Vol. 1(4), pp. 130-138, 3 FEB, 2016
ISSN Print : 2454-1435 © 2015 IJRMMAE
ISSN Online : 2454-1443 © 2015 IJRMMAE
http://www.ijrmmae.in

International Journal of Research in Mechanical, Mechatronics and Automobile Engineering

DECENTRALIZED SECURITY MODEL BASED ON ETHEREUM NETWORK WITH SMART CONTRACT BLOCKCHAIN ECOSYSTEM FOR VEHICLES BATTERY SWAPPING

B. Jareena Banu 1, *, S. Nallusamy 2, M. Saravanakumar 3

[1] Lecturer, Department of Instrumentation and Control Engineering, Dr. Dharmambal Government Polytechnic College for Women, Tharamani, Chennai-600113, Tamilnadu, India
[2] Department of Mechanical Engineering, [3] Department of Computer Science Engineering, Dr. M G R Educational and Research Institute, Chennai- 600095, India

[1,] *e-mail: jareenabanu67@gmail.com, [2] e-mail: ksnallu@gmail.com,
[3] e-mail: navarasamblue@gmail.com

Abstract

The aim of this research article is to propose a decentralized security model based on the Ethereum network and smart contract in the blockchain ecosystem for vehicle battery swapping. Battery swapping is an effective approach in supplying power to the electric vehicles, while mitigating long waiting times in a battery charging station. For electric vehicles owners, the battery information and transaction's correctness, openness, traceability and immutability is difficult to get guarantee in traditional centralized system. Blockchain technology is one of solutions because it embraces a decentralized system and the entire database is owned by many users. All key logics are driven by smart contracts. The battery registration and battery assignment between electric vehicles owners and charging station are realized by smart contracts automatically and accurately. The smart contract is deployed and tested in the Ethereum consortium blockchain network in azure cloud. A primary prototype based on Ethereum is analyzed and implemented to illustrate the feasibility of managing battery swapping based on blockchain system.

Keywords: Ethereum Network, Blockchain Ecosystem, Vehicle, Battery, Smart Contracts

INTRODUCTION

In the present scenario, the trust lacking between electric vehicles owners and swapping station is caused, and becomes a big challenge to electric vehicles rapid development. The Indian government has talked about the importance of electric vehicles, and about making India a fully electric nation in the years to come, but the task of getting there involves a number of challenges. In last decades, with the increasing development of battery technologies and concerns for the environment, Electric Vehicles (EV) technologies got rapid development. Large-scale utilization of EV not only makes deep cuts in the release of greenhouse gases, but also reduces

the fuel cost for EV drivers. However, EV drivers have to face the problem of battery refueling on a daily basis. Once the battery runs out, electric vehicle drivers are able to swap a depleted battery for a fully charged one provided by the charging station and eliminate much of the waiting time. How to ensure the fairness and justice about battery swapping procedure is the most important issue. In this paper we proposed a solution using blockchain, a distributed secure and private ledger of blocks to address the trust issues for electric vehicle battery swapping application. In the battery swapping process the most important transaction is the battery assignment between the EV owner and charging station owner. In the traditional centralized system, all information about battery and transaction were stored unilaterally in central servers. Some of the problems that can occur in traditional centralized systems are with an organization that has full control over the database and system it is possible to tamper with the database of considerable opportunities. Blockchain technology is one of solutions because it embraces a decentralized system and the entire database is owned by many users.

LITERATURE REVIEW

Blockchain was first introduced in Bitcoin, which is a distributed crypto currency system allowing users to exchange coins in an anonymous manner. Each block contains a number of transactions, and chains together using the previous block's hash value. This kind of structure makes transactions immutable. A blockchain is basically a decentralized, distributed ledger of all the transactions or events which takes place only after involving multiple parties. It ensures high level of security as the transaction which takes place is entirely anonymous. Each transactions or digital events taking place in a blockchain network is verified, only if it is agreed upon by the consensus of the majority party of the users participating in this process [1-4]. All data will be duplicated and stored in every node. Hence if hackers want to modify one transaction, they must modify all the subsequent blocks with huge majority collisions in network. All the system participants collaboratively maintain blockchain through verifying and storing new transactions into blocks. A transaction is verified by reviewing its signature and checking the previous transaction on the same block. Once verified, the transaction will be added to a block. Once the block size reaches the present value, the miner of the blockchain network will execute a consensus algorithm to generate a new block. Proof of Work (PoW) and Proof of Stake (PoS) are the most popular consensus algorithms. In blockchain, users only show public key to others. So users have anonymous identities. Network participants can use the accordingly public key to verify a transaction and meanwhile protect the privacy. In conclusion, blockchain provides an elegant way to achieve decentralization, makes sure that all transactions are believable and also protects user's privacy [5-8].

Like bitcoin, Ethereum is a distributed public blockchain network. Although there are some significant technical differences between the two, the most important distinction to note is that Bitcoin and Ethereum differ substantially in purpose and capability. Bitcoin offers one particular application of blockchain technology, a peer to peer electronic cash system that enables online Bitcoin payments. Ethereum blockchain focuses on running the programming code of any decentralized application. In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn a type of crypto token that fuels the network. Beyond a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network. Smart contracts are executable codes to express logic of transactions in blockchain, such as solidity format in Ethereum [10-

14]. Ethereum blocks thus contain both smart contracts and the final state produced by executing those contracts. The contracts themselves are stored in the blockchain as byte-code instructions for the Ethereum Virtual Machine (EVM). Several higher-level languages like solidity are available for writing smart contracts [15-17]. Typically, after all the parties have signed it, smart contract will be attached to the blockchain in the form of program code such as a record of bitcoin trading data. After P2P network propagation and validated by receiving nodes, smart contract will be deployed into a specific block on the blockchain. Blockchain can monitor the status of smart contracts in real time. By examining the external data source and make sure specific conditions are triggered, smart contract will be activated and executed.

This section discusses the existing, related work in the management of EV charging issues and the state-of-the-art blockchains. After sweeping over the financial industry, blockchain becomes popular in energy industry. Many blockchain applications have been proposed by energy sectors, such as power purchasing, coal and solar-power trading [18-20]. These applications provide environmental protection and create new business opportunities.

In a decentralized control strategy is proposed to reduce the price of recharging. In a secure energy trading system is proposed in the Industrial Internet of Things (IIoT) to support fast and frequent energy trading. An optimal pricing strategy using the Stackelberg game is also proposed. Considering that the waiting time can be a non-negligible portion of the total work hours, several mechanisms are proposed to reduce the EV driver's wait time at charging stations [21-23]. In a real-time charging station recommendation system for electric vehicle taxis using large-scale GPS data mining is proposed, which provides suggestions for EV taxi drivers and allows them to make their own choices. Different from the above mechanisms, this paper aims to study the feasibility of battery swapping in electric vehicles using the blockchain technology. We propose a new method to solve the problems about the fairness and justice of trade procedure, as well as the trust issue of battery information.

DEVELOPING ATMOSPHERE

The smart contract is deployed on the private Ethereum blockchain network created on Microsoft azure cloud platform. Figure 1 shows the Ethereum consortium network architecture on azure. The network created using Azure Consortium Blockchain template consists of shared transaction nodes and mining nodes. Transaction nodes maintain a copy of the distributed ledger. User application will interact with transaction nodes for any operation like submit transaction etc. For each consortium member and a specified number of mining nodes are created. Mining nodes record all the transactions being executed within the network.

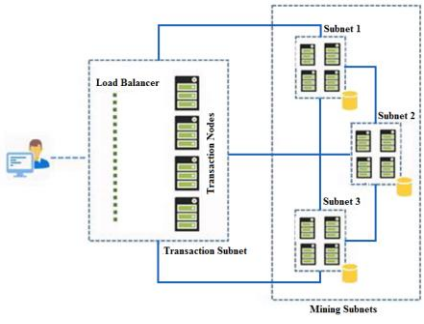

Figure 1. Ethereum Consortium Network Architecture

Transaction Nodes: All consortium members share a set of load-balanced transaction nodes. These nodes are reachable from outside the virtual network so that applications can use these nodes to submit transactions or execute smart contracts within the blockchain networks. All nodes have the latest stable Go Ethereum (Geth) client software and are configured to maintain a complete copy of the distributed ledger. These nodes use the same Ethereum account, protected by the Ethereum account password provided.

Mining Nodes: Mining nodes assigned to a member are kept in a separate subnet. Nodes in individual subnets communicate with each other by application gateways. As members need to record transactions, mining subnet is also facilitated with storage. As it is a private network, inbound traffic is not allowed on mining nodes. Nodes communicate with each other using Ethereum's Discovery Protocol. Go Ethereum client software (Geth) is installed on each mining node. Software is configured to enable these nodes to bemining nodes. These nodes use the Ethereum address of the default account, termed as coin base. When mining nodes mine the block, mining reward is added to this account. Mining nodes communicate with other mining nodes to come to the consensus on the state of the underlying distributed ledger. In the cloud we created one transaction node and two mining nodes. After creating the Ethereum consortium network on the azure, we can see the three important configuration information's. Figure 2 shows the configuration information for the blockchain. The configuration information is described below.

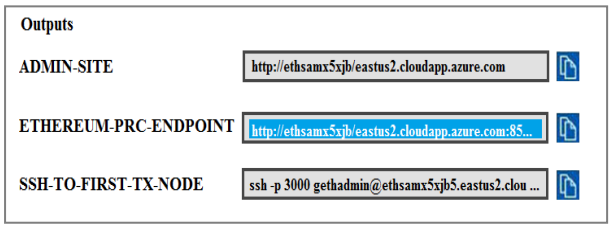

Figure 2. Configuration Information

SYSTEM MODEL

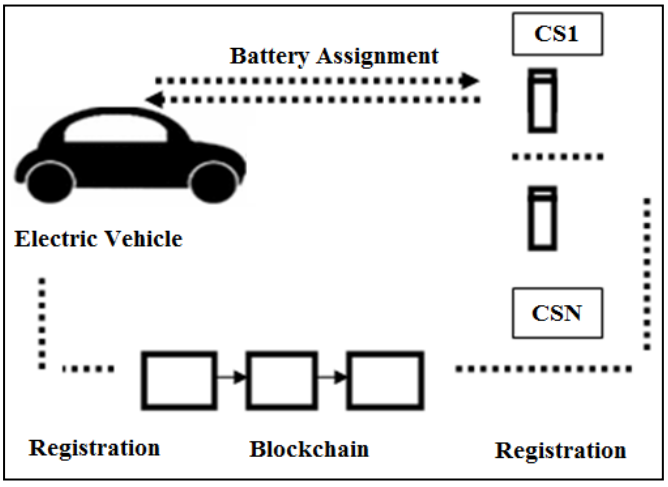

Figure 3. Battery Swapping Model

Admin Site: A website we can navigate to showing the status for the nodes on the Ethereum network

Ethereum-RPC-Endpoint: An endpoint for connecting to the Ethereum network via an API like web3 js.

Ssh-to-first-tx-node: To interact with the blockchain, we can log in using SSH client.

The smart contracts are deployed on the Ethereum network through the RPC endpoint. The corresponding block updation details can be viewed by opening the admin site in the browser**.** The model given in the Figure 3 consists of mainly two phases, registration phase and battery assignment phase. In the registration phase EV owner submits the battery id and other information related to battery like battery State of Charge (SOC) and State of Health (SOH) etc to the blockchain. Similarly charging station owner will also submit his battery id details to the blockchain. The charging station owner can have multiple batteries. In the battery assignment phase, EV owner will choose the charging station and assign the depleted battery to the selected charging station. Each EV owner will have unique id. After submitting the discharged battery EV owner can query the charging stations to get the details of batteries of charging station owner. The charging station will assign the fully charged battery to EV owner. Each transaction is stored as transaction ids in the blockchain. The user can refer back to the transaction with these transaction ids..The transaction ids are hash values. If an attacker tries to manipulate the transaction details it will be impossible. Because blockchain, which records some or all of the recent transactions. Once completed, a block goes into the blockchain as a permanent database. Every block contains a hash of the previous block. The blockchain has complete information about different user addresses and their transactions right from the genesis block to the most recently completed block. The completed transaction is recorded into blocks and eventually into the blockchain, where it's verified and relayed by other users. On an average, a new block is appended to the blockchain every ten minutes through mining.

Deployed Environment: A real and available blockchain environment is generated for our demonstration. We have achieved three Ethereum nodes as the private blockchain network. In three nodes, there are two miners and one transaction nodes. Mining node mines blocks for the network, meanwhile Remote Procedure Call (RPC) nodes support RPC service for frontend user interface (UI).

SMART CONTRACTS DEPLOYMENT

Smart Contract is just a phrase used to describe computer code that can facilitate the exchange of money, content, property, shares, or anything of value. When running on the blockchain a smart contract becomes like a self-operating computer program that automatically executes when specific conditions are met. Because smart contracts run on the blockchain, they run exactly as programmed without any possibility of censorship, downtime, fraud or third party interference. Smart contracts are written in solidity programming language. The contract for the above swapping process is named as swap. The swap contract consists of three data structures to store the details of battery information, EV owner and the charging station owner details. We will write mainly three methods to process the transactions. The three methods are for battery registration, battery retrieval and battery assignment. The smart contract is deployed on the real blockchain network

created on the azure cloud. Ethereum comes with a handy JavaScript library called web3.js which connects to the blockchain node. An ubuntu virtual machine created inside the cloud is used for smart contract deployment and compilation. We can access the ubuntu virtual machine by opening the terminal. To compile the solidity code, we will first install npm module called sole. We will use this library within a node console to compile our contract. web3js is a library which lets us to interact with the blockchain through RPC.

We are deploying the smart contracts into the network using the RPC endpoint mentioned in the Figure 2. We will use that library to deploy our application and interact with it. After the compilation we can view the two important fields which are, byte code and abi interface. Bytecode is the code which will be deployed to the blockchain. Abi interface is an interface or template of the contract (called abi) which tells the contract user what methods are available in the contract. Whenever we have to interact with the contract in the future, we will need this abi definition. There are hundreds of thousands of contracts deployed on the blockchain. So each contract in the blockchain is identified by the deployed contract address and abi definition. The UI for battery swapping process is hosted on the public IP of the ubuntu virtual machine inside the cloud. Whenever the transaction is completed, the block number will get updated. The block updation can be viewed by opening the admin site as shown in the Figure 2. The block is updated within two seconds.

RESULTS AND DISCUSSION

This section discusses the sample UI created for interacting with the smart contracts in the blockchain. The index page consists of three buttons as shown in the Figure 4.

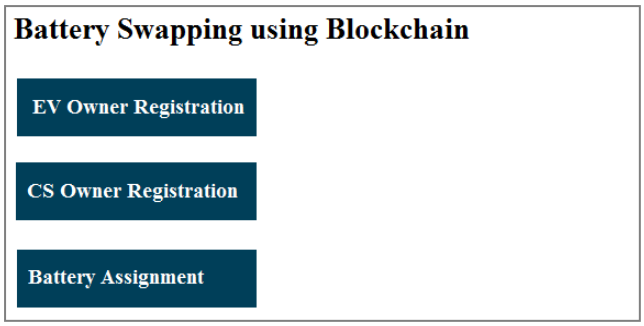

Figure 4. Index Page for Battery Swapping

The EV owner and charging station owner can choose the corresponding button in the index page for the battery registration. As shown in the Figure 5 the EV owner can enter their battery information in the respective fields. Similarly the charging station owner can also enter the details in his corresponding page. The charging station owner will have multiple batteries as shown in Figure 6. In the battery assignment page the EV owner can choose the charging station. We considered the case of three charging stations. Among the three stations EV owner can choose one station and enter the battery id of discharged battery that he wants to swap. As shown in the Figure 7 EV owner can click the assign button and initiate the swapping process.

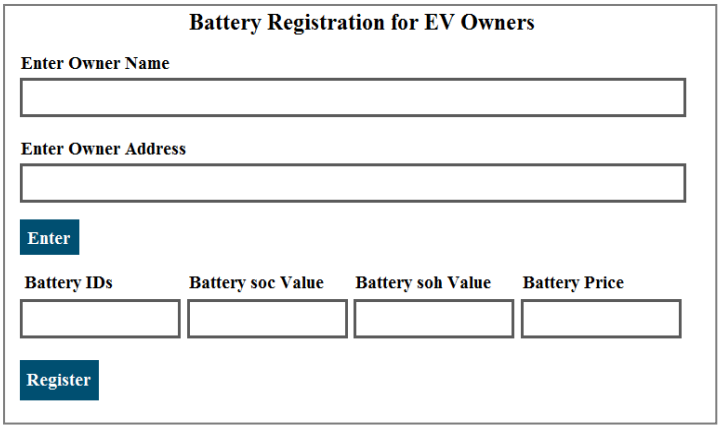

Figure 5. Registration Page for EV Owners

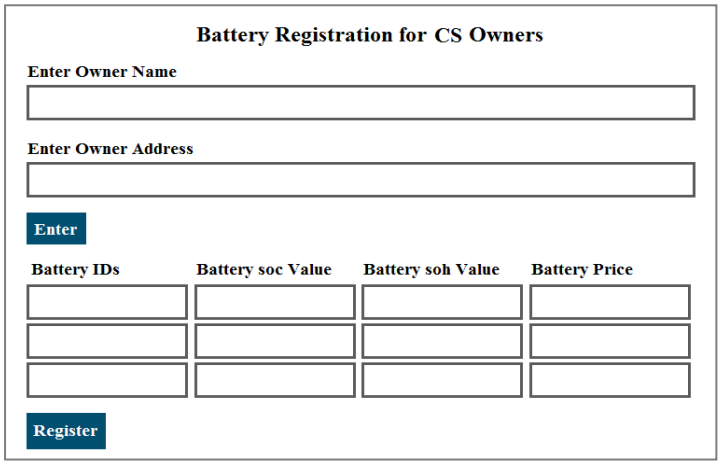

Figure 6. Registration Page for Charging Station

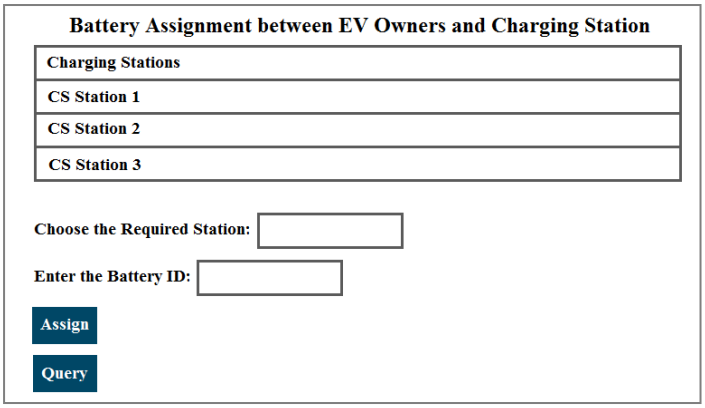

Figure 7. Battery Swapping Page for EV Owners

On clicking the query button EV owner can check the details of each charging station. Figure 8 shows the battery detail page of charging station. On clicking the remove button the charging station will assign fully charged battery to the EV.

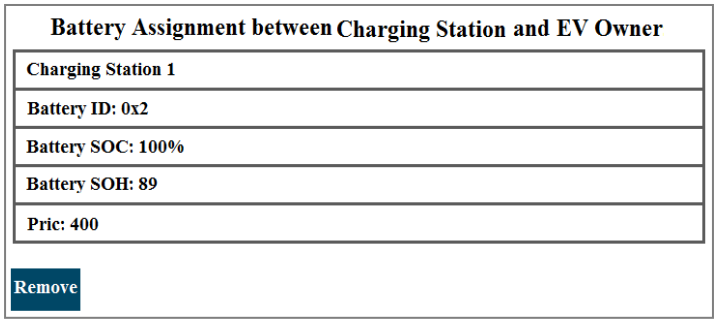

Figure 8. Battery Detail Page of Charging Station

The transactions are recorded on the blockchain. On each transaction the block will update. Figue.9 shows the block updation details on the azure. We can see the corresponding Ethereum nodes that we created. The blocks will get updated in every two seconds.

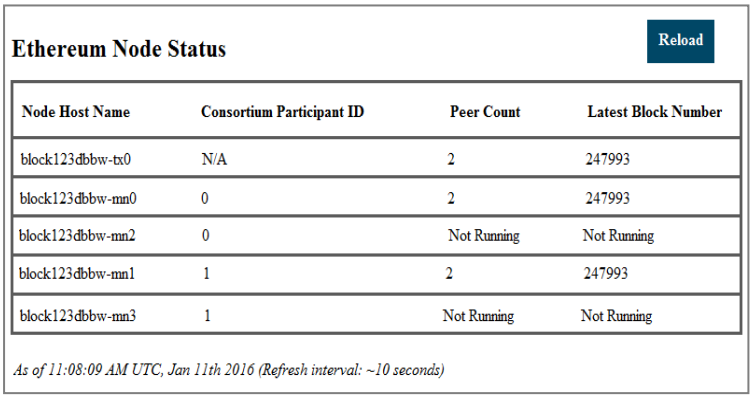

Figure 9. Change in the Block Number after Transaction

CONCLUSION

A blockchain based decentralized application for battery swapping is proposed. Battery related operations are implemented with smart contract. Besides that, information of battery is stored in blockchain network, keeping data immutable and traceable. These data are public to both EV owners and stations, to check the status of battery. As a result, it ensures fair transactions between trustless EV owner and station operator. The blocks will get updated without any delay. However, there are some aspects we have not considered very well. In blockchain, each battery has a unique virtual identification. All information related with the battery has been mapped to its virtual ID. Ideally, each battery can be attached with radio-frequency identification in physic world. Future work will be on integrating the batteries radio-frequency identification information on the Ethereum blockchain.

REFERENCES

1. H. Lee, K. Shin and D.H. Lee, “PACPs: practical access control protocols for wireless sensor networks”, Consumer Electronics, IEEE Transactions, 58(2), 2012, 491-499
2. A.G. Boulanger et al., “Vehicle electrification: Status and issues”, Journal, Proceedings of the IEEE, 99(6), 2011, 1116-1138

3. Debnath, Singaravelu and Verma, “Privacy in wireless sensor networks using ring signature”, Journal of King Saud University Computer and Information Sciences, 26(2), 2014, 228-236
4. D. Sobya, “Discrete wavelet transform for image compression and reconstruction via VLSI”, International Research Journal in Advanced Engineering and Technology, 1(1), 2015, 31-35
5. M. A. Ortega-Vazquez, F. Bouffard, and V. Silva, “Electric vehicle aggregator/system operator coordination for charging scheduling and services procurement”, IEEE Transactions on Power Systems, 28(2), 2013, 1806-1815
6. P. Zeng, K.K.R. Choo and D.Z. Sun, “On the security of an enhanced novel access control protocol for wireless sensor networks”, Consumer Electronics, IEEE Transactions, 56(2), 2010, 566-569
7. S. Sicari, L.A. Grieco, G. Boggia and A. Coen Porisini, “DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks”, Journal of Systems and Software, 85(1), 2012, 152-166
8. Y. Yao, J. Liu and N.N. Xiong, “Privacy preserving data aggregation in two-tiered wireless sensor networks with mobile nodes”, Sensors, 14(11), 2014, 174-194
9. X. Liu, “A survey on clustering routing protocols in wireless sensor networks”, Sensors, 12(8), 2012, 113-153
10. S. Nallusamy, G.B. Dinagaraj, K. Balakannan and S. Satheesh, “Sustainable green lean manufacturing practices in small scale industries-A case study”, International Journal of Applied Engineering Research, 10(62), 2015, 143-146
11. Ismail Mansour, Gerard Chalhoub and Pascal Lafourcade, “Key management in wireless sensor networks”, Journal of Sensor and Actuator Networks, 4, 2015, 251-273
12. J. Zhang and V. Varadharajan, “Wireless sensor network key management survey and taxonomy”, Journal of Network and Computer Applications, 33, 2010, 63-75
13. I. Mansour, G. Chalhoub and P. Lafourcade, “Evaluation of secure multi-hop node authentication and key establishment mechanisms for wireless sensor networks”, Journal of Sensor and Actuator Networks, 3, 2014, 224-244
14. S. Chattopadhyay and A.K. Turuk, “A Scheme for key revocation in wireless sensor networks”, International Journal of Advanced Computer Engineering and Communication Technology, 1, 2012, 16-20
15. D. Sobya, “Data compression analysis of rocket engines with vector quantization based on FCM algorithm”, Int. Journal of Engineering Research in Africa, 22, 2016, 135-140
16. Chuang, Chang and Lin, “Node revocation scheme using public key cryptography in wireless sensor networks”. Journal of Information Science and Engineering, 26, 2010, 1859-1873
17. D. Sobya, “Lab view based multi-input fuzzy logic controller of DC motor speed control”, International Journal of Research in Mechanical, Mechatronics and Automobile Engineering, 1(1), 2015, 55-60
18. J. Yang, H. Sun, “Battery swap station location-routing problem with capacitated electric vehicles”, Computers and Operations Research, 55, 2015, 217-232
19. K. Balakannan, S. Nallusamy, P.S. Chakraborty and Gautam Majumdar, “Selection and evaluation of supplier by decision model of hybrid data envelopment analysis”, International Journal of Applied Engineering Research, 10(62), 2015, 123-127
20. S. Nallusamy, Sri Lakshmana Kumar, K.Balakannan and P.S.Chakraborty, “MCDM tools application for selection of suppliers in manufacturing industries using AHP, Fuzzy Logic and ANN”, International Journal of Engineering Research in Africa, 19, 2015, 130-137
21. D. Sobya, “Design and implementation of FPGA based wave-pipelining for digital signal processing circuits”, International Research Journal in Advanced Engineering and Technology, 1(2), 2015, 36-42
22. Purohit and Rawat, “Revocation and self-healing of keys in hierarchical wireless sensor network”, Int. Journal of Computer Science and Information Tech., 2, 2011, 2909-2914
23. Y. Zheng, Z. Y. Dong, Y. Xu, K. Meng, J. H. Zhao, and J. Qiu, “Electric vehicle battery charging/swap stations in distribution systems: Comparison study and optimal planning”, IEEE Transactions on Power Systems, 29(1), 2014, 221-229