International Journal of Psychosocial Rehabilitation, Vol. 23, Issue 04, 2019
ISSN: 1475-7192

# Empowered Smartgrid Systems Using SDN

R. Aarthi, D. Mohanapriya, V. Jeyageetha and
S. Thiruvenkatasamy

***Abstract---*** *Software Defined Networks (SDNs) is a emerging networking paradigm that has gained a allocation of consideration in recent years especially in applying data center networks and in providing efficient security solutions. The approval of SDN and its smart safety structures gives that it can be used in the context of smart grid systems to address many of the liabilities and security problems facing such critical infrastructure systems. The impact of different cyber-attacks that can target smart grid communication network which is implemented as a software defined networks on the process of the smart grid systems. We perform different attack situations including DDoS occurrences, location high jacking and link overloading in contradiction of SDN networks of dissimilar controller types that include POX, Floodlight and RYU. Our experiments were carried out using the mini net simulator. The experiments show that SDN-empowered smart grid systems are exposed to different types of occurrences.*

***Keywords---*** *Smartgrid, SDN, DDoS.*

## I. INTRODUCTION

Electric power systems are among the most important systems in our life that enable transformation of electricity flow from transformer to buyer. However, the growing require resulted from the rising people cannot be satisfied by the conservative electric structure that has no data replace for management or monitoring. Therefore, it was essential to enhance the infrastructure, integrating information and communication technology and improving the system security [1]. In order to reach this goal, the design of smart grid has raised. Smart Grids is an improved electric grid with communication network on top of it, which permit the two-way communication between suppliers and clients and given that more control over the grid. It ensures the consistency and maintainability of the manufacture and supply of power through analyzing the gathered information that reveal the dynamics of consumer-producer behavior.

The ultimate goal of Smart Grid is to develop power resources efficiently and cheaply based on information gathered and information together. Normally a smart grid system is self-possessed factories of control center, smart houses, and reusable energy power plants nuclear power plants and cites. The major components in smart grid are communication network, control center, and power grid. In this paper work the aim of investigating the implementation of software defined networks as a announcement network restore the heritage network and its blow on smart grid securities. Now a day's network must extent to provide accommodation improved workloads with

*R. Aarthi, Assistant Professor, Department of Computer Science & Engineering, Nandha College of Technology, Erode.*
*E-mail: aarthikalai@gmail.com*
*D. Mohanapriya, Assistant Professor, Department of Computer Science & Engineering, Nandha College of Technology, Erode.*
*E-mail: spriyasasmi@gmail.com*
*V. Jeyageetha, Assistant Professor, Department of Computer Science & Engineering, Nandha College of Technology, Erode.*
*E-mail: jeyageetha.v@gmail.com*
*S. Thiruvenkatasamy, Assistant Professor, Department of Computer Science & Engineering, Nandha College of Technology, Erode.*
*E-mail: samys.com@gmail.com*

**Received: 16 Sept 2019 | Revised: 18 Oct 2019 | Accepted: 15 Nov 2019** 

better alertness, and maintaining costs at least. To meet this vital need, software defined

SDN delivers an exposed and programmable approach to networking over an exposed Application Programming Interfaces (APIs) for rule based organization and safety. Fundamentally, providing a way to automate what has conventionally been complicated physical configuration. Also, this newfangled expertise is helping with many developing difficulties in networks today, such as traffic importance that cannot be preserved statically as before [4], sometimes video traffic is further imperative than vocal sound traffic and sometimes it is the additional method everywhere. However, in modern networks we cannot energetically configure traffic importance. That is when SDN comes in to act, we can energetically model and figure traffic in dynamic time depend on our present requests. SDN's worldwide opinion of the net link provides another property through the concept of ideas; this opinion fleeces away the distribution of the network letting the programmer to agree the essential progressing actions without caring about vendor- specific hardware and agreeing goals of general network without having details of how the physical net link will applied to them.

In this paper, we focus on safety problems of SDN-empowered smart grid systems. clearly implementing smart grid's communication network as a software defined network would transport numerous compensations in terms of safety and organization. However, it is main part to take into consideration the issues to SDN networks in common and their influence on smart grid systems. Therefore, we clarify the flexibility of POX [5], Floodlight [6] and RYU [7]SDN controllers to the following types of attacks: DoS in contradiction of the controller, path congestion DoS, host location hijacking, and ARP poisoning.The rest of this paper is prepared as follows: Section II discusses related work. Section III discusses SDN-Enabed smart grid systems and their security issues. Performance evaluation is obtainable in Section IV. Finally, conclusion is presented in Section V..

## II. RELATED WORK

Smart Grid and SDN has been a hot research topic during the past few years. Smart grids depends on the use of communication information technology which makes it different than conventional power grids. This leads the power grid to communication networks security vulnerabilities [8]. Smart grid needs to live up to a certain level of security requirements concerning availability, confidentiality and integrity, a survey paper points to these challenges [9], [10]. Different cyber-attacks can affect the power-grid security requirements. According to [11] two main attacks are Denial of service attack and Man-In-The- Middle attack. The calculations of the data delay and packet loss for wide-area monitoring and control system is based on the work presented in [12].

Open Networking Foundation (ONF) and International Telecommunication Union (ITU) are responsible of SDN standardizations [13]. Traditional networks rely on securing hosts using firewalls, IDSs and NAT, which are all placed at the edge of the network due to the lake of network routing control. On the other hand, SDN has more control over the data flow which means it can place security middle boxes at any part of the network [2], [3]. Open flow proposed to allow researchers to test new protocols regardless of the switch vendors [14]. This does not protect SDN from security threats instead, it promises future development of countermeasures. SDN can be vulnerable to traditional security threats [15], [16]. Yet traditional counter measures need to adapt to SDN before they can be used. Also new attacks targeting SDN vulnerabilities are being developed such as: (i) Link fabrication attack and (ii)

Host location hijacking [17]. These attacks target the network discovery capabilities of SDN exploiting the lake of authentication in announcing topology changes.

Several papers (e.g [16], [18]) points to the possibility of designing applications to protect against various attacks such as: Host- and switch-based attacks, this can be in the form of forging control packets, DoS on different services, network DoS and traffic hijacking or rerouting. Network topology: compromised hosts can spoof messages that tamper with the topology. Data Plain forwarding: Malicious hosts performing DoS or spreading malware. SPHINX [16] which collects topological and forwarding metadata from OpenFlow control messages to build an incremental flow graph in real-time and uses this information to detect security attacks on topology and data plane. TopoGuard is used to protect SDN against Host Location Hijacking and Link Fabrication attack. These two papers points to the possibility of building scripts to prevent from the previous mentioned attacks [19]. In [20] the researchers suggest using SDN as the communication network over which the smart grid traffic flows to benefit from all the new promising advantages of having a programmable environment.

Smart grid and SDN testbeds have been developed at various universities and national labs to investigate the security of smart grid systems. Testbed components can be categorized into communication, control and power system elements. These elements were represented entirely using software [17] or using software-hardware integration [14], [22]. In some cases, legacy networks were used to represent the communication network and simulators like DeterLab [14], ISEAGE [22]. On the other hand, other research papers suggested SDN instead to test the benefits of its new features when integrated with smart grid. Mininet is the most used SDN emulator in research [23]. Smart grid traffic can be represented using real physical devices traffic behaviors. In this paper, we focus mainly on Phasor Data concentrator PDC and Phasor Measurement Unit PMU communication.

## III. SDN ENABLED SMARTGRID

The idea of implementing smart grid communication net- work based on SDN technology was first proposed in [20]. Subsequently, several research efforts have been made in the same direction (e.g. [21]). The motive is to take advantage of SDN technology in providing dynamic network configurations, quality of service, real-time optimization, malicious attacks and accidental failures rapid response. The most important aspect of SDN is the separation of control plane and data plane, the switches are simple forwarding devices that can be dynamically configured by a central controller which has a global view of the whole network. It is envisioned that using SDN technology in the context of smart grid power systems would provide the ability to reset the switches or re- establish the grid control application routing when detecting compromised switches. Besides SDN provides fast network recovery in the presence of attacks. Also, SDN can facilitate and improve the networking of many intelligent electric de- vices by load balancing, shortest path forward, traffic shaping, and multiple grid applications with different quality of service requirements.

SDN-enabled smart grid approach will benefit from the programmability feature of SDN. It simply uses applications written in some high level programming language and run it over the SDN controller. Thus, helping the controller send commands to the network forwarding devices dynamically, to achieve the lowest delay possible according to the smart grid traffic needs. As well as reacting to possible attacks such as malicious rerouting and

denial-of-service attacks. Mainly, a simplified architecture of an SDN enabled grid has three major components: a control center, a communication network, and a power grid.

Phasor Measurement Unit (PMU) is one of the most important measuring devices in power systems. It provides synchronized measurements of voltages and currents in Electrical grid. This ability achieved by real-time voltage sampling [24]. PMU measurements are sent by rate 20-60 time/sec. Those measurements are sent to the Phasor Data concentrator (PDC) that is used to aggregate and align the data from various PMUs. IEEE defines four message parts for PMUs output: data, configuration, header and command. Data will be carrying the measurements. The length of data used is in range of 50-100 bytes. In this paper, we study the effect of attacks targeting the smart grid communication network on the latency of PMU-PDC communication because of its time sensitivity as highlighted in [25].

### *A. Security of SDN-Enabled Smart Grid Systems*

A comprehensive analysis of the security issues of smart grid systems was presented in [9], where threats to confidentiality, integrity and availability of smart grid information and infrastructure were explained in detail. In this paper, we focus mainly on three attack types that affect data availability and message delay requirements in smart grid communication systems. These attacks are:

- *Denial of Service*: DoS attacks are crucial security threats to communication network. If DoS attack successfully launched, it may cause losing connectivity between stations and the electric grid. That may issue catastrophic results such as, losing real time synchronization that will lead to power delivery delay with data misreading or total loss.

- *ARP Poisoning*: SDN is vulnerable to ARP poisoning even more than legacy networks, due to the lake of barriers between LANs. Legacy networks are divided into LANs and VLANs, where routers and layer three switches act as a barrier between broadcast domains. In consequence, end-to-end transmission depends on MAC address only inside a LAN limiting the number of hosts vulnerable to ARP cache poisoning. In comparison, SDN does not change MAC address during transmission resulting a greater domain for ARP cache poisoning making it a serious concern. ARP poisoning can be used to perform many attacks such as man-in the-middle attack and DoS. It affects Confidentiality, integrity and availability depending on the level of security used on the transferred data.

- *Host Location Hijacking*: This attack exploits the lake of security in the Host Tracking service provided by the controller. Host tracking service is keeping track of the hosts on the network by maintaining a host profile for each host. The host profile includes: (i) MAC address,

(ii) IP address and (iii) Location information. Some controllers keep more information such as VLAN ID. The lack of authentication in the location update mechanism used by OpenFlow controller makes it vulnerable to host location hijacking attack. The Attacker exploits this vulnerability by pretending to be another host and fooling the controller to think that host has changed its location. To do this, the attacker needs to know the target IP address and MAC address which is trivial if a target is already chosen. On the other hand, MAC address can be probed using ARP especially that SDN does not change MAC during packet transmission.

**Received: 16 Sept 2019 | Revised: 18 Oct 2019 | Accepted: 15 Nov 2019** 

## IV. PERFORMANCE EVALUATION

The security of SDN-enabled smart grid is evaluated through extensive simulation experiments using Mininet simulator. In order to simulate the different components in smart grid system and get closer to the real environment as much as possible, the suggested environment consists of three major parts: (i) Communication network implemented.

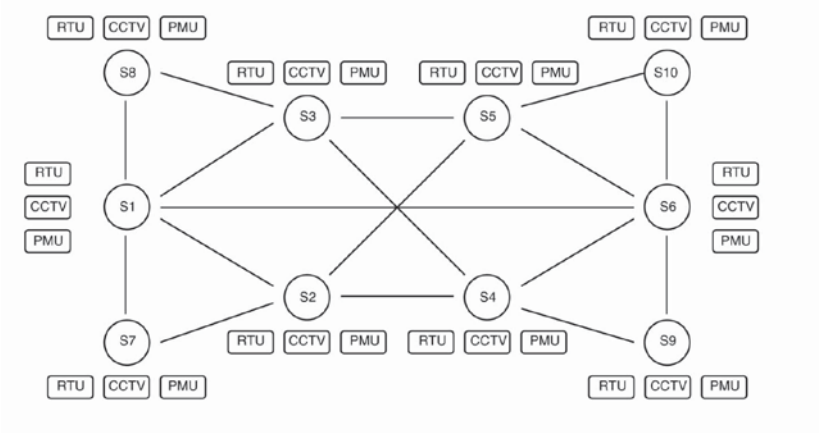


Fig. 1: Network topology

as SDN network (ii) Smart grid traffic and (iii) Background traffic, assuming this network is dedicated for smart grid communication. Smart grid traffic was generated using traffic generation tools that inject packets into the network carrying specified characteristics. The network designed to emulate real life Smart Grid System considering network topology based on studies of the power grid in some countries [26]. The topology was built using python implemented over Mininet as shown in Figure 1. The topology has ten switches, connected as a partial mesh. Substations are distributed over nine switches through the network, sending data to their master station that is located on switch one. Data is represented by three types of services: CCTV, RTU and PMU application. Each communication link is assumed as full duplex UTP copper with a bandwidth of 1 Gbps, and an assumption of 100 km distance between each two switches resulting in a propagation delay of about 0.5 ms. In general, a smart grid system has different applications that are classified base on: tasks, QoS and traffic rate. PMU and PDC were the applications chosen for our testbed, due to their critical delay requirements. The packet size and data rate of the PMU were specified as, 60 Bytes and 30 packets sec respectively over UDP/IP [12]. Background traffic was modeled by Closed-Circuit Television (CCTV) and Remote Terminal Units (RTU). CCTV traffic is video streaming application assumed to have QCIF resolution represented by 93 packets/sec each of size 1000 bytes. RTU traffic is represented by 500 Byte packet size with 2 packets/sec rate. Different attacks were performed targeting Availability, Integrity and Confidentiality.

These attacks will have an impact on Smart Grid performance that may cause critical delay.

### *A. Denial of Service Attacks*

The main objective of a DoS attack in SDN-enabled smart grid system is to achieve complete disruption of the communication network or to cause significant packet delay resulting in major problems in the power system

**Received: 16 Sept 2019 | Revised: 18 Oct 2019 | Accepted: 15 Nov 2019** 

components that rely on timely sensitive control messages. Denial of service attacks in SDN networks can take several forms. In our experiments, we performed *path congestion* attack in order to create a congestion in certain links between the set of PMUs and the PDC. Also, we performed denial of service attack

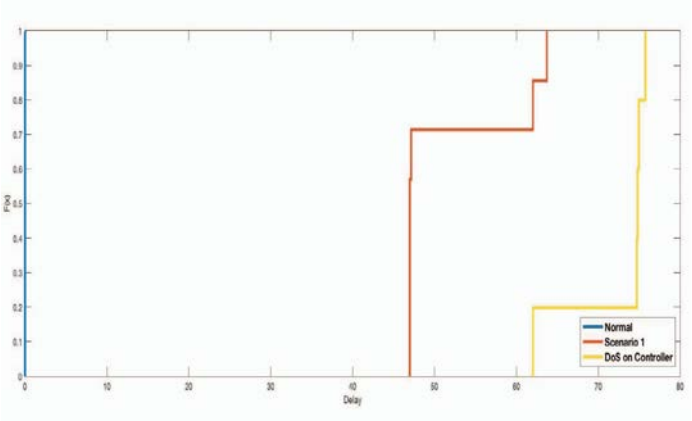


Fig. 2: POX based SDN. The cumulative distribution function (CDF) of the average delay for the packets sent from the PMUs to the PDC in the absence of an attack, in the case of path congestion attack, and in the case of DoS attack against the controller

against the controller in order to disrupt the operation of the SDN network. These attacks were applied on three different controllers; Pox, Floodlight, and RYU. For path congestion attacks, we performed two attack scenarios. In Scenario 1, the attack is launched from 5 compromised machines that is attached to switches directly connected to Switch1. In Scenario 2, the attack was launched from 3 compromised machines. For DoS attack against the controller, the attack is conducted by sending huge number of messages that will cause the switch to generate PACKETIN packets. The code was implemented using SCAPY by generating spoofed source IPs in result when the packet reaches a switch the switch thinks it is a new host added into the network and sends this information to the controller through PACKETIN message. These PACKETINs will consume the controller resources and processing power.

Figures 2, 3 and 4 show the cumulative distribution function (CDF) of the average delay for the packets sent from the PMUs to the PDC in the absence of an attack, in the case of path congestion attack, and in the case of DoS attack against the controller. Results for POX controller based SDN are shown in Figure 2. Normal delay was about 2.6 ms on average. In attack scenario 1 and in case of DDoS controller attack, the PMU-PDC has suffered from huge delay increase. The reason is that the POX controller does not support multi-pathing and cache the flows on the OpenFlow enabled switch. High traffic will cause high PACKETIN due the short time out. This attack was performed with different rate as shown in scenario2 and scenario 3. Applying DDos on the controller attack with 24 Mbps rate from 2 compromised hosts was able to cause the POX to crash. All DoS attacks caused more than 10 ms delay, which is unacceptable for PMU-PDC communication.

Results for Floodlight controller based SDN are shown in Figure 3. Normal delay had average of 2.9 ms. After performing scenario 1, PMU-PDC delay had an acceptable delay rate with an average of 7.5 ms. That is because of

**Received: 16 Sept 2019 | Revised: 18 Oct 2019 | Accepted: 15 Nov 2019** 

Flood- light multipathing and the permanent flow table entries.

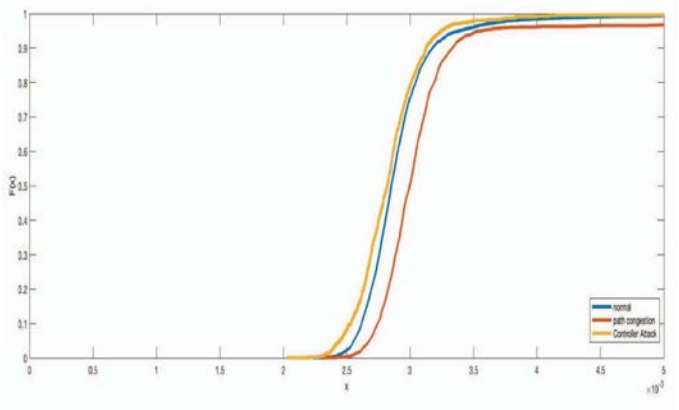


Fig. 3: Floodlight based SDN. The cumulative distribution function (CDF) of the average delay for the packets sent from the PMUs to the PDC in the absence of an attack, in the case of path congestion attack, and in the case of DoS attack against the controller

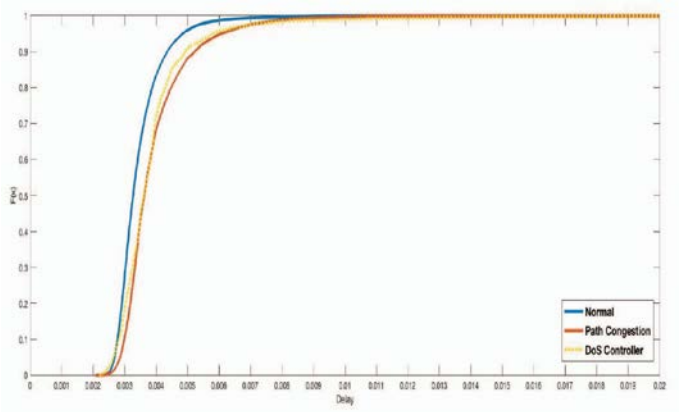


Fig. 4: RYU based SDN. The cumulative distribution function (CDF) of the average delay for the packets sent from the PMUs to the PDC in the absence of an attack, in the case of path congestion attack, and in the case of DoS attack against the controller DoS.

Controller attack had average of. Results for RYU controller based SDN are shown in Figure 4.

### *B. Host Location Hijacking*

Host location Hijacking attack is completely circumstantial. Each of the controllers behaved differently towards this attack depending on a few factors such as: (i) the activeness of the target and (ii) The flow table entry idle time out. Assuming that the attackers is attached to a network where the connections are already established, the flow entries are added to each switch appropriately. In this attack, the attacker will try to hijack the location of the PDC and try to redirect flow with the different PMUs. The attack on POX was the most successful. The attacker injected packets into the network carrying the identifiers of the legitimate server, after waiting for a while for the old flow entries to expire, the new flow entries will lead the legitimate flow to the attacker.

The default idle time out for most flow table entries added by the controller to the switches across the network is infinity, making this attack harder to perform over Floodlight. As we suggested earlier the attacker is attached to a network that is already active and the connections between different parts are established. This means that the switches already have flow entries leading to the PDC. When the attacker starts injecting packets the host profile changes but the flow entries do not in consequence, the flows existing before the attack will not change. Nevertheless, new hosts will be tricked to be forwarded towards the attacker.

### *C. ARP Poisoning*

Generally, SDN networks are vulnerable to ARP poisoning. Using simple tools like arpspoof or Ettercap, attacker can poi- son the target's ARP cache. If the attacker is located between a master station and a substation, it can be a silent MIM. Since SCADA protocols do not use encryption, confidential information will be easily captured by the attacker. Integrity is another concern, because of the ability to change packet contents as they pass through. The attacker can also perform many levels of DoS attack such as: capturing the packets and preventing them from reaching their destination resulting a complete DoS or delaying time critical packets enough to cause problem.

## V. CONCLUSION

In this project, Smart Grid SDN integration Resilience in contradiction of attacks, using a key advantage of SDN, which is the ability to vigorously configure the network to prevent fault and attacks which isolate them if possible. We studied the effect of Host Location Hijacking, ARP cache poisoning and two types of Denial of Service DoS on our network. The results obtained indicate the liability of all three used controllers to the before mentioned attacks. However, different performances were observed on each controller. In path jamming attack, FloodLight controller shows the best results. FloodLight and RYU showed better resilience against Host Location Hijacking attack than POX. On the other hand, all controllers showed low resilience against controller DoS and ARP poisoning, with significant differences.

In the presence of DDoS attack, we quantitatively exhibited that by usually all controllers tested are exposed. Our next step involves using the data from our simulations to build cyber security solution for justifying and avoiding the DoS attack.

## REFERENCES

[1] Amin, S. Massoud, and Bruce F. Wollenberg. "Toward a smart grid: power delivery for the 21st century." *Power and energy Magazine, IEEE* 3.5 (2005): 34-41.

[2] Braun, Wolfgang, and Michael Menth. "Software-Defined Networking Using Openflow: Protocols, Applications And Architectural Design Choices". *Future Internet* 6.2 (2014): 302-336.

[3] Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." *Proceedings of the IEEE* 103.1 (2015): 14-76.

[4] Craig, Alexander, et al. "Load balancing for multicast traffic in SDN using real-time link cost modification." *Communications (ICC), 2015 IEEE International Conference on. IEEE,* 2015.

[5] Shivayogimath, Chaitra N., and NV Uma Reddy. "MODIFICATION OF L3 LEARNING SWITCH CODE FOR FIREWALL FUNCTIONALITY IN POX CONTROLLER (WORKING ON SDN WITH MININET)."

[6] Wallner, Ryan, and Robert Cannistra. "An SDN approach: quality of service using big switchs floodlight open-source controller." *Proceedings of the Asia-Pacific Advanced Network* 35 (2013): 14-19.

**Received: 16 Sept 2019 | Revised: 18 Oct 2019 | Accepted: 15 Nov 2019** 

[7] Durairajan, Ramakrishnan, Joel Sommers, and Paul Barford. "Controller-agnostic SDN debugging." *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies. ACM*, 2014.

[8] H. Farhangi, "The path of the smart grid," *Power and Energy Magazine, IEEE,* vol. 8, no. 1, pp. 1828, January 2010

[9] Wang, Wenye, and Zhuo Lu. "Cyber security in the Smart Grid: Survey and challenges." *Computer Networks* 57.5 (2013): 1344-1371.

[10] Aloul, Fadi, et al. "Smart grid security: Threats, vulnerabilities and solutions." *International Journal of Smart Grid and Clean Energy* 1.1 (2012): 1-6.

[11] Liu, R., and A. Srivastava. "Integrated simulation to analyze the impact of cyber-attacks on the power grid." *Modeling and Simulation of Cyber- Physical Energy Systems (MSCPES), 2015 Workshop on. IEEE,* 2015.

[12] Zhu, Kun, Lars Nordstrom, and Ahmad T. Al-Hammouri. "Examination of data delay and packet loss for wide-area monitoring and control systems." *Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International. IEEE,* 2012.

[13] Open Netwok Foundation, "SDN Architecture Overview," *Version* 1.0, 2013

[14] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. "OpenFlow: enabling innovation in campus networks." *SIGCOMM Computer Communication Review,* 38(2):6974, 2008

[15] D. Kreutz, F. Ramos, and P. Verissimo. "Towards secure and depend- able software-defined networks." *In Proceedings of ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN),* 2013

[16] Dhawan, Mohan, et al. "SPHINX: Detecting Security Attacks in Software-Defined Networks." *NDSS.* 2015.

[17] Hong, Sungmin, et al. "Poisoning Network Visibility in Software- Defined Networks: New Attacks and Countermeasures." *NDSS.* 2015.

[18] Shin, Seungwon, et al. "FRESCO: Modular Composable Security Ser- vices for Software-Defined Networks." *NDSS.* 2013.

[19] Masoud, Mohammad Z., Yousf Jaradat, and Ismael Jannoud. "On preventing ARP poisoning attack utilizing Software Defined Network (SDN) paradigm." *Applied Electrical Engineering and Computing Tech- nologies (AEECT), 2015 IEEE Jordan Conference on. IEEE,* 2015.

[20] Dong, Xinshu, et al. "Software-defined networking for smart grid resilience: Opportunities and challenges." *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. ACM,* 2015.

[21] Kim, Jaebeom, Fethi Filali, and Young-Bae Ko. "Trends And Potentials Of The Smart Grid Infrastructure: From ICT Sub-System To SDN- Enabled Smart Grid Architecture." *Mdpi.com. N.p.,* 2015. Web. 29 Dec. 2015

[22] Hahn, Anna, et al. "Cyber-physical security testbeds: Architecture, ap- plication, and evaluation for smart grid." *Smart Grid, IEEE Transactions on* 4.2 (2013): 847-855.

[23] mininet.org. "Mininet: An Instant Virtual Network On Your Laptop (Or Other PC) - Mininet." *Mininet.org. N.p.,* 2015. Web. 29 Dec. 2015

[24] Xu, Yuzhe. "Latency and bandwidth analysis of lte for a smart grid." (2011).

[25] Shahzad, S., et al. "Conceptual model of real time infrastructure within cloud computing environment." *Int. J. Comput. Networks* 5 (2013): 18- 24.

[26] Germano da Silva, Eduardo, et al. "Capitalizing on SDN-based SCADA systems: An anti-eavesdropping case-study." *Integrated Network Man- agement (IM), 2015 IFIP/IEEE International Symposium on. IEEE,* 2015.

[27] Dhivyaa C R, Nithya K and Saranya M, "Automatic detection of diabetic retinopathy from color fundus retinal images", *International Journal on Recent and Innovation Trends in Computing and communication,* Vol.2, Issue 3, ISSN:2321-8169, 2012.

[28] Saveetha P, Arumugam S and Kiruthikadevi K, "Cryptography and the Optimization Heuristics Techniques", *Int. Journal of Advanced Research in Computer Science and Software Engg,* volume. 4, Issue.10, ISSN: 2277 128X, October 2014.

[29] Gokulraj P and Kiruthikadevi K, "Revocation and security based ownership deduplication of convergent key creating in cloud", *International Journal of Innovative Research in Science, Engineering and technology.* Vol. 3, Issue 10, ISSN: 2319-8753, October 2014.

[30] Sureshkumar V S, Chandrasekar A," Fuzzy-GA Optimized Multi-Cloud Multi-Task Scheduler For Cloud Storage And Service Applications" *International Journal of Scientific & Engineering Research*, Vol.04, Issue.3, pp-1-7, 2013.

[31] Preethi, B.C. and Vijayakumar, M. " A novel Cloud Integration Algorithm(CIA) for Energy Efficient High Performance Computing Applications in Big Data Multimedia Applications", *Romanian Journal of Information Science and Technology*, vol. 2, no.1, pp. 1-11, March 2018.

[32] Vijayakumar M, Prakash s, "An Improved Sensitive Association Rule Mining using Fuzzy Partition Algorithm", *Asian Journal of Research in Social Sciences and Humanities*, Vol.6,Issue.6, pp.969-981, 2016.

[33] Prakash S, Vijayakumar M, " Risk assessment in cancer treatment using association rule mining techniques", *Asian Journal of Research in Social Sciences and Humanities*,Vol.6,Issue.10, pp.1031-1037, 2016.

[34] Prabhakar E, " Enhanced adaboost algorithm with modified weighting scheme for imbalanced problems, *The SIJ transaction on Computer science & its application*,Vol.6,Issue.4, pp.22-26, 2018.

[35] Nandagopal S, Malathi T, "Enhanced Slicing Technique for Improving Accuracy in Crowd Sourcing Database", *International Journal of Innovative Research in Science, Engineering and Technology*, Vol.3,Issue.1, pp.278-284, 2014.

[36] Prabhakar E, Santhosh M, Hari Krishnan A, Kumar T, Sudhakar R," Sentiment Analysis of US Airline Twitter Data using New Adaboost Approach", *International Journal of Engineering Research & Technology (IJERT)*, Vol.7,Issue.1, pp.1-6, 2019.

[37] Dhivyaa C R ,Vijayakumar M," An effective detection mechanism for localizing macular region and grading maculopathy", *Journal of medical systems*, Vol.43,Issue.3, pp.53-, 2019.

[38] Ragunath V, Dhivyaa C R "Privacy Preserved Association Rule Mining for Attack Detection and Prevention" *published in International Journal of Innovative Research in Computer and Communication Engineering*, Vol.2, Issue 1, March 2014

[39] Nithya K, Krishnamoorthi M, KalamaniM, "Tweets: Review of Micro-Blog Based Recommendation Systems (RS) for News Recommendation (NR)", *in International Journal of Recent Technology and Engineering (IJRTE)*, ISSN: 2277-3878, Volume-7 Issue-4S, November 2018. pp. 444-448

[40] K Nithya, M Saranya, CR Dhivyaa, "Concept Based Labeling of Text Documents Using Support Vector Machine", *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 2, no. 3, pp. 541-544, (2014).

[41] Suresh kumar V S , Booma K, Suma K "IOT Smart Classrooms", *International Journal Of Science Technology and Humanities*, Vol 6 , pp: 1-6,Issue 1,2019.

[42] Nandagopal S., Arunachalam V.P., Karthik S."A novel approach for inter-transaction association rule mining, *Journal of Applied Sciences Research* VOL, 8, Issue 7, 2012.

[43] Kannan R., Selvambikai M., Jeena Rajathy I., Ananthi S. Rasayan, A study on structural analysis of electroplated Nano crystalline nickel based thin films, *Journal of Chemistry*, Vol 10, issue 4, 2017.

[44] Arunvivek G.K., Maheswaran G., Senthil Kumar S., Senthilkumar M., Bragadeeswaran T. Experimental study on influence of recycled fresh concrete waste coarse aggregate on properties of concrete. *International Journal of Applied Engineering Research*, Vol 10, issue 11, 2015

[45] Krishna S.K., Sathya M. Usage of nanoparticle as adsorbent in adsorption process. *A review International Journal of Applied Chemistry*, vol 11, Issue 2, 2015.

[46] Sudha S., Manimegalai B., Thirumoorthy P. A study on routing approach for in-network aggregation in wireless sensor networks, *International Conference on Computer Communication and Informatics: Ushering in Technologies of Tomorrow, Today, ICCCI* 2014.

[47] Satheesh A., Jeyageetha V. Improving power system stability with facts controller using certain intelligent techniques, *International Journal of Applied Engineering Research*, Vol 9, no 23, 2014.

[48] Ashok V., Kumar N, Determination of blood glucose concentration by using wavelet transform and neural networks, *Iranian Journal of Medical Sciences*, Vol 38, Issue 1, 2013.

[49] Somasundaram K., Saritha S., Ramesh K, Enhancement of network lifetime by improving the leach protocol for large scale WSN, *Indian Journal of Science and Technology*, Vol 9, Issue 16, 2016.

[50] Jayavel S., Arumugam S., Singh B., Pandey P., Giri A., Sharma A. Use of Artificial Intelligence in automation of sequential steps of software development / production, *Journal of Theoretical and Applied Information Technology*, Vol 57, Issue 3, 2013.

[51] Ramesh Kumar K.A., Balamurugan K., Gnanaraj D., Ilangovan S, Investigations on the effect of flyash on the SiC reinforced aluminium metal matrix composites, *Advanced Composites Letters*, Vol 23, Issue 3, 2014.

[52] Suresh V.M., Karthikeswaran D., Sudha V.M., Murali Chandraseker D, Web server load balancing using SSL back-end forwarding method. *IEEE-International Conference on Advances in Engineering, Science and Management, ICAESM-2012*, 2012.

[53] Karthikeswaran D., Sudha V.M., Suresh V.M., Javed Sultan A, A pattern based framework for privacy preservation through association rule mining, *IEEE-International Conference on Advances in Engineering, Science and Management, ICAESM-2012*, 2012.

[54] Senthil J., Arumugam S., Shah P, Real time automatic code generation using generative programming paradigm, *European Journal of Scientific Research*, vol. 78, issue 4, 2012.

[55] Vijayakumar J., Arumugam S, Certain investigations on foot rot disease for betelvine plants using digital imaging technique, *Proceedings - 2013 International Conference on Emerging Trends in Communication, Control, Signal Processing and Computing Applications, IEEE-C2SPCA*", 2013.

[56] Vijayakumar J., Arumugam S. Odium piperis fungus identification for piper betel plants using digital image processing, *Journal of Theoretical and Applied Information Technology*, vol 60, issue 2, 2014.

[57] Manchula A., Arumugam S, Face and fingerprint biometric fusion: Multimodal feature template matching algorithm, *International Journal of Applied Engineering Research*, vol 9, issue 22, 2014.

[58] Ramesh Kumar K.A., Balamurugan K., Arungalai Vendan S., Bensam Raj J, Investigations on thermal properties, stress and deformation of Al/SiC metal matrix composite based on finite element method. Carbon - Science and Technology, Vol 6, Issue 3, 2014.

[59] Kanchana A., Arumugam S, Palm print texture recognition using connected-section morphological segmentation, *Asian Journal of Information Technology* Vol 6, Issue 3, 2014.

[60] Padmapriya R., Thangavelu P, Characterization of nearly open sets using fuzzy sets, *Global Journal of Pure and Applied Mathematics*, vol 11, issue 1, 2015.

[61] P.B. Narandiran, T. Bragadeeswaran, M. Kamalakannan, V. Aravind, Manufacture of Flyash Brick Using Steel Slag and Tapioca Powder. *Jour of Adv Research in Dynamical & Control Systems*, Vol. 10, No. 12, 2018, 527-532

[62] R. Girimurugan*, N. Senniangiri, K. Adithya, B. Velliyangiri, Mechanical Behaviour of Coconut Shell Powder Granule Reinforced Epoxy Resin Matrix Bio Composites, J*our of Adv Research in Dynamical & Control Systems*, Vol. 10, No. 12, 2018, 533-541.