ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Distributed Block Chain for Security in an Ecommerce Environment

Anandhapriya S[1] , Navya Jayapal[2] ,Nandhini K [3], Mrs Pranamita Nanda[4]

UG Scholars, Department of Computer Science and Engineering, Velammal Institute of Technology, Tiruvallur, Tamil Nadu, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Tiruvallur, Tamil Nadu, India[4]

ABSTRACT: The cyber security of modern power systems has drawn increasing attention in both academia and industry. Many detection and defense methods for cyber-attacks have therefore been proposed to enhance robustness of modern power systems. In this paper, we propose a new, distributed block chain-based protection framework to enhance the self-defensive capability of modern power systems against cyber-attacks. We present a comprehensive discussion on how block chain technology can be used to enhance the robustness and security of the power grid, by using meters as nodes in a distributed network which encapsulates meter measurements as blocks.

KEYWORDS: denial of service (DoS), false data injection attack (FDIA), security, cyber-attacks, Permission.

I. INTRODUCTION

Modern power systems have experienced a profound evolution to facilitate social development. Unlike conventional power systems, the infrastructure of modern power systems relies strongly on advanced communication and control technologies. While this technological trend on the one hand provides new opportunities to optimize the energy efficiency of the grid, it also imposes significant requirements and challenges on the robustness, efficiency, and security of the underlying information infrastructure. These advances have been driving modern power systems towards becoming complex cyber-physical systems. However, due to the deep integration of both cyber and physical resources, attacks from the cyber layer have the potential to mislead decision-making in the control center and cause system disturbances, financial loss, or even more serious consequences, e.g., blackouts. In this sense, data vulnerability has become an unelectable issue, as evidenced by malicious events caused by cyber-attacks, a recent high-profile example of which was the 2015 Ukraine blackout. As a representative cyber-attack, the false data injection attack (FDIA) manipulates system data to mislead the control center without being detected by the bad data detection module. Many studies have demonstrated the impacts of FDIAs on modern power systems. In real situations, the system security could be threatened by not only FDIAs but also many other kinds of cyber-attacks, such as denial of service (DoS) attacks, data framing attacks, and cyber topology attacks. Therefore, ensuring the integrity and consistency of data is of critical importance for the secure and economical operation of the grid. In existing system methods have been proposed to detect and defend against cyber-attacks based on existing centralized data communication and storage mechanisms. However, existing communication and storage of meter measured data mechanism in modern power systems are less than fully effective against cyber-attacks, even if some meters are upgraded to pharos measurement units (PMUs). Centralized Data Communication and StorageMechanisms.

II. LITERATURE REVIEW

F.F. Wu, K. Moslehi and A. Bose [1] said that the functions and architectures of control centers: their past, present, and likely future. The evolving changes in power system operational needs require a distributed control center that is decentralized, integrated, flexible, and open. Present-day control centers are moving in that direction with varying degrees of success. The technologies employed in today's control centers to enable them to be distributed are briefly

DOI: 10.15680/IJIRCCE.2019. 0702143

reviewed. With the rise of the Internet age, the trend in information and communication technologies is moving toward Grid computing and Web services, or Grid services. A Grid service-based future control center is stipulated.

F. Luo, J. Zhao, Z.Y. Dong, Y. Chen, Y. Xu, X. Zhang and K.P. Wong [2] This paper gives a comprehensive discussion on applying the cloud computing technology as the new information infrastructure for the next-generation power system. First, this paper analyzes the main requirements of the future power grid on the information infrastructure and the limitations of the current information infrastructure. Based on this, a layered cloud-based information infrastructure model for next-generation power grid is proposed. Thus, this paper discussed how different categories of the power applications can benefit from the cloud-based information infrastructure. For the demonstration purpose, this paper develops three specific cloud-enabled power applications. The first two applications demonstrate how to develop practical compute-intensive and data-intensive power applications by utilizing different layered services provided by the state-of-the-art public cloud computing platforms. In the third application, we propose a cloud-based collaborative direct load control framework in a smart grid and show the merits of the cloud-based information infrastructure on it. Some cybersecurity considerations and the challenges and limitations of the cloud-based information infrastructure are also discussed.

Y. Liu, P. Ning, and M. K. Reiter [3] A power grid is a complex system connecting electric power generators to consumers through power transmission and distribution networks across a large geographical area. System monitoring is necessary to ensure the reliable operation of power grids, and state estimation is used in system monitoring to best estimate the power grid state through analysis of meter measurements and power system models. Various techniques have been developed to detect and identify bad measurements, including the interacting bad measurements introduced by arbitrary, non-random causes. At first glance, it seems that these techniques can also defeat malicious measurements injected by attackers. In this paper, we present a new class of attacks, called false data injection attacks, against state estimation in electric power grids. We show that an attacker can exploit the configuration of a power system to launch such attacks to successfully introduce arbitrary errors into certain state variables while bypassing existing techniques for bad measurement detection. Moreover, we look at two realistic attack scenarios, in which the attacker is either constrained to some specific meters (due to the physical protection of the meters), or limited in the resources required to compromise meters. We show that the attacker can systematically and efficiently construct attack vectors in both scenarios, which can not only change the results of state estimation, but also modify the results in arbitrary ways. We demonstrate the success of these attacks through simulation using IEEE test systems. Our results indicate that security protection of the electric power grid must be revisited when there are potentially malicious attacks.

O. Kosut, L. Jia, R.J. Thomas, and L. Tong[4] Malicious attacks against power systems are investigated, in which an adversary controls a set of meters and is able to alter the measurements from those meters. Two regimes of attacks are considered. The strong attack regime is where the adversary attacks a sufficient number of meters so that the network state becomes unobservable by the control center. For attacks in this regime, the smallest set of attacked meters capable of causing network unobservability is characterized using a graph theoretic approach. By casting the problem as one of minimizing a supermodular graph functional, the problem of identifying the smallest set of vulnerable meters is shown to have polynomial complexity. For the weak attack regime where the adversary controls only a small number of meters, the problem is examined from a decision theoretic perspective for both the control center and the adversary. For the control center, a generalized likelihood ratio detector is proposed that incorporates historical data. For the adversary, the trade-off between maximizing estimation error at the control center and minimizing detection probability of the launched attack is examined. An optimal attack based on minimum energy leakage is proposed.

X. Liu, Z. Li and Z. Li [5] It was revealed that modern power systems are at high risk of cyber-attacks, as an attacker can stealthily execute false data injection attacks against the state estimation without knowing the full topology and parameter information of the entire power network. To mitigate the risk, in this paper, we propose a bilevel mixed integer linear programming (MILP) model to determine the least number of measurements to be protected. A decomposition approach is adopted to obtain the suboptimal solution. To further reduce the computation complexity, we also propose to separate the power grid into several subnetworks using a MILP approach and apply distributed protection strategy to each subnetwork. The simulations on the IEEE 14-bus, IEEE 24-bus, IEEE 30-bus, and IEEE 118-bus systems verify the correctness and effectiveness of the proposed protection strategy.

III. PROPOSED SYSTEM

The proposed framework substantially increases the self-defensive capabilities of modern power systems against data manipulation by cyber attackers. In conventional power systems, an attack is deemed successful if cyber attackers tamper with meter measurement data locally, replace data packages transmitted to the control center via a communication channel, or hacks into control center. Its self-defensive capability. Very defensive on state-of-the-art security attacks

IV. METHODOLOGIES

The Blockchain, is designed to achieve peer-to-peer electronic payments directly, without participation of a trusted third party. In blockchain, all peers form a distributed network. Each peer acts as a node of the network and can participate in calculating the solution to a hash-based mathematical problem ensuring integrity of transactions. Each transaction record is encapsulated as a block and added onto the existing block chains. The recorded block contents are collectively referred to as the ledger. All information is then updated synchronously to the entire network so that each peer keeps a record of the same ledger. A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

V. ARCHITECTURE DIAGRAM

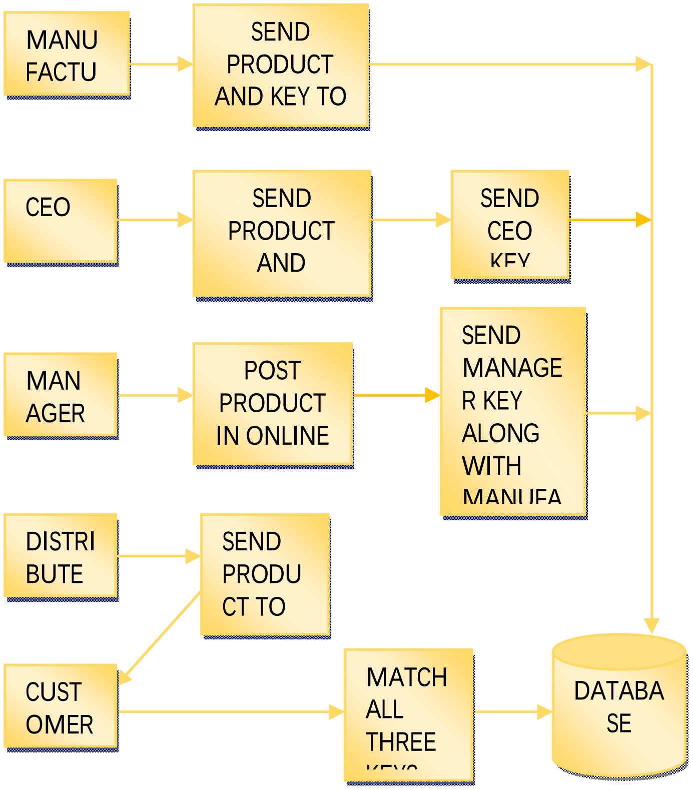


Fig.1 Architecture Diagram

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

VI. MODULES

1. CUSTOMER

If you are the new user going to login into the application then you have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user needs to enter exact username and password. If login success means it will take up to upload page else it will remain in the login page itself. User can receive the Product from the Distributor Person. User can receive the Manufacture key and CEO key from the Distributor.

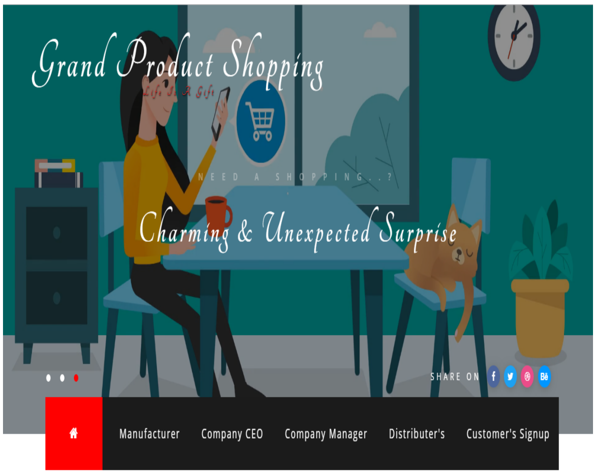
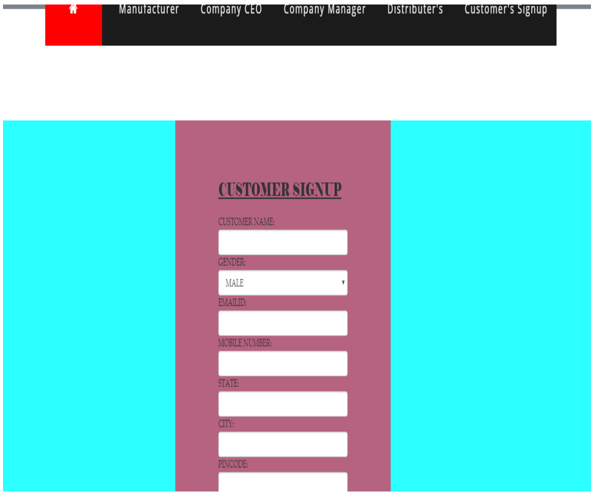


Fig.1.1 Home Page

Customer Register:
If the new user are going to login into the application then they have to register first by providing necessary details.



CUSTOMER SIGNUP

CUSTOMER NAME:

GENDER: MALE

EMAILID:

MOBILE NUMBER:

STATE:

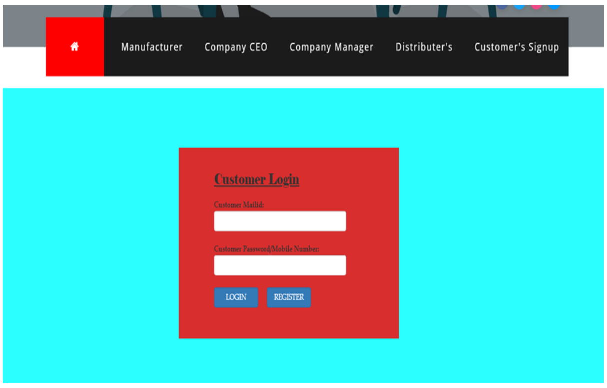
CITY:

PINCODE:

Fig.1.2 Customer Register

Customer Login:

After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user needs to enter exact username and password.



Customer Login

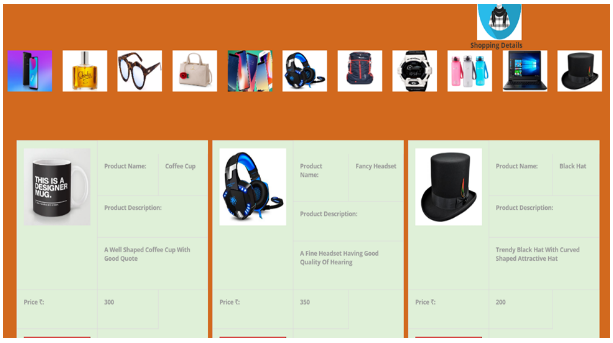
Customer Mailid:

Customer Password/Mobile Number:

Fig.1.3 Customer Login

Customer Shopping Page:

. If login success means it will take up to upload page else it will remain in the login page itself. User can receive the Product from the Distributor Person.



Product Name:	Coffee Cup	
Product Description:		
A Well Shaped Coffee Cup With Good Quote		
Price ₹:	300	

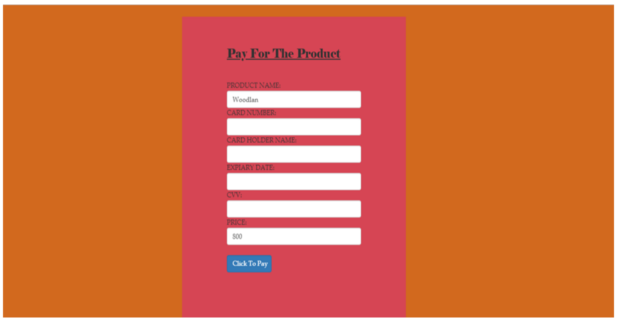
Product Name:	Fancy Headset	
Product Description:		
A Fine Headset Having Good Quality Of Hearing		
Price ₹:	350	

Product Name:	Black Hat	
Product Description:		
Trendy Black Hat With Curved Shaped Attractive Hat		
Price ₹:	200	

Fig.1.4 Customer Shopping Page

Customer Payment:

User can receive the Manufacture key and CEO key from the Distributor and the payment process takes place.



Pay For The Product

PRODUCT NAME: Woodlan

CARD NUMBER:

CARD HOLDER NAME:

EXPIARY DATE:

CVV:

PRICE: 800

Fig.1.5 Customer Payment

2. CEO

The user needs to enter exact username and password. If login success means it will take up to upload page else it will remain in the login page itself. CEO can send the Product to the Company Manager Person. CEO will generate the Key and send the key to Manager. Generate key and send the key to Manager Person.

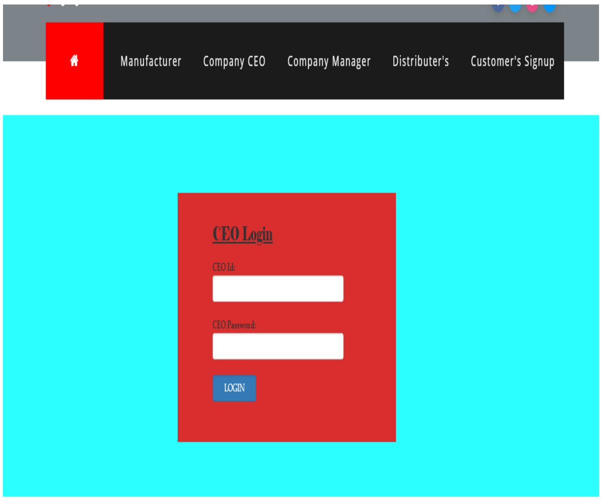


Fig.2.1 CEO Login

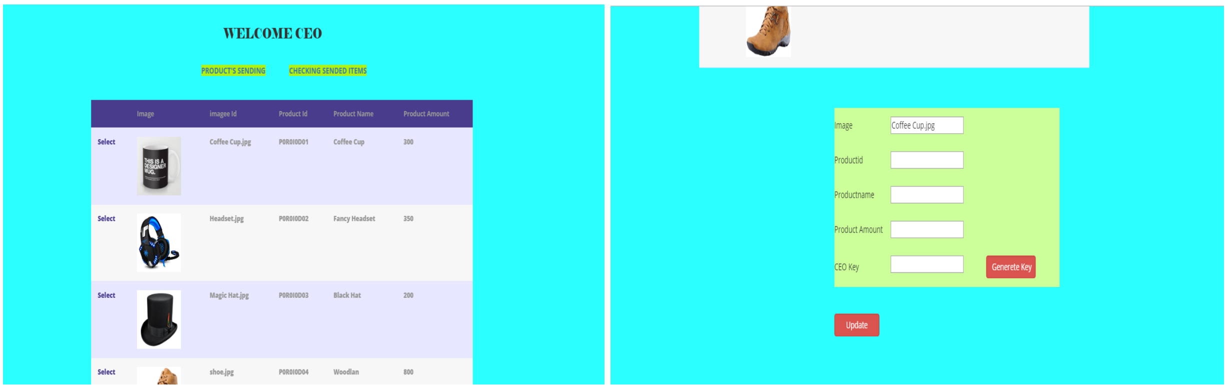


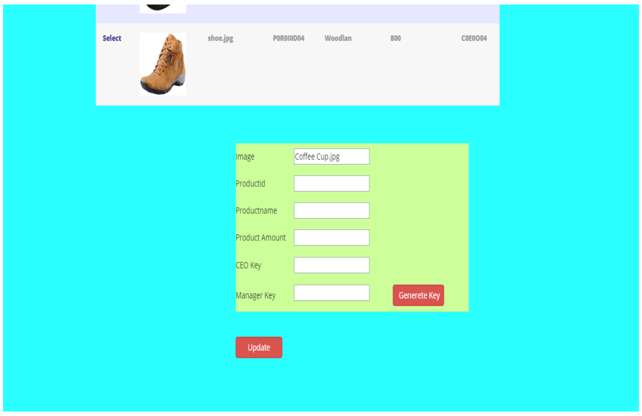
	Image	imagee Id	Product Id	Product Name	Product Amount
Select		Coffee Cup.jpg	P0R0I0D01	Coffee Cup	300
Select		Headset.jpg	P0R0I0D02	Fancy Headset	350
Select		Magic Hat.jpg	P0R0I0D03	Black Hat	200
Select		shoe.jpg	P0R0I0D04	Woodlan	800

Image: Coffee Cup.jpg
Productid:
Productname:
Product Amount:
CEO Key:

Fig.2.2 CEO sending Products

3. MANAGER

The user needs to enter exact username and password. If login success means it will take up to upload page else it will remain in the login page itself. Manager Post the Product in online Shopping website. Manager will generate the key and send the key to Customer. Generate key and send the key to Manager Person.



Select		shoe.jpg	P0R0I0D04	Woodlan	800	C0E0O04

Image: Coffee Cup.jpg

Productid

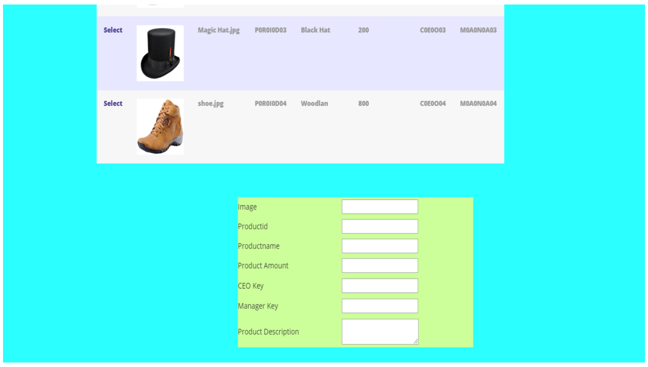
Productname

Product Amount

CEO Key

Manager Key

Fig3.1 Manager Check Products



Select		Magic Hat.jpg	P0R0I0D03	Black Hat	200	C0E0O03	M0A0N0A03
Select		shoe.jpg	P0R0I0D04	Woodlan	800	C0E0O04	M0A0N0A04

Image

Productid

Productname

Product Amount

CEO Key

Manager Key

Product Description

Fig.3.2 Manager Upload Shopping Portal

4. DISTRIBUTOR

If you are the new user going to login into the application then you have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user needs to enter exact username and password. If login success means it will take up to upload page else it will remain in the login page itself. Distributor can send the Product to the Customer Person. Distributor will send Manufacture and CEO Key to Customer Person.

Distributor Allocated Product:

Distributor can send the Product to the Customer Person. Distributor will send Manufacture and CEO Key to Customer Person.

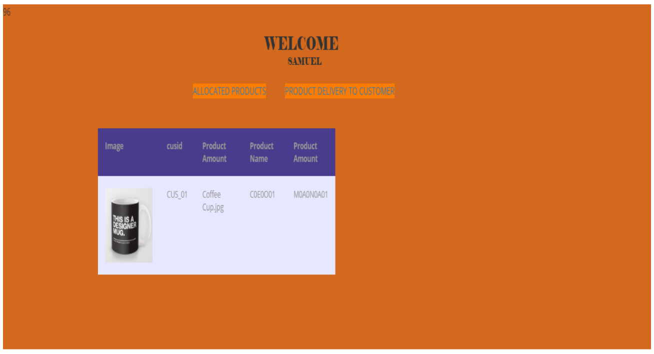


Image	cusid	Product Amount	Product Name	Product Amount
	CUS_01	Coffee Cup.jpg	C0E0O01	M0A0N0A01

Fig.4.1 Distributor Allocated Product

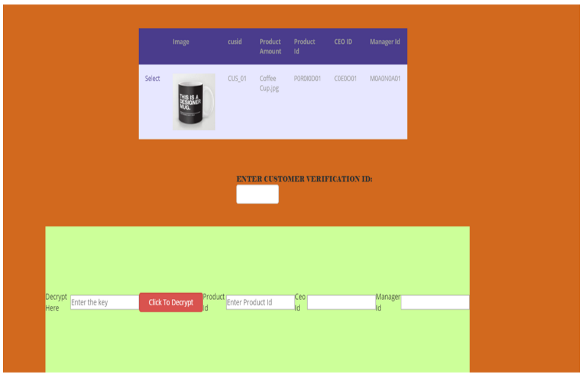
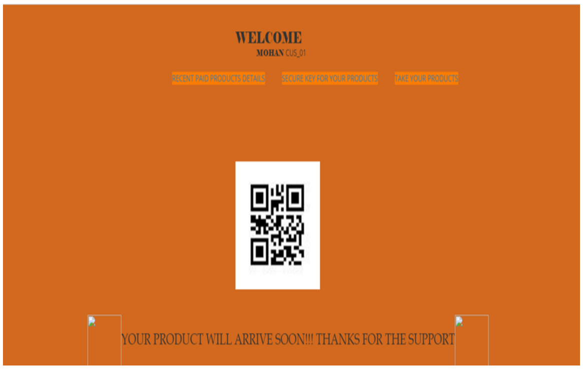


	Image	cusid	Product Amount	Product Id	CEO ID	Manager Id
Select		CUS_01	Coffee Cup.jpg	P0R0I0D01	C0E0O01	M0A0N0A01

ENTER CUSTOMER VERIFICATION ID:

Decrypt Here: Enter the key Product Id: Enter Product Id Ceo Id: Manager Id:

Fig.4.2 Distributor Product Delivery



YOUR PRODUCT WILL ARRIVE SOON!!! THANKS FOR THE SUPPORT

Fig.4.3 QR Code Generator

VII. CONCLUSION

This paper proposes a distributed block chain-based data protection framework for enhancing the data security of the modern power system against cyber-attacks. The proposed framework substantially enhances the self-defensive capabilities of power systems against cyber-attack by harnessing the distributed security features of block chain

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

technology first employed in the Bit coin crypto-currency. The proposed framework therefore represents a promising new direction in cyber-security for modern power systems. Key technical details are presented, Block chain technology innovation and comparisons are illustrated, and key implementation challenges are highlighted. We also present an efficiency evaluation of the proposed framework against cyber-attacks. Our work shows that block chain can be considered as a promising solution for the data security of the modern power system.

VIII. FUTURE ENHANCEMENTS

Improvements in the underlying block chain technology, including improvement of blocks' connection speed, acceleration of reliability and security, reduction of investment and risk, are expected to benefit block chain-based applications. As one concrete example, the so-called "Red Belly Block chain" can process 660,000 transactions per second on 300 machines in a single data center, whereas the Bit coin network is limited to around seven transactions per second. Future breakthroughs in block chain technology are to be anticipated, thereby enhancing industrial acceptance and deployment in practical power system settings. In future research, we will consider further refinement of the consensus algorithm, and perform an assessment of associated software and hardware investment costs vs. benefits.

REFERENCES

[1] F.F. Wu, K. Moslehi and A. Bose, "Power system control centers: Past, present, and future," Proc. IEEE, vol. 93, no. 11, pp. 1890–1908, 2005.

[2] F. Luo, J. Zhao, Z.Y. Dong, Y. Chen, Y. Xu, X. Zhang and K.P. Wong "Cloud-based information infrastructure for next-generation power grid: conception, architecture, and applications," IEEE Trans. Smart Grid, vol. 7, no. 4, pp. 1896–1912, Jul. 2016.

[3] NCCIC/ICS-CERT, "Cyber-attack against Ukrainian critical infrastructure," released 25 February 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [Accessed: 22 Jan. 2018].

[4] E-ISAC and SANS, "Analysis of the cyber attack on the Ukrainian power grid: Defense use case," released 18 March 2016. [Online]. Available: https://ics.sans.org/duc5 [Accessed: 22 Jan. 2018].

[5] G. Liang, S.R. Weller, J. Zhao, F. Luo and Z. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," IEEE Trans. Power Syst., vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM Trans. Inf. and Syst. Security (TISSEC), vol. 14 , no.1, May 2011.

[7] G. Liang, J. Zhao, F. Luo, S.R. Weller, and Z. Dong. "A review of false data injection attacks against modern power systems," IEEE Trans. Smart Grid, vol. 8, no. 4, pp. 1630 – 1638, Jul. 2017.

[8] R. Deng, G. Xiao, R. Lu, H. Liang and A.V. Vasilakos, "False data injection attack on state estimation in power systems – attacks, impacts, and defense: A survey," IEEE Trans. Industrial Informatics, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[9] O. Kosut, L. Jia, R.J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 645–658, Oct. 2011.

[10] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data injection attacks against power system state estimation: Modelling and countermeasures," IEEE Trans. Parallel Distrib. Syst., vol. 25, pp. 717–729, March 2013.

[11] V. Kounev, D. Tipper, A. A. Yavuz, B. M. Grainger, and G. F. Reed, "A secure communication architecture for distributed microgrid control," IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2484–2492, Sept 2015.

[12] Z. Lu, W. Wang, and C. Wang, "Camouflage traffic: Minimizing message delay for smart grid applications under jamming," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 31–44, Jan 2015.