Applications of Cloud Computing for Smart Grid: A Survey

Gokula Rani Vallabhu
CIISE. Concordia University
Montreal, Canada
40161606

Sai Chandra Sekhar Reddy Dwarampudi
CIISE. Concordia University
Montreal, Canada
40189233

Henisha Panchhiwala
CIISE. Concordia University
Montreal, Canada
40192678

***Abstract*—The concept of the "Smart Grid" will significantly change over the coming years to enable a more reliable, dependable, sustainable, efficient, and cheap system. Only the widespread application of information and communications technology will enable the integration and management of this complete system. To address these needs, we present a detailed analysis of several cloud computing applications for smart grid architecture in three areas: energy management, information management, and security. These topics examine the value of cloud computing applications and provide insight on potential future pathways for the growth of the smart grid. This paper focuses on the possible applications of cloud computing in smart grid systems. It also highlights many difficulties that the traditional smart grid (without cloud application) faces that can be resolved with the help of the cloud.**

***Keywords* — Smart grid, cloud computing, demand and response, energy management, information management, privacy, security**

I. Introduction

A combination of equipment is known as the electric power system, and it is in charge of producing, transmitting, and supplying electricity to final users. The world's energy consumption has been rising continuously during the majority of the 20th century, and this reality necessitates strategic planning to meet the demands of its expansion [5]. In addition, utilities are working to address issues including carbon emission reduction, demand response, and more efficient use of sustainable energy sources.

The idea of the "Smart Grid" (SG) emerged to solve these problems. With growing integration of renewable energy sources, the Smart Grid aims to be a more dependable, safe, affordable, efficient, and sustainable power system, enabling the final consumer to take a more active role in the energy market. Strong utilization of information and communications technologies facilities, as well as control and automation, is required to accomplish these aims. It is also crucial to note that the distribution systems act as a "bottleneck" in terms of SG because better consumer monitoring devices will be required (now performed primarily by electromechanical/standalone digital meters in underdeveloped nations) [5]. There are many customers per feeder, which is very worrying since there would be a tone of data that would need to be carried through the communication systems, creating a lot of traffic. In this regard, cloud computing has emerged as an innovative technology that has produced positive outcomes. Cloud computing is promoted for enabling dependable and on-demand access to various computing sources that can be swiftly created and released in a way that is cost-effective to the service providers. In this paper, we present a methodical overview of integrating cloud computing applications in smart grids from three perspectives: energy management, information management and security in the smart grid design

II. Cloud Applications For Energy Management

The energy management system can share or exchange energy among the many energy resources available, as well as economically supplying loads in a reliable, safe, and effective manner under any conditions necessary for the operation of the power grid.

Customers' energy needs change dynamically over time. The current power networks require an effective balancing of electricity supply and demand between consumers and utility suppliers. A dynamic energy system called the "smart grid" uses information technology, tools, and methods to increase grid efficiency. The stability of power technology and distribution networks is at risk due to the integration of highly volatile distributed generation sources including solar panels, wind power, electric vehicles, and energy storage devices. The major reason, however, may be an unbalanced relationship between the supply and demand for power. Too much or too little electricity generation or consumption can cause system disruption, major problems including voltage fluctuations, and in the worst situations, power outages. Energy management systems (EMS), such as building energy management (BEMS), demand side management (DSM), and home energy management (HEM), are included into the smart grid to meet these criteria. [4]. In addition, the Smart grid reduces the need for traditional fossil fuels in the production of power, allaying environmental worries about climate change and global warming. Increased energy efficiency and the use of renewable energy sources in both large- and small-scale centralized systems, such as micro- and nano-grids, are used to achieve this. Cloud computing, which employs an ad hoc, on-demand computing strategy, is an emerging solution to the aforementioned issues.

In this section, first, we use current methods for energy management without cloud apps in smart grid to handle various issues. After that, we go into how cloud computing can be used to tackle these issues. We finish this part by suggesting some potential future study areas on various facets of cloud applications for smart grid

A. Cloud – based energy management system

With a cloud-based energy management system (EMS), all data, software, and controls may be accessed from any computer over the Internet. While enterprises with various plants or buildings may utilize a cloud system, this system requires energy specialty configuration using these readings, which should be put on display within 48 hours. An EMS allows for the storing of maximum historical data with accuracy, which makes it possible to obtain readings less frequently. Understanding energy consumption trends is essential for making wise decisions. For managing massive amounts of data, cloud computing is helpful. Nowadays, with the integration of renewable energy sources into the smart grid, it is difficult to synchronize the operation of the production sources and the load, necessitating a major connection between the distributed storage and processing requirements.

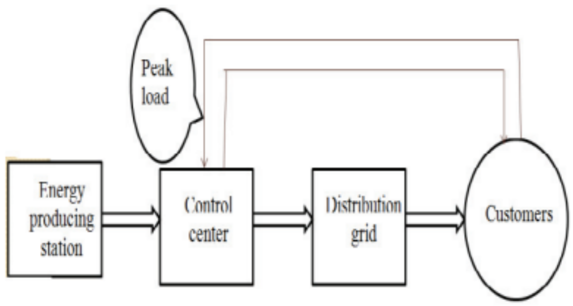

Fig 1: Block diagram of Internet of Energy (IOE) [2]

In this figure, energy-generating facilities provide electricity to consumers, and between them there are a control facility and a distribution system. Energy trends are visible at the control center; therefore, managing the power needs requires analysis of this data. The Internet of Things and renewable energy sources are combined in this IOE block diagram. It is feasible to manage the smart grid's energy usage with this approach. The control center is where consumer data is managed. Figure 1 demonstrates that the control center is situated between the energy-producing facility and the consumers, making it possible to keep an eye on how much electricity each user is using. Utilizing this technology, the supply side and consumer side of the electrical demand are managed.

The usage of cloud computing technology, commonly referred to as a cloud provider, allows for the management of applications while simultaneously lowering hardware costs. IT services and businesses greatly benefit from cloud computing.

B. Intelligent cloud-based Energy management system

Recently, the idea of machine-to-machine communication (M2M) has been acknowledged as a practical way to do away with human interaction, lower the communication costs of the system devices, and increase reliability, efficiency, and scalability. The M2M concept can then be seen as the foundation of the smart grid, supporting the development of more intelligent applications and the management of infrastructure. The authors of Byun et al introduce an intelligent cloud-based energy management system (ICEMS), which is illustrated in Figure 2 [3].

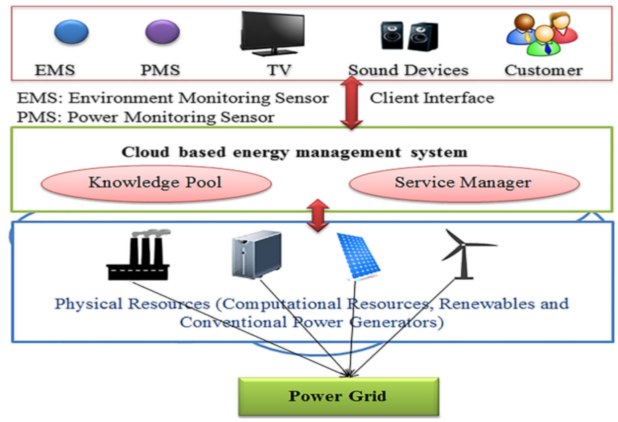

Fig 2: Energy management system using the cloud [3]

As it is seen, ICEMS is composed primarily of three different components: end users, an intelligent energy management system, and physical resources, such as computing power, storage, conventional power plants, and renewable energy sources. The last two components are compromised by the cloud platform. In this regard, the cloud level has four crucial characteristics, which are described below:

- By using dynamic energy management, renewable energy sources can be managed to provide consistent electricity.
- Enhancing energy efficiency through the use of the best possible energy source mix.
- Offering user-friendly energy management services to increase energy efficiency with user involvement.
- In order to improve energy efficiency, sensors are being deployed to monitor power usage, user devices and load profiles, and the environment in order to refresh the knowledge pool in the ICEMS.

C. Cloud – based demand and response

Demand and Response succeeds in changing the end consumers' consumption patterns

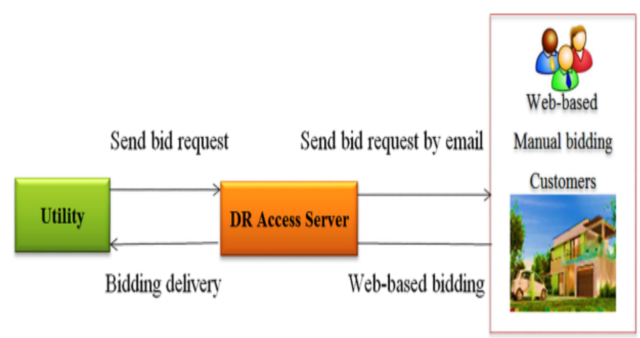

Fig 3: Conventional Demand and Response [3]

The limitations of traditional master-slave-based DR (Fig 3) in terms of scalability, security, and reliability make the transition to cloud participation easy:

- First, the standard DR architecture, which is suited

only for small-scale systems and does not support participation from large-scale consumers due to server, storage, and memory capacity restrictions, is the first factor that prevents it from meeting the smart grid's scalability needs.
- Second, due to their installation distance from the utility, customer-side equipment such as metres and energy management systems are vulnerable to cyber-attacks.
- Third, the shared DR architecture is vulnerable to a single point of failure from the perspective of reliability. Furthermore, the smart grid applications must operate quickly and efficiently, which is not entirely doable with the existing provisions.
- Lastly, the smart grid applications must operate quickly and efficiently, which is not totally feasible with the existing provisions.

A more effective game between the participants in DR situations, which can be fairly challenging with the most popular designs, results from real-time pricing communication. Then, utilities and customers go to cloud computing.

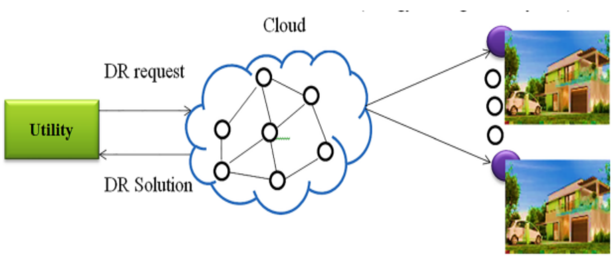

Fig 4: Cloud – based Demand and Response [3]

In the common architecture, utilities and customers communicate (exchange bid information) via email platforms or phone calls; in the cloud-based DR, cloud providers handle this communication (Figure 4). Then, the cloud computing offers more scalability, security, efficiency, and dependability. Customers benefit from quick response times, high-quality service, and bill discounts while utilities are freed from having to consider the aforementioned difficulties while controlling costs. Contrary to the typical approach, the participants in the CDR share information without being aware of one another's IP addresses.

In the DR strategy, consumers are given a DR client to connect to the DR servers, which then adjust the load in accordance with the customer contracts. DR clients are relocated to the cloud using cloud technology, where they can communicate directly with customers or indirectly through aggregators. The topic-group communication serves as the foundation for the discussed communication. The DR data are referred to in this method as cloud topics. The utilities' request for DR or end consumers' propensity to attend DR events could be the subjects of discussion. As a result, the CDR is more resistant to hackers [3].

D. Solution concept utilizing Cloud Applications:

For many years, researchers suggested several solutions approaches for demand response and micro-grid control.

The Deployment Method of a power dispatching automation system based on cloud computing was proposed by Ming Chen et al. [4] after an analysis of the necessity and viability of cloud computing technology in power dispatching. Cloud computing technology can be used to easily standardize power dispatching procedures, supply advanced features quickly, and significantly increase the stability of IT systems. It lowers administrative expenses and resolves the conflict in the energy sector between hierarchical administration and "integrated construction".

The idea of cloud dispatching, a type of general framework for an intelligent dispatching center based on cloud computing, was put forward by the ZHANG Liang [4]. The layered architecture for cloud computing includes Physical resource layers include physical hardware, platform resources, and application systems like SCADA, EMS, TMR, and WARMS. Virtual resource layers map different types of physical resources into virtual resources. Cloud service layers package virtual resources into services that are posted to the clouds. Cloud management layers offer users integrated management of cloud services. And cloud access layers are how users access cloud dispatching. It combines the resource requirements of the multiple dispatching centers, lowers the cost of system installation and extension, and enhances the overall dispatching business capability.

The use of dynamic pricing can also be used to address energy management. Peak demand and dynamic pricing were two smart grid-related challenges that were proposed by Xuan Li and Lo. [4] With the integration of the cloud, customer requests are scheduled and executed based on the priority, resources, and other relevant limitations. Meter reading messages are more frequent during peak hours than off-peak hours.

One of the best methods for lowering costs, optimizing resources, and managing servers is virtualization [4]. Micro-grids can be used to create cloud computing in a variety of ways. Global deployment of smart grid infrastructure is required. Scalable software platform is necessary for the quick integration and analysis of data that streams from several smart meters at once in order to balance the real-time demand and supply curves. According to Yang et al. [1], cloud systems are well adapted to host constantly running, computationally intensive applications and large amounts of data. The scalable resource requirements afforded by cloud apps can be used to create software architecture to support such dynamic and always-on applications.

Cloud platforms are crucial components in these systems due to the numerous benefits they provide, as listed below:
- Cloud technology responds flexibly to prevent the utility from making expensive capital investments during peak usage times.
- Flexibility in cloud technology allows the utility to avoid making costly capital investments during periods of high consumption.
- After conforming to the data privacy policies, some data can be shared with a third party by using cloud services to create intelligent apps that are specific to the requirements of the user.

One of the important technologies for real-time monitoring to make judgments at different times is the installation of specialized data abstraction for data streams generated from various components. On the other hand, such a real-time monitoring system does permit participation from outside vendors. Determining a successful privacy policy is therefore seen as a secure procedure that permits third-party providers to conduct real-time monitoring

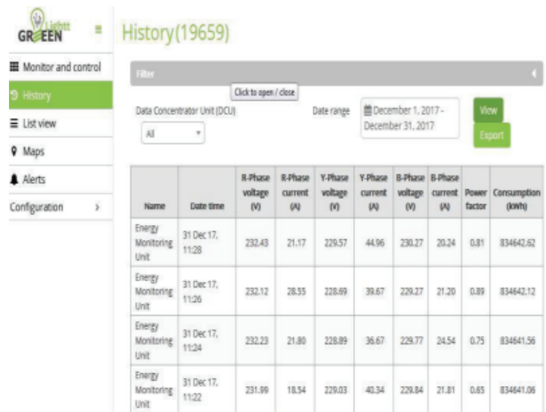

Fig 5: Snapshot of real-time data monitoring [2]

This fig. 5 shows statistics for the 16th of April's real-time monitoring of current, voltage, power factor, and energy usage. When the current demand figure is exceeded, this system sounds an alarm. It is feasible to monitor data online using this method for data analysis. When the MCB trips, this system also sends notifications. Utilizing cloud computing, this method is highly helpful for managing the energy of a smart grid [2].

Cloud Applications	Demand side management	Micro-grid management	Load shifting	Dynamic pricing
Demand Response [3]	Yes	Yes	Yes	Yes
Peak demand & dynamic pricing [1]	Yes	No	Yes	Yes
Real-time monitoring [2]	Yes	No	No	No
Dynamic Demand and response [1][3]	Yes	Yes	No	No

Fig 6: Comparison of Cloud Computing Applications for Energy Management [1]

E. Future opportunities for cloud-based energy management:

- Create cloud-based "software as a service" to address data privacy concerns in large-scale smart grid deployment.
- Establish a smart grid security system while utilising technologies for public cloud computing.
- Policies for privacy and security that is effective and efficient to accommodate the growing amount of data from smart metres.
- Enhance quality of service mechanisms in the smart grid by expanding the use of power cloud applications for non-technical issues.
- To stop information leakage in the smart grid, use the distributed verification protocol

III. Cloud Applications For Information Management

Several initiatives are proposed to reduce communication latency, with the goal of enabling real-time communication via cloud data management in smart grid. To achieve this aim of data management, a cloud data warehouse application in smart grid was proposed. The authors developed a cloud data warehouse model using extract transform load (ETL), data mining (DM), online analytical processing (OLAP), and business intelligence (BI) report technologies. [1]

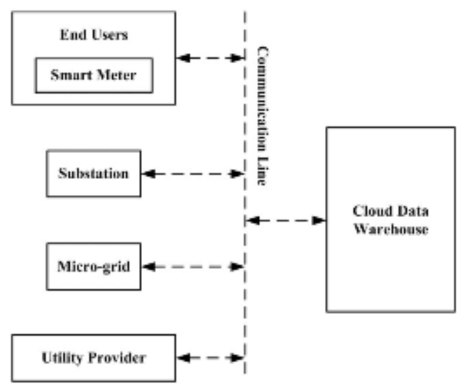

Fig 7: Schematic view of using cloud data-warehouse in smart grid communication

This cloud data warehouse architecture offers a variety of services for smart grid information management, including multidimensional data analysis and data mining. Users have varied standards for energy consumption in multidimensional data analysis. However, to provide services to all consumers, a software platform based on a cloud data warehouse must be built. Coordination methods between a smart grid and a cloud data warehouse must be addressed in the future [1].

Figure 7 displays a schematic picture of a smart grid cloud data warehouse, where the warehouse serves as data storage for all components such as smart meters, microgrids, utilities, and substations. A cost-cutting strategy employing cloud-based architecture to achieve easy and cost-effective information management for smart grid. Electric cars, such as plug-in electric vehicles (PHEV), can benefit from the introduction of cost-effective information exchange. PHEV owners may access real-time pricing and the smart grid's current condition and can charge and discharge their vehicles accordingly. The utility may also determine where most of the PHEVs are located and how much electricity is required using this way.

The major benefit of this net-AMI technology is that it is linked with the current BTS cellular service using cloud computing. The net-AMI does not support Ethernet protocols in such an environment. To enable such protocols while assuring that they can operate in the vicinity of radio-waves in smart grid contexts, a cloud-based unique protocol for cloud computing must be defined. A smart energy meter is an essential element of smart grid design since it allows for two-way communication. Large number of smart meters are placed at the distribution level. Cloud technology may be used to successfully extract large amounts of data from smart meters [1].

The smart grid using data cloud application enables real-time distributed data management and parallel information processing. Cloud computing is used as a Platform as a Service (PaaS) in such smart grid data cloud scenarios. Cost and data management are shared in the smart grid data cloud infrastructure. Because of the flexibility of cloud computing, information is more easily accessible from the data cloud. A dynamic pricing model based on the load on cloud data services can be put in place. In this case, the load on the data-cloud is greater during peak hours, and hence the real-time charge is higher.[1]

Cloud Applications	Smart Grid Features			
	Cost Optimization	Data Storage	Dynamic Pricing	PaaS/ SaaS/ Iaas
Cloud Data Warehouse	✗	✓	✗	SaaS, PaaS
Information management cloud ward	✓	✓	✓	IaaS, PaaS
Net-AMI infrastructure	✓	✓	✓	PaaS, SaaS, IaaS
Smart Meter data streams in cloud	✗	✓	✓	IaaS
Smart Grid data cloud	✓	✓	✓	PaaS
Dynamic Data center operations	✓	✓	✓	PaaS

Fig 8: Comparison of Cloud Computing Applications information management [1]

Cloud computing services are being used as dynamic data centers to store real-time information gathered from smart meters. In this case, cloud-based data centers serve as Internet data centers (IDC), which are accessible to customers via the Internet. The real-time pricing system is also addressed as a non-linear function based on the data center load. Table 1 compares cloud-based information management in the smart grid design, and various applications support different cloud services such as IaaS, PaaS, and SaaS.

A. Information Management in the smart grids and its challenges:

Smart Grid (SG) is an intelligent power system that revolutionizes power generation, distribution, and consumption by utilizing two-way communication and information technology, as well as computational intelligence. Its evolution is dependent on the use and integration of sophisticated information technologies, which convert the energy system from analogue to digital. According to the SG's vision, information is critical and must be managed efficiently and effectively [5]. Smart meters are also installed at the customer's end to interact with the service provider and share real-time data. Because of this design, enormous amounts of data are created on both the provider and user sides. Due to several restrictions, managing massive amounts of such data is difficult using typical data management methodologies (like processing unit, storage, and memory) [1].

B. Smart Grid System Architecture and Technical Challenges in the Information Management

As shown in fig 1, the architecture of the smart grid system is depended on the connectivity of three subsystems:

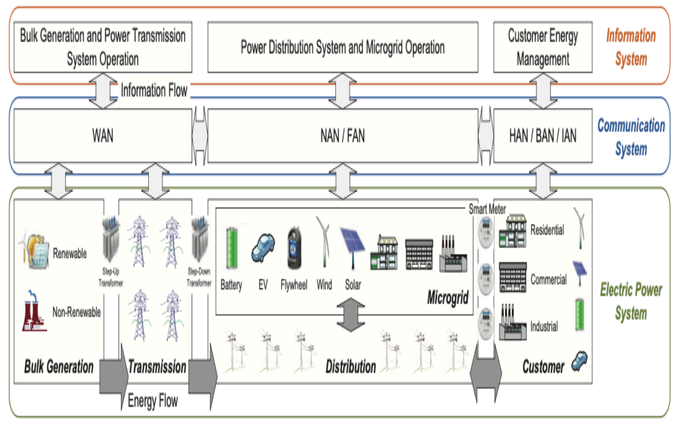

Fig 9: Smart grid System Architecture [6]

- Electricity generation system that generates, transmits, distributes, and consumes electricity.
- Communication system that establishes connectivity links for data exchange among various systems.
- Information system that gathers and analyses data for operation and management decisions of power system. [6]

In compared to traditional electric power networks, the smart grid incorporates more renewable-energy-based distributed generation (DG) units and energy storage devices (including EVs). As a result, conventional electricity customers are increasingly being turned into electricity "prosumers," who may not only consume but also create and supply energy into the power system. As a result, the traditional assumption of unidirectional electricity transmission (from centralised generators to electricity users) is no longer viable. As indicated in Fig. 1, bidirectional energy flows must be created between electricity users and power distribution networks.[6]

In the smart grid, three types of communication networks may be implemented. A wide area network (WAN) allows bulk generators and transmission facilities to communicate with one another for broad-area situational awareness. A field area network (FAN) enables communication between substations and field electrical equipment used in power distribution and microgrid operation. Home area networks (HAN), business area networks (BAN), and industrial area networks (IAN) can be implemented within residential, commercial, and industrial facilities, respectively.[6] The information system can make optimum judgments on electric power systems based on information obtained through the communication system. Even though fundamental information management features are currently in existence, implementing an advanced information management system in the context of smart grid is technically challenging due to the following challenges:

- The random nature of renewable energy resources results in considerable variations in power supply.
- The buffering impact of energy storage devices not only introduces extra state variables into power system operation. Efficient management techniques for energy storage devices with minimal computing complexity should be developed. [6]
- Customer behaviour patterns are more dynamic in the presence of DSM than in the traditional energy grid, resulting in substantial changes in load demand. Different clients can work together to minimise their overall energy expenditures.
- EV drivers might choose alternative charging locations in reaction to energy pricing, resulting in substantial changes in charging demand and poor prediction accuracy

C. *Requirement of Cloud based Applications for Information Management*

Cloud computing in information management is one of the important trends in building a smart grid. Cloud computing is built on large data centers with massive compute and storage capacity that are maintained by cloud providers that supply computing and storage services as utilities. [5]

- First, cloud providers' highly scalable computing and storage capabilities are perfectly suited to the SG's information processing needs.
- Second, the level of information from the different components in the SG can be easily integrated in the SG by leveraging cloud information sharing.
- Third, the SG's sophistication may result in a highly complicated information management system. Realizing such complex information systems may be extremely costly or perhaps impossible for typical power companies. As a result, adopting the cloud might be a more cost-effective and better storage alternative.
- Fourth, distributed energy generation removes barriers for new players to enter i.e., small players can easily generate power without worrying about building a data centre to process their data which ultimately creates a new SG ecosystem. [5]

Thus, using a cloud-based information management system can help in overcoming such disadvantages

D. *Model of Cloud Based information management in Smart Grid*

A prototype of cloud service-based smart grid information management depicts in figure 10, is made up of the SG domain and the CC domain. The SG domain is made of seven sub-domains while CC domain is built of three sub-domains. In the following sections, we will discuss about cloud computing domain and discuss a model for enforcing protection policy [7].

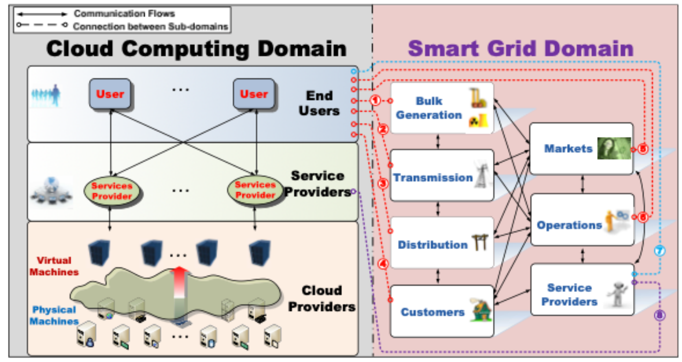

Fig 10: Model of Cloud Based Smart Grid Information Management [7]

The Cloud Computing domain consists of three subsections Cloud providers, service providers, and end users.

- Cloud Providers: They are the owner of the cloud infrastructure who is responsible maintaining the virtual servers and cloud services like storing the data, managing it and user applications.
- Service Providers: These are leases resources in the Cloud environment who offers applications and services that will be used by end users.
- End User: An end user generates requests for the Cloud to process and utilises the services offered. [7]

We primarily use CC in the model to support in information management tasks in the SG, such as storage, integration, validation, analysis, and optimization of various data and information in the SG domain. These duties can be outsourced and delivered as pay-as-you-go and on-demand services via the CC domain. The actors are primarily concerned with gathering and abstracting information service requirements from the SG, which oversees the development, deployment, maintenance, optimization, and upgrade of such services.[7]

The services or applications needed by the players in the SG domain may already exist, such as vast volume of information storage service. If such services or apps do not exist, the CC service providers may need to create and deliver these new services. The SG service providers may work as end users or even CC service providers. In the CC domain, SG service providers act as end users. However, SG service providers may also work as CC service providers on occasion. The relating applications and services are designed by SG service providers using the Cloud architecture. As the number of new services supported in the CC domain grows, end users may have more difficulty locating the most appropriate one that meets their needs. Moreover, SG service providers have a better knowledge of the electric power industry, they are helpful to end users while acting as service brokers.[7]

E. Smart Frame

The smart frame architecture is shown in figure 11. In this architecture, a smart grid can be divided into several regions which are managed by a cloud computing center that can be setup from either a public cloud or a private cloud. The role of a regional cloud computing center is to manage smart systems in the region as well as to provide an initial computation for data gained from these devices. Besides regional cloud computing centers, there is a special cloud computing center at the top level, which oversees trying to manage and handling data for the whole grid.[8]

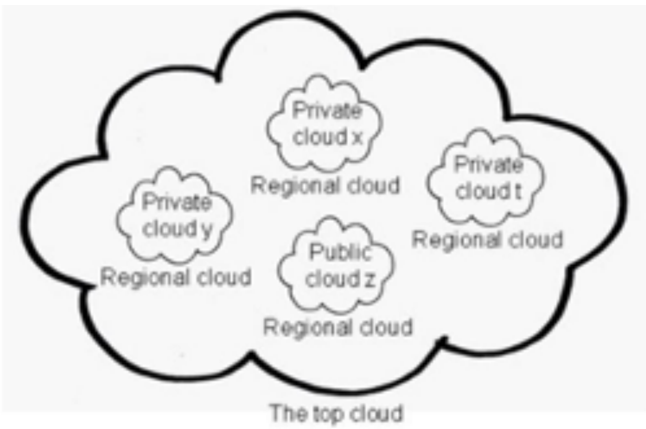

Fig 11: Smart Frame Architecture [8]

The following cloud computing services could be deployed in each of these cloud computing centers:

- Infrastructure-as-a-service (IaaS) serves as the backbone of the system. It aids in the provision of on-demand resources for all apps and services implemented in the system.
- Software-as-a-service (SaaS) is a service in which all the smart grid services will be deployed at the top of the system.[8]
- Platform-as-a-service (PaaS) delivers tools and frameworks to construct cloud computing software and services. Salesforce is a classic PaaS example.
- Data-as-a-service (DaaS) might be installed to deliver relevant information for statistical purpose which are utilized for optimization reasons for not only electricity customers but also power providers at different levels [8]

F. Future Research and Challenges

The hybrid design of a smart grid permits vast quantity of data that are created form smart meters, and, consequently, cloud solutions are beneficial for handling this data. There are some challenges in smart grid, while implementing the cloud solutions as follows

- Integration of public cloud with the private cloud is possible but security and privacy are two of the essential challenges, when permitting information interchange between them.
- For cost-effective information systems in the smart grid, an adequate mobility strategy for the agent is essential. Otherwise, it will be more costly rather than less affordable.
- Smart components cannot reduce their latency by altering their course. As a result, improving the delay caused by smart meters utilizing cloud computing apps is a difficult issue.
- Cloud computing can help you recover from network outages. Failures in one of the protocols used for communication might impact the entire system.
- The basic concept of smart grid is decentralized electricity supply with the existing centralized infrastructure which demand ongoing active engagement from the consumers which cannot be accurately evaluated.

IV. Cloud Applications For Security in Smart Grid

A smart grid may be thought of as a cyber-physical system that links actual electrical systems with digital infrastructure and incorporates the Internet. Consumer appliances can connect with this service, which also acts as the foundation for service providers to take in material and manage operations. It is quite difficult to stop cyberattacks on the smart grid with the availability of internet connectivity that might perhaps interrupt the power supply [1].

Consumer power theft is one of the crucial challenges. This can be accomplished by altering real-time information via accessing a communication channel or by hacking a smart meter to manipulate the reported power use. Additionally, one of the biggest security risks with the smart grid is data tampering. To solve these problems, a safe and dependable smart grid design must be implemented. On the consumer side, transmission side, and generation side, security can be incorporated [1].

The following are the key feature issues with smart grids:

- It is challenging to secure track business system interactions due to the grid.
- The architecture of the smart grid is more complicated than that of the conventional electrical system. The use of wireless communication, smart meters, and smart sensor networks adds to the complexity of the information security system.
- The distribution of the network to the end-user systems occurs with the installation of millions of smart meters. Therefore, it is necessary to improve the end-user protection capability.
- The stability of the smart grid apps was impacted by the denial-of-service (DoS) attack.
- The privacy of the users is impacted by the fact that utilities and third parties have access to both private information and user data.

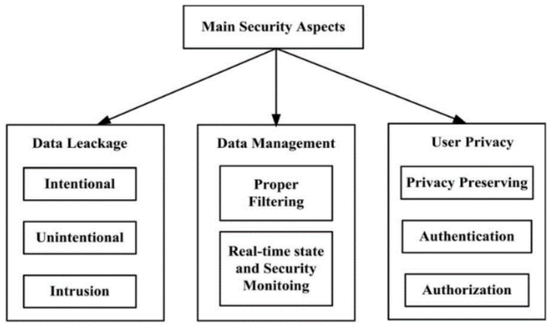

Fig 12: Security Concerns with Smart Grid [1]

The primary security concerns with the Smart Grid Architecture are displayed in Fig. 12

1. Data leakage: Both intentional and unintentional data outages are possible. Unintentional data leaking can occur when there is a cyber-physical attack, according to a third party. Even data outage, which is referred to as purposeful data leaking, may occur with the assistance of a user for her facility.
2. Data management: One of the main issues is deciding which data should be preserved and which should be destroyed. Real-time status monitoring needs an appropriate data handling method. Data may be managed correctly by using the right filtering technique.
3. Privacy: One of the key concerns with smart grid technology is protecting privacy. Users' private information may be given to the utility and other suppliers due to a lack of privacy policies. For protecting users' privacy, an appropriate authentication and authorization mechanism must be created [1].

The three main players in the Smart Grid ecosystem are users, utilities, and third-party service providers, each of whom has a unique viewpoint on the need for privacy and security. Each has a unique viewpoint on the privacy and security requirements. Here, we analyze the interactions between these stakeholders and the Smart Grid software architecture running on Clouds and point out security and privacy issues that result from those interactions. Figure 13 provides a summary of these [9].

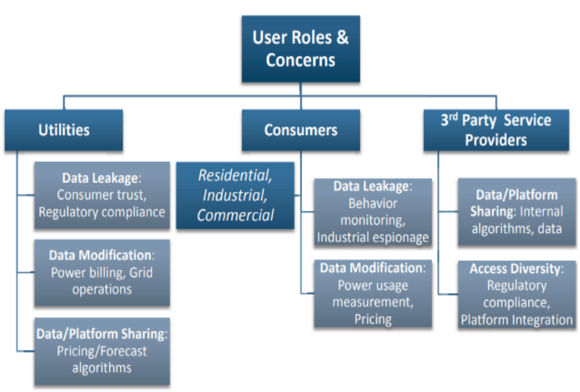

Fig 13: User roles and their security concerns in a Smart Grid ecosystem. [9]

A. *Smart Grid Utilities*

The Smart Grid ecosystem depends on utilities, and possess a range of obligations, including ensuring reliable grid operations, power generation, transmission, and distribution, maintaining customer satisfaction, and complying with various regulatory norms. The utilities store and process massive amounts of data obtained from Smart meters, appliances, and sensors installed throughout the Smart Grid using the Cloud infrastructure [9].

Since the data may be stored and processed in a distributed manner across geographic boundaries, this raises concerns about regulatory compliance. Additionally, it widens the attack surface that can be used to disrupt grid operations, creates concerns regarding data leakage during data transit and sharing that can jeopardize consumer trust and exposes to the cloud provider various forecasting and pricing techniques used by the utilities. The utilities may also provide an infrastructure for third party services to execute their apps in the Cloud and access consumer and other data available in the Cloud. This further adds to the security and privacy concerns such as unauthorized access to the Cloud resources [9].

B. *Consumers*

Residential, commercial, and industrial consumers all use electricity. When notified of real-time pricing or other incentives by the utility, residential consumers, such as those who live in single or multi-family residential units, may grant utilities limited access to directly control their appliances. Industrial consumers include large manufacturing facilities, which typically have high power needs and are willing to pay more for power quality guarantees than residential consumers. Commercial customers encompass corporations, malls, schools and universities, restaurants, shops and so on [9].

Smart meters installed at the consumers' end interact with various smart appliances within the home and building area network (HAN and BAN) to collect data on power consumption and send control signals to these appliances and equipment inside the facility. These networks have software logic that can optimize energy use in accordance with user preferences and signals from the utility's demand response system. However, consumer error in network configuration could make these systems vulnerable to attacks. As a result, hackers may break into HANs and produce scam usage data or control signals, resulting in data leakage and data modification attacks [9].

C. *Third Party Service Providers*

Smart Grid ecosystem where, in addition to the main use case of optimized demand response, several other applications will be created and put into use by outside providers offering a variety of value-added services to the consumers. Along with the primary application of optimized demand response, other applications will be created and implemented by third-party providers as part of a Smart Grid ecosystem, providing consumers with a variety of value-added services [9].

However, legal restrictions may prevent Smart Grid data from flowing out of the utility infrastructure and hence require the 3rd parties' providers to implement their services within the sandboxed environment supplied by the utility in the Cloud. This raises security and privacy concerns for the application providers. For example, it might possibly reveal numerous secret algorithms as well as intellectual property containing data from private sources utilized by the third party to deliver different services to the user. The integration of internal infrastructure, including legacy security and privacy software, with the utility Cloud infrastructure presents yet another significant challenge. This makes demonstrating regulatory compliance difficult because the required features will be distributed across private and utility public infrastructure [9].

The present adoption of cloud computing is also accompanied with some problems opposite to the objective of utilizing it on smart grid systems since smart grid utilities still have negative opinions about cloud computing's authenticity. Therefore, while developing cloud computing for smart grid systems, these problems must be carefully considered and examined. There may be challenges ahead regarding inefficiencies for smart grid. key challenges of deploying cloud computing for Smart grid applications may be described as follows [10]

- *Location of data:* Cloud servers are put in any area, therefore location of these servers that store and run smart grid apps are not known by the business enterprise. This is extremely critical problem to meet the requirements of data management in smart grid. Therefore, specifying the data location by Cloud Service Providers (CSPs) has a key role for the security of Smart grid applications

- *Mixing of data:* Cloud computing provides a model to access the apps through a location independent resource pool. There are numerous multi-user apps in Cloud Service Providers but, security and scalability of them is an outstanding concern for organizations. Therefore, specific security measures such as data encryption algorithms must be implemented on Cloud Service Providers for reliability and confidentiality in Smart grid applications

- *Inefficient cloud security policy*: Some Cloud Service Providers implement lesser security policies than others. These discrepancies may be exclusive to utilities, so they may generate problems amongst Smart Grid utilities. Utilities can tackle this challenge by putting service level agreements into existence between each other's to offer appropriate security levels for Smart Grid applications

- *Term of agreement:* When the service level agreement expires, Smart Grid utilities may be required to pay enormous fees to Cloud Service Providers for the requested data if the contract agreement contains commercial papers that contain data kept in the Cloud.

- *Dependence of Cloud service provider's Application Programming Interfaces (APIs):* Cloud service providers implement many applications in cloud computing, and these apps are all compatible with utility-specific APIs. As a result, moving smart grid services from one cloud service provider to another in cloud computing becomes challenging and takes longer.

- *Compatibility:* Cloud Computing does not fulfil with audit standards. This is the most important problem that Cloud Computing must solve to comply with smart grid auditing criteria. However, because of the location of the data, ineffective security measures, etc., cloud computing faces several difficulties. Therefore, it is difficult for Cloud Computing to become comply with auditing criteria including privacy laws.

- *Redundant Data Management and Disaster Recover:* As Cloud Computing sends data to various servers in different geographical locations, Smart Grid utilities are most concerned about disaster recovery. Therefore, adequate dependability cannot be offered by Cloud Computing for Smart Grid applications when data in a particular time is not defined. In the existing scenario, Smart Grid utilities know the location of their data and access it eventually when a disaster recovery arises. However, under the cloud computing system, cloud service providers have the option to outsource benefits, services, and recovery procedures to third parties. This creates a challenging position when the primary cloud service providers do not keep the data.

The present information protection systems for electric power are weak in managing the continually changing and rising nature of security threats. To overcome these challenges in the smart grid development, researchers proposed many security approaches in terms of cloud computing applications.

1. *Anti-virus System on Cloud Security:* The client is no longer required in the anti-virus system on cloud security to maintain the virus features. The Internet will be used to store all data. The end users of the company connect to the Internet and communicate with a cloud server. When a virus or unusual activity is discovered, all data are automatically sent to the cloud's server group for analysis and processing. The Anti-virus system on cloud security will then produce a risk management opinion and distribute it to all the company's clients. Clients can automatically destroy viruses by blocking it. The network perimeter security both inside and outside the firm is considerably secured, and the virus killing accuracy is also improved [11].
2. *Spam Mails Filtering based on Cloud Security:* The cloud security-based spam mail filtering creates a robust analysis and computing platform. The platform dynamically connects to the resources it needs, gathers, and continuously tracks global mail characteristics, trends, and behaviors. Unexpected e-mail network attacks are quickly identified, response times to mail threat outbreaks are shortened, and users are given access to the greatest real-time upgrades and security measures to lessen the likelihood of threat intrusion. Spam emails were blocked using spam filtering based on cloud security, sender reputation, distributed honeypots,

and threat perception. The sender's reputation score is determined using cloud computing's parallel and distributed computing. Then, network security threats that spread like zombies are stopped from entering the network by dynamically assessing data on sending behavior, activity range, and history records of mail. Distributed Honey pot technology is frequently utilized as a spam capture device. A set number of distributed honey pots are placed in the information internal and external network within the current district and zone environment of the company's information network to achieve collection of malicious email of internal and external network [11].

Using distributed honey pots on cloud computing, perceived threat technology can quickly identify unusual mail activity. Following a quick study of cloud computing, the relevant preventive measures based on cloud security are sent to the company's anti-spam processing center for automatic verification. To stop mail threats in real-time, the business updates its anti-spam signature database through pressure and judgement testing of a vast number of samples [11].

3. *Threat Detection based on Cloud Security:* Detecting security risks within the corporate network is the initial stage of the threat detection system based on cloud security. Second, employing association analysis, threat tracking, threat analysis, identifying malicious behavior, locating the threat source, and using cloud security technology architecture. Utilize cloud security to its fullest to discover the most recent security danger and to receive thorough and prompt defensive support via the cloud security center. Numerous internal hazards are avoided by analyzing and treating the three stages [11].

The literature review of various other researchers is descried as follows:
Information security and protection for electric power, a cloud security-based solution is presented by Yanliang al. The writers divided cloud security into two categories. client and server components. Clients mostly gather data and act in accordance with the server's replies. The server, however, makes use of the cloud computing platform to put the distributed storage into practice, serving as a capable decision-maker. The outcomes are then communicated via the Internet to the clients.[11]

Different security and privacy concerns in the smart grid software architecture operating on various cloud environments were examined by Simmhan et al. [9]. Customers of public clouds receive services that are powered by the same hardware. The data of several organizations is separated in this form of cloud via a cloud fabric. Public clouds may appear effective, but they lack security and dependability due to potential cyberattacks. They are not appropriate for Smart Grid applications because of this. Private cloud systems are well suited for scaling out and processing millions of user data, therefore smart grid applications employ them for monitoring and transmitting consumer data. Since hybrid clouds enjoy the benefits of both public and private clouds and have a stable workload, they can be a preferable cloud type for smart grid systems. Hybrid clouds collaborate with private clouds to provide reliability. To improve performance, it shifts to operation with public clouds during periods of high workload. As a result, a smart grid may occasionally choose hybrid clouds to satisfy customer demands for high performance or high security.
To ensure the security of data storage in cloud computing, distributed verification protocol (DVP) was proposed by Ugale et al. The benefits of using cloud computing in this way were highlighted by the authors in order to lower user costs for the smart grid architecture. The DVP protocol's implementation, according to Ugale et al., is suited for supporting data storage and power management systems for smart grids.

Cloud Applications for smart grid security Approaches	Smart Grid Security Features		
	Cyber-Security	Data Security & Privacy	Threat Detection
Software platform for server and client's security [4]	✓	✗	✓
Software architecture for security and privacy [2]	✓	✓	✓
Cloud Computing Applications for Smart Grid [1]	✓	✗	✗

Fig 14: Comparison of Cloud Computing Applications for Smart Grid Security approaches

D. *Future Research and Challenges*

- Third parties are welcome to join the real-time monitoring systems in the smart grid and applications for cloud computing are expected to offer sufficient security to protect user data privacy. However, it is currently unclear from the state-of-the-art technology how this security may be offered while permitting external participation in the systems. Hence, it is necessary to concentrate on providing cloud security to prevent outages while allowing diverse vendors to control and monitor the customers' equipment.
- Different pieces of equipment must work effectively together in a smart grid architecture. Therefore, we must implement a coordinated fault protection system in the smart grid with the use of cloud-based infrastructure.
- Service providers should adopt an appropriate strategy to manage microgrids in a proactive and adaptive manner using a cloud-based state estimate method to deliver dependable energy services to end customers.
- Applications for cloud computing should be able to identify deliberate data leaks in the smart grid.

However, unintended data leaking is also possible. Therefore, limiting accidental data leakage when integrating cloud computing applications in the smart grid is a research challenge [13]

V. Individual Section

My contribution to the project is to implement cloud applications in the information management field of smart grid. From the available three fields energy, information, and security, I have chosen the information management since every component communicate through this layer which is important for the functionality of the smart grid. To progress, I've have referred various research papers, publications, and blogs in the process of developing the report. I have identified the key challenges for information management in smart grids and the possible applications that can be developed using the cloud. I identified the concepts like smart frame [8], cloud based smart grid information management system [7] and the applications like Information management cloud ward, net-AMI infrastructure, smart meter data streams in cloud, smart grid data cloud, dynamic data center operations and cloud data warehouse [5] [6] could solve the existing problems in the smart grid. I also discussed the future research challenges in implementing the cloud solutions. The following are the research papers that I have referred for my topic:

[1] Cloud Computing Applications for Smart Grid: A Survey
[5] Evolving Smart Grid Information Management Cloudward: A Cloud Optimization Perspective. Smart Grid
[6] Stochastic Information Management in Smart Grid
[7] Managing smart grid information in the cloud
[8] A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid

We are a group of three people worked on the project. Right from the beginning me and my teammates were interested in cloud computing technology. Through the class we were able to identify the challenges the smart grids were facing and by integrating them we wanted to develop the solutions that the smart grids were facing using cloud. We focused on three main fields energy management, information management and security of the smart grids, we shared the work equally by each teammate working possible solutions on each field. We have frequent team meetings and support each other from the gathering of the contents to the development final report and presentation. As the work is equally shared, I hope all my teammates will get the same grade.

VI. Conclusion

Smart grids are made up of a vast network of parts that produce a lot of data. High end technology is needed to process, analyses, and store this data, and in the modern world, that technology is the cloud. The cloud can quickly handle massive volumes of data and store it remotely where adequate failover strategies are used. This paper provides a summary of the activities that have been done to integrate cloud computing with the smart grid to create an effective, dependable, and secure method of power distribution. In our discussion, we covered the usage of cloud applications in smart grids for information management, energy management, and smart grid security. We reviewed numerous upcoming tasks required for the construction of a cloud-based smart grid while also identifying some critical technological difficulties. Even if establishing cloud apps has certain difficulties, the advantages outweigh the difficulties. As a result, it is believed that integrating cloud computing into smart grid would help to advance the design of the smart grid in terms of factors like data management, power management, and security.

References

[1] S. Bera, S. Misra and J. J. P. C. Rodrigues, "Cloud Computing Applications for Smart Grid: A Survey," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, pp. 1477-1494, 1 May 2015, doi: 10.1109/TPDS.2014.2321378.

[2] M. Hans, P. Phad, V. Jogi and P. Udayakumar, "Energy Management of Smart Grid using Cloud Computing," 2018 International Conference on Information , Communication, Engineering and Technology (ICICET), 2018, pp. 1-4, doi: 10.1109/ICICET.2018.8533692.

[3] "A survey on cloud computing in Energy Management ... - wiley online library." [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/2050-7038.12094.

[4] "Cloud computing for energy management in smart grid - iopscience." [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/121/1/012010. [Accessed: 02-Dec-2022].

[5] Fang, Xi & Yang, Dejun & Xue, Guoliang. (2013). Evolving Smart Grid Information Management Cloudward: A Cloud Optimization Perspective. Smart Grid, IEEE Transactions on. 4. 111-119. 10.1109/TSG.2012.2230198.

[6] H. Liang, A. K. Tamang, W. Zhuang and X. S. Shen, "Stochastic Information Management in Smart Grid," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1746-1770, Third Quarter 2014, doi: 10.1109/SURV.2014.020614.00115.

[7] Xi, Fang., Satyajayant, Misra., Guoliang, Xue., Dejun, Yang. "Managing smart grid information in the cloud: opportunities, model, and applications." IEEE Network, 26 (2012).:32-38. doi: 10.1109/MNET.2012.6246750

[8] Devadharshini L, Nivetha R, 0, A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Confcall – 2018 (Volume 06 – Issue 14).

[9] Y. Simmhan, A. G. Kumbhare, B. Cao and V. Prasanna, "An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds," 2011 IEEE 4th International Conference on Cloud Computing, 2011, pp. 582-589, doi: 10.1109/CLOUD.2011.107.

[10] Melike Yigit, V. Cagri Gungor, Selcuk Baktir, Cloud Computing for Smart Grid applications, Computer Networks, Volume 70,2014,Pages 312-329,ISSN 13891286,https://doi.org/10.1016/j.comnet.2014.06.007.

[11] Y. Wang, S. Deng, W. -M. Lin, T. Zhang and Y. Yu, "Research of electric power information security protection on cloud security," 2010 International Conference on Power System Technology, 2010, pp. 1-6, doi: 10.1109/POWERCON.2010.5666728.

[12] Jeovane V. de Sousa, Denis V. Coury & Ricardo A. S. Fernandes (2018) A Survey on Cloud Computing Applications in Smart Distribution Systems, Electric Power Components and Systems, 46:14-15, 1554-1569, DOI: 10.1080/15325008.2018.1509156

[13] B. Chen and X. Yu, "Research on the Application and Security of Cloud Computing in Smart Power Grids," 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 2019, pp. 784-7842, doi: 10.1109/ICMCCE48743.2019.00180.

However, unintended data leaking is also possible. Therefore, limiting accidental data leakage when integrating cloud computing applications in the smart grid is a research challenge [13]

V. Individual Section

My contribution to the project is to implement cloud applications in the information management field of smart grid. From the available three fields energy, information, and security, I have chosen the information management since every component communicate through this layer which is important for the functionality of the smart grid. To progress, I've have referred various research papers, publications, and blogs in the process of developing the report. I have identified the key challenges for information management in smart grids and the possible applications that can be developed using the cloud. I identified the concepts like smart frame [8], cloud based smart grid information management system [7] and the applications like Information management cloud ward, net-AMI infrastructure, smart meter data streams in cloud, smart grid data cloud, dynamic data center operations and cloud data warehouse [5] [6] could solve the existing problems in the smart grid. I also discussed the future research challenges in implementing the cloud solutions. The following are the research papers that I have referred for my topic:

[1] Cloud Computing Applications for Smart Grid: A Survey
[5] Evolving Smart Grid Information Management Cloudward: A Cloud Optimization Perspective. Smart Grid
[6] Stochastic Information Management in Smart Grid
[7] Managing smart grid information in the cloud
[8] A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid

We are a group of three people worked on the project. Right from the beginning me and my teammates were interested in cloud computing technology. Through the class we were able to identify the challenges the smart grids were facing and by integrating them we wanted to develop the solutions that the smart grids were facing using cloud. We focused on three main fields energy management, information management and security of the smart grids, we shared the work equally by each teammate working possible solutions on each field. We have frequent team meetings and support each other from the gathering of the contents to the development final report and presentation. As the work is equally shared, I hope all my teammates will get the same grade.

VI. Conclusion

Smart grids are made up of a vast network of parts that produce a lot of data. High end technology is needed to process, analyses, and store this data, and in the modern world, that technology is the cloud. The cloud can quickly handle massive volumes of data and store it remotely where adequate failover strategies are used. This paper provides a summary of the activities that have been done to integrate cloud computing with the smart grid to create an effective, dependable, and secure method of power distribution. In our discussion, we covered the usage of cloud applications in smart grids for information management, energy management, and smart grid security. We reviewed numerous upcoming tasks required for the construction of a cloud-based smart grid while also identifying some critical technological difficulties. Even if establishing cloud apps has certain difficulties, the advantages outweigh the difficulties. As a result, it is believed that integrating cloud computing into smart grid would help to advance the design of the smart grid in terms of factors like data management, power management, and security.

References

[1] S. Bera, S. Misra and J. J. P. C. Rodrigues, "Cloud Computing Applications for Smart Grid: A Survey," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, pp. 1477-1494, 1 May 2015, doi: 10.1109/TPDS.2014.2321378.

[2] M. Hans, P. Phad, V. Jogi and P. Udayakumar, "Energy Management of Smart Grid using Cloud Computing," 2018 International Conference on Information , Communication, Engineering and Technology (ICICET), 2018, pp. 1-4, doi: 10.1109/ICICET.2018.8533692.

[3] "A survey on cloud computing in Energy Management ... - wiley online library." [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/2050-7038.12094.

[4] "Cloud computing for energy management in smart grid - iopscience." [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/121/1/012010. [Accessed: 02-Dec-2022].

[5] Fang, Xi & Yang, Dejun & Xue, Guoliang. (2013). Evolving Smart Grid Information Management Cloudward: A Cloud Optimization Perspective. Smart Grid, IEEE Transactions on. 4. 111-119. 10.1109/TSG.2012.2230198.

[6] H. Liang, A. K. Tamang, W. Zhuang and X. S. Shen, "Stochastic Information Management in Smart Grid," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1746-1770, Third Quarter 2014, doi: 10.1109/SURV.2014.020614.00115.

[7] Xi, Fang., Satyajayant, Misra., Guoliang, Xue., Dejun, Yang. "Managing smart grid information in the cloud: opportunities, model, and applications." IEEE Network, 26 (2012).:32-38. doi: 10.1109/MNET.2012.6246750

[8] Devadharshini L, Nivetha R, 0, A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Confcall – 2018 (Volume 06 – Issue 14).

[9] Y. Simmhan, A. G. Kumbhare, B. Cao and V. Prasanna, "An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds," 2011 IEEE 4th International Conference on Cloud Computing, 2011, pp. 582-589, doi: 10.1109/CLOUD.2011.107.

[10] Melike Yigit, V. Cagri Gungor, Selcuk Baktir, Cloud Computing for Smart Grid applications, Computer Networks, Volume 70,2014,Pages 312-329,ISSN 13891286,https://doi.org/10.1016/j.comnet.2014.06.007.

[11] Y. Wang, S. Deng, W. -M. Lin, T. Zhang and Y. Yu, "Research of electric power information security protection on cloud security," 2010 International Conference on Power System Technology, 2010, pp. 1-6, doi: 10.1109/POWERCON.2010.5666728.

[12] Jeovane V. de Sousa, Denis V. Coury & Ricardo A. S. Fernandes (2018) A Survey on Cloud Computing Applications in Smart Distribution Systems, Electric Power Components and Systems, 46:14-15, 1554-1569, DOI: 10.1080/15325008.2018.1509156

[13] B. Chen and X. Yu, "Research on the Application and Security of Cloud Computing in Smart Power Grids," 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 2019, pp. 784-7842, doi: 10.1109/ICMCCE48743.2019.00180.