IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

Vol. 9, Issue 6, June 2021

DOI 10.17148/IJIREEICE.2021.9612

Transforming grid system and energy market using blockchain technology

Nitin Kumar singh[1], Manoj kumar[2], Rakesh narvey[3]

[1]Student, Electrical Engineering, Madhav institute of Technology and Science, Gwalior, M.P, India.

[2] Associate Professor, Electrical Engineering, Madhav institute of Technology and Science, Gwalior, M.P, India

[3] Assistant Professor, Electrical Engineering, Madhav institute of Technology and Science, Gwalior, M.P, India

Abstract: The conventional grid and power grid infrastructure is monitored employing a centralized approach. Whereas remote terminal units are ruled using a master control facility. In the wake of dispersed generations where every consumer is additionally becoming a producer with solar powered PV panels or wind, managing power is becoming a difficult task. This situation can become unmanageable in an event of cyber-attack on a smart grid. In this paper, we develop a way of using blockchain technology to share transaction information among different power grids in a secure, controlled, monitored, and efficient manner. The biggest concern regarding the data is integrity. By leveraging blockchain technology, the info are going to be reliable and resilient to attacks, like man-in-the-middle and data spoofing attacks. The Blockchain implementation provides a permissioned network in which power grids will act as nodes that maintain ledger information. By employing a distributed ledger to validate transactions though the method of consensus, the system can share information during a manner that's safer and transparent than traditional information. The additional layers of security and speed that Blockchain technology provide help to prevent issues, such as power grid failures, that could stem from the latency or integrity.

Key Words: - Smart grid, Block chain, power system protection, data security, Cyberattacks, Smart contract, Power distribution.

I.INTRODUCTION

Like any other industry sector, the electric power industry is facing challenges involved the increasing demand for interconnected system operations and control under the restructured electrical industry thanks to deregulation of the electrical market and therefore the trend of the Smart Grid. This moves automation networks from outdated, proprietary, closed networks to the more current arena of data Technology (IT). However, while gaining all of the value and performance benefits of IT, existing IT security challenges are acquired also . The power grid automation network has inherent security risks thanks to the very fact that the systems and applications within the network weren't originally designed for the overall IT environment.

On 23 December 2015, hackers manipulated information systems of three energy distribution companies in Ukraine and for a while disrupted the electricity supply to consumers. The Ukraine cyberattack was complex and consisted a compromise of corporate networks using spear-phishing emails then seizing SCADA under control, remotely switching substations off and destroying IT infrastructure components (uninterruptible power supplies, modems, RTUs, commutators) whereas destruction of files stored on servers and workstations, denial-of-service attack on call-centre to deny consumers up-to-date information on the blackout.

In order to chop the carbon footprint, that's coal-based generation, India has committed 200GW of non-conventional power. This target is predicted to be achieved through photovoltaics, windmill, and a mixture of such technologies. A bulk, of the targeted power is backed upon, rooftop PV generation through households. this suggests that the role of consumer of power won't only be restricted to power consumption but they're going to be ready to generate power also. they're going to be called prosumers. to deal with this significant issue Advanced Metering Infrastructure are getting used.

Smart meters will provide utilities with features like load control switching (LCS). this may enable them to turn-off appliance and meters during peak hours for better balancing of the load. Integration of smart features into existing grids results in cyber vulnerabilities. within the case of a cyber-attack, where a hacker is in a position to disrupt the communication link either by disrupting an influence switch or tampering with data, the safety and stability of power grid are going to be in mayhem.

Sharing information across large networks poses many issues and potential risks involving security and usefulness. For the aim of sharing information between microgrids, our team has posited that, while availability, integrity and confidentiality of knowledge are important, the appliance of blockchain technology to also achieve non-repudiation of shared data will substantially improve resilience of microgrids to man-in-the-middle and data spoofing attacks. Blockchain architectures provide a spread of solutions to sharing information.

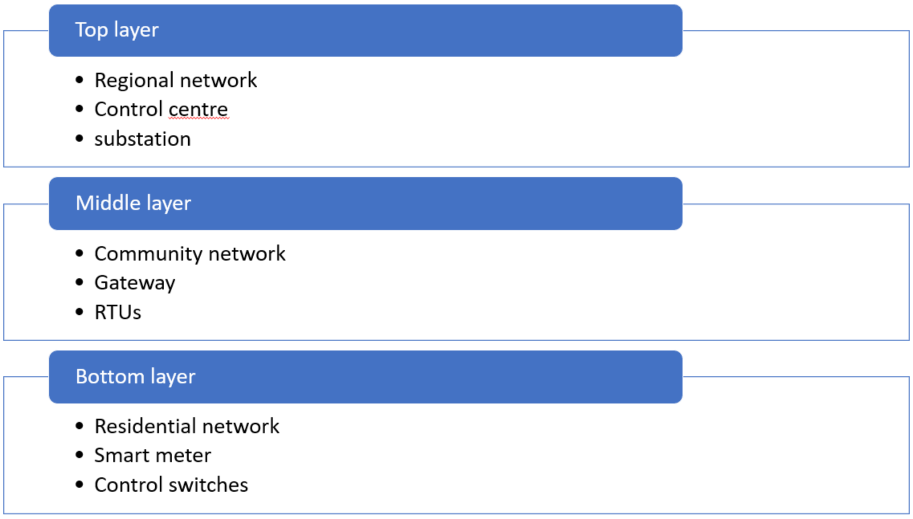
II. Smart grid Architecture

It consists of three layers namely:

At the lowest layer are residential networks, each sort of a definite customer. A residential network features a star-like topology, composed of a wise meter at the center and a few of control switches (if any exist) at the periphery. because the interface of the network, the smart meter provides real-time raw metering data to the middle at the very best layer, and detailed energy usage and price information to the customer. It also accepts control commands from the upper layers to connect/disconnect particular appliances (through pre-installed control switches) for load balancing purposes.

At the middle layer are community networks. A community network connects the residential networks, intelligent electric devices (IEDs), and neighborhood together. Data storage devices may additionally be included within the network to support networked storage, local fault diagnosis, and distributed deciding. there is a communication gateway in each community network. It manages the communication among the network elements, performs data aggregation, and bridges the lowest and top layers to allow data exchange. An example of a community network is that the network during a sensible community.

At the very best layer are regional networks. A regional network connects the community networks, power plants, renewable power sources, substations, feeders, and other grid devices during a geographic area. Dedicated hub nodes could even be deployed within the network to make a multiple-hop overlay structure for efficient and reliable data communication. an impression center is implemented in each regional network. It provides supervisory control and data acquisition (SCADA) functionalities within the regional grid: collecting electricity usage data and grid operation status, detecting and responding to anomalies, and optimizing power generation, transmission, and distribution.



III. VARIOUS TYPE OF ATTACKS ON SMART GRID:

A device attack aims to compromise (control) a grid device. it's often the initial step of a classy attack, during which the compromised device is going to be wont to launch further attacks like data attacks and network availability attacks toward the smart grid or perform malicious physical actuation (if the device may be a control element). for instance, a compromised IED like a breaker may break a circuit maliciously and cause power failure. Another example is that a compromised grid device might abruptly increase load to cause circuit overflow. To resist device attacks, strict access control is important.

A data attack attempts to insert, alter, or delete data or control commands within the network traffic so on mislead the smart grid to form wrong decisions/actions. One commonly observed data attack is that a customer jeopardizes the smart meter so as to scale back its electricity bill. Another example is that a compromised RTU is informed a few faults detected by a faulted circuit indicator (FCI) device, but it refuses to report the fault to the centre, leading to increased outage time. To resist this attack, data integrity and authenticity must be protected, and effective intrusion detection mechanisms need to be developed.

A privacy attack aims to learn/infer users' private information by analysing electricity usage data. In smart grid, electricity usage information is collected multiple times per hour by smart meters so on obtain fine-grained information about the grid status and improve grid operation efficiency. The detailed information may easily reveal customers' physical activities. for instance, during a residential setting, lack of electricity use for stove and microwave during a particular period of time indicates that the house isn't occupied. Using this information, physical attacks like robbery are often planned when nobody is reception. Clearly, such privacy-sensitive information must be shielded from unauthorized access.

A network availability attack takes place within the sort of denial of service (DoS). Its objectives are to spend or overwhelm the communication and computational resources of the smart grid, leading to delay or failure of knowledge communications. for instance, an adversary may flood an impact centre with false information at very high frequency such the centre spends most of the time verifying the authenticity of the knowledge and isn't ready to timely answer

IV. PRELUDE

Blockchain may be a group of transactions that are linked to their previous modification on a selected channel . The chain may be a log that contains the transactions of all previous 'blocks' for that specific chain. When a replacement block is appended unto the chain, the transaction from that previous block is additionally appended . an outsized feature of a blockchain is that the use of a distributed ledger . Blockchain ledgers are often decentralized because everyone on the network is functioning with their own replication of the block . Utilizing a decentralized ledger helps add security to the network as all information isn't funnelling into one node.

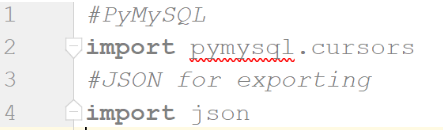
The purpose of this project is to supply a foundation to unravel the matter of the info distribution that might be a serious driving force in implementing a secure and efficient WAMC (wide area management centre) within the world . within the future, WAMC can help to stop issues and errors that stem from anomalous activity during a power system . Traditional Supervisory Control and Data Acquisition (SCADA) systems are limited in their capability to detect anomalies in power grids.

V. USING BLOCKCHAIN TECHNOLOGY TO SECURE GRIDS AGAINST CYBER-ATTACKS:

A smart grid are often made more reliable by using block chain technology. during this project we've successfully communicated between two nodes and this might be later uprooted to million plus nodes.

Data is obtained by running a database query algorithm. This algorithm which is explained within the next paragraph. Then from the client, data are going to be sent out the VPN concentrator with an update request to the remainder of the nodes on the network, and therefore the nodes will confirm the request to update the ledger. the opposite nodes are then ready to hook up with the VPN concentrator so as to send confirmation requests back to our client. Once the request is shipped back to our client node validating the update, the ledger state is updated with the acceptable information. Each node on the network will run an identical instance .

The modules that are used are MySQL and JSON. The MySQL module enables us to interface with the SQL database. The JSON module acts like and encoder and decoder to assist us convert our data into a useable JSON format



```
#PyMySQL
import pymysql.cursors
#JSON for exporting
import json
```

IJIREEICE

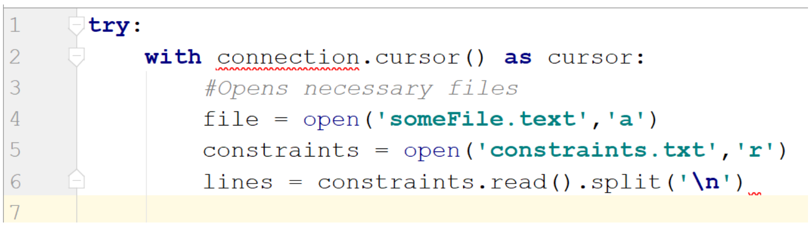
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 6, June 2021

DOI 10.17148/IJIREEICE.2021.9612

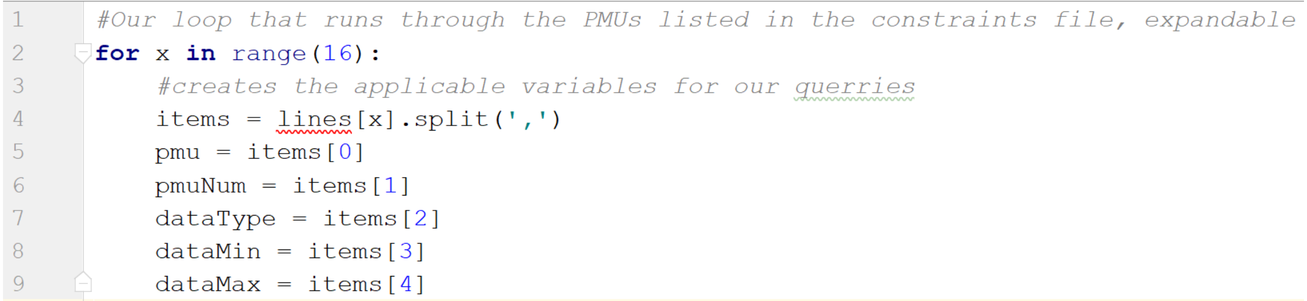
ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

The python script maintain a connection to the SQL database. After securing the connection, the script obtains information related to PMU data from a text file.



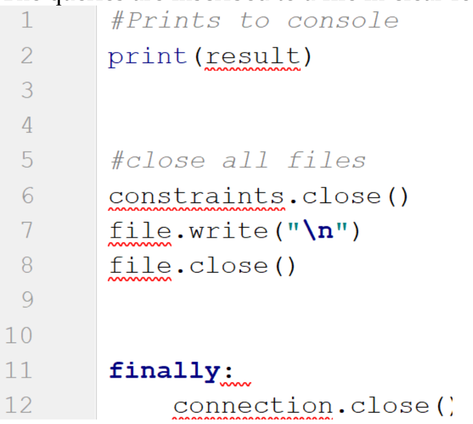
```
try:
    with connection.cursor() as cursor:
        #Opens necessary files
        file = open('someFile.text','a')
        constraints = open('constraints.txt','r')
        lines = constraints.read().split('\n')
```

This file have the specific identifiers for all PMU measurements and related variables necessary for queries. The program then loops through each PMU and enquiries the SQL data for the updated value.



```
#Our loop that runs through the PMUs listed in the constraints file, expandable
for x in range(16):
    #creates the applicable variables for our querries
    items = lines[x].split(',')
    pmu = items[0]
    pmuNum = items[1]
    dataType = items[2]
    dataMin = items[3]
    dataMax = items[4]
```

The queries are inscribed to a file in clear format. so, each query is published to the console.

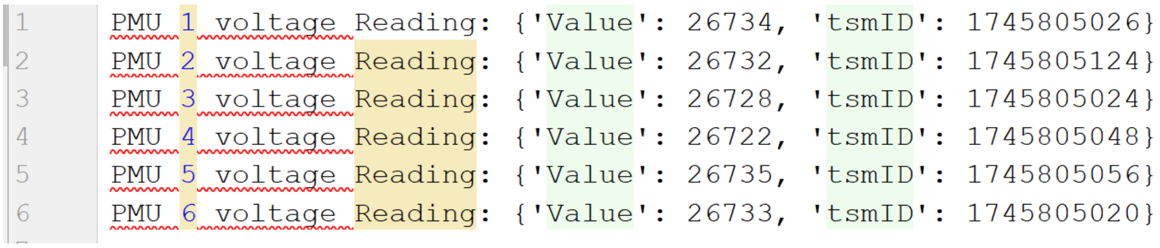


```
#Prints to console
print(result)


#close all files
constraints.close()
file.write("\n")
file.close()


finally:
    connection.close()
```

After performing the above actions, the script shut down all files and networks. Therefore, historic data for our network is created, the script is being rationalized to house JSON file.

Once a successful proof of concept are often run, this framework are often adapted on a bigger scale to permit peer nodes to speak over large distances. Latency would be suffering from the changes within the environment. This project has successfully created a database query algorithm with python with a successful update to accommodate JSON formatting.

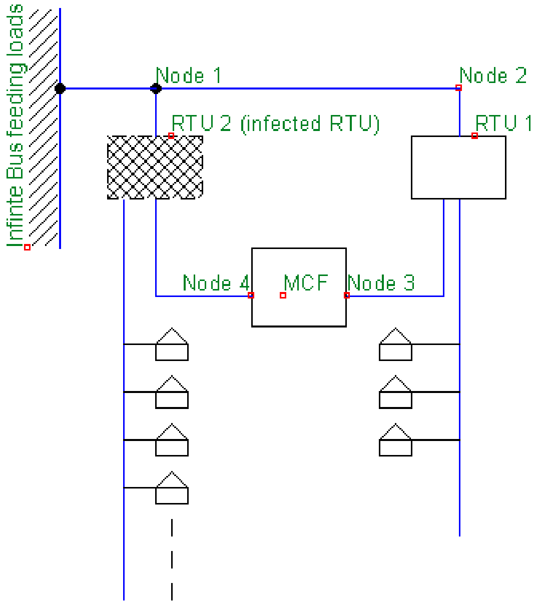
The data is collected from PMUs connected to the local power system . These units collect voltage and current measurements from different parts. Through python coding, we are ready to successfully pull data from some Point. the info includes: current phasors, voltage phasors, frequency, rate of change of frequency and time stamps.



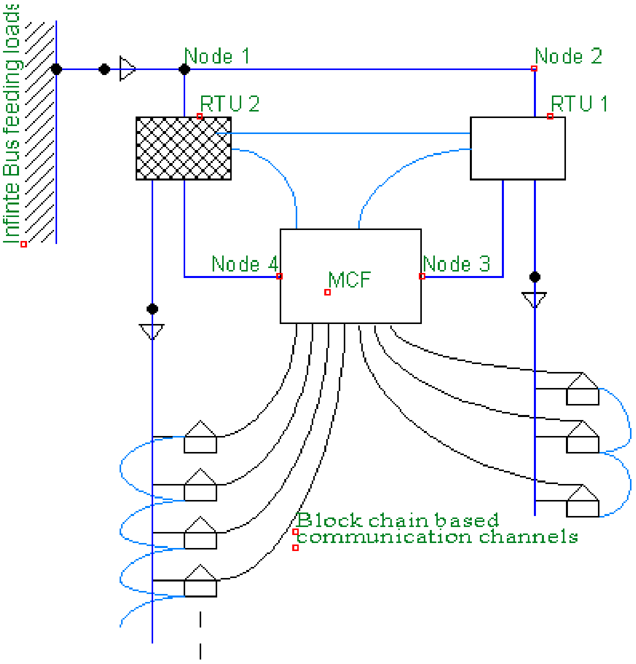
```
PMU 1 voltage Reading: {'Value': 26734, 'tsmID': 1745805026}
PMU 2 voltage Reading: {'Value': 26732, 'tsmID': 1745805124}
PMU 3 voltage Reading: {'Value': 26728, 'tsmID': 1745805024}
PMU 4 voltage Reading: {'Value': 26722, 'tsmID': 1745805048}
PMU 5 voltage Reading: {'Value': 26735, 'tsmID': 1745805056}
PMU 6 voltage Reading: {'Value': 26733, 'tsmID': 1745805020}
```

Once a successful proof of concept are often run, this framework are often adapted on a way bigger scale to permit peer nodes to speak over large distances. Latency would be suffering from the changes within the environment. This project has successfully created a database query algorithm with python with a successful update to accommodate JSON formatting.

The data is collected from PMUs connected to the local power system . These units collect voltage and current measurements from different parts. Through python coding, we are ready to successfully pull data from some Point. the info includes: current phasors, voltage phasors, frequency, rate of change of frequency and time stamps.



Earlier model of grid communication



blockchain based grid communication

Use of Blockchain will make cyber-attacks like denial-of-service attack on a message node very tough, in a smart grid. So because of a block chain, a hacker will have to get to the control of top >50% computing capacity of a smart grid to allow vulnerability. Therefore, the cost of attack, energy and time will increase knowingly. Thereby, reducing chances of such attacks on a smart grid.

VI. APPLICATION OF BLOCKCHAIN TECHNOLOGY IN FORE COMING ENERGY SECTOR:

Electric vehicle Battery Swapping:

The government has set a target that 30% of all vehicles be electrically driven by 2030. For this aim to be realized requires that strong incentives be created for the manufacture, sale, and usage of electrical vehicles. additionally , it's expected that the increased usage of EVs will substantially increase the usage of batteries to power them. Though technology is improving, a drag of battery charging is particularly troubling. 'Charging station' infrastructure required to allow large scale proliferation of EVs remains limited, and affects choice in buying of vehicles. A proposed method to affect this challenge is to bypass cumbersome charging stations and make battery sharing ecosystems - which could (very basically) allow users to swap batteries out on the exhaustion of charge.

The storage of parameters describing each battery on blockchain, used in conjunction with IoT, emerges as a possible solution to the problems highlighted above.

Immutable battery information storage: The blockchain may store information like age of the battery and its previous treatment in an immutable fashion, thus removing the likelihood of misrepresentation to increase price or lower cost of usage.

Usage of blockchain to store information on the types of energy used to charge the battery will help to inform the incentivize usage of sources of renewable energy.

Programmable transfers: Exploiting the 'smart contract' feature of blockchain applications would go away more efficient swapping of batteries at charging stations, since simple rules on costing are often applied on the thought of battery attributes and executed on exchange.

Energy Trading platform:

India currently faces a dual problem of poor access to energy, and high proportion of fuel mix. As of 2016, only 86.8 percent of the Indian population has access to energy. A recent report also highlights that the central grid (which powers most Indian households) is driven largely by fossil fuels, with this percentage predicted to remain above 50 percent in 2040.

Renewable energy driven microgrids are suggested as a possible means of solving the dual problems with poor access and source mix. These would be particularly valuable in areas with no grid connectivity. because the central grid expands, these grids would enjoy the potential to interface with the central grid through mechanisms like Power Purchase Agreements (PPAs) to help increase renewable energy mix, and permit conscious consumers to choose the energy of their preference.

In today’s market, there are different authorities and intermediaries within the method where there's an entity responsible for registering assets, verifying whether or not they're renewable, measuring their production, and eventually creating REC certificates. plenty of buyers aren't dealing directly with specific generation assets rather they're browsing brokers or intermediaries. There are different authorities that are responsible for reporting and verification and preventing things like double-counting and ensuring that once you claim a credit.

Blockchain may function a valuable platform to understand the proposed targets because of the inherent features it'd help deploy. Blockchain may enable a sustainable energy trading system by implementing smart PPAs (Purchase Power Agreements), smart microgrids, REC Certificates Issuance etc. Making energy resources into digital assets which can be traded on a blockchain could open new investing and trading opportunities allowing simple entry to the new players and fostering innovations. It can also cause a community-driven change which may solve the matter of walk access.

VII.**CONCLUSION**

The implications of this technology apply to a worldwide level of communication amongst power grids that believe each other to supplement power when needed. A Blockchain architecture supports a secure method of communication during a highly scalable network. This process expedites the sharing of data which ends up within the prevention of potential blackouts relevant to power grids. during this paper, we've introduced block chain as solution, to mitigate cyber-attacks on a sensible grid. Implementing block chain technique and thereby helping substations to function as autonomous decentralized units will help the utilities to manage the facility with ease. While the buyer tariffs are going to be justified, as they're going to pay just for what they use. Hence, efficient, and enhanced control of power alongside , demand-based tariff will become a reality soon. Future work will specialise in extending this block chain technology to small devices.

REFERENCES

[[1] https://www.blockchain.org/projects/fabric
[2] https://blockchain-fabric.readthedocs.io/en/release-1.2/glossary.html
[3] https://blockchain-fabric.readthedocs.io/en/release-1.2/ledger/ledger.html
[4] https://www.cfr.org/report/applying-blockchain-technology-electricpower-systems
[5] https://www.researchgate.net/
[6] https://media.kasperskycontenthub.com › ...PDF Analysis of the Cyber Attack on the Ukrainian Power Grid