Intelligent digital twins and the development and management of complex systems,” *Digital Twin*, vol. 2, p. 8, May 2022, doi: 10.12688/DIGITALTWIN.17574.1.

[175] T. Ruohomaki, E. Airaksinen, P. Huuska, O. Kesaniemi, M. Martikka, and J. Suomisto, “Smart City Platform Enabling Digital Twin,” *9th International Conference on Intelligent Systems 2018: Theory, Research and Innovation in Applications, IS 2018 - Proceedings*, pp. 155–161, Jul. 2018, doi: 10.1109/IS.2018.8710517.

[176] A. Bilberg and A. A. Malik, “Digital twin driven human–robot collaborative assembly,” *CIRP Annals*, vol. 68, no. 1, pp. 499–502, Jan. 2019, doi: 10.1016/J.CIRP.2019.04.011.

[177] Y. Liu *et al.*, “A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin,” *IEEE Access*, vol. 7, pp. 49088–49101, 2019, doi: 10.1109/ACCESS.2019.2909828.

[178] V. Damjanovic-Behrendt, “A Digital Twin-based Privacy Enhancement Mechanism for the Automotive Industry,” *9th International Conference on Intelligent Systems 2018: Theory, Research and Innovation in Applications, IS 2018 - Proceedings*, pp. 272–279, Jul. 2018, doi: 10.1109/IS.2018.8710526.

[179] C. Mandolla, A. M. Petruzzelli, G. Percoco, and A. Urbinati, “Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry,” *Comput Ind*, vol. 109, pp. 134–152, Aug. 2019, doi: 10.1016/J.COMPIND.2019.04.011.

[180] E. H. Glaessgen and D. S. Stargel, “The digital twin paradigm for future NASA and U.S. Air force vehicles,” *Collection of Technical Papers - AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference*, 2012, doi: 10.2514/6.2012-1818.

[181] E. J. Tuegel, “The airframe digital twin: Some challenges to realization,” *Collection of Technical Papers - AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference*, 2012, doi: 10.2514/6.2012-1812.

[182] D. P. Maher, “On software standards and solutions for a trusted internet of things,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, vol. 2018-January, pp. 5666–5675, 2018, doi: 10.24251/HICSS.2018.710.

[183] “Gartner Top 10 Strategic Technology Trends For 2019.” Accessed: Dec. 18, 2024. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019

[184] “Past, present, and future research of digital twin for smart manufacturing - National Institutes of Health.” Accessed: Dec. 18, 2024. [Online].

[185] M. Liu, S. Fang, H. Dong, and C. Xu, “Review of digital twin about concepts, technologies, and industrial applications,” *J Manuf Syst*, vol. 58, pp. 346–361, Jan. 2021, doi: 10.1016/J.JMSY.2020.06.017.

[186] J. Wang, X. Li, P. Wang, and Q. Liu, “Bibliometric analysis of digital twin literature: a review of influencing factors and conceptual structure,” *Technol Anal Strateg Manag*, vol. 36, no. 1, pp. 166–180, 2024, doi: 10.1080/09537325.2022.2026320.

[187] S. Werbińska-Wojciechowska, R. Giel, and K. Winiarska, “Digital Twin Approach for Operation and Maintenance of Transportation System—Systematic Review,” *Sensors 2024, Vol. 24, Page 6069*, vol. 24, no. 18, p. 6069, Sep. 2024, doi: 10.3390/S24186069.

[188] F. Tao, J. Cheng, Q. Qi, M. Zhang, H. Zhang, and F. Sui, “Digital twin-driven product design, manufacturing and service with big data,” *International Journal of Advanced Manufacturing Technology*, vol. 94, no. 9–12, pp. 3563–3576, Feb. 2018, doi: 10.1007/S00170-017-0233-1/METRICS.

[189] W. Hu, T. Zhang, X. Deng, Z. Liu, and J. Tan, “Digital twin: a state-of-the-art review of its enabling technologies, applications and challenges,” *Journal of Intelligent Manufacturing and Special Equipment*, vol. 2, no. 1, pp. 1–34, Aug. 2021, doi: 10.1108/JIMSE-12-2020-010.

[190] K. Sivalingam, M. Sepulveda, M. Spring, and P. Davies, “A Review and Methodology Development for Remaining Useful Life Prediction of Offshore Fixed and Floating Wind turbine Power Converter with Digital Twin Technology Perspective,” *Proceedings - 2018 2nd International Conference on Green Energy and Applications, ICGEA 2018*, pp. 197–204, May 2018, doi: 10.1109/ICGEA.2018.8356292.

[191] “GE Renewable Energy Introduces New Suite of Digital Wind Farm Apps | GE News.” Accessed: Dec. 18, 2024. [Online]. Available: https://www.ge.com/news/press-releases/ge-renewable-energy-introduces-new-suite-digital-wind-farm-apps

[192] “GreenPowerMonitor – Monitoring, Control and Asset Management Solutions.” Accessed: Dec. 18, 2024. [Online]. Available: https://www.greenpowermonitor.com/

[193] D. Knezevic, E. Fakas, and H. J. Riber, “Predictive Digital Twins for Structural Integrity Management and Asset Life Extension – JIP Concept and Results,” *Day 1 Tue, September 03, 2019*, 2019, doi: 10.2118/195762-MS.

[194] A. Ciuriuc, J. I. Rapha, R. Guanche, and J. L. Domínguez-García, “Digital tools for floating offshore wind turbines (FOWT): A state of the art,” *Energy Reports*, vol. 8, pp. 1207–1228, Nov. 2022, doi: 10.1016/J.EGYR.2021.12.034.

[195] Q. Qi *et al.*, “Enabling technologies and tools for digital twin,” *J Manuf Syst*, vol. 58, pp. 3–21, Jan. 2021, doi: 10.1016/J.JMSY.2019.10.001.

[196] A. Ciuriuc, J. I. Rapha, R. Guanche, and J. L. Domínguez-García, “Digital tools for floating offshore wind turbines (FOWT): A state of the art,” *Energy Reports*, vol. 8, pp. 1207–1228, Nov. 2022, doi: 10.1016/J.EGYR.2021.12.034.

[197] D. van Huynh, Y. Li, T. Do-Duy, E. Garcia-Palacios, and T. Q. Duong, “Digital twin-enabled aerial edge networks with ultra-reliable low-latency communications,” *Digital Twins for 6G: Fundamental theory, technology and applications*, pp. 27–48, Jan. 2024, doi: 10.1049/PBTE109E_CH2.

[198] “DNV.com - When trust matters - DNV.” Accessed: Dec. 18, 2024. [Online]. Available: https://www.dnv.com/

[199] J. Walker, A. Coraddu, M. Collu, and L. Oneto, “Digital twins of the mooring line tension for floating offshore wind turbines to improve monitoring, lifespan, and safety,” *J Ocean Eng Mar Energy*, vol. 8, no. 1, pp. 1–16, Feb. 2022, doi: 10.1007/S40722-021-00213-Y/FIGURES/6.

[200] A. A. Nasir, “Latency Optimization of UAV-Enabled MEC System for Virtual Reality Applications under Rician Fading Channels,” *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1633–1637, Aug. 2021, doi: 10.1109/LWC.2021.3075762.

[201] R. Dong, C. She, W. Hardjawana, Y. Li, and B. Vucetic, “Deep Learning for Hybrid 5G Services in Mobile Edge Computing Systems: Learn from a Digital Twin,” *IEEE Trans Wirel Commun*, vol. 18, no. 10, pp. 4692–4707, Oct. 2019, doi: 10.1109/TWC.2019.2927312.

[202] C. She, C. Yang, and T. Q. S. Quek, “Radio Resource Management for Ultra-Reliable and Low-Latency Communications,” *IEEE Communications Magazine*, vol. 55, no. 6, pp. 72–78, 2017, doi: 10.1109/MCOM.2017.1601092.

[203] D. Van Huynh, S. R. Khosravirad, A. Masaracchia, O. A. Dobre, and T. Q. Duong, “Edge Intelligence-Based Ultra-Reliable and Low-Latency Communications for Digital Twin-Enabled Metaverse,” *IEEE Wireless Communications Letters*, vol. 11, no. 8, pp. 1733–1737, Aug. 2022, doi: 10.1109/LWC.2022.3179207.

[204] A. Ben-Tal and A. Nemirovski, “Lectures on Modern Convex Optimization,” *Lectures on Modern Convex Optimization*, Jan. 2001, doi: 10.1137/1.9780898718829.

[205] J. Virgili-Llop, C. Zagaris, R. Zappulla, A. Bradstreet, and M. Romano, “A convex-programming-based guidance algorithm to capture a tumbling object on orbit using a spacecraft equipped with a robotic manipulator,”

https://doi.org/10.1177/0278364918804660, vol. 38, no. 1, pp. 40–72, Dec. 2018, doi: 10.1177/0278364918804660.

[206] D. Augustyn, R. R. Pedersen, U. T. Tygesen, M. D. Ulriksen, and J. D. Sørensen, "Feasibility of modal expansion for virtual sensing in offshore wind jacket substructures," *Marine Structures*, vol. 79, Sep. 2021, doi: 10.1016/J.MARSTRUC.2021.103019.

[207] D. Augustyn, U. Smolka, U. T. Tygesen, M. D. Ulriksen, and J. D. Sørensen, "Data-driven model updating of an offshore wind jacket substructure," *Applied Ocean Research*, vol. 104, Nov. 2020, doi: 10.1016/J.APOR.2020.102366.

[208] D. Augustyn, M. D. Ulriksen, and J. D. Sørensen, "Reliability Updating of Offshore Wind Substructures by Use of Digital Twin Information," *Energies 2021, Vol. 14, Page 5859*, vol. 14, no. 18, p. 5859, Sep. 2021, doi: 10.3390/EN14185859.

[209] S. Qiu *et al.*, "Digital-Twin-Assisted Edge-Computing Resource Allocation Based on the Whale Optimization Algorithm," *Sensors 2022, Vol. 22, Page 9546*, vol. 22, no. 23, p. 9546, Dec. 2022, doi: 10.3390/S22239546.

[210] B. Q. Chen, K. Liu, T. Yu, and R. Li, "Enhancing Reliability in Floating Offshore Wind Turbines through Digital Twin Technology: A Comprehensive Review," *Energies 2024, Vol. 17, Page 1964*, vol. 17, no. 8, p. 1964, Apr. 2024, doi: 10.3390/EN17081964.

[211] J. Xia and G. Zou, "Operation and maintenance optimization of offshore wind farms based on digital twin: A review," *Ocean Engineering*, vol. 268, Jan. 2023, doi: 10.1016/J.OCEANENG.2022.113322.

[212] Muhammad Adnan, H. Zahid, A. Zulfiqar, M. Sajid Iqbal, A. Shah, and K. Fida, "Global Renewable Energy Transition: A Multidisciplinary Analysis of Emerging Computing Technologies, Socio-Economic Impacts, and Policy Imperatives," Nov. 2024, doi: 10.31224/4112.

[213] "U.S.–Canada Power System Outage Task Force. (Apr. 2004). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. U.S. and Canadian Governments. ." Accessed: Oct. 10, 2024. [Online].

[214] S. Zarrabian, R. Belkacemi, and A. A. Babalola, "Real-time smart grids control for preventing cascading failures and blackout using neural networks: Experimental approach for N-1-1 contingency," *International Journal of Emerging Electric Power Systems*, vol. 17, no. 6, pp. 703–716, Dec. 2016, doi: 10.1515/IJEEPS-2016-0039.

[215] R. Belkacemi, A. Bababola, S. Zarrabian, and R. Craven, "Multi-Agent System algorithm for preventing cascading failures in smart grid systems," *2014 North American Power Symposium, NAPS 2014*, Nov. 2014, doi: 10.1109/NAPS.2014.6965442.

[216] R. Belkacemi and A. Bababola, “Experimental implementation of Multi-Agent System algorithm for distributed restoration of a Smart Grid System,” *Conference Proceedings - IEEE SOUTHEASTCON*, Nov. 2014, doi: 10.1109/SECON.2014.6950646.

[217] Z. Liu, Z. Chen, C. Liu, H. Sun, and Y. Hu, “Multi agent system based wide area protection against cascading events,” *10th International Power and Energy Conference, IPEC 2012*, pp. 445–450, 2012, doi: 10.1109/ASSCC.2012.6523309.

[218] M. Negnevitsky, N. Voropai, V. Kurbatsky, N. Tomin, and D. Panasetsky, “Development of an intelligent system for preventing large-scale emergencies in power systems,” *IEEE Power and Energy Society General Meeting*, 2013, doi: 10.1109/PESMG.2013.6672099.

[219] S. R. Islam, D. Sutanto, and K. M. Muttaqi, “Application of multi-agent system for preventing power interruption in a large power system,” *Proceedings of International Conference on Harmonics and Quality of Power, ICHQP*, pp. 226–231, 2012, doi: 10.1109/ICHQP.2012.6381211.

[220] M. Koenig, P. Duggan, J. Wong, M. Y. Vaiman, M. M. Vaiman, and M. Povolotskiy, “Prevention of cascading outages in Con Edison’s network,” *2010 IEEE PES Transmission and Distribution Conference and Exposition: Smart Solutions for a Changing World*, 2010, doi: 10.1109/TDC.2010.5484278.

[221] B. Shi and J. Liu, “Decentralized control and fair load-shedding compensations to prevent cascading failures in a smart grid,” *International Journal of Electrical Power and Energy Systems*, vol. 67, pp. 582–590, 2015, doi: 10.1016/J.IJEPES.2014.12.041.

[222] L. F. Grisales-Noreña, J. C. Morales-Duran, S. Velez-Garcia, O. D. Montoya, and W. Gil-González, “Power flow methods used in AC distribution networks: An analysis of convergence and processing times in radial and meshed grid configurations,” *Results in Engineering*, vol. 17, Mar. 2023, doi: 10.1016/j.rineng.2023.100915.

[223] R. Pinto and G. Gonçalves, “Application of Artificial Immune Systems in Advanced Manufacturing,” *Array*, vol. 15, Sep. 2022, doi: 10.1016/j.array.2022.100238.

[224] J. Timmis, T. Knight, L. N. de Castro, and E. Hart, “An Overview of Artificial Immune Systems,” pp. 51–91, 2004, doi: 10.1007/978-3-662-06369-9_4.

[225] “‘Wide area measurement systems—Monitoring and control for the grid of the future,’ ”, Accessed: Oct. 10, 2024. [Online].

[226] “University of Washington Electrical Engineering Resources: Power Systems Test Case Archive. .” Accessed: Oct. 10, 2024. [Online].

[227] Z. Liu, Z. Chen, H. Sun, and C. Liu, “Emergency load shedding strategy based on sensitivity analysis of relay operation margin against cascading events,” *2012 IEEE*

International Conference on Power System Technology, POWERCON 2012, 2012, doi: 10.1109/POWERCON.2012.6401450.

[228] A. Rose, G. Oladosu, and S. Y. Liao, "Business interruption impacts of a terrorist attack on the electric power system of Los Angeles: Customer resilience to a total blackout," *Risk Analysis*, vol. 27, no. 3, pp. 513–531, Jun. 2007, doi: 10.1111/J.1539-6924.2007.00912.X.

[229] P. Hines, J. Apt, and S. Talukdar, "Large blackouts in North America: Historical trends and policy implications," *Energy Policy*, vol. 37, no. 12, pp. 5249–5259, Dec. 2009, doi: 10.1016/J.ENPOL.2009.07.049.

[230] C. W. Anderson, J. R. Santos, and Y. Y. Haimes, "A Risk-based Input–Output Methodology for Measuring the Effects of the August 2003 Northeast Blackout," *Economic Systems Research*, vol. 19, no. 2, pp. 183–204, Jun. 2007, doi: 10.1080/09535310701330233.

[231] H. H. Alhelou, M. E. Hamedani-Golshan, T. C. Njenda, and P. Siano, "A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges," *Energies 2019, Vol. 12, Page 682*, vol. 12, no. 4, p. 682, Feb. 2019, doi: 10.3390/EN12040682.

[232] J. J. Romero, "Blackouts illuminate India's power problems," *IEEE Spectr*, vol. 49, no. 10, pp. 11–12, 2012, doi: 10.1109/MSPEC.2012.6309237.

[233] L. L. Lai, H. T. Zhang, S. Mishra, D. Ramasubramanian, C. S. Lai, and F. Y. Xu, "Lessons learned from July 2012 Indian blackout," *IET Conference Publications*, vol. 2012, no. 616 CP, 2012, doi: 10.1049/CP.2012.2173.

[234] "The Major Outage in South Vietnam in 2013: The Nature of Blackout, Security Measures and Strategy of National Power System Modernization." Accessed: Nov. 12, 2024. [Online]. Available: https://isem.irk.ru/publications/conference_paper2015000003184/

[235] P. Gomes, "New strategies to improve bulk power system security: Lessons learned from large blackouts," *2004 IEEE Power Engineering Society General Meeting*, vol. 2, pp. 1703–1708, 2004, doi: 10.1109/PES.2004.1373163.

[236] N. Phuangpornpitak and S. Tia, "Opportunities and Challenges of Integrating Renewable Energy in Smart Grid System," *Energy Procedia*, vol. 34, pp. 282–290, Jan. 2013, doi: 10.1016/J.EGYPRO.2013.06.756.

[237]. "United States Annual Report 2013; Technical Report, 2013. Available online: http://powerquality. eaton.com -." Accessed: Nov. 13, 2024. [Online].

[238] M. A. Kabir, M. M. H. Sajeeb, M. N. Islam, and A. H. Chowdhury, "Frequency transient analysis of countrywide blackout of Bangladesh Power System on 1st November, 2014," *Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering, ICAEE 2015*, pp. 267–270, Jul. 2016, doi: 10.1109/ICAEE.2015.7506847.

[239] "(PDF) Avoidance of Blackouts using Automatic Node Switching Technique through ETAP." Accessed: Nov. 12, 2024. [Online]. Available: https://www.researchgate.net/publication/374087561_Avoidance_of_Blackouts_using_Automatic_Node_Switching_Technique_through_ETAP

[240] A. U. Rehman, M. A. Mengal, I. Ahmad, A. U. Rehman, and S. Mehmood, "Voltage fluctuations and very low voltage profile problems in distribution system under extreme load growth," *Asia-Pacific Power and Energy Engineering Conference, APPEEC*, vol. 2016-December, pp. 205–210, Dec. 2016, doi: 10.1109/APPEEC.2016.7779498.

[241] "Rebels Tied to Blackout Across Most of Pakistan – The Energy Bulletin Daily." Accessed: Nov. 12, 2024. [Online]. Available: https://daily.energybulletin.org/2015/01/rebels-tied-to-blackout-across-most-of-pakistan/

[242] O. P. Veloza and F. Santamaria, "Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes," *The Electricity Journal*, vol. 29, no. 7, pp. 42–49, Sep. 2016, doi: 10.1016/J.TEJ.2016.08.006.

[243] S. Imai, D. Novosel, D. Karlsson, and A. Apostolov, "Unexpected Consequences: Global Blackout Experiences and Preventive Solutions," *IEEE Power and Energy Magazine*, vol. 21, no. 3, pp. 16–29, May 2023, doi: 10.1109/MPE.2023.3247096.

[244] "The anatomy of a power grid blackout - Root causes and dynamics of recent major blackouts | IEEE Journals & Magazine | IEEE Xplore." Accessed: Dec. 20, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1687814

[245] I. Ahmed, M. Adnan, S. Iqbal, A. Raza, W. Hassan, and S. E. G. Mohamed, "A survey of challenges and potential of implementing a resilient network for Pakistan's electric power infrastructure to avoid blackouts," *Results in Engineering*, vol. 24, p. 103004, Dec. 2024, doi: 10.1016/J.RINENG.2024.103004.

[246] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," *70th Annual Conference for Protective Relay Engineers, CPRE 2017*, Oct. 2017, doi: 10.1109/CPRE.2017.8090056.

[247] " '"A survey on security communication and control for smart grids under malicious cyber attacks,"' IEEE Trans. Syst., Man, Cybern., Syst., vol. 49, no. 8, pp. 1554–1569, Aug. 2019. ", Accessed: Dec. 20, 2024. [Online].

[248] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan. 2012, doi: 10.1109/MPE.2011.943114.

[249] V. S. Rajkumar, A. Stefanov, A. Presekal, P. Palensky, and J. L. R. Torres, "Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures," *IEEE Access*, vol. 11, pp. 103154–103176, 2023, doi: 10.1109/ACCESS.2023.3317695.

[250] C. Peng, H. Sun, M. Yang, and Y. L. Wang, “A Survey on Security Communication and Control for Smart Grids under Malicious Cyber Attacks,” *IEEE Trans Syst Man Cybern Syst*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019, doi: 10.1109/TSMC.2018.2884952.

[251] S. Paul, F. Ding, K. Utkarsh, W. Liu, M. J. O’Malley, and J. Barnett, “On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review,” *IEEE Syst J*, vol. 16, no. 2, pp. 2367–2378, Jun. 2022, doi: 10.1109/JSYST.2021.3123904.

[252] H. Zhang, B. Liu, and H. Wu, “Smart Grid Cyber-Physical Attack and Defense: A Review,” *IEEE Access*, vol. 9, pp. 29641–29659, 2021, doi: 10.1109/ACCESS.2021.3058628.

[253] M. Abdelmalak, V. Venkataramanan, and R. MacWan, “A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems,” *IEEE Access*, vol. 10, pp. 99875–99896, 2022, doi: 10.1109/ACCESS.2022.3206830.

[254] M. M. Hossain and C. Peng, “Cyber–physical security for on-going smart grid initiatives: a survey,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 3, pp. 233–244, Sep. 2020, doi: 10.1049/IET-CPS.2019.0039.

[255] A. Clark and S. Zonouz, “Cyber-physical resilience: Definition and assessment metric,” *IEEE Trans Smart Grid*, vol. 10, no. 2, pp. 1671–1684, Mar. 2019, doi: 10.1109/TSG.2017.2776279.

[256] L. D. Valdez *et al.*, “Review: Cascading failures in complex networks,” *J Complex Netw*, vol. 8, no. 2, 2020, doi: 10.1093/COMNET/CNAA013.

[257] R. Meyur, A. Vullikanti, M. V. Marathe, A. Pal, M. Youssef, and V. Centeno, “Cascading effects of targeted attacks on the power grid,” *Studies in Computational Intelligence*, vol. 812, pp. 155–167, 2019, doi: 10.1007/978-3-030-05411-3_13.

[258] M. Zhou, C. Liu, A. A. Jahromi, D. Kundur, J. Wu, and C. Long, “Revealing Vulnerability of N-1 Secure Power Systems to Coordinated Cyber-Physical Attacks,” *IEEE Transactions on Power Systems*, vol. 38, no. 2, pp. 1044–1057, Mar. 2023, doi: 10.1109/TPWRS.2022.3169482.

[259] A. Volkova, M. Niedermeier, R. Basmadjian, and H. De Meer, “Security challenges in control network protocols: A survey,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 619–639, Jan. 2019, doi: 10.1109/COMST.2018.2872114.

[260] P. Wang and M. Govindarasu, “Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid,” *IEEE Trans Smart Grid*, vol. 11, no. 4, pp. 3447–3456, Jul. 2020, doi: 10.1109/TSG.2020.2970755.

[261] L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, “Evaluation of cyber-physical power systems in cascading failure: Node vulnerability and systems connectivity,” *IET*

Generation, Transmission and Distribution, vol. 14, no. 7, pp. 1197–1206, Apr. 2020, doi: 10.1049/IET-GTD.2019.1286.

[262] M. Ma and A. Lahmadi, "On the Impact of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems," *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2018*, Dec. 2018, doi: 10.1109/SMARTGRIDCOMM.2018.8587491.

[263] I. L. Carreno, A. Scaglione, A. Zlotnik, D. Deka, and K. Sundar, "An Adversarial Model for Attack Vector Vulnerability Analysis on Power and Gas Delivery Operations," Oct. 2019, Accessed: Dec. 20, 2024. [Online]. Available: http://arxiv.org/abs/1910.03662

[264] X. Zhang, D. Liu, C. Zhan, and C. K. Tse, "Effects of Cyber Coupling on Cascading Failures in Power Systems," *IEEE J Emerg Sel Top Circuits Syst*, vol. 7, no. 2, pp. 228–238, Jun. 2017, doi: 10.1109/JETCAS.2017.2698163.

[265] G. Raman, B. AlShebli, M. Waniek, T. Rahwan, and J. C. H. Peng, "How weaponizing disinformation can bring down a city's power grid," *PLoS One*, vol. 15, no. 8 August, Aug. 2020, doi: 10.1371/JOURNAL.PONE.0236517.

[266] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Trans Smart Grid*, vol. 9, no. 5, pp. 4490–4502, Sep. 2018, doi: 10.1109/TSG.2017.2661307.

[267] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids," *ACM International Conference Proceeding Series*, vol. Part F132521, pp. 303–314, Dec. 2017, doi: 10.1145/3134600.3134639.

[268] P. Du and J. Matevosyan, "Forecast system inertia condition and its impact to integrate more renewables," *IEEE Trans Smart Grid*, vol. 9, no. 2, pp. 1531–1533, 2018, doi: 10.1109/TSG.2017.2662318.

[269] M. F. M. Arani, A. Abiri Jahromi, D. Kundur, and M. Kassouf, "Modeling and simulation of the aurora attack on microgrid point of common coupling," *7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2019 - Held as part of CPS Week, Proceedings*, Apr. 2019, doi: 10.1109/MSCPES.2019.8738801.

[270] F. Li *et al.*, "Detection and Diagnosis of Data Integrity Attacks in Solar Farms Based on Multilayer Long Short-Term Memory Network," *IEEE Trans Power Electron*, vol. 36, no. 3, pp. 2495–2498, Mar. 2021, doi: 10.1109/TPEL.2020.3017935.

[271] Y. Isozaki *et al.*, "Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids with PVs," *IEEE Trans Smart Grid*, vol. 7, no. 4, pp. 1824–1835, Jul. 2016, doi: 10.1109/TSG.2015.2427380.

[272] B. Chen, K. L. Butler-Purry, S. Nuthalapati, and D. Kundur, “Network delay caused by cyber attacks on SVC and its impact on transient stability of smart grids,” *IEEE Power and Energy Society General Meeting*, vol. 2014-October, no. October, Oct. 2014, doi: 10.1109/PESGM.2014.6938963.

[273] A. M. Abdullah and K. Butler-Purry, “Distance protection zone 3 misoperation during system wide cascading events: The problem and a survey of solutions,” *Electric Power Systems Research*, vol. 154, pp. 151–159, Jan. 2018, doi: 10.1016/J.EPSR.2017.08.023.

[274] F. Xue, E. Bompard, T. Huang, L. Jiang, S. Lu, and H. Zhu, “Interrelation of structure and operational states in cascading failure of overloading lines in power grids,” *Physica A: Statistical Mechanics and its Applications*, vol. 482, pp. 728–740, Sep. 2017, doi: 10.1016/j.physa.2017.04.061.

[275] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, “Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes,” *IEEE Transactions on Power Systems*, no. 1, pp. 440–450, 2020, doi: 10.1109/tpwrs.2019.2924441.

[276] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, “Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes,” *IEEE Trans Smart Grid*, vol. 9, no. 4, pp. 2862–2872, Jul. 2018, doi: 10.1109/TSG.2016.2622686.

[277] M. Noebels, I. Dobson, and M. Panteli, “Observed Acceleration of Cascading Outages,” *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3821–3824, Jul. 2021, doi: 10.1109/TPWRS.2021.3071028.

[278] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, “A critical review of cascading failure analysis and modeling of power system,” *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9–22, 2017, doi: 10.1016/j.rser.2017.05.206.

[279] C. W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, “Impact assessment of hypothesized cyberattacks on interconnected bulk power systems,” *IEEE Trans Smart Grid*, vol. 9, no. 5, pp. 4405–4425, Sep. 2018, doi: 10.1109/TSG.2017.2656068.

[280] R. Yan, N. Al-Masood, T. Kumar Saha, F. Bai, and H. Gu, “The anatomy of the 2016 South Australia blackout: A catastrophic event in a high renewable network,” *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5374–5388, Sep. 2018, doi: 10.1109/TPWRS.2018.2820150.

[281] “Indonesia blackout: Huge outage hits Jakarta and surrounding area.” Accessed: Dec. 20, 2024. [Online]. Available: https://www.bbc.com/news/world-asia-49227033

[282] H. H. Alhelou, M. E. Hamedani-Golshan, T. C. Njenda, and P. Siano, “A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges,” *Energies 2019, Vol. 12, Page 682*, vol. 12, no. 4, p. 682, Feb. 2019, doi: 10.3390/EN12040682.

[283] R. Yao, S. Huang, K. Sun, F. Liu, X. Zhang, and S. Mei, “A Multi-Timescale Quasi-Dynamic Model for Simulation of Cascading Outages,” *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3189–3201, Jul. 2016, doi: 10.1109/TPWRS.2015.2466116.

[284] R. Pfitzner, K. Turitsyn, and M. Chertkov, “Controlled Tripping of Overheated Lines Mitigates Power Outages,” Apr. 2011, Accessed: Dec. 20, 2024. [Online]. Available: http://arxiv.org/abs/1104.4558

[285] L. Liu, H. Wu, L. Li, D. Shen, F. Qian, and J. Liu, “Cascading Failure Pattern Identification in Power Systems Based on Sequential Pattern Mining,” *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 1856–1866, May 2021, doi: 10.1109/TPWRS.2020.3028999.

[286] J. De La Ree, Y. Liu, L. Mili, A. G. Phadke, and L. Dasilva, “Catastrophic failures in power systems: Causes, analyses, and countermeasures,” *Proceedings of the IEEE*, vol. 93, no. 5, pp. 956–964, 2005, doi: 10.1109/JPROC.2005.847246.

[287] D. Pal, B. Mallikarjuna, P. Gopakumar, M. J. B. Reddy, B. K. Panigrahi, and D. K. Mohanta, “Probabilistic Study of Undervoltage Load Shedding Scheme to Mitigate the Impact of Protection System Hidden Failures,” *IEEE Syst J*, vol. 14, no. 1, pp. 862–869, Mar. 2020, doi: 10.1109/JSYST.2019.2901350.

[288] I. Dobson and D. E. Newman, “Cascading blackout overall structure and some implications for sampling and mitigation,” *International Journal of Electrical Power and Energy Systems*, vol. 86, pp. 29–32, Mar. 2017, doi: 10.1016/J.IJEPES.2016.09.006.

[289] Z. Ma, C. Shen, F. Liu, and S. Mei, “Fast screening of vulnerable transmission lines in power grids: A pagerank-based approach,” *IEEE Trans Smart Grid*, vol. 10, no. 2, pp. 1982–1991, Mar. 2019, doi: 10.1109/TSG.2017.2785267.

[290] M. Z. Islam, Y. Lin, V. M. Vokkarane, and V. Venkataramanan, “Cyber-physical cascading failure and resilience of power grid: A comprehensive review,” *Front Energy Res*, vol. 11, p. 1095303, Feb. 2023, doi: 10.3389/FENRG.2023.1095303.

[291] H. Sheikh, C. Prins, and E. Schrijvers, “Artificial Intelligence: Definition and Background,” pp. 15–41, 2023, doi: 10.1007/978-3-031-21448-6_2.

[292] N. U. Huda, I. Ahmed, M. Adnan, M. Ali, and F. Naeem, “Experts and intelligent systems for smart homes’ Transformation to Sustainable Smart Cities: A comprehensive review,” *Expert Syst Appl*, vol. 238, p. 122380, Mar. 2024, doi: 10.1016/J.ESWA.2023.122380.

[293] “A DEFINITION OF AI: MAIN CAPABILITIES AND SCIENTIFIC DISCIPLINES,” 2018, Accessed: Dec. 18, 2024. [Online]. Available: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

[294] K. P. Murphy, “Machine learning - a probabilistic perspective,” *Adaptive computation and machine learning series*, 2012.

[295] Y. Lei, N. Li, L. Guo, N. Li, T. Yan, and J. Lin, “Machinery health prognostics: A systematic review from data acquisition to RUL prediction,” *Mech Syst Signal Process*, vol. 104, pp. 799–834, May 2018, doi: 10.1016/J.YMSSP.2017.11.016.

[296] C. E. Garcia, M. R. Camana, and I. Koo, “Machine learning-based Scheme for Fault Detection for Turbine Engine Disk,” *International Conference on ICT Convergence*, vol. 2020-October, pp. 11–16, Oct. 2020, doi: 10.1109/ICTC49870.2020.9289399.

[297] K. Zhong, M. Han, and B. Han, “Data-driven based fault prognosis for industrial systems: A concise overview,” *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 2, pp. 330–345, Mar. 2020, doi: 10.1109/JAS.2019.1911804.

[298] J. J. Gertler, “Fault detection and diagnosis in engineering systems,” *Fault Detection and Diagnosis in Engineering Systems*, pp. 1–488, Jan. 2017, doi: 10.1201/9780203756126/FAULT-DETECTION-DIAGNOSIS-ENGINEERING-SYSTEMS-JANOS-GERTLER/ACCESSIBILITY-INFORMATION.

[299] A. Abid, M. T. Khan, and J. Iqbal, “A review on fault detection and diagnosis techniques: basics and beyond,” *Artif Intell Rev*, vol. 54, no. 5, pp. 3639–3664, Nov. 2020, doi: 10.1007/S10462-020-09934-2.

[300] S. Nandi and H. A. Toliyat, “Fault diagnosis of electrical machines-a review,” *IEEE International Electric Machines and Drives Conference. IEMDC’99. Proceedings (Cat. No.99EX272)*, pp. 219–221, 1999, doi: 10.1109/IEMDC.1999.769076.

[301] H. LI, J. HE, X. WANG, and H. YANG, “Research Review and Prospect of Fault Diagnosis Method of Satellite Power System Based on Machine Learning,” *DEStech Transactions on Computer Science and Engineering*, no. ccme, Mar. 2019, doi: 10.12783/DTCSE/CCME2018/28665.

[302] E. Zio and T. Aven, “Industrial disasters: Extreme events, extremely rare. Some reflections on the treatment of uncertainties in the assessment of the associated risks,” *Process Safety and Environmental Protection*, vol. 91, no. 1–2, pp. 31–45, Jan. 2013, doi: 10.1016/J.PSEP.2012.01.004.

[303] C. E. Garcia, M. R. Camana, and I. Koo, “Machine learning-based Scheme for Fault Detection for Turbine Engine Disk,” *International Conference on ICT Convergence*, vol. 2020-October, pp. 11–16, Oct. 2020, doi: 10.1109/ICTC49870.2020.9289399.

[304] S. Nandi and H. A. Toliyat, “Condition monitoring and fault diagnosis of electrical machines-a review,” *Conference Record of the 1999 IEEE Industry Applications*

Conference. Thirty-Forth IAS Annual Meeting (Cat. No.99CH36370), vol. 1, pp. 197–204, 1999, doi: 10.1109/IAS.1999.799956.

[305] M. D. C. Moura, E. Zio, I. D. Lins, and E. Droguett, "Failure and reliability prediction by support vector machines regression of time series data," *Reliab Eng Syst Saf*, vol. 96, no. 11, pp. 1527–1534, Nov. 2011, doi: 10.1016/J.RESS.2011.06.006.

[306] M. D. C. Moura, E. Zio, I. D. Lins, and E. Droguett, "Failure and reliability prediction by support vector machines regression of time series data," *Reliab Eng Syst Saf*, vol. 96, no. 11, pp. 1527–1534, Nov. 2011, doi: 10.1016/J.RESS.2011.06.006.

[307] N. R. Prasad, S. Almanza-Garcia, and T. T. Lu, "Anomaly detection," *ACM Computing Surveys (CSUR)*, vol. 14, no. 1, pp. 1–22, Jul. 2009, doi: 10.1145/1541880.1541882.

[308] M. Riera-Guasp, J. A. Antonino-Daviu, and G. A. Capolino, "Advances in electrical machine, power electronic, and drive condition monitoring and fault detection: State of the art," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 3, pp. 1746–1759, Mar. 2015, doi: 10.1109/TIE.2014.2375853.

[309] J. Baxter and A. S. Leger, "Methodology for Machine Learning Anomaly Detection in Phasor Measurement Unit Data," *2022 IEEE Kansas Power and Energy Conference, KPEC 2022*, 2022, doi: 10.1109/KPEC54747.2022.9814789.

[310] T. Inoue, D. Sugiyama, and T. Shimotomai, "Machine Learning Approaches to Anomaly Detection of Top Drive Torque Causing Drill Pipe Failure," *Volume 8: Polar and Arctic Sciences and Technology; Petroleum Technology*, vol. 8, 2018, doi: 10.1115/OMAE2018-77882.

[311] N. Tamascelli, A. Campari, T. Parhizkar, and N. Paltrinieri, "Artificial Intelligence for safety and reliability: A descriptive, bibliometric and interpretative review on machine learning," *J Loss Prev Process Ind*, vol. 90, p. 105343, Aug. 2024, doi: 10.1016/J.JLP.2024.105343.

[312] K. Fida, U. Abbasi, M. Adnan, S. Iqbal, and S. E. Gasim Mohamed, "A comprehensive survey on load forecasting hybrid models: Navigating the Futuristic demand response patterns through experts and intelligent systems," *Results in Engineering*, vol. 23, p. 102773, Sep. 2024, doi: 10.1016/J.RINENG.2024.102773.

[313] S. Pfaffel, S. Faulstich, and K. Rohrig, "Performance and Reliability of Wind Turbines: A Review," *Energies 2017, Vol. 10, Page 1904*, vol. 10, no. 11, p. 1904, Nov. 2017, doi: 10.3390/EN10111904.

[314] E. Chai, P. P. Zeng, S. Ma, H. Xing, and B. Zhao, "Artificial Intelligence Approaches to Fault Diagnosis in Power Grids: A Review," *Cybersecurity and Cyberforensics*

Conference, vol. 2019-July, pp. 7346–7353, Jul. 2019, doi: 10.23919/CHICC.2019.8865533.

[315] K. Leahy, C. Gallagher, P. O'Donovan, and D. T. J. O'Sullivan, "Issues with Data Quality for Wind Turbine Condition Monitoring and Reliability Analyses," *Energies 2019, Vol. 12, Page 201*, vol. 12, no. 2, p. 201, Jan. 2019, doi: 10.3390/EN12020201.

[316] B. Frénay and M. Verleysen, "Classification in the presence of label noise: A survey," *IEEE Trans Neural Netw Learn Syst*, vol. 25, no. 5, pp. 845–869, 2014, doi: 10.1109/TNNLS.2013.2292894.

[317] J. R. Quinlan, "Induction of decision trees," *Machine Learning 1986 1:1*, vol. 1, no. 1, pp. 81–106, Mar. 1986, doi: 10.1007/BF00116251.

[318] S. Yang, A. Bryant, P. Mawby, D. Xiang, L. Ran, and P. Tavner, "An industry-based survey of reliability in power electronic converters," *IEEE Trans Ind Appl*, vol. 47, no. 3, pp. 1441–1451, May 2011, doi: 10.1109/TIA.2011.2124436.

[319] S. Zhao, F. Blaabjerg, and H. Wang, "An overview of artificial intelligence applications for power electronics," *IEEE Trans Power Electron*, vol. 36, no. 4, pp. 4633–4658, Apr. 2021, doi: 10.1109/TPEL.2020.3024914.

[320] S. Yang, D. Xiang, A. Bryant, P. Mawby, L. Ran, and P. Tavner, "Condition monitoring for device reliability in power electronic converters: A review," *IEEE Trans Power Electron*, vol. 25, no. 11, pp. 2734–2752, 2010, doi: 10.1109/TPEL.2010.2049377.

[321] B. Bossoufi, H. A. Aroussi, and M. Boderbala, "Direct Power Control of Wind Power Systems based on DFIG-Generator (WECS)," *Proceedings of the 12th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2020*, Jun. 2020, doi: 10.1109/ECAI50035.2020.9223136.

[322] S. Pfaffel, S. Faulstich, and K. Rohrig, "Performance and reliability of wind turbines: A review," *Energies (Basel)*, vol. 10, no. 11, Nov. 2017, doi: 10.3390/EN10111904.

[323] K. Mahmud, J. Ravishankar, M. J. Hossain, and Z. Y. Dong, "The impact of prediction errors in the domestic peak power demand management," *IEEE Trans Industr Inform*, vol. 16, no. 7, pp. 4567–4579, Jul. 2020, doi: 10.1109/TII.2019.2946292.

[324] B. Ray, R. Shah, M. R. Islam, and S. Islam, "A New Data Driven Long-Term Solar Yield Analysis Model of Photovoltaic A New Data Driven Long-Term Solar Yield Analysis Model of Photovoltaic Power Plants Power Plants", doi: 10.1109/ACCESS.2020.3011982.

[325] A. Ismail, L. Saidi, M. Sayadi, and M. Benbouzid, "A New Data-Driven Approach for Power IGBT Remaining Useful Life Estimation Based On Feature Reduction Technique and Neural Network," *Electronics 2020, Vol. 9, Page 1571*, vol. 9, no. 10, p. 1571, Sep. 2020, doi: 10.3390/ELECTRONICS9101571.

[326] J. M. M. Arce and E. Q. B. MacAbebe, “Real-time power consumption monitoring and forecasting using regression techniques and machine learning algorithms,” *Proceedings - 2019 IEEE International Conference on Internet of Things and Intelligence System, IoTaIS 2019*, pp. 135–140, Nov. 2019, doi: 10.1109/IOTAIS47347.2019.8980380.

[327] X. Li, Q. Ding, and J. Q. Sun, “Remaining useful life estimation in prognostics using deep convolution neural networks,” *Reliab Eng Syst Saf*, vol. 172, pp. 1–11, Apr. 2018, doi: 10.1016/J.RESS.2017.11.021.

[328] K. Mahmud, S. Azam, A. Karim, S. Zobaed, B. Shanmugam, and D. Mathur, “Machine Learning Based PV Power Generation Forecasting in Alice Springs,” *IEEE Access*, vol. 9, pp. 46117–46128, 2021, doi: 10.1109/ACCESS.2021.3066494.

[329] G. Ciaburro, G. Iannace, V. Puyana-Romero, and A. Trematerra, “Machine Learning-Based Tools for Wind Turbine Acoustic Monitoring,” *Applied Sciences 2021, Vol. 11, Page 6488*, vol. 11, no. 14, p. 6488, Jul. 2021, doi: 10.3390/APP11146488.

[330] R. K. Behara and A. K. Saha, “Artificial Intelligence Methodologies in Smart Grid-Integrated Doubly Fed Induction Generator Design Optimization and Reliability Assessment: A Review,” *Energies 2022, Vol. 15, Page 7164*, vol. 15, no. 19, p. 7164, Sep. 2022, doi: 10.3390/EN15197164.

[331] “Bitcoin: A Peer-to-Peer Electronic Cash System.” Accessed: Dec. 19, 2024. [Online]. Available: https://www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System

[332] R. Huo *et al.*, “A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges,” *IEEE Communications Surveys and Tutorials*, vol. 24, no. 1, pp. 88–122, 2022, doi: 10.1109/COMST.2022.3141490.

[333] M. Dotan, Y. Pignolet, and S. Stefan Schmid, “Survey on Blockchain Networking: Context, State-of-the-Art, Challenges”.

[334] S. R. Vinta, S. A. Patel, A. Z. Sameen, M. Soni, D. I. R. Khan, and H. M. Salman, “Dynamic Defense Model against Eclipse Attacks in Proof-of-Work Blockchain Systems,” *Procedia Comput Sci*, vol. 235, pp. 1202–1212, Jan. 2024, doi: 10.1016/J.PROCS.2024.04.114.

[335] S. E. Thomsen and B. Spitters, “Formalizing Nakamoto-Style Proof of Stake,” *IEEE Computer Security Foundations Symposium*, vol. 2021-June, 2020, doi: 10.1109/CSF51468.2021.00042.

[336] X. Jian, P. Leng, Y. Wang, M. Alrashoud, and M. S. Hossain, “Blockchain-Empowered Trusted Networking for Unmanned Aerial Vehicles in the B5G Era,” *IEEE Netw*, vol. 35, no. 1, pp. 72–77, Mar. 2021, doi: 10.1109/MNET.011.2000177.

[337] T. Huynh-The *et al.*, “Blockchain for the metaverse: A Review,” *Future Generation Computer Systems*, vol. 143, pp. 401–419, Jun. 2023, doi: 10.1016/J.FUTURE.2023.02.008.

[338] P. Boobalan *et al.*, “Fusion of Federated Learning and Industrial Internet of Things,” *Computer Networks*, vol. 212, Jul. 2022, doi: 10.1016/J.COMNET.2022.109048.

[339] A. A. Zarir, G. A. Oliva, Z. M. J. Jiang, and A. E. Hassan, “Developing Cost-Effective Blockchain-Powered Applications,” *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 30, no. 3, Mar. 2021, doi: 10.1145/3431726.

[340] T. Reddy Gadekallu *et al.*, “IEEE INTERNET OF THINGS JOURNAL 1 Blockchain for Edge of Things: Applications, Opportunities, and Challenges”.

[341] T. Reddy Gadekallu *et al.*, “Blockchain for Edge of Things: Applications, Opportunities, and Challenges,” *ArXiv*, p. arXiv:2110.05022, Oct. 2021, doi: 10.48550/ARXIV.2110.05022.

[342] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, “Fusing Blockchain and AI with Metaverse: A Survey,” *IEEE Open Journal of the Computer Society*, vol. 3, pp. 122–136, Jan. 2022, doi: 10.1109/OJCS.2022.3188249.

[343] H. Ning *et al.*, “A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges,” Nov. 2021, Accessed: Dec. 19, 2024. [Online]. Available: http://arxiv.org/abs/2111.09673

[344] H. Jeon, H. Youn, S. Ko, and T. Kim, “Blockchain and AI Meet in the Metaverse,” *Blockchain Potential in AI*, Jan. 2022, doi: 10.5772/INTECHOPEN.99114.

[345] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, “Evaluating Suitability of Applying Blockchain,” *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS*, vol. 2017-November, pp. 158–161, Jul. 2017, doi: 10.1109/ICECCS.2017.26.

[346] S. K. Lo, X. Xu, M. Staples, and L. Yao, “Reliability analysis for blockchain oracles,” *Computers & Electrical Engineering*, vol. 83, p. 106582, May 2020, doi: 10.1016/J.COMPELECENG.2020.106582.

[347] N. Vashistha, M. M. Hossain, M. R. Shahriar, F. Farahmandi, F. Rahman, and M. M. Tehranipoor, “EChain: A Blockchain-Enabled Ecosystem for Electronic Device Authenticity Verification,” *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 23–37, Feb. 2022, doi: 10.1109/TCE.2021.3139090.

[348] T. Huynh-The *et al.*, “Blockchain for the metaverse,” *Future Generation Computer Systems*, vol. 143, pp. 401–419, Jun. 2023, doi: 10.1016/J.FUTURE.2023.02.008.

[349] “Engineering Reliability New Techniques And Applications BS Dhillon : Free Download, Borrow, and Streaming : Internet Archive.” Accessed: Dec. 19, 2024. [Online]. Available: https://archive.org/details/EngineeringReliabilityNewTechniquesAndApplicationsBSDhillon

[350] “August 2003 Blackout | Department of Energy.” Accessed: Nov. 07, 2024. [Online]. Available: https://www.energy.gov/oe/august-2003-blackout

[351] “Lessons Learnt from Recent Emergencies and Blackout Incidents | eCIGRE.” Accessed: Nov. 07, 2024. [Online]. Available: https://www.e-cigre.org/publications/detail/608-lessons-learnt-from-recent-emergencies-and-blackout-incidents.html

[352] M. Vaiman *et al.*, “Risk assessment of cascading outages: Methodologies and challenges,” *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012, doi: 10.1109/TPWRS.2011.2177868.

[353] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, “Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization,” *Chaos*, vol. 17, no. 2, Jun. 2007, doi: 10.1063/1.2737822/934765.

[354] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, “Evidence for self-organized criticality in a time series of electric power system blackouts,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 51, no. 9, pp. 1733–1740, 2004, doi: 10.1109/TCSI.2004.834513.

[355] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, “Critical points and transitions in an electric power transmission model for cascading failure blackouts,” *Chaos*, vol. 12, no. 4, pp. 985–994, 2002, doi: 10.1063/1.1505810.

[356] M. J. Eppstein and P. D. H. Hines, “A ‘random chemistry’ algorithm for identifying collections of multiple contingencies that initiate cascading failure,” *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1698–1705, 2012, doi: 10.1109/TPWRS.2012.2183624.

[357] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, “Critical points and transitions in an electric power transmission model for cascading failure blackouts,” *Chaos*, vol. 12, no. 4, pp. 985–994, 2002, doi: 10.1063/1.1505810.

[358] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, “Criticality in a cascading failure blackout model,” *International Journal of Electrical Power & Energy Systems*, vol. 28, no. 9, pp. 627–633, Nov. 2006, doi: 10.1016/J.IJEPES.2006.03.006.

[359] Q. Chen and L. Mili, “Composite power system vulnerability evaluation to cascading failures using importance sampling and antithetic variates,” *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2321–2330, 2013, doi: 10.1109/TPWRS.2013.2238258.

[360] S. Mei, Y. Ni, G. Wang, and S. Wu, “A study of self-organized criticality of power system under cascading failures based on AC-OPF with voltage stability margin,” *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1719–1726, 2008, doi: 10.1109/TPWRS.2008.2002295.

[361] D. Bienstock, “Adaptive online control of cascading blackouts,” *IEEE Power and Energy Society General Meeting*, 2011, doi: 10.1109/PES.2011.6039012.

[362] R. Fitzmaurice, E. Cotilla-Sanchez, and P. Hines, “Evaluating the impact of modeling assumptions for cascading failure simulation,” *IEEE Power and Energy Society General Meeting*, 2012, doi: 10.1109/PESGM.2012.6345378.

[363] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, “Stochastic analysis of cascading-failure dynamics in power grids,” *IEEE Transactions on Power Systems*, vol. 29, no. 4, pp. 1767–1779, 2014, doi: 10.1109/TPWRS.2013.2297276.

[364] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. U. Hwang, “Complex networks: Structure and dynamics,” *Phys Rep*, vol. 424, no. 4–5, pp. 175–308, Feb. 2006, doi: 10.1016/J.PHYSREP.2005.10.009.

[365] I. Dobson, “Estimating the propagation and extent of cascading line outages from utility data with a branching process,” *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 2146–2155, 2012, doi: 10.1109/TPWRS.2012.2190112.

[366] P. D. H. Hines, I. Dobson, E. Cotilla-Sanchez, and M. Eppstein, “‘Dual graph’ and ‘random chemistry’ methods for cascading failure analysis,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 2141–2150, 2013, doi: 10.1109/HICSS.2013.1.

[367] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, “Topological models and critical slowing down: Two approaches to power system blackout risk analysis,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2011, doi: 10.1109/HICSS.2011.444.

[368] J. Yan, Y. Tang, H. He, and Y. Sun, “Cascading failure analysis with DC power flow model and transient stability analysis,” *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285–297, Jan. 2015, doi: 10.1109/TPWRS.2014.2322082.

[369] K. Sun, Ed., “Cascading Failures in Power Grids,” 2024, doi: 10.1007/978-3-031-48000-3.

[370] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. U. Hwang, “Complex networks: Structure and dynamics,” *Phys Rep*, vol. 424, no. 4–5, pp. 175–308, Feb. 2006, doi: 10.1016/J.PHYSREP.2005.10.009.

[371] Y. Yu *et al.*, “System crash as dynamics of complex networks,” *Proc Natl Acad Sci U S A*, vol. 113, no. 42, pp. 11726–11731, Oct. 2016, doi: 10.1073/PNAS.1612094113/SUPPL_FILE/PNAS.1612094113.SAPP.PDF.

[372] S. Soltan, D. Mazauric, and G. Zussman, “Cascading failures in power grids - Analysis and algorithms,” *e-Energy 2014 - Proceedings of the 5th ACM International Conference on Future Energy Systems*, pp. 195–206, 2014, doi: 10.1145/2602044.2602066.

[373] C. Zhai, H. Zhang, G. Xiao, and T.-C. Pan, “Modeling and Identification of Worst-Case Cascading Failures in Power Systems,” Mar. 2017, Accessed: Nov. 07, 2024. [Online]. Available: http://arxiv.org/abs/1703.05232

[374] E. G. Cate, K. Hemmaplardh, J. W. Manke, and D. P. Gelopulos, “Time frame notion and time response of the models in transient, mid-term and long-term stability programs,” *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-103, no. 1, pp. 143–151, 1984, doi: 10.1109/TPAS.1984.318592.

[375] M. Ouyang, L. Zhao, Z. Pan, and L. Hong, “Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks,” *Physica A: Statistical Mechanics and its Applications*, vol. 403, pp. 45–53, Jun. 2014, doi: 10.1016/J.PHYSA.2014.01.070.

[376] G. A. Pagani and M. Aiello, “The Power Grid as a complex network: A survey,” *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 11, pp. 2688–2700, Jun. 2013, doi: 10.1016/J.PHYSA.2013.01.023.

[377] J. W. Wang and L. L. Rong, “Cascade-based attack vulnerability on the US power grid,” *Saf Sci*, vol. 47, no. 10, pp. 1332–1336, Dec. 2009, doi: 10.1016/J.SSCI.2009.02.002.

[378] R. Albert, I. Albert, and G. L. Nakarado, “Structural Vulnerability of the North American Power Grid,” *Phys Rev E Stat Nonlin Soft Matter Phys*, vol. 69, no. 2 2, Jan. 2004, doi: 10.1103/PhysRevE.69.025103.

[379] H. T. Zhang, C. Zhai, and Z. Chen, “A general alignment repulsion algorithm for flocking of multi-agent systems,” *IEEE Trans Automat Contr*, vol. 56, no. 2, pp. 430–435, Feb. 2011, doi: 10.1109/TAC.2010.2089652.

[380] C. Zhai and Y. Hong, “Decentralized sweep coverage algorithm for uncertain region of multi-agent systems,” *Proceedings of the American Control Conference*, pp. 4522–4527, 2012, doi: 10.1109/ACC.2012.6315305.

[381] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, “Do topological models provide good information about electricity infrastructure vulnerability?,” *Chaos*, vol. 20, no. 3, Jul. 2010, doi: 10.1063/1.3489887/932307.

[382] T. M. Hong, M. L. Crow, B. H. Chowdhury, and A. Lininger, “Cascading line outage prevention with multiple UPFCs,” *2007 39th North American Power Symposium, NAPS*, pp. 273–278, 2007, doi: 10.1109/NAPS.2007.4402322.

[383] D. Fabozzi and T. Van Cutsem, “Simplified time-domain simulation of detailed long-term dynamic models,” *2009 IEEE Power and Energy Society General Meeting, PES ’09*, 2009, doi: 10.1109/PES.2009.5275463.

[384] S. K. Khaitan, C. Fu, and J. McCalley, “Fast parallelized algorithms for on-line extended-term dynamic cascading analysis,” *2009 IEEE/PES Power Systems Conference and Exposition, PSCE 2009*, 2009, doi: 10.1109/PSCE.2009.4840238.

[385] S. Abhyankar and A. J. Flueck, “Real-time power system dynamics simulation using a parallel Block-Jacobi preconditioned Newton-GMRES scheme,” *Proceedings - 2012 SC Companion: High Performance Computing, Networking Storage and Analysis, SCC 2012*, pp. 299–305, 2012, doi: 10.1109/SC.COMPANION.2012.48.

[386] C. Parmer, E. Cotilla-Sanchez, H. K. Thornquist, and P. D. H. Hines, “Developing a dynamic model of cascading failure for high performance computing using trilinos,” *HiPCNA-PG’11 - Proceedings of the 1st International Workshop on High Performance Computing, Networking and Analytics for the Power Grid, Co-located with SC’11*, pp. 25–33, 2011, doi: 10.1145/2096123.2096131.

[387] “Power System Stability and Control; McGraw-Hill: New York, NY, USA, 1994; Volume 7 .” Accessed: Nov. 12, 2024. [Online]. Available: https://www.google.com/search?q=Power+System+Stability+and+Control%3B+McGraw-Hill%3A+New+York%2C+NY%2C+USA%2C+1994%3B+Volume+7&oq=Power+System+Stability+and+Control%3B+McGraw-Hill%3A+New+York%2C+NY%2C+USA%2C+1994%3B+Volume+7&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCTE0ODJqMGoxNagCCLACAQ&sourceid=chrome&ie=UTF-8

[388] H. Haes Alhelou, M. E. Hamedani-Golshan, R. Zamani, E. Heydarian-Forushani, and P. Siano, “Challenges and Opportunities of Load Frequency Control in Conventional, Modern and Future Smart Power Systems: A Comprehensive Review,” *Energies 2018, Vol. 11, Page 2497*, vol. 11, no. 10, p. 2497, Sep. 2018, doi: 10.3390/EN11102497.

[389] “Simulation of the september 8, 2011, san diego blackout | Proceedings of the 2014 Winter Simulation Conference.” Accessed: Nov. 12, 2024. [Online]. Available: https://dl.acm.org/doi/10.5555/2693848.2694043

[390] “Empirical analysis of the impact of 2003 blackout on security values of US utilities and electrical equipment manufacturing firms. - Google Search.” Accessed: Nov. 12, 2024. [Online].

[391] K. Yamashita, S. K. Joo, J. Li, P. Zhang, and C. C. Liu, “Analysis, control, and economic impact assessment of major blackout events,” *European Transactions on Electrical Power*, vol. 18, no. 8, pp. 854–871, Nov. 2008, doi: 10.1002/ETEP.304.

[392] A. M. Attia, N. Aziz, and B. Friedman, “The Impact of Social Networks on Behavioral Change: A Conceptual Framework,” 2012.

[393] J. L. Corwin and W. T. Miles, “Impact assessment of the 1977 New York City blackout. Final report,” Jul. 1978, doi: 10.2172/6584645.

[394] C. Vogel, “Business and climate change: Initial explorations in South Africa,” *Clim Dev*, vol. 1, no. 1, pp. 82–97, 2009, doi: 10.3763/CDEV.2009.0007.

[395] M. M. Adibi and N. Martins, “Impact of power system blackouts,” *IEEE Power and Energy Society General Meeting*, vol. 2015-September, Sep. 2015, doi: 10.1109/PESGM.2015.7286025.

[396] “(PDF) Regional economic impacts of terrorist attacks on the electric power system of Los Angeles: A computable general disequilibrium analysis.” Accessed: Nov. 12, 2024. [Online]. Available: https://www.researchgate.net/publication/253885123_Regional_economic_impacts_of_terrorist_attacks_on_the_electric_power_system_of_Los_Angeles_A_computable_general_disequilibrium_analysis

[397] “(PDF) THE IMPACT OF ELECTRICITY CRISES ON THE CONSUMPTION BEHAVIOUR OF SMALL AND MEDIUM ENTERPRISES: EVIDENCE FROM PAKISTAN.” Accessed: Nov. 12, 2024. [Online].

[398] L. G. Kong and G. W. Cai, “Research on control method of inverters for large-scale grid-connected photovoltaic power system,” *Dianli Xitong Baohu yu Kongzhi/Power System Protection and Control*, vol. 41, no. 22, pp. 57–63, Nov. 2013, doi: 10.4236/EPE.2013.54B284.

[399] Y. Huang, J. Liu, X. Shen, and T. Dai, “The Interaction between the Large-Scale EVs and the Power Grid,” *Smart Grid and Renewable Energy*, vol. 04, no. 02, pp. 137–143, 2013, doi: 10.4236/SGRE.2013.42017.

[400] H. Posthumus, J. Morris, T. M. Hess, D. Neville, E. Phillips, and A. Baylis, “Impacts of the summer 2007 floods on agriculture in England,” *J Flood Risk Manag*, vol. 2, no. 3, pp. 182–189, Sep. 2009, doi: 10.1111/J.1753-318X.2009.01031.X.

[401] M. Kezunovic, I. Dobson, and Y. Dong, “Impact of Extreme Weather on Power System Blackouts and Forced Outages : New Challenges,” 2008.

[402] U. Qazi and M. Jahanzaib, “An integrated sectoral framework for the development of sustainable power sector in Pakistan,” *Energy Reports*, vol. 4, pp. 376–392, Nov. 2018, doi: 10.1016/J.EGYR.2018.06.001.

[403] L. L. Lai, H. T. Zhang, S. Mishra, D. Ramasubramanian, C. S. Lai, and F. Y. Xu, “Lessons learned from July 2012 Indian blackout,” *IET Conference Publications*, vol. 2012, no. 616 CP, 2012, doi: 10.1049/CP.2012.2173.

[404] X. Zhang, D. Liu, C. Zhan, and C. K. Tse, “Effects of Cyber Coupling on Cascading Failures in Power Systems,” *IEEE J Emerg Sel Top Circuits Syst*, vol. 7, no. 2, pp. 228–238, Jun. 2017, doi: 10.1109/JETCAS.2017.2698163.

[405] H. Guo, S. S. Yu, H. H. C. Iu, T. Fernando, and C. Zheng, “A complex network theory analytical approach to power system cascading failure-From a cyber-physical perspective,” *Chaos*, vol. 29, no. 5, May 2019, doi: 10.1063/1.5092629.

[406] Y. Han, C. Guo, S. Ma, and D. Song, “Modeling cascading failures and mitigation strategies in PMU based cyber-physical power systems,” *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 944–957, Sep. 2018, doi: 10.1007/S40565-018-0407-3/FIGURES/6.

[407] L. Lee and P. Hu, “Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks,” *International Journal of Electrical Power & Energy Systems*, vol. 111, pp. 182–190, Oct. 2019, doi: 10.1016/J.IJEPES.2019.03.062.

[408] X. Gao, M. Peng, C. K. Tse, and H. Zhang, “A Stochastic Model of Cascading Failure Dynamics in Cyber-Physical Power Systems,” *IEEE Syst J*, vol. 14, no. 3, pp. 4626–4637, Sep. 2020, doi: 10.1109/JSYST.2020.2964624.

[409] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, “Cyber-security in smart grid: Survey and challenges,” *Computers and Electrical Engineering*, vol. 67, pp. 469–482, Apr. 2018, doi: 10.1016/J.COMPELECENG.2018.01.015.

[410] H. Pan, H. Lian, C. Na, and X. Li, “Modeling and Vulnerability Analysis of Cyber-Physical Power Systems Based on Community Theory,” *IEEE Syst J*, vol. 14, no. 3, pp. 3938–3948, Sep. 2020, doi: 10.1109/JSYST.2020.2969023.

[411] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber-physical system security for the electric power grid,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012, doi: 10.1109/JPROC.2011.2165269.

[412] N. Ahmad, Y. G. Ghadi, M. Adnan, and M. Ali, “From Smart Grids to Super Smart Grids: A Roadmap for Strategic Demand Management for Next Generation SAARC and

European Power Infrastructure," *IEEE Access*, vol. 11, pp. 12303–12341, 2023, doi: 10.1109/ACCESS.2023.3241686.

[413] D. Liu and C. K. Tse, "Cascading Failure of Cyber-Coupled Power Systems Considering Interactions between Attack and Defense," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 11, pp. 4323–4336, Nov. 2019, doi: 10.1109/TCSI.2019.2922371.

[414] T. Zang, S. Gao, B. Liu, T. Huang, T. Wang, and X. Wei, "Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks," *Reliab Eng Syst Saf*, vol. 189, pp. 232–241, Sep. 2019, doi: 10.1016/J.RESS.2019.04.024.

[415] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017, doi: 10.1109/JPROC.2017.2686394.

[416] L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, "Study on attack paths of cyber attack in cyber-physical power systems," *IET Generation, Transmission and Distribution*, vol. 14, no. 12, pp. 2352–2360, Jun. 2020, doi: 10.1049/IET-GTD.2019.1330/CITE/REFWORKS.

[417] L. Che, X. Liu, T. Ding, and Z. Li, "Revealing Impacts of Cyber Attacks on Power Grids Vulnerability to Cascading Failures," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 6, pp. 1058–1062, Jun. 2019, doi: 10.1109/TCSII.2018.2869941.

[418] D. Liu and C. K. Tse, "Cascading Failure of Cyber-Coupled Power Systems Considering Interactions between Attack and Defense," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 11, pp. 4323–4336, Nov. 2019, doi: 10.1109/TCSI.2019.2922371.

[419] Z. Shuai, Y. Hu, Y. Peng, C. Tu, and Z. J. Shen, "Dynamic Stability Analysis of Synchronverter-Dominated Microgrid Based on Bifurcation Theory," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 9, pp. 7467–7477, Sep. 2017, doi: 10.1109/TIE.2017.2652387.

[420] H. Wu and X. Wang, "A Mode-Adaptive Power-Angle Control Method for Transient Stability Enhancement of Virtual Synchronous Generators," *IEEE J Emerg Sel Top Power Electron*, vol. 8, no. 2, pp. 1034–1049, Jun. 2020, doi: 10.1109/JESTPE.2020.2976791.

[421] M. Cespedes and J. Sun, "Impedance modeling and analysis of grid-connected voltage-source converters," *IEEE Trans Power Electron*, vol. 29, no. 3, pp. 1254–1261, 2014, doi: 10.1109/TPEL.2013.2262473.

[422] T. N. Nguyen, B. H. Liu, N. P. Nguyen, and J. Te Chou, “Cyber Security of Smart Grid: Attacks and Defenses,” *IEEE International Conference on Communications*, vol. 2020-June, Jun. 2020, doi: 10.1109/ICC40277.2020.9148850.

[423] Z. Ni and S. Paul, “A Multistage Game in Smart Grid Security: A Reinforcement Learning Solution,” *IEEE Trans Neural Netw Learn Syst*, vol. 30, no. 9, pp. 2684–2695, Sep. 2019, doi: 10.1109/TNNLS.2018.2885530.

[424] M. Z. Gunduz and R. Das, “Cyber-security on smart grid,” *Computer Networks*, vol. 169, Mar. 2020, doi: 10.1016/J.COMNET.2019.107094.

[425] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas, “Smart Grid Security: Threats, Challenges, and Solutions,” Jun. 2016, Accessed: Oct. 12, 2024. [Online]. Available: http://arxiv.org/abs/1606.06992

[426] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, “Privacy-preserving energy trading using consortium blockchain in smart grid,” *IEEE Trans Industr Inform*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019, doi: 10.1109/TII.2019.2893433.

[427] H. Jiang, Z. Wang, and H. He, “An Evolutionary Computation Approach for Smart Grid Cascading Failure Vulnerability Analysis,” *2019 IEEE Symposium Series on Computational Intelligence, SSCI 2019*, pp. 332–338, Dec. 2019, doi: 10.1109/SSCI44817.2019.9002979.

[428] Q. Gao, Y. Wang, X. Cheng, J. Yu, X. Chen, and T. Jing, “Identification of vulnerable lines in smart grid systems based on affinity propagation clustering,” *IEEE Internet Things J*, vol. 6, no. 3, pp. 5163–5171, Jun. 2019, doi: 10.1109/JIOT.2019.2897434.

[429] L. Xing, “Cascading Failures in Internet of Things: Review and Perspectives on Reliability and Resilience,” *IEEE Internet Things J*, vol. 8, no. 1, pp. 44–64, Jan. 2021, doi: 10.1109/JIOT.2020.3018687.

[430] L. D. Valdez *et al.*, “Cascading Failures in Complex Networks,” *J Complex Netw*, vol. 8, no. 2, Jul. 2020, doi: 10.1093/comnet/cnaa013.

[431] Z. Guo, K. Sun, X. Su, and S. Simunovic, “A Review on Simulation Models of Cascading Failures in Power Systems,” *iEnergy*, vol. 2, no. 4, pp. 284–296, Dec. 2023, doi: 10.23919/IEN.2023.0039.