https://dx.doi.org/10.22161/ijaers.6.4.46 ISSN: 2349-6495(P) | 2456-1908(O)

Transaction Security in Energy Trading System using Block chain

Mrs.Gunavathie.M.A[1], Sabitha Sree.K [2], Raageshwari.M [3], Keerthikaa.T [4], Divya.S[5]

[1] Assistant Professor in Department of Information Technology, Panimalar Engineering College, Chennai, India
[2,3,4,5] B.Tech, Department of Information Technology Panimalar Engineering College, Chennai, India

Abstract*— *Transaction Security (TS) is a framework that intercepts real-time Sales force events and applies appropriate actions and notifications based on security policies we create. In the earlier system of transactions all the nodes in the network are connected using centralized approach in which a node act as a server and all other nodes are connected to it. It is similar to client server model. All the information are stored in the centralized node. When the centralized node is been hacked by the hacker then it provides entire details about the transaction and doesn't provide enough security. Since the privacy of these data is very less we proposed to have more secured system. The proposed system uses a decentralized network that doesn't rely on a central point of control. A lack of a single authority makes the system fairer and considerably more secure using block chain and multi signature. A block chain is a public ledger of information collected through a network that sits on top of the internet. It is how this information is recorded that gives block chain its ground breaking potential and it is extremely important that the information being stored is honest and accurate. The main aim of this system is to provide transaction security without using a trusted third party since it reviews all the critical transaction communications between the parties, based on the ease of creating fraudulent digital content. This system provides high security and the hacker meets the difficulty level to retrieve the data..

Keywords*— *Block chain, Centralized node, Decentralized network, Multi signature Transaction Security, Trusted third party.

I. INTRODUCTION

A block chain consist of growing list of records called blocks, where each block contains cryptographic hash of previous block, timestamp and data which are connected to each other using cryptography. In general block chain doesn't allow the modification of data. It is a system that facilitates the transaction between two parties [1]. The introduction of the block chain for bitcoin solved the double-spending problem without the need of a trusted authority [2]. There are two types of block chain i) Public block chain ii) Private block chain where the private block chain is proposed for business use.The drawbacks faced in the existing system are as follows:

1. Capture the entire data- In the existing system all the details regarding the ownership of the transaction are stored in the database. Once the hackers enters the database he would capture the entire details.
2. High timestamp- Since for each transaction the nodes checks their previous history of stored transactions timestamp is merely high.

To overcome these drawbacks we proposed a system in which the transaction details stored in the database expires once the transaction gets completed. High security is employed in this system so that hacker meets difficulty level to retrieve the data.

II. RELATED WORKS

Sidharth Quamara[3] proposed the system to overcome the limitations associated with the conventional approach of bitcoin based electronic financial transactions. But this system had a drawback of inability of doing non-reversible payments for non-reversible services. Exploratory Simulation Models for Fraudulent Detection in Bitcoin System was proposed by Vincent Lee[4]. Their main objective is to identify one of the possible method of double spending under the circumstance that the network connection status is not stable. The main drawback of this system is that it is expected to replace the traditional currencies among online transactions. Building on that, we believe that the security issues during Bitcoin payment must be put in high priority.

An improved approach has been put forth by Haozheng Wei[5] called Coin Express which aimed to achieve outstanding payment acceptance ratio with low routing overhead. This system failed because all transactions via a channel are stacked, and will be jointly published to the public block chain upon channel expiration. The next approach proposed by Ravi Vatrapu[6] aimed in using supervised learning techniques for appropriate classification of the Bitcoin entities. The main drawback faced by this system is pseudo-anonymity. Krishnan Kanoorpatti[7]designed a new

https://dx.doi.org/10.22161/ijaers.6.4.46 ISSN: 2349-6495(P) | 2456-1908(O)

system to analyze the complete process of transaction of Bitcoins and anonymity that lies in that process. This approach failed because while downloading the Bitcoin wallets to the devices, they install software which is either a web wallet that is found in the host or a mobile wallet that is found in smart phone devices

Filip Caron[8] described a system that operate a diverse set of payment systems that facilitate these transfers of funds according to formal arrangements and standardized rules. This failed to meet the specifications of guaranteeing an orderly and timely settlement of wholesale payments is crucial for the wellbeing of financial markets. Dimaz Ankaa[9] Wijaya revised this system and put forth a system to extend the functionality of asset management systems which are limited to a maximum of80 bytes data. This system faced a limitation where there is no central controller in Bitcoin as in flat monetary system and therefore it employs cryptographic technique to verify the validation of the transaction.

An advanced system that facilitated single-fee micropayment protocol that aggregates multiple smaller payments incrementally into one larger transaction needing only one transaction fee was put forward by H.Robert[10]. This system failed because many low-value payment applications will suffer from the high transaction fee currently present in the bitcoin network. To reduce the complexity in purchase between customer and the traders a new system called BPCSS was introduced by Chia-Hui Wang[11] where all the details were stored in the cloud database for easy retrieval. But this system too failed because storage space is high. All these drawbacks has been overcome and Nurzhan Zumbabekuly Aitzhan[12] proposed a system that provides transaction security without using trusted third party. But this system faced the drawback of having high timestamp and when the hacker hacks 50% of the network the entire details will be known to the hacker. The modified password generation and storage method paved the way for providing high transaction security in the energy trading system.

III. PROPOSED SYSTEM AND CORE COMPONENTS

3.1. Proposed system

The earlier system using block chain were developed to overcome the security issues related to the traditional transaction processing system. The cryptographic proof of work has been introduced to provide basic security to the system. But it failed in providing non-reversible payment for non-reversible services. Later the system developed doesn't meet the user specifications it was able to find only the cause of double spending attack but couldn't find a perfect solution to it. Few years later system with supervised learning techniques were developed. Unfortunately due to the inclusion of these additional features they failed to meet major issue of pseudo anonymity.

Then a cloud database has been setup to store the details of the customer who perform the transaction. Keeping this as a scratch Aitzhan designed a system in which each time when a transaction enters the network all other nodes in the network checks the previous available history of the transaction which resulted in high timestamp. And when the hacker successfully enters the network he could capture the entire transaction details of all the user. So there is no transaction security. To overcome all these above problems we have designed a system that provides high transaction security without using a trusted third party and multisignature. The timestamp is highly reduced in the system since there is no need of accessing the database each time when transaction enters into the network. The password stored in the database expires once the transaction is completed.

3.2. Core Components

The proposed system is implemented in such a way that it has four important modules:

i)Fragmentation of the transaction ii) Signing of packets by all the nodes iii) Hacker identification and notification iv) Reassembly of packets.

Our system constitutes of 4 nodes and 1 server. The overall project is implemented using Net beans Integrated Development Environment (IDE). We have also used MySQL as backend to store the passwords that are created by the user. The Graphical User Interface (GUI) is created in such a way that the transaction can be selected by the user. First the connection has to be established. As soon as the sender browses the transaction the path of the transaction is displayed and the user sets the password for the entire transaction. Then it is fragmented into packets using file hashing algorithm. Then a key is generated using AES algorithm in which the length of the key is 4.

Once the transaction is fragmented it is sent through the router. The fragments are signed by all the nodes in the network implementing the concept of multi signature using DSA algorithm. After the completion of this process the number of packets and the encrypted format are displayed in the side pane. The fragments passing through each node can be viewed if the right password is entered. The user is given 2 attempts if he enters the wrong password. If it is repeated for the third time then the user will be identified as a hacker and notified to the sender. This will be acknowledged to the user by turning green to red light. This information passes through all the nodes in the network.

At the destination node the total number of packets reached the destination is displayed. Also the number of packets flowed through each node is also displayed in the overall window where the active nodes and hacker nodes

https://dx.doi.org/10.22161/ijaers.6.4.46 *ISSN: 2349-6495(P) | 2456-1908(O)*

are displayed. Then finally reassembly occurs at the destination node using sequence number and when the right password is entered the entire file will be retrieved. We provide a webpage in which a button is displayed. Once the button is clicked the entire path through which the packets travels from source to destination is displayed. The entire proposed system is designed as shown in Fig 3.2.

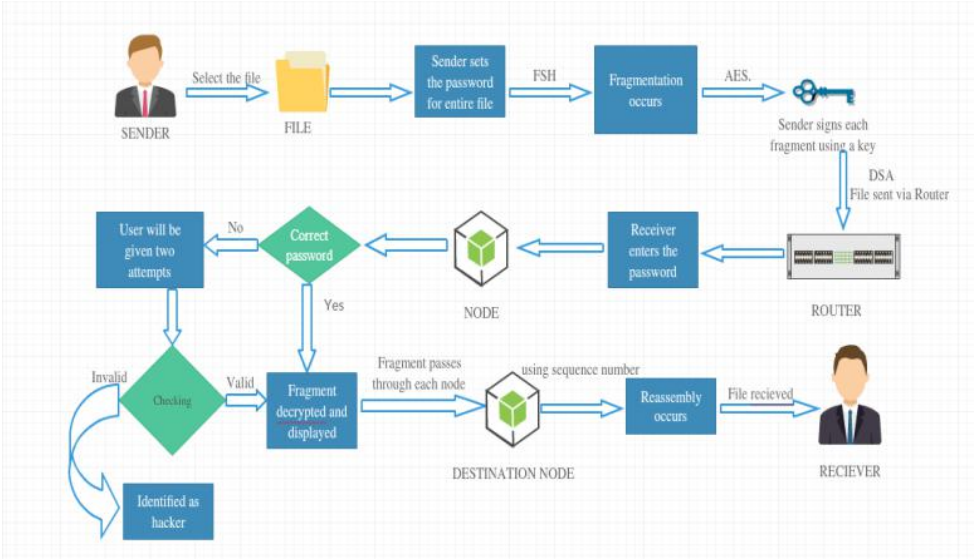

Fig. 3.2: Architecture Diagram

3.3. Algorithms Implemented

3.3.1. Fragmentation of transaction

Once the sender browses the transaction it is divided into fragments using file hashing algorithm. The algorithm is explained below

File Hashing Algorithm

File hashing module generates two random keys from the main key. It divides the key bits into half i.e. if key is of length n then the generated random two keys will be of length n/2. The pseudo code is given below:

Step1: Select the input as n bit key

Step2: Key1 and Key2 is set as n/2 bit value and it is initialized to 0

Step3: Random function is initialized with seed value. 323

Step4: Initialize length as n, x=0, y=0, flag=0.

Step5: While (length != 0)

5.1: If Flag==0 then

Find a randomly unused bit position.

Find out the value at that bit position in main key.

If value at that bit position is 1 then

The x'th bit of key1 is set as 1 and x value should be incremented

else

The x'th bit of key1 is set as 0 and x value should be incremented

Set Flag=1, Set the above found bit position is used.

Go to Step 5.3

5.2: Else

Find a unused bit position.

Find out the value at that bit position in main key.

If value at that bit position is 1 then

The x'th bit of key2 is set as 1 and y value is incremented.

Else

The x'th bit of key2 is set as 0 and y value is incremented.

Set Flag=0, Set the above found bit position is used.

Go to Step 5.3

5.3: Decrement the Length;

5.4: Go to step 5

Step6: Return the keys key1 and key2 of size n/2.

3.3.2. Key Generation

To encrypt all the fragmented packets a key is generated using Advanced Encrypted Standard Algorithm. The algorithm is explained below in Fig 3.3.2

AES Algorithm

https://dx.doi.org/10.22161/ijaers.6.4.46 ISSN: 2349-6495(P) | 2456-1908(O)

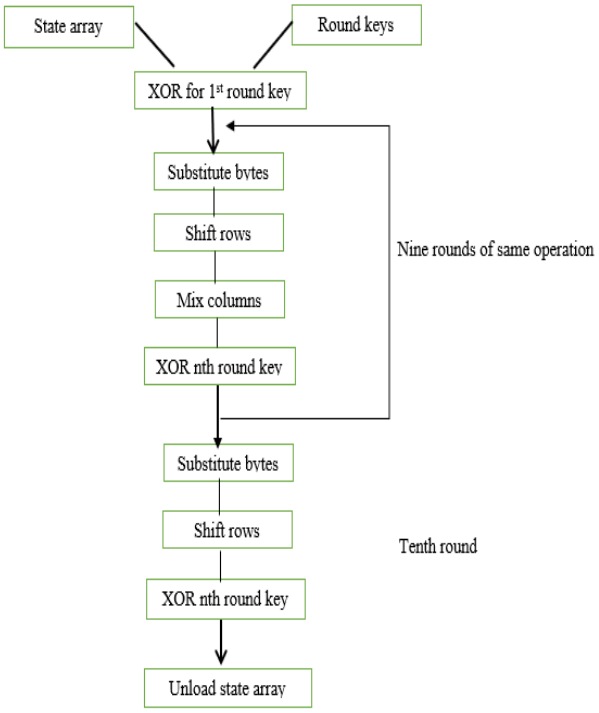

Fig 3.3.2: AES Algorithm Steps

Step1: A set of round keys should be obtained from the cipher key.
Step2: State array is initialized with the plain text.
Step3: Initial round key is added to the starting state array.
Step4: Nine rounds of state manipulation is performed.
Step5: Finally tenth and final round of state manipulation is performed.
Step6: Encrypted cipher text is the contents of final state array.

3.3.3. Signing of packets

Once the key is generated it is signed by all the nodes in the network using Digital Signature Algorithm. Now all the packets remain in encrypted form. The algorithm is explained below in Fig 3.3.3

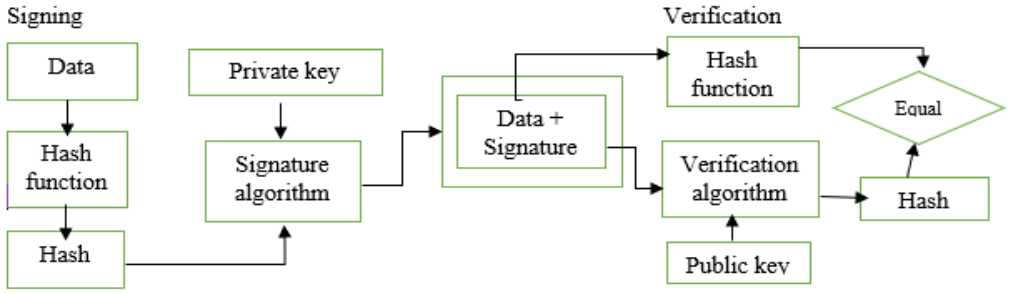

Fig.3.3.3: Digital Signature Generation and Verification

Digital Signature Algorithm

Signature Generation

INPUT: Global parameters (p, q, g); sender's private key a; message M, h = Hash(M).
OUTPUT: Signature (r, s).
Step1: Choose a random integer k in the range [1, q − 1].
Step2: Calculate $X = g^k \bmod p$ and $r = X \bmod q$. If r = 0 go to step 1.
Step3: Calculate $k^{-1} \bmod q$.
Step4: Compute h = Hash(M).
Step5: Compute $s = k^{-1}(h + ar) \bmod q$. If s = 0 go to step 1.
Step6: Return (r, s).

Signature Verification

INPUT: Global parameters (p, q, g); sender's public key A; message, M, with message digest h = Hash(M); signature (r, s).
OUTPUT: "Valid" or "Invalid".
Step1: Verify that r and s are in the range [1, q − 1]. If not then return "Invalid" and exit.
Step2: Calculate $w = s^{-1} \bmod q$.
Step3: Compute h = Hash(M).
Step4: Calculate two componenets $x_1 = hw \bmod q$ and $x_2 = rw \bmod q$.
Step5: Compute $X = g^{x_1}A^{x_2} \bmod p$ and $v = X \bmod q$.
Step6: If v = r then return "Valid" else return "Invalid".

IV. IMPLEMENTATION

This system is implemented using NetBeans IDE. It is depicted using 4 nodes that are connected in the block chain and 1 server from which the instructions are passed

https://dx.doi.org/10.22161/ijaers.6.4.46 *ISSN: 2349-6495(P) | 2456-1908(O)*

to the network. MySQL acts as a backend which is used to store the passwords for the particular transaction. The hacker can be identified in at node at a time. The implementation of modules are discussed below:

4.1. Connection Establishment

This is to ensure that whether all the nodes in the network are connected to the server. Initially connect the server and all the nodes in the network using its IP address. To ensure this all the active nodes are represented using green light as shown in Fig 4.1.

Fig 4.1: General structure of all nodes

4.2. Fragmentation and Signing of Packets

Once all the nodes are connected the sender determines the transaction and it is divided into fragments using file hashing algorithm. The sender selects the destination. Once the destination is selected the sender sets the password for overall transaction. Keys are generated for each fragment using AES algorithm. After the key is generated all the nodes in the network signs the fragment with the key generated using Digital Signature algorithm implementing the concept of multi signature. As a result all the packets will remain in encrypted form. Once the transaction reaches the destination successfully tick mark appears as shown in Fig 4.2.

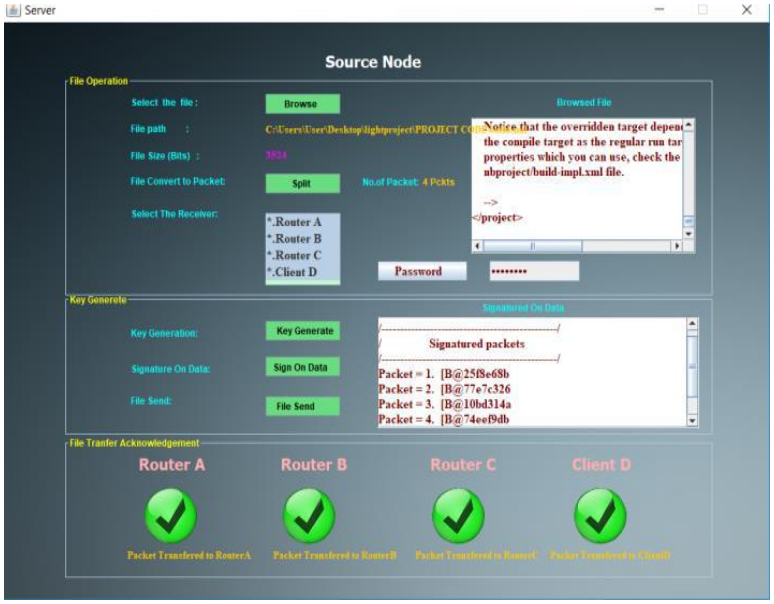

Fig 4.2 : Fragmentation and Signing of packets

4.3. Privilege provided to the user

In each node the receiver should enter the password to see the particular fragment flowing through it. When the receiver enters the right password the fragment will be displayed as shown in Fig 4.3 else the user will be given 2 attempts for the wrong password. If the user enters wrong password for the third time the user will be identified as hacker and will be notified to the sender by changing the colour of active node from green to red as shown in Fig 4.3.1.

https://dx.doi.org/10.22161/ijaers.6.4.46 ISSN: 2349-6495(P) | 2456-1908(O)

Fig 4.3: Node represented when right password is entered

Fig 4.3.1: Representation of node when hacker is identified

4.4 Receiving of packets:

Once all the packets are received at the destination and the receiver enters the right password the entire transaction will be received at the destination node and the total number of packets received is also displayed as shown in Fig 4.4.

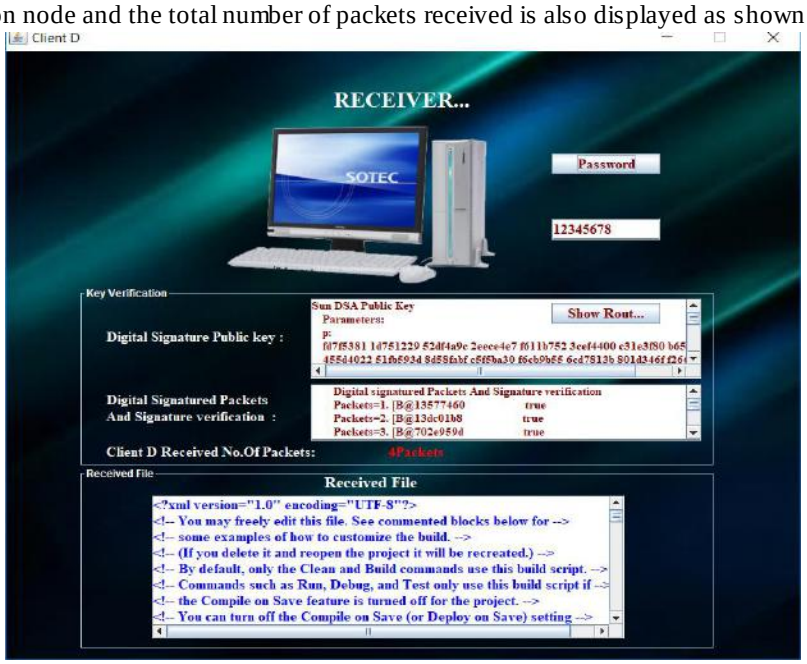

Fig 4.4 : Destination node structure

https://dx.doi.org/10.22161/ijaers.6.4.46 ISSN: 2349-6495(P) | 2456-1908(O)

4.5 Displaying the path

Once the file is received we need to start the server to view the path in which the packet is transferred.

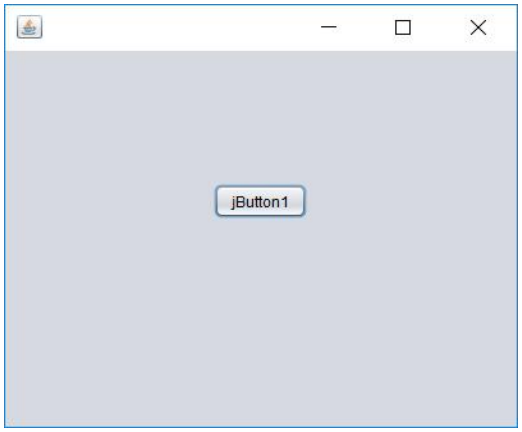

Fig 4.5: Graph button

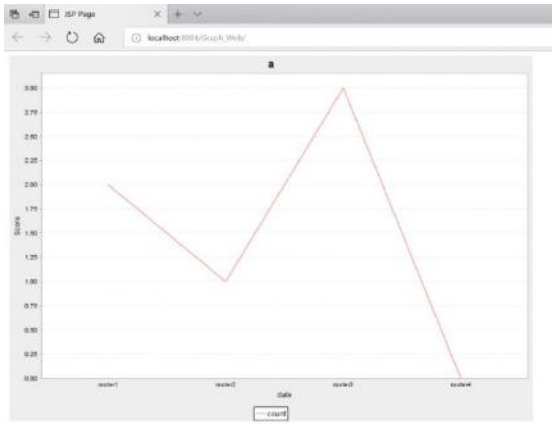

Fig 4.5.1: Path in which the packet is transferred

V. RESULTS AND DISCUSSION

It is found that in the existing system of block chain the transaction security is very less and the probability of hacking is extremely high. The key generated for the transaction are stored in the database and this paved the way for the hacker to completely steal the data. Most of these systems were not decentralized and hence central node failure causes the entire system to be collapsed. In our proposed system the chance of hacking is completely avoided since their entry is identified and reported to the sender so there is no way for the hacker to enter into the network. All the passwords for the particular transaction stored in the database expires after the completion of the transaction. Also it doesn't limit the amount the data to be transferred. It protects against the overflowing of data. Since the hacker entry is detected it is immediately notified to the sender thus this system provides high transaction security without using trusted third party.

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we have proposed a energy trading system that provides high transaction security without using trusted third party. The technique efficiently combines AES and DSA to sign the packets to exploit their complementary strengths. It consists of four main elements: password generation, fragmentation and signing, Password attempts and Reassembly. The overall password for the entire transaction is set by the sender. The experimental outcomes advised that an overall password and hacker notification gives high security because all the data is in encrypted form and will be decrypted only when the receiver enters the correct password and if number of attempts increases by 2 the user will be identified as hacker and notified to the sender. As a result of accuracy comparison proposed method have 98% accuracy, that is it have 6% more than existing method. Thus this systemis proved to be the best method adopted for secured electronic transactions.

For future work, we plan to work towards various directions. In the future mode of project we have planned to combine Artificial Intelligence (AI) in which the number of packets that can be split will be estimated before. The arrival of any unauthorized user will be automatically detected by intelligence without the attempts provided when the user enters the wrong password.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"2008.
[2] J. Warren, "Bitmessage: A peer-to-peer message authenticationand delivery system," 2012.
[3] Sidharth Quamara,, " Bitcoins and secure financial transaction processing, recent advances", 2016.
[4] Vincent Lee ,"ExploratorySimulation Models for Fraudulent Detection in Bitcoin System", 2016
[5] Haozheng Wei"Coin Express," 2016.
[6] Ravi Vatrapu," A First Estimation of the Proportion of Cybercriminal Entities in the BitcoinEcosystem using Supervised Machine Learning",2017.
[7] Krishnan Kanoorpatti,"A critical review of Bitcoins usage by cybercriminals",2017.
[8] Filip Caron," The Evolving PaymentsLandscape",2017.
[9] DimazAnkaa,"Extending Asset Management System Functionalityin Bitcoin Platform",2017.
[10] H.Robert,"Thing-to-Thing Electricity Micro Payments UsingBlockchain Technology",2018.
[11] Chia-Hui Wang,"Blockchain-based Payment Collection SupervisionSystem using Pervasive Bitcoin Digital Wallet",2018.

https://dx.doi.org/10.22161/ijaers.6.4.46 ISSN: 2349-6495(P) | 2456-1908(O)

[12] NurzhanZumbabekulyAitzhan,"Security and privacy in energy trading system using block chain, multisignature and anonymous messaging stream",2018
[13] NIST, "Introduction to NISTIR 7628 guidelines for smart gridcyber security," 2010.
[14] Moise and J. Brodkin, "ANSI C12.22, IEEE 1703, and MC12.22transport over IP," 2011.
[15] F. Mendel, T. Peyrin, M. Schläffer, L. Wang, and S. Wu,"Improved cryptanalysis of reduced RIPEMD-160," in Proc. Int.Conf. Theory Appl. Cryptology Inf. Secur., 2013, pp. 484–503.
[16] Y. Sasaki, L. Wang, and K. Aoki, "Preimage attacks on 41-stepSHA-256 and 46-step SHA-512," IACR Cryptology ePrint Archive,vol. 2009, 2009, Art. no. 479.
[17] Biehl, B. Meyer, and V. Meuller, "Differential fault attacks onelliptic curve cryptosystems," in Proc. Annu. Int. Cryptology Conf.,2016, pp. 131–146.
[18] Extance, "The future of cryptocurrencies: Bitcoin and beyond,"Nature, vol. 526, pp. 21–23, 2015.
[19] M. Mihaylov, S. Jurado, K. Van Moffaert, N. Avellana, and A.Nowe, "NRG-X-change—A novel mechanism for trading of renewable energy in smart grids," in Proc. SMARTGREENS, 2014,pp. 101–106.
[20] G. Acs and C. Castelluccia, "I have a DREAM! (DiffeRentiallyprivatEsmArt Metering)," in Information Hiding. Berlin, Germany:Springer, 2011, pp. 118–132.