International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Enhancing Cyber Security in Power Sector systems using Block chain

R. Prabhakaran, S. Asha

Abstract: ***With the promotion of electric power reforms, Power plants are at a high risk associated with potential disclosure of privacy data. They should overcome various kinds of threats like SQL injection Denial of Service(DOS), Cross Site Scripting(XSS), Phishing and Malware. In this paper we propose a secure and trustworthy method to protect power plant in which data is stored in Block chain instead of general centralized databases in which data is stored in distributed blocks across the network after validation.***

Index Terms: Block Chain, Cyber security, Power sector systems, Blockchain.

I. INTRODUCTION

Cyber security is the developing field across all fields of Tasks. We depend on digital technology to travel, communicate, power our houses and work places. Our daily life's, monetary essentials and national security depend on a steady, protected and flexible defense against cyber attacks. Power plants use the traditional Centralized mode of power transmission using third Parties. In order to enhance the cyber security of power plant, they are preparing for safe and Secured Technologies for decades into the future [4].

To solve this problem we propose, a scheme by using Block chain Technology which is a decentralize, off trust and safe. In this scheme the terminals communicate directly and at the same time communication information is encrypted and distributed thus ensuring the safety of the communication.

II. BLOCK CHAIN TECHNOLOGY

Block chain technology is the underlying technology of Bitcoin [2]. The essence of block chain is distributed database system based on peer-to-peer network. It uses, Peer to Peer transmission, Consensus Algorithm. A data storage unit with time stamp is a block that is linked to a block chain in chronological order.

Revised Manuscript Received on 22 May 2019.

***** Correspondence Author

R. Prabhakaran*, Assistant Professor, School of Computing Science and Engineering, VIT University, Chennai Campus, Chennai 600127, Tamil Nadu, India.

S. Asha, Associate Professor, School of Computing Science and Engineering, VIT University, Chennai Campus, Chennai 600127, Tamil Nadu, India.

The block header consist of timestamp, data, previous hash and computed hash. The storage and transmission of data is happened through a consensus algorithm. The value of data after hashing is stored in the block header of the next block. It does not require manual operation. Each block has two parts namely: header and body.

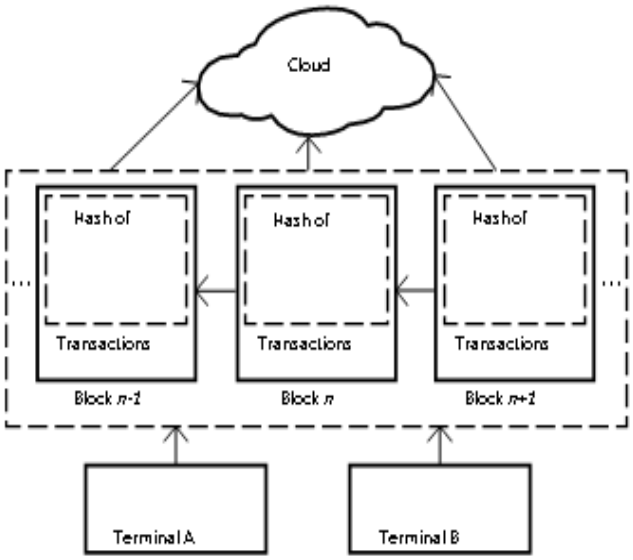

Fig. 1 System structure

A. Block chain Infrastructure

Each Block has the following layers namely: Application layer, Contract layer, Incentive layer, Consensus layer, Network layer and Data layer. The encoded data information and the storage location are stored in data layer of the block. the network layer is a peer to peer network which validates the Information, Consensus mechanisms and algorithms are present in Consensus Layer. DPOS, POS, POW are used as a consensus mechanism; The Security and maintenance protocols are present in Incentive Layer ; The Programmable characteristics are present in Contract layer; Application layer has various application scenarios (Fig. 2) [4]

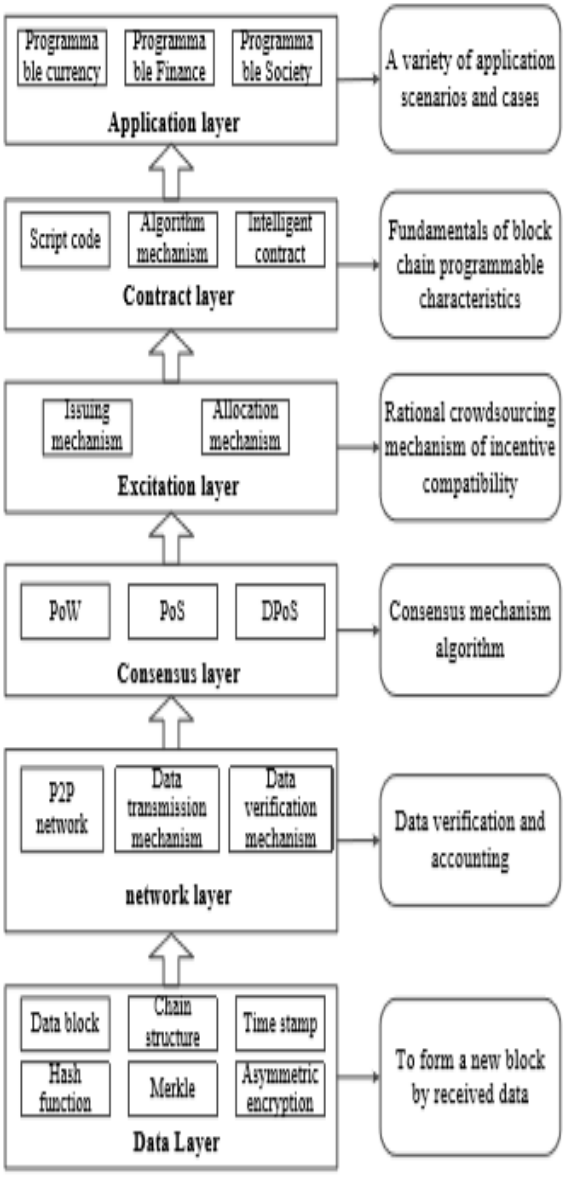

Fig. 2 System structure

B. Digital Signature Used In Blockchain

Every client has a couple of Public and Private Keys. Using private key transactions are signed. Digitally Signed Transactions are distributed throughout the network and are visible using Public Keys. Fig.3 shows Digital Signature block example.

There are two phases of digital signature: the phase of signing and the phase of verification. Take the example of Fig.3 When the user A (Alice) wants to sign an Exchange, A will generate Exchange. Then, using his private key, he encrypts the hash value and then sends the encrypted hash with the original data to another user B (bob). B checks the exchange received by comparing hash value derived from the data received by the same hash function as A's and the hash decrypted (using A's public key). The Block chain uses elliptic curve digital signature algorithm (ECDSA) as it's Digital Signature Algorithm [1].

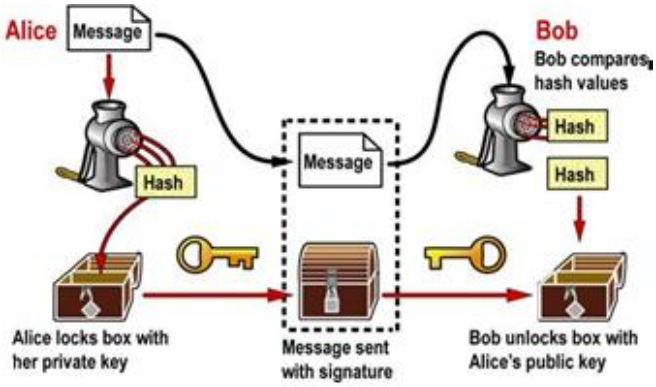

Fig. 3 Digital signature block

III. CONSENUS ALGORITHMS

Bitcoin network uses POW (Proof of work) Consensus Algorithm [2], the most popular algorithm used in the block chains. The Consensus Algorithm takes a shot at the rule that the determined hash esteem must be equivalent to or littler than a specific given esteem.

If the single block is validated, this new block will be added to their block chains by other miners. Nodes calcul ating the hash values are called miners and the procedure for proof of work is called mining. [5].

Example - hash is a hypothetical hash function that has the listed as below

y = 10, X = 'test'

hash(X) = hashr('test') = OxOf = 15 > 10

hash(X+1) = hash('test1') = Oxff = 255 > 10

hash(X+2) = hash('test2') = 0x09 = 9 <10 OK, Solved.

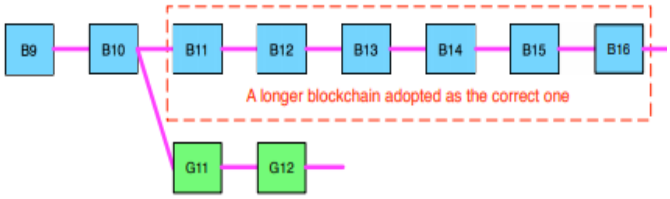

Fig. 4 An scenario of blockchain branches (the longer branch would be admitted as the main chain while the shorter one would be deserted) (see online version for colours). [8].

Delegated proof of stake:

The contrast between Proof of Stake and Delegated Proof Of Stake is that proof of stake is democratic direct while Delegated Proof Of Stake is democratic representative. Stakeholders elect blocks to be produced and approved by their agents. If there are less nodes to validate the block, that block could be quickly affirmed and transactions are quickly confirmed. DPOS is the basis of Bit shares [3].

IV. BLOCK CHAIN APPLICATIONS IN POWER GRID

Block chain technology can give an ease, secured and straight forward Platform for energy Transactions. It assures Security to the People participating in Electricity exchange under any circumstance [4].

A. Structure of blockchain transaction

The Block chain is derived from the word "Block + Chain". It provides the total history of the database. Block Chain stores all the Chronological data from the Beginning of the Block to the recently generated block. Additionally, we can search for a particular transaction data by following to its source and validate it carefully. The Block chain can be applied in these parts of the power plant as shown in the Fig. 5 [6]

The Fig. 5 demonstrates the power framework utilized in generating scenarios. In the figure we have several segments; double Power generators are G1 and G2. R1 through R4 are Smart Electronic Devices (IEDs) capable of switching on or off the breakers. The Breakers are called BR1 by BR4. There are also two lines. Line One ranges from breaker 1 (BR1) to breaker 2 (BR2) and Line 2 ranges from breaker 3 (BR3) to breaker 4 (BR4) [6]

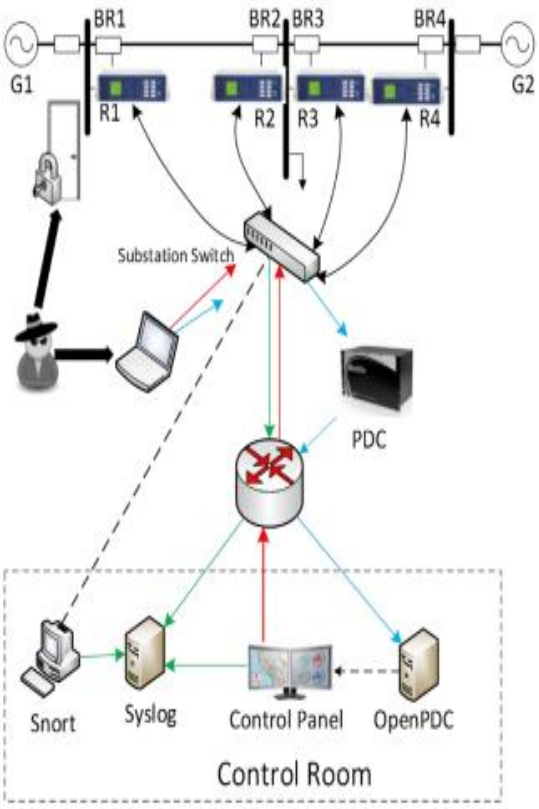

Fig. 5 Architecture of power plant [6]

There are 4 PMUs (phasor measuring unit) in our system that measure 29 features for a total of 116 PMU columns. The index for each column is in the form of "R#-Signal Reference" indicating a measurement type from a PMU specified in "R#." Fig. 6 lists the references to the signal and the corresponding descriptions. R1-PA1:VH, for example, is the phase angle of Phase A voltage measured by PMU R1. PMU measurement Columns followed by Snort alerts and relay logs of the 4 PMU / relay (relay and PMU are integrated together) 12 columns for control panel logs. [6].

Feature	Description
PA1:VH – PA3:VH	Phase A - C Voltage Phase Angle
PM1: V – PM3: V	Phase A - C Voltage Phase Magnitude
PA4:IH – PA6:IH	Phase A - C Current Phase Angle
PM4: I – PM6: I	Phase A - C Current Phase Magnitude
PA7:VH – PA9:VH	Pos. – Neg. – Zero Voltage Phase Angle
PM7: V – PM9: V	Pos. – Neg. – Zero Voltage Phase Magnitude
PA10:VH - PA12:VH	Pos. – Neg. – Zero Current Phase Angle
PM10: V - PM12: V	Pos. – Neg. – Zero Current Phase Magnitude
F	Frequency for relays
DF	Frequency Delta (dF/dt) for relays
PA:Z	Appearance Impedance for relays
PA:ZH	Appearance Impedance Angle for relays
S	Status Flag for relays

Fig. 6 signal references and corresponding descriptions

Types of Attacks in the above scenario include Data Injection, Line maintenance, Relay setting change, Short circuit fault.

B. Blockchain for Power Transmission

We can provide security to this device by using blockchain. We use RKG Algorithm for encryption and SHA 256 for Hashing.

Source Code:

```
import pandas as pd
import hashlib
import random
a=pd.read_csv("C:\\Users\\Yashwanth\\Downloads\\data1.csv")
def hash_block(s):
    shas= hashlib.sha256(s.encode()).hexdigest()
    return shas
block=[]
def last():
    return block[-1]

def add(value,lastinit):
    block.append([lastinit,value])
    add("genesis",[1])
for i in temp[0] :
    i=hash_block(str(i))
add(i, last())

print(*block,sep='\n')
```

Fig. 7 Output

C. Comparison of Block Chain and Encryption algorithms:

From this Paper [7] the results of various encryption algorithms are showed in Fig. 8.

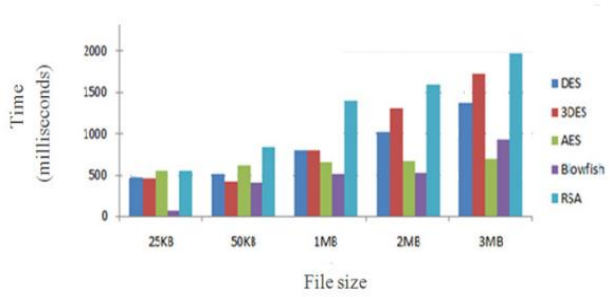

Fig. 8 Encryption time

As the blow Fish Encryption algorithm has the less time of encryption we are going to consider it to compare with the block Chain Performance. The Fig. 9 shows the time Complexity of the Block Chain, Blow Fish, and RKG Encryption Algorithms.

Table 1 Comparison of algorithms

Algorithm	Total time(ms)
RKG	49
Block Chain	55
Blow Fish	410

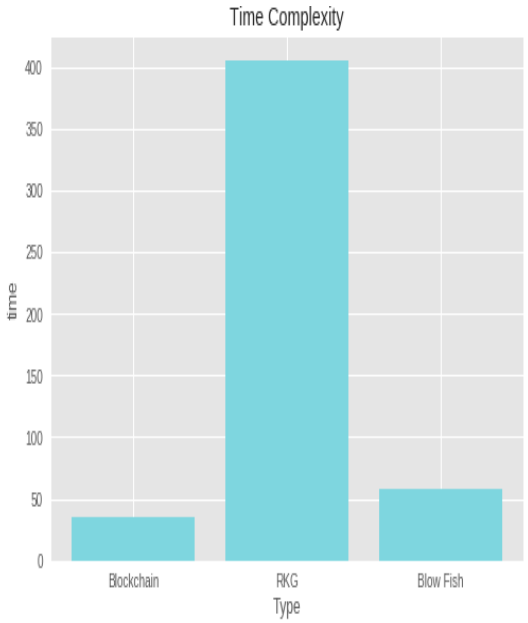

Fig. 9 Time Complexity of algorithms

Fig.10 Shows the System-time, wall-time, user-time comparisons of the encryption algorithms and Block Chain. The results show that the block Chain takes less time to process and secure the data when compared with the other encryption Algorithms.

Table 2 Comparison of Algorithms

Algorithm	System time(ms)	Wall time (ms)	User time(ms)
RKG	170	322	269
Block chain	5.45	27.5	23.2
Blow-fish	16.6	51.2	41.9

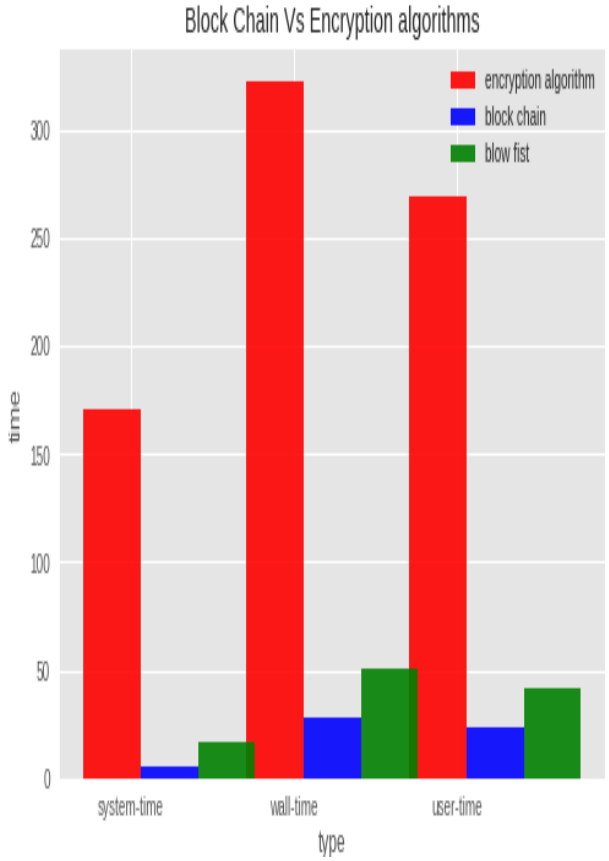

Fig. 10 Time Complexity of algorithms

V. CONCLUSION

From this we can conclude that the Block chain Technology is secured and Time Saving approach for Power Supply Utilities. With the Block Chain Technology we can Certify, Transmit and Distribute Power. It leads to a secured Power Transaction and Distribution.

REFERENCES

1. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ecdsa). International Journal of Information Security 1(1), 36–63 (2001)
2. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
3. “Bitshares - your share in the decentralized exchange.” [Online]. Available: https://bitshares.org/

4. Yujie Xu,Mingming Wu ,Yue Lv,Shujun Zhai, "Research on Application of Block Chain in Distributed Energy Transaction" 957-960(2017)
5. Xia. F.J.Zhang, and C. Zue, "Review for consensus mechanism of cryptocurrency system" computer systems & Applications, 2017.
6. Power System Attack Datasets - Mississippi State University and Oak Ridge National Laboratory - 4/15/2014
7. Priyadarshini P, Prashant N, Narayan DG, Meena SM. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science. 2016;78:617-624.
8. Zibin Zheng and Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang,"Blockchain challenges and opportunities: a survey" Int. J. Web and Grid Services, Vol. 14, No. 4, 2018.

AUTHORS PROFILE

Prof.R. Prabhakaran, is an Assistant Professor (Senior) from the School of Computing Science and Engineering, VIT University, Chennai. He graduated in Computer Science and engineering from Madras University, Chennai and Post graduated in Computer Science and engineering from PSG College of Technology, Coimbatore, Tamil Nadu. He is pursuing his Ph.D from VIT University Chennai. His area of interest includes Network security, Biometric security, Computational Intelligence, Cloud security and Cyber security. He has published nearly 9 papers in international journal. His current research interests include power system reliability and resiliency, critical infrastructure protection and smart grid cyber security.

Dr. S. Asha, is an Associate Professor from the School of Computing Science and Engineering, VIT University, Chennai. She graduated from Madras University, Chennai and completed her Ph.D from Anna University Chennai. Her area of interest includes Network security, Biometric security, Computational Intelligence, Cloud security and Cyber security. She has published nearly 25 papers in international journal and conferences. Currently she is working in computational intelligence and Cyber security.