An Agile Black-Out Detection and Response Paradigm in Smart Grids Incorporating IoT-Oriented Initiatives and Fog-Computing Platform

Hossein Shahinzadeh
Department of Electrical Engineering
Amirkabir University of Technology
Tehran, Iran
h.s.shahinzadeh@ieee.org

Arezou Mahmoudi
Faculty of electrical and computer engineering
University of Tabriz
Tabriz, Iran
ar-mahmoudi@tabrizu.ac.ir

Gevork B. Gharehpetian
Department of Electrical Engineering
Amirkabir University of Technology
Tehran, Iran
gptian@aut.ac.ir

S.M. Muyeen
Department of Electrical Engineering
Qatar University
Doha 2713, Qatar
sm.muyeen@qu.edu.qa

Mohamed Benbouzid
Institut de Recherche Dupuy de Lôme
University of Brest
29238 Brest, France
Mohamed.Benbouzid@univ-brest.fr

Ersan Kabalci
Department of Electrical Engineering
Nevsehir Haci Bektas Veli University
Nevsehir, Turkey
kabalci@nevsehir.edu.tr

Abstract— Voltage and frequency stability are fundamental subjects for power system operators. There are unwanted faults and factors, which affect the stability of the system and may result in a major instability (blackout). Thereby, predicting the possibility of consecutive and cascading incidences, diagnosing faults, distinguishing damaged system components, detecting overloaded lines, and examining bus voltage limits are among the topics, which should be considered by power system operators. Such an analysis facilitates decision-making for security measures and prevents global instability issues. IoT-oriented technologies can create instantaneous detection, swift warning, and agile response. Therefore, by incorporating and modeling successful initiatives and projects proposed and implemented in leading developed countries, the targeted objectives can be achieved while meeting prevailing constraints of the system. This paper intends to introduce a three-layer IoT-based security architecture in alignment with Cisco standards while taking advantage of the fog-computation platform subject to diagnose and intelligently react against instability threats.

Keywords- Internet of Things (IoT), Fog-computing, Black-out, Power system stability and security, Power system protection.

1. Introduction

The benefits of electrical energy and the increased tendency to more consumption of this type of energy have led to the expansion of power grids. With regard to the incremental demand and the expansion of electricity networks, complex and unpredictable phenomena, as well as unexpected events in electricity systems, have also increased [1]. These incidences can cause the power system to go out of balance and ultimately can be led to a wide collapse and shutdown. Blackout is an English term that has been used in various articles to describe the phenomenon of the wide shutdown of the entire electricity grid [2-3]. This phenomenon may be widespread and cover the entire power system, or it may cover only a certain part of a grid (also called brown-out) [4]. The blackout phenomenon has distinctive differences with the outages that occur due to lack of power, either by the operation of frequency stability relays or by voltage relays during voltage drops. The reason is that the mentioned types of outages are controlled or unpredictable, but blackouts are a type of unwanted outages that occurs as a result of complex interactions and are unexpected, uncontrolled, and very hard to predict. Moreover, the level of the severity, the extent of the affected area, and the consequences are relatively unknown for the operators and planners [5].

Consecutive incidences or cascading failures are one of the most important facets of blackouts that can be seen in all blackout events. This means that blackouts do not occur as a result of a single fault, but several correlated events and failures push the power system operation state toward uncontrolled collapses and finally blackouts. In the process of blackout occurrence, in addition to contingencies caused by natural factors and operating failures, some phenomena such as angular instability, thermal instability, voltage, and frequency instabilities are also involved [6-7].

Recent major blackouts around the world have shown that the probability of such blackouts is considerably increasing. These large-scale blackouts affect the economy and society. Security is one of the most vital features for the reliable operation of power systems. The security of the power system is always evaluated by the occurrence of disturbances. In traditional methods, the dynamic security of the power system is the consequence of the occurrence of a disturbance for only the first few seconds and is based on the criterion of transient stability. In these methods, the reaction of those elements of the power system that have a slower response and are not examined for transient stability over time, and also some protection and control systems are not considered [8]. Some of these elements include on-load tap changer transformers, generator excitation current limiter, line protection distance relay, high and low-frequency protection of turbines, and frequency control system of generating plants. Therefore, in order to be able to accurately and comprehensively assess the severity of an event, the subsequent behavior of the power
system after fault occurrence must be simulated for a longer period, so that all elements participate in it with both quick and slow responses [9].

The US Department of Energy has propounded the Smart Grid as an extensive automated energy grid that transmits electrical power and exchanges information in a two-way direction. This network can monitor and respond to any changes in the network from production sources to consumers and equipment. Immediate monitoring of consumption and more accurate modeling of production resources lead to the optimal and economical operation of the network and thus reduce consumer costs. Identification and outage of devices that lead to faults in the network as well as rapid detection of leakage current are prominent features of smart distribution networks [10]. In addition, the rapid detection of unserved subscribers increases performance efficiency. In smart grids, the power management unit, which includes a set of equipment, is responsible for controlling and protecting the network based on the information received from the network. Power consumption monitoring is possible based on comprehensive information received from the network with the help of IoT technology, which consists of the power monitoring system, high-burden processors, network information integration terminals centers, Intelligent Electronic Devices (IED) enabled by the Internet of Things (IoT) technology, and the possibility of remote consumption monitoring and control of electrical equipment in factories, companies, residential and institutional places [11]. This unit is also able to send remote control commands to the equipment, which enables the management of demand response potential. Another important issue in smart grids is network security, which depends on the precise operation of all network components and towers and transmission lines. IoT is an appropriate choice in terms of monitoring and protecting power transmission lines against the mechanical, environmental, and electrical problems, and the physical security of these lines. By installing special sensors for line monitoring and creating a suitable communication and telecommunication network by identifying the destructive and threatening factors of transmission lines caused by natural disasters or human failures, optimal and favorable conditions can be provided for the operation, maintenance, and security of the distribution network [12]. The fog-computing platform brings a new generation of services to the edge of technology to offer a wide range of IoT applications. It also supports mobility, location awareness, heterogeneity, large-scalability, low latency, and geographical distribution. In general, the goals of the fog computing model are to reduce the data volume and traffic for cloud servers, reduce latency and delay in data transfer, and improve service quality. The incremental trend of the pervasiveness of communication devices and sensors in smart grids and smart wireless sensor networks is forming the big data computing network in the form of an IoT network. The fog computing platform is considered a significant expansion of a cloud-based platform. Thus, it is inevitable that some security issues still exist. While some existing solutions in the field of cloud computing can address many security and privacy issues in cloud computing, fog computing can introduce new security challenges due to its distinctive features [13]. These challenges may affect the compatibility of fog computing with the Internet of Things. Fog computing, on the other hand, can provide an ideal platform for addressing many IoT security and privacy issues.

Many factors caused extensive damages to the electrical network. In some cases, natural hazardous disasters (such as dust and dust particles, massive fires, floods, heat and cold waves, storms, and earthquakes) or human-made crises (e.g. revolts due to political and social reasons) [14]. The role of the IoT in early warning systems has become even more prominent in crisis management. Currently, one of the most important topics in the field of electricity and smart grid industry is dedicated to the issue of security and being prepared against system instability. The development of IoT technology in recent years on the one hand, and the use of cyber-computing and artificial intelligence as well as fast and effective data transfer technologies, on the other hand, have increased the security and flexibility of operation in the smart grid and reduced financial detriments and technical damages to the system in the face outages and faults [15]. Therefore, in this paper, a native architecture is presented to implement a system for detecting, warning, and responding to instability and global network blackouts incorporating IoT-enabled devices based on a fog-computing platform.

II. Early fault and black-out warning system

There are many definitions of smart grid early warning systems aiming to guide the roles and instructions for the consumers, system managers, and experts in the electricity industry. The official definition of the International Energy Agency is as follows:

An early warning scheme is a time-oriented and effective provision of information through a specific paradigm that helps power system operators avoid or reduce the risk of contingencies and be prepared to respond effectively to them.

Typically, as shown in Fig.1, an effective early warning system includes the following criteria: risk analysis, monitoring and forecasting the location and severity of the disaster, informing system and market operators as well as power industry managers, and GENCOs and consumers who are potentially affected and making the best decision for a prompt reaction against failures and blackout [16-17].

The cycle of fault risk assessment includes pre-fault, during a fault, and post-fault phases. The early warning system mainly emphasizes the steps to prevent, adjust, and prepare for the fault cycle. This definition covers a range of factors necessary to achieve timely alerts for effective response. An IoT-based early warning system necessarily has four main components:

- Awareness of network risks
- Monitoring, data analysis
- Predicting faults, triggering, communicating, or propagating alarms

![Figure 1. Paradigm facets of fast warning system](image-url)
• Local capacity to respond to incoming alerts
The US Department of Energy has announced four main components of early warning system to reduce the effects of faults and cascading failures as follows:
• Risk knowledge: Risk assessment provides the information needed to prioritize mitigation and prevention strategies as well as the information required for the design of early warning systems.
• Monitoring, Analysis, and Forecasting: The systems with monitoring and forecasting capabilities provide timely estimates of faults and blackouts and their technical and economic effects on customers and generators.
• Distributed information: Communication systems are required to provide alerts. To send messages to potentially affected locations to inform local and regional operators in dispatching units. Messages should be reliable, artificial, and simple to be understood by users as well as electrical industry experts.
• Answer: Good coordination, operation and management, and appropriate action plans are important features in an effective early warning system. Likewise, the rapid awareness of users and managers through the Internet and cyberspace are vital aspects of reducing vulnerability.

A. Importance of early warning system
The implementation of an early warning system prevents staggering costs of detriments due to blackouts. The following items show the necessity of such paradigms.
• Ability to obtain information before the occurrence of a global blackout.
• Early warning systems can help to reduce damage.
• Network and microgrid operators in the vicinity of the points with high vulnerability to natural disasters and close to strategic loads are informed promptly so that they can isolate their network and use their internal grid in islanding mode to avoid blackouts and to serve to most possible loads.
• It is possible to use emergency generators, storage devices, or power supply through a secure network for sensitive loads.
• Divide the network into independent island networks to prevent the spread of faults to other parts of the network and the occurrence of global blackouts.
• An early warning system is involved in enhancing network reliability and security.
• Electricity producers, operators, and consumers all benefit from an early warning system.

The improved framework of early warning systems according to Table 1 and Fig.2 consists of four phases.

Early warning systems should be the basis for the exchange of information between various tools for evaluating, monitoring, forecasting, warning or reporting faults and errors, and decision-making support. All these measures can be provided using cutting-edge initiative tools. Many steps need to be taken to deploy capable early warning systems, including:
• Fault assessment and the performance of power grid protection systems should be adjusted based on key factors and processes, instead of fault symptoms.
• To provide the data needed to track faults, and understand changes in the power system state and protection network, a long-term monitoring scheme of the power system must be established and new IoT communication facilities must be deployed.
• Mechanisms and processes of information transfer must be provided in a correct and prompt timely manner to reach the targets.
• Close cooperation should be established between network operators and managers as well as warning and decision-making components.
• The link between future work in the field of indicators and criteria for evaluation and monitoring of power grids and early warning systems should be clarified and professional working groups should be established [18-20].

<table>
<thead>
<tr>
<th>Phase</th>
<th>Key components</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Faults monitoring</td>
</tr>
<tr>
<td>2</td>
<td>Predicting symptoms blackout</td>
</tr>
<tr>
<td>3</td>
<td>Fault warning or alarm</td>
</tr>
<tr>
<td>4</td>
<td>Reaction</td>
</tr>
</tbody>
</table>

Figure 2. Improved framework for early warning systems

B. Characteristics and procedure of early warning system paradigm
As an example, the specifications of an early warning system in a smart grid environment based on the telecommunication platform should be as follows:
• Power grid segmentation in terms of time and location: The Ministry of Energy along with the Independent System Operator (ISO) divides the global grid into different parts in terms of power supply and protection and warning system. This segmentation helps to send warning messages to local operators and local dispatching units in the event of cascading failures via the Internet of Things and the existing telecommunications system so that they can start to operate in islanding mode by examining the warning. Depending on the sensitivity of the zone, aside from the local operators and dispatching units, the warning alarm can also be sent to independent energy producers (GENCOs), as well as energy distribution companies (DISCOs), and also subscribers with sensitive loads.
• Content of the sent warning message: As much as possible, specific and identical messages should be used. IoT technology applied to a global blackout, as shown in Fig.3, provides an integrated hierarchical architecture of the telecommunications and information network to obtain fault information in real-time. As shown in Fig.3, IoT sub-technologies such as the Sensor Web Enablement Framework (SWE) and the IoT communication protocol, called MQTT (Message Queue Telemetry Transport), can achieve the delivery time of up to 15 seconds for an early warning system. The system examines time and spatial analysis and has a precise and adjustable structure that is compatible with the features of the geographical area [21-22].
The procedure of black-out occurrence in power systems

By analyzing the recent global blackouts worldwide, it is possible to suggest the process of cascading failures that lead to a blackout as depicted in Fig. 4.

The mechanism of blackout in power systems can be divided into two overall periods. In the first period, the occurred faults lay a foundation for the occurrence of cascading failures and incline the system toward insecure margins, which is an operation point, in which by the occurrence of an incident, the cascading failures may propagate within the network and finally end up to a blackout. The changes in this period occur gradually, and if there is a proper network monitoring platform and it can detect the high-risk scenarios and make the best operation-related decisions. Such preventive analyses can considerably mitigate the risk of cascading failures and vast blackouts [23].

In the second period, changes and events occur rapidly and uncontrollably, and it is no longer possible to prevent a blackout. These incidents are referred to as cascading failures. The system suffers from power fluctuations, overloaded equipment, and voltage violations, as a result of protection systems operation, which can exacerbate power fluctuations, overloaded equipment, and voltage issues, and eventually will be lead to islanding zones, voltage collapse, and instability issues, or frequency instability, leading to a blackout. A schematic view of the blackout process is pictured in Fig. 4.

A. First phase

The first phase can be introduced concisely as follows:

- The system state before blackout: In a normal operation period, the state parameters of the system are in acceptable ranges and no signs of blackout symptoms can be perceived. In this period, some factors increase the risk of blackout occurrence. These factors include high energy demand, heavy network loading over various equipment, congested lines, voltage disruptions, a high percentage of input power from neighboring regions as well as scheduled outages for requirements and maintenance.

- Incidents before the occurrence of triggering events and cascading failures: Before a blackout, the network is severely weakened by unplanned outages and the operation point is so close to insecurity margins, the network is severely compromised by unplanned events and contingencies. These weakening factors involve the outages of transmission lines, particularly highly congested branches, and the outage of power plants. The first event in this period may occur due to natural factors such as the collision of trees with transmission lines or human mistakes that cause the protective relays to trip the switching function.

- Triggering event: a triggering event occurs at a specific time in a blackout process. This incident separates two periods of events from each other.

* The first period in which multiple events and factors are indirectly involved in the weakening of the system before the occurrence of a blackout.
* The second period in which the series of events directly contributes to the occurrence of blackout. In fact, before the incident, the consecutive outages have not yet been accelerated, and there is a possibility of preventing blackout with appropriate corrective actions and measurements [24].

B. Second phase

An introduction to the second phase is presented as follows:

- Power flow fluctuations, overload of equipment, as well as voltage and frequency instability: In a blackout, the triggering event and the events that occur consecutively, cause power fluctuations, overloads, and voltage and frequency problems. The functioning of protective relays may be the reason why the next incidents occur (for instance, the line and power plant outages from the grid). In such a condition, low frequency and low voltage relays are highly probable to be tripped to try to improve conditions locally, while in a general point of view, the grid operation state is deteriorating toward a collapse.

- The performance of protection systems, transformers, and generators: The protection relays play a crucial role in the formation of blackouts (The effect of protection relays on the spread of events and blackouts will be investigated in the following sections). Their performance may be directly due to overload and voltage drop or may occur due to collision of the overloaded transmission lines with trees. The performance of protection relays and network elements may lead to more power flow fluctuations, voltage, and frequency problems, or disconnecting low voltage and low-frequency loads.

- The system islanding mode, frequency instability, and voltage collapse can occur in the final stages of the blackout process. Ultimately, the system blackout may occur, or after the islanding, on some islands, the generation-consumption balance has been established, and the purported section will continue to operate. For example, when the blackout occurred in North America and Canada, the network was in the final stages of the voltage collapse, and when the collapse occurred in Italy, a frequency reduction (frequency instability) led to the blackout.

- Blackout: The block out may be general and the whole system may suffer from blackout due to the frequency and voltage drop, or as mentioned, after the system transforms to islanding zones, some islands drop in blackout condition and others work by striking a balance between production and consumption [25].

For example, Fig. 5 demonstrates the sequence of events that have occurred in a blackout. The process of this blackout begins with the outage of a transmission line from the network due to a collision with a tree and continues with the outage of other lines due to overload.

![Figure 5. The process of power system blackout.](image)

IV. Fog computing architecture

This is how the Open Fog Consortium defines fog computing: Fog Computing is a system-oriented horizontal architecture that provides computation burden and storage capacity, smart controlability, and networking resources and services anywhere in the cloud supply chain of objects. The fog-computing layer introduced by Cisco extends the cloud space, as shown in Fig. 6, to the nearest place where IoT data is generated and processed [26].

![Figure 6. Position of fog relative to cloud space and its proximity to IoT objects](image)
This place is called the fog nodes. Any device with the ability of computing, storage and network communication can be a node. Such as industrial controllers, switches, routers, servers used in dispatching centers, substations, video surveillance cameras, etc. There are many different types of fog applications in smart grids. However, what they do in a general sense is uninterrupted monitoring and analysis of data from a network of connected and interconnected objects and the initiation of a post-analysis reaction. This paradigm enables Machine-to-Machine (M2M) or human-to-machine interactions (HMI) accessibility and possibility. Fog computing, also called edge computing, basically means that data can be processed on smart devices instead of being sent to the cloud for processing. This approach is a very attractive concept in the IoT architecture design because it allows real-time response to the input data and works with limited bandwidth. This strategy reduces costs and improves efficiency [27]. Fig. 7 shows the details of the network and the fog-computing layers.

Architecture plays a decisive role in determining the success of a system. Likewise, many efforts are being made by standard industry associations and scientific institutes to design a more efficient IoT architecture. The fog-based IoT architecture brings computing, networking, and storage services closer to the end nodes of an IoT-enabled network. This layer of computing is highly distributed and imposes additional services on end devices located in the perceptual layer [28].

<table>
<thead>
<tr>
<th>Component</th>
<th>Fog nodes close to IoT's devices</th>
<th>Fog complex nodes</th>
<th>Cloud space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response time</td>
<td>Milliseconds to smaller subsets</td>
<td>Seconds to minutes</td>
<td>Minutes, days, weeks</td>
</tr>
<tr>
<td>Time and storage of IoT's data</td>
<td>Short</td>
<td>Maybe hours, days, or weeks</td>
<td>Months or years</td>
</tr>
<tr>
<td>Covered area</td>
<td>Local: For example, a microgrid</td>
<td>Wide</td>
<td>Global</td>
</tr>
</tbody>
</table>

Fog computing is often used when data analysis and subsequent reactions are less urgent on a scale of less than a second or a very short period. Fog nodes closer to the edges of the network consume data output from IoT devices [29]. This software then sends different types of data to the appropriate place for analysis, as shown in Table 2. Ultimately, the adoption and the incorporation of fog computing leads to agile and in-depth insights into the business, and the organization's observability, higher service levels, and improved safety [30].

v. Function method of the proposed architecture

The proposed functional plan for the architecture of IoT is based on a fog-computing platform, shown in Fig. 9, and the mentioned instruction for its implementation is as follows:

- Layer 1 (sensor): Cascading failures are first detected by protection relays or by sensors in a wireless sensor network.
- * The boundary of the first and the second layer (communication): The data obtained from fault detection are sent to the center of prediction and monitoring of large blackouts using long-range wireless communication channels such as low-consumption wireless communication networks, satellites, cellular networks, etc.
- Layer 2 (middleware): The data received from communication channels are considered as input to node computing centers of the monitoring center. These data are quickly analyzed applying technologies such as artificial intelligence, expert system, decision system, and data mining system, and accordingly, parameters such as size, location, speed, severity, of a fault along with the subsequent system vulnerability are determined and immediately sent to the alert node in the same layer.
- The below-mentioned processes can be performed by the resident alert system in the monitoring center by using technologies and techniques such as intelligent agents, semantic web, etc.
  - Sending predefined commands for protection and operating systems and controlling of power switches (Machine-to-Machine connections), such as maneuvering power switches, to disconnect from the universal network and isolate the damaged area by the fault.
  - Alarming in dispatching centers and control stations of power plants, transmission, and distribution.
  - Sending a message with the theme of large-scale blackout warning, for, users, managers, operators of the system, and in general all the predetermined beneficiaries of the system.
  - Sending a full version with all the details of the recent large-scale blackout alert to cloud space in the third layer.
- The boundary of the second and third layers (communications): This interlayer is responsible for sending control commands and warning messages on a very static communication medium and long-range communication platforms, such as low-power wireless networks, satellites, and cellular networks.
- The third layer (application): This layer consists of two parts, the application section, and the cloud section.
  - Application section in real-time
    - All systems and services required to receive and replay universal alarms and blackout warning messages are pre-defined by the Ministry of Energy (MoE) and ISO.
All devices and controllers that can receive predetermined commands and control commands of the blackout center and can execute the appropriate response to the commands issued by the blackout center.

**B. Cloud Services section**

- Permanent storage of all instantaneous reports related to cascading failures and blackout for future use;
- Software services for cases such as data mining and analysis of recorded and existing records from the past, discovering knowledge in the field of operation and protection of the power system (reliability, stability, security, etc.).
- Prompt responding to requests from individuals and relevant organizations for management reports of outages, failures, blackouts, and system operation state.

It should be noted that among the basic and reference architectures in the field of IoT technology, the proposed architecture is designed based on a three-layer architecture presented by Cisco in 2015, in which for the first time, a fog-computing platform is close to the first layer is introduced for the early warning systems.

The analysis of the issues indicates that the IoT architecture based on fog-computing techniques has the potential to create and support the system of real-time response to faults and blackouts. Implementing this system will lead to reduced technical and economic damages and eliminate the security and social risks of blackouts. In addition, the implementation of this system will be a positive step towards the realization of integrated crisis management in the electricity industry.

**VI. Conclusion**

In this article, the process of blackouts and the corresponding methods of prediction and prevention are studied. Generally, by the occurrence of the initial incidence, the protection system trips and opens the power switches around the faulted point or zone. These initial events can cause severe load changes, consequently resulting in significant voltage volatilities and system frequency changes. Accordingly, predicting the probability of cascading failures, identifying faults in vulnerable power system components and overloaded lines, and examining bus voltage limits are all factors that can help to recognize damaged parts of the power system and make decisions to prevent propagating instability. Based on the targeted objectives defined in this paper, first, the early warning system, as well as its framework and process cycle, are introduced, and then the IoT architecture based on the fog-computing platform was investigated to cover the functional aspects of early warning systems before, during, and after cascading failures. The results of these studies led to the proposal of a three-layer architecture for the Internet of Things based on fog computing to implement the system of diagnosis, warning, and instant failure response, which are fully described. A general summary of large blackouts, investigated in this paper delineates that the IoT-based architecture based on a fog-computing scheme has a high potential to create and support a system for immediate fault detection, alert, and fast response to extensive blackouts. It can also be claimed that the three-layer IoT architecture proposed in this paper can be generalized to other areas of crisis management. The final result of this article indicates that nowadays, due to the presence of skilled IT experts in the field of operation and protection of power systems in Iran, as well as the existence of appropriate infrastructure, systems in the field of integration of crisis management processes can be designed and developed innovative technologies and initiatives such as IoT technology, low-consumption long-distance communication networks, artificial intelligence, big data analytics, etc., which are known as the most decisive cutting-edge and state-of-the-art drivers of the digital revolution in the present age.

![Diagram of Proposed Architecture](image9)

*Figure 9. Proposed architecture for large-scale blackout detection, alert, and response system according to IoT architecture based on computing fog*
REFERENCES


