UNIZIK JOURNAL OF ENGINEERING AND APPLIED SCIENCES (UJEAS)

Research Article

Comparing impact of open-flow firewall on the SG-IoT-AMI-infrastructure, a well-designed cloud-based network against non-open flow firewall

Ilokanuno O, Okezie C. C

Special Issue
A Themed Issue in Honour of Professor Ekedimogu Eugene Nnuka on His retirement.

This themed issue honors Professor Ekedimogu Eugene Nnuka, celebrating his distinguished career upon his retirement. His legacy of exemplary scholarship, mentorship, and commitment to advancing knowledge is commemorated in this collection of works.

Edited by
Chinonso Hubert Achebe PhD.
Christian Emeka Okafor PhD.

UJEAS

UNIZIK JOURNAL OF ENGINEERING AND APPLIED SCIENCES

UNIZIK Journal of Engineering and Applied Sciences 3(2), June (2024), 631-643
Journal homepage: https://journals.unizik.edu.ng/index.php/ujeas
PRINT ISSN: 2992-4383 || ONLINE ISSN: 2992-4391

Comparing impact of open-flow firewall on the SG-IoT-AMI-infrastructure, a well-designed cloud-based network against non-open flow firewall

Ilokanuno O[1*] and Okezie C. C[2]
[12]Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka
[*]Corresponding Author's E-mail: deyorky2@gmail.com

Abstract
This work presents a novel smart grid tampering detection system re-engineered for end user monitoring and pipeline automation. The research focused on distributed energy resources. In context, the end user load profile, and generation capacity were processed in the cloud environment for tampering management. Computational pipelined methodology was adopted using baseline data from an independent electricity consumption data from 2018-2021 Abuja. First, a smart grid (SG) survey was carried using existing home estate at Abuja to ascertain tampering procedures in distributed energy resource domain. From the energy survey, the system architecture was developed and implemented based on computational model curve for dynamic attack vector mitigation. An Unsupervised layered SG Architecture with local concentrator was introduced including Advanced Metering Infrastructure Smart Grid (AMI SG) gateway and control Load Balancer Docker Agent with Binomial sink.SG AMI Network packet processing Scheme and docker Orchestration were characterized for SG AMI Traffic Model. Furthermore, Smart Grid Internet of Things Coordinating Infrastructure (SG-IoT-CI) Dynamic Resource Allocation and Load Balancing/Scheduling was presented. The results showed that there was a significant improvement when leveraging SG-IoT-CI unsupervised grid management. Also, a robust distributed SG-IoT based management architecture that links the processes for end-users was developed. To determine the efficiency of the computational algorithm for SG grid deployment, an experiment was carried out on SG-IoT-CI-AMI optimization model using schemes such as K-Nearest Neighbourhood with Isolated Forest (KNN +IF), Load Prediction with Regression (LPBSVR), Support vector machine (SVM), Load Prediction with Neural Network (LPBNN), Local Outlier Factor (LOF) and Lightweight On-line Detector of Anomaly (LODA) for validation study. For Full Scale Query Response Time (FSQRT) under Open Flow security control, it was observed that the SG-IoT-CI AMI Overflow and Non-Open Flow gave 47.82% and 52.17% respectively from the simulation statistic engine. Full Scale Resource Utilization under Open Flow security aggregation layer and Non Open Flow security aggregation layer gave 2.73% and 92.27% percentile utilization respectively. Using the unsupervised contexts, the Secure SG-IoTCI_AMI Latency for LPBSVR, Proposed KNN +IF, SVM, LPBNN, LOF and LODA gave 20.96%, 11.98%, 19.31%, 19.76%, 19.01% and 8.98% respectively. Secure SGIoTCI_AMI service rate gave 14.03%, 35.09%, 5.26%, 8.77%, 15.79% and 21.05% respectively. Secure SG-IoTCI_AMI Throughput gave 19.13%, 25.04%, 19.27%, 15.47%, 18.28% and 28.12% respectively. Secure SGIoTCI_AMI Accuracy Response gave 26.66%, 31.11%, 15.55%, 0.00%, 22.22% and 4.46% respectively. The results show that tampering control within SG grid ecosystems is feasible and very efficient.

Keywords: Put Advance Metering Infrastructure, Computational Pipeline, Neural Network, Smart Grid, support vector machine

1. Introduction

The dream of every Nigerian is to have an automated power system with adequate supply. The current electric power systems in Nigeria that has been serving us for more than five decades lack robust automation and security. The system depends heavily on fossil fuels, including oil, coal, and natural gas, as energy sources without any form of smart initiative. These fossil fuels are non-renewable and the reserves on the earth are being consumed rapidly (Rong et al., 2014). The present energy crisis has brought serious global attention to finding alternative energy resources that can sustain long-term industrial development. The identified renewable energy resources include wind, hydro, solar, tidal, geothermal, and waste (Naji et al., 2018). These are referred to as green energy as they do not release carbon dioxide (CO2) into the atmosphere in the process of electric energy generation. The global

consensus is that distributed energy sources should be designed to complement and possibly replace fossil fuels due to their exploitation durability and environmental friendliness. The system must be resilient and highly secured.

Active research studies and deployment activities across the world are now focusing on how to effectively harness renewable energy resources as well as the legacy grid model (Naji, 2018; Depuru, 2011). A next-generation power grid now incorporates diversified distributed energy sources, automated and intelligent management as a critical component that determines the effectiveness and efficiency of these power systems. This is called a smart grid (SG)(Naji, 2011). It is an advanced electrical grid that uses composite information and communications technologies to gather and act on real-time information, such as the behavior of suppliers and consumers in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity (Depuru, 2011; Naji, 2011).

The idea behind transforming an existing electrical grid to SG is to offer stable, accessible, reliable, economic and high quality electricity while reducing environmental impacts and driving economic growths. This initiative seeks to drive energy sustainability and better service delivery to end users. Again, modernizing the existing utility grid to intelligently and efficiently respond to available power generation, power transmission and consumer demand offers numerous advantages. This comes through management automation and intelligence subsystem integration. The merits over the current systems include: flexibility, intelligence, resilience, sustainability, and customization (Depuru et al., 2012).Obviously, the SG control centers are expected to monitor and interact with the electric devices remotely in real time while other subsystems focus on enhancing the power quality as well as coordinate their local devices self-consciously. Enab1ed by the significant advancements in system automation and intelligence, the concept of Energy Internet (Depuru et al., 2013) has been proposed that envisions an exciting prospect of the future energy utilization paradigm throughout all the energy generation, storage, and transmission and distribution phases.

Smart grid convoluted network (SGCN) (Hearst et al., 1998) has been proposed to halt possible cyber-attacks which affects the computational requirements of SG applications, un-fortunately the security of SG supporting core infrastructures are still been compromised like the remote monitoring and control system, known as the Supervisory Control and Data Acquisition (SCADA) system, Energy Management System (EMS), power system communication infrastructure, and the computational and storage resources. Without adequate security to protect SG phasor measurement units (PMU), Wide Area Measurement systems, Substation Automation, and Advanced Metering Infrastructure (AMI), the exploitation of its vulnerabilities can lead to SG crisis. This is because the EMS usually resides in a utility control centre and performs state estimation functions, contingency analysis and automatic generation control (AGC). The EMS state estimator receives data from SCADA which is conveyed through the Inter-Control Centre Communication Protocol (ICCP) from other utility's control centres. This data is used to estimate the operational state of the smart grid every few minutes. This gives situational awareness information which is needed by the power grid operators for making timely and informed decisions.

In fact, the deployment of the above SG technologies will greatly improve the reliability of the grid and reduce costs of power delivery while presenting new dependency on cyber resources which may be open to threats and attacks (Hearst et al., 1998). For example, a compromise of the metering networks may allow an attacker access to the control functions that, if corrupted, will threaten the availability of the data in the system and consequently violate the integrity of the system. The Advanced Metering Infrastructure (AMI) is currently regarded as the foundation of the smart grid. The AMI is responsible for the bi-directional communication of loads and user consumption data between utility companies and energy consumers. This action helps in the implementation of control signals and commands that are needed in taking necessary control actions as well as in Demand Side Management (DSM).SG AMI could be configured to integrate a couple of technologies to achieve its desired objectives. This AMI includes smart meters, communication networks, and data management systems. It also incorporates in its design a means of collecting data into software applications and interfaces.

As such, SG Internet of Things (IoT) coordination infrastructure (SG-IoT-CI) is proposed in this work. Electricity theft in the SG model will be solved via IoT unsupervised machine learning algorithm (UMLA) in SG-IoT-CI.
Current approaches mostly have relied on data acquired from utility companies for analysis that are time-consuming and very complex and which have left the problems unresolved besides its unreliability. However, this method of acquisition of such data could infringe on the privacy of consumers. Hence, the system must respect and protect the privacy of consumers even in the cloud. Instead of relying on energy consumption data alone to detect illegal consumers, this work will employ a disruptive IoT unsupervised machine learning algorithm in the smart grid AMI

to detect energy theft without allowing private energy profile data of consumers to be violated. The actual metering data can be captured by analytics from the AMI micro grid switches. By incorporating cloud technology in smart grid architecture, will offer resilience for bandwidth data offloading from the edge devices (AMI) into the cloud through the fog layer. The advantage is that the huge computational capability of the cloud datacentre for utility load stations will be relieved of the burden of storage processing, and maintenance of energy consumption data using smart type-1 virtualization technologies**.**

More so, preserving the privacy of consumers can be achieved by designing robust and resilient AMI communication architectures with state-of-the-art cryptographic algorithms and data aggregation protocols that will ensure the privacy and security of end user's data in the face of different cyber-attacks. One major drawback from current approaches for providing privacy of final consumers in AMI systems for smart grid is the unavailability of predictive analytics for tampered AMI systems in a distributed smart grid system. On the other hand, the existing network platforms are highly inefficient for deploying and hosting a secured monitoring application such as the SG AMI, feedback communication, and DSM (full-duplex communication). As such, there is a need to develop a reliable SG-IoTCI that can address the limitations of traditional models while offering smarter integration with renewable micro-grid sources on metering and end-user profile

2.0 Material and methods

The Open-Flow firewall is introduced in SG-IoT-AMI-infrastructure, to mitigate and dynamically handle the tampering attack vectors. In this case, DDoS (distributed denial of service) is monitored such that only legitimate traffic is allowed through the Open-Flow firewall service while using the AMI to reach the cluster-backed servers. Illegal traffic is stopped at the border, before it reaches the network. At the level of network tampering, DDoS mitigation focuses on maintaining TCP/IP web characteristics 24 hours a day, 7 days a week, independent of network conditions. To investigate and confirm the impact of the Open-Flow firewall on the SG-IoT-AMI-infrastructure, a well-designed cloud-based network was built using the parameters in Table 1.

To investigate and verify the impact of the Open-Flow firewall on AMI-based infrastructure in Table 1., a hostile hacker targeted the target network with a volumetric DDoS assault flood. This was accomplished using data packets that can entirely saturate the available network bandwidth. The assault exploited a 250 Gbps bandwidth, which resulted in extremely high traffic volumes, saturating the targeted SG-IoT AMI network and server subsystems. In essence, this can result in significant service disruption for valid location-based users attempting to use the web http/TCP/IP service. In the absence of effective security mechanisms, this volumetric attack (250 Gbps DDoS), which can literally endure for longer in a production environment, can hijack and maybe bring down the entire SG-IoT AMI network within minutes. This assault is particularly noticeable at the network layer (layers 3 and 4), where it can overwhelm a server's internet connection, network resources, and network nodes that are unable to absorb the increasing traffic volumes**.**

Table1: SG-IoT Design Parameters for Unsupervised ML Scenarios

1	Design Details	Setup values
2	Number of SGIoT AMI network units	5-10 (min)
3	Number of SGIoT AMI CIU	5-10(min)
4	Number of SGIoT AMI Concentrator G	1(min)
5	Number of Utility datacenter Backend	1: 6 Server Clusters
6	Number of SGIoT AMI OpenFlow Firewall	1(Cisco Nexus 9000 firewall as an embedded network device with support for Virtual DDoS protection in the SG-IoTCI threat mitigation design)
7	Number of SGIoT AMI Master Station	1:5 Server clusters
	SGIoT AMI Payload	Volumetric Traffic Model based on TCP/IP
9	Number of SGIoT AMI Type-1 Virtual Machine Instance	Infinity docker workloads
10	Number of SGIoT AMI Servers	9:SunUltra10:333MHz;1CPU;1Core (Simple CPU Mode)
11	Attack Vector Traffic	DDoS 250Gbps
12	AMI Traffic	On-demand DB Query
13	Ethernet Technology	PPT1 (40Gbps)

This work made comparison between two major DDoS attack scenarios viz: SG-IoT Open-Flow firewall and Non SG-IoT Open-Flow firewall (conventional) in a distributed cloud based smart grid system. With compatible C++ library, a simulation with Riverbed Modeller Engine 17.5 was carried out. Various layers of integration were satisfied while using the external libraries to populate and build the network map shown in Fig. 1, Fig. 2 and Fig. 3 depict a successful trace file engine build work design for the network and a successful simulation trace file compilation, respectively.

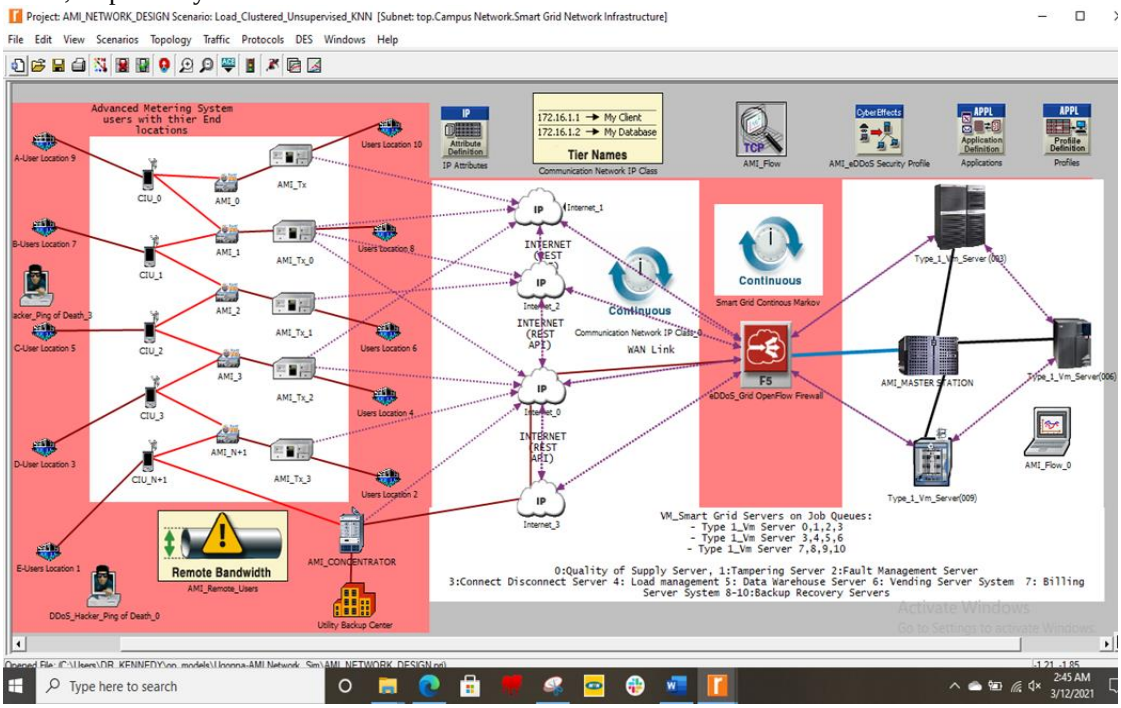

Fig. 1: SGIoT AIM Cloud Design Testbed

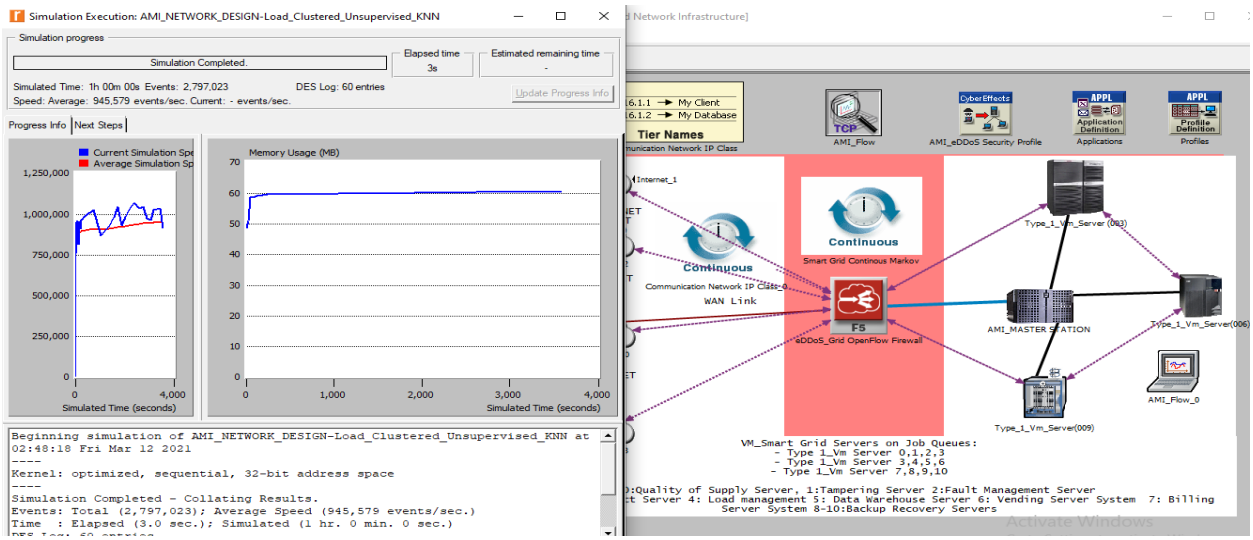

Fig. 2: Successful Trace File Engine Build Work Design for Network

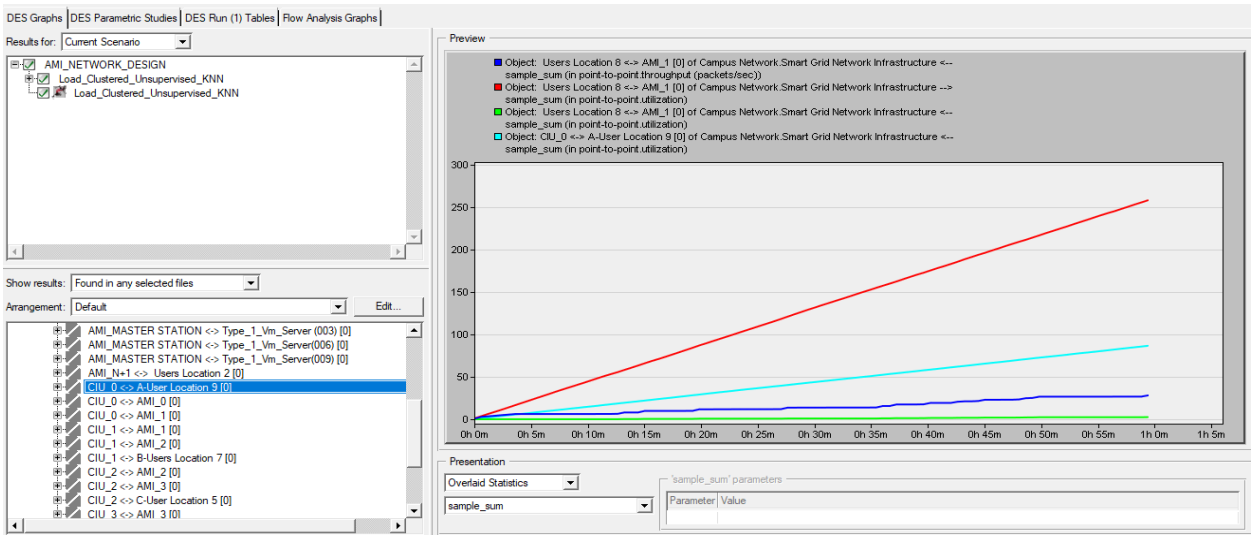

Fig. 3: Simulation Result Window

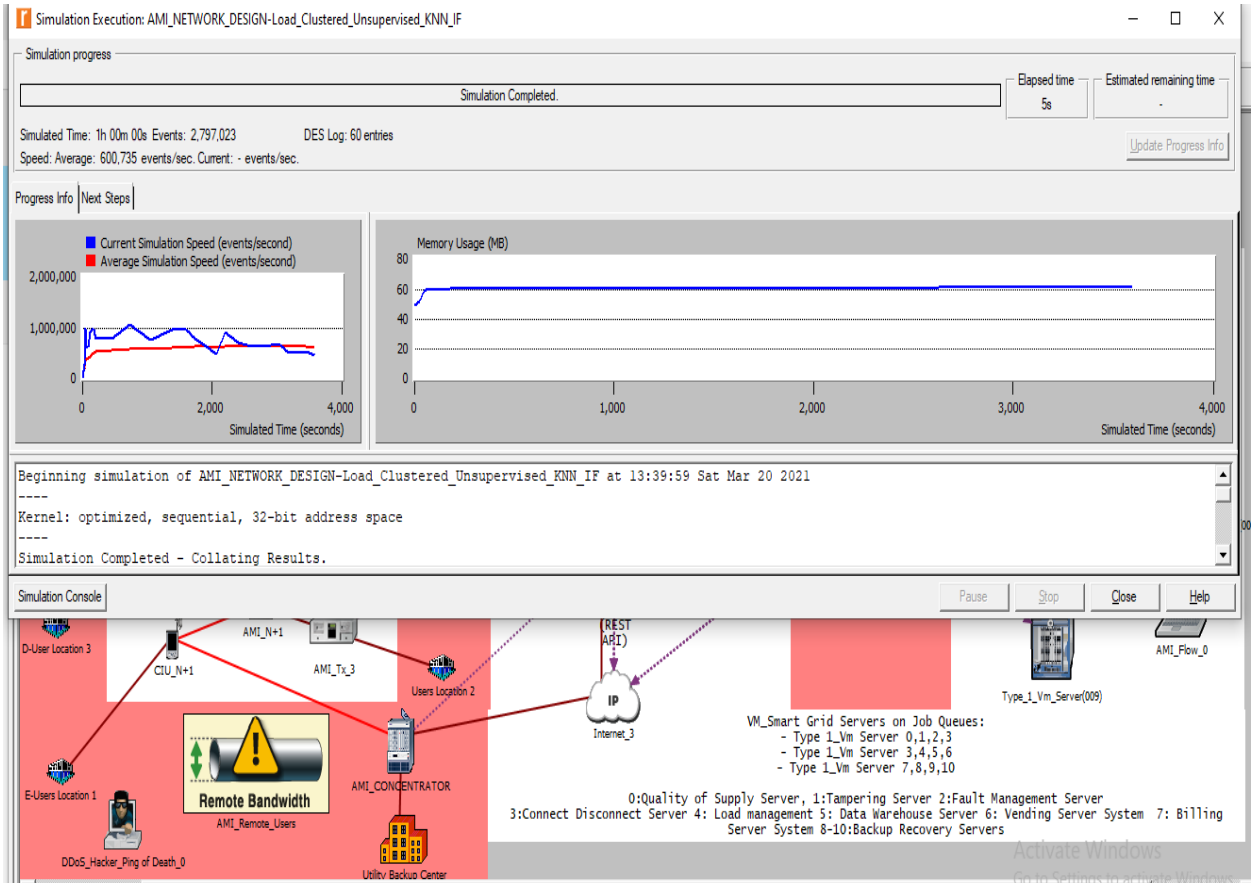

Fig. 4: Refactored Simulation Script Collation Window

3.0 Results and Discussions

3.1 SG-IoT Simulation Result Analysis on Full Scale Query Response Time (FSQRT)

The local response time can be used to assess access to the AMI server for the purpose of dispatching the query result value with ML scheme. The SG-IoT-CI AMI Open-Flow and Non-Open-Flow gave 47.82% and 52.17% respectively from the simulation statistic engine. The slow query log shows the exact amount of time used by the queries that were run. There are a high number of requests on the remote utility that may take some time to complete. This AMI server feature provides a tool for evaluating data by counting and reporting the number of queries proportional to the time it takes to execute them. Data is collected after the server has completed bypass sensing processing. The implication of Fig. 5 is that the tampering attack vector profiles for Open-Flow enabled scenario is lower thereby providing much faster backend database records. Also, diagram below depicts tampering effects for Open Flow and Non-Open Flow instance, no noticeable behaviour was detected until a payload of 2000 seconds into the plot. A progressive gradient may be seen from 2000 seconds to 3500 seconds of simulation duration. The query response time of the Open Flow AMI firewall is somewhat faster (53,000 Msec) than that of the non-Open Flow AMI firewall from 3700 to 4000 seconds of simulation time (56,000 Msec). For the SG AMI traffic model, AMI docker Orchestration will work at its best while employing the Open-Flow firewall. In this situation, obtaining the query result set data from the database will significantly enhance response time.

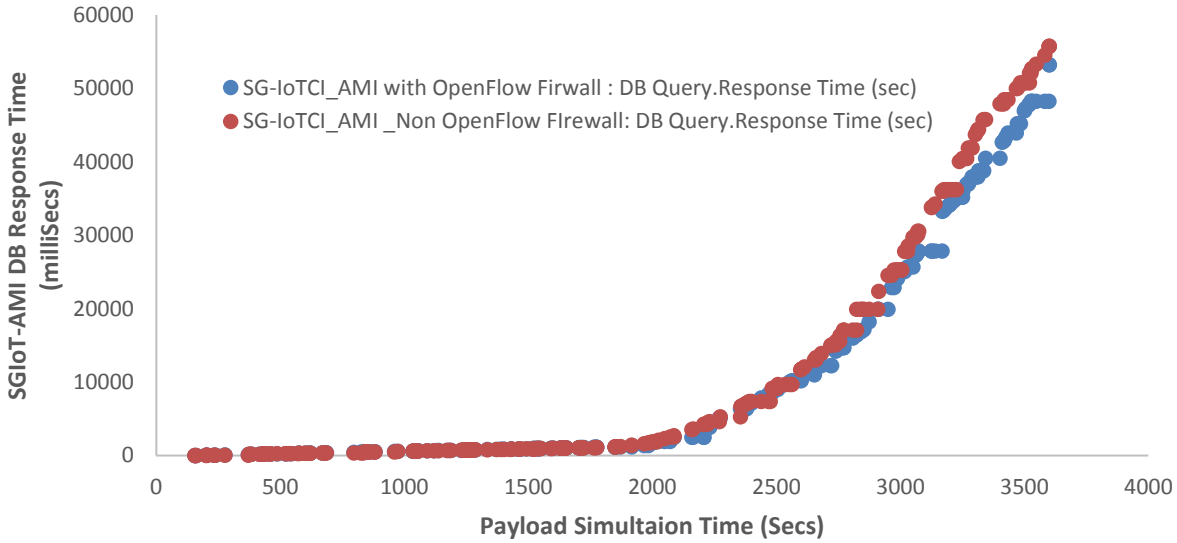

Fig. 5: SG-IoT Open-Flow Firewall full scale query response behaviour

3.1.1 Full Scale Resource Utilization

Another important parameter of the SG-IoT-CI network employed in this study was resource consumption. The temporal patterns of data traffic model were defined using packet traces after first reviewing the traffic data used to evaluate connection use and possible packet loss at the network core. The findings were utilized to compare and contrast different firewall strategies for traffic engineering in SG-IoT-CI AMI infrastructure. Recall that, the AMI network's firewall devices are divided into Open-Flow and Non-Open-Flow multiple levels. In two instances, these have differing physical capacities. This evaluates how the security module will benefit from traffic engineering by characterizing the link use for tampering situation. Fig. 6 indicates that link use in the Open-Flow security aggregation layer is much lower (2.73%) than in the Non-Open Flow security aggregation layer, which has roughly 92.27% percentile utilization. This is to be expected, because in most circumstances, numerous users connect to the SG-IoT-CI AMI via aggregation links at the edge. Possible resource allocation areas are first established when end users seek a connection. From the end-user's perspective, all workload sources poll resources from these servers As a result, resource use in these regions is quite high in the case of Non-Open-Flow security integration, as evidenced by the peaks. These are the areas where the AMI network's computing power and bandwidth are drained the most. The Non-Open-Flow firewall method has a high priority weight during an attack (tampering) on the AMI network; therefore, the AMI servers' processing power is high. In contrast, using the Open-Flow security system, connection requests are established as a geometric expansion at zero load time from the plot. This is a literal representation of a high-performance and secure SG-IoT AMI network.

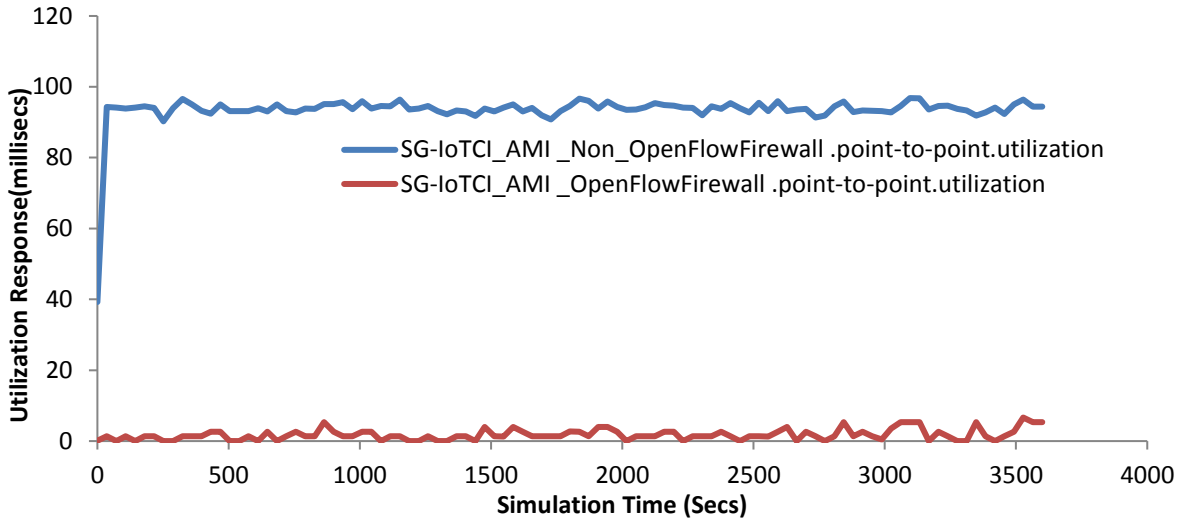

Figure 6. SG-IoT Open Flow Firewall Resource Consumption During Tampering

3.1.1.1 Full Scale Network Throughput hits

The throughput characteristics of the SG-IoT-CI AMI network under both tampered and untampered settings is fascinating as depicted in Fig. 7. The network's throughput has remained relatively constant at around 260000 bytes per second. This is in line with the minimal network resource use and quick query response times that are typical of the system. The Open-Flow security module carefully detects such anomalies in any attack scenario and carefully constructs an isolation mechanism. As illustrated in Fig. 7, this usually has a positive influence on network throughput. In Fig. 8, the situation is the different. Any disruptive assault on the AMI network will generally damage the network throughput under the Non-Open-Flow security approach. By introducing tampering attack vector on the network, Fig. 8 depicts degraded throughput pattern on the network. An increase in the tampering attack will result in more unstable and unreliable network with huge potential for saturation

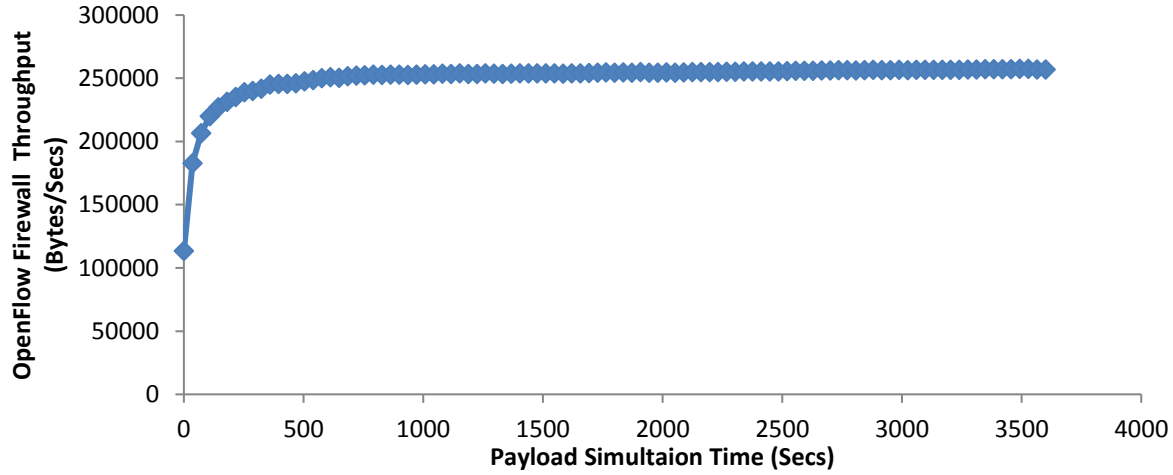

Figure 7: SG-IOTCI AMI Throughput with Openflow Firewall

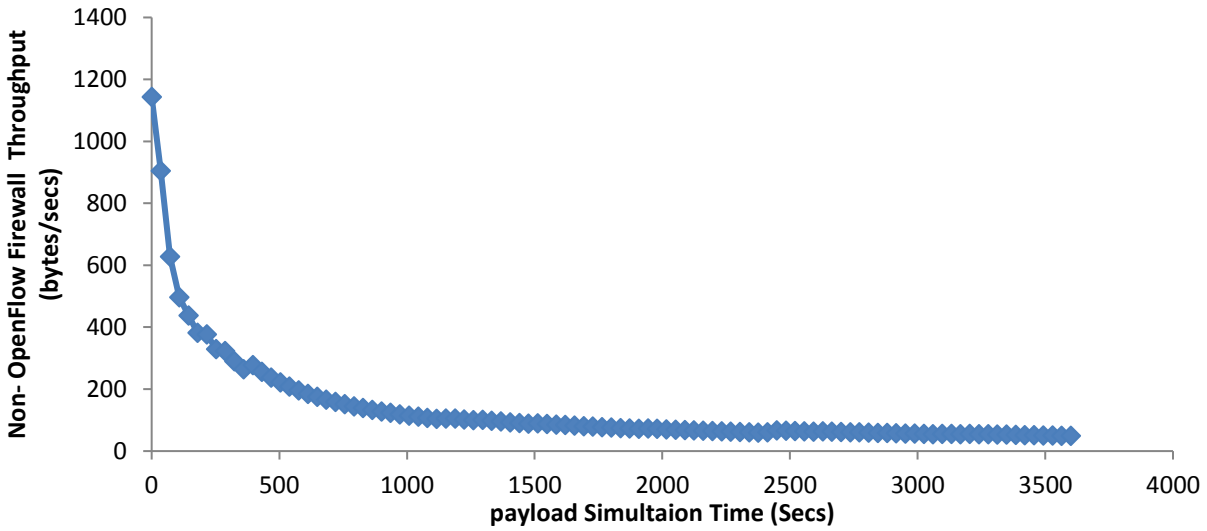

Figure 8: SG-IOTCI AMI Throughput with Openflow Firewall

3.2 SG-IoT-CI Traffic Model Validations

In this Section, the computational modeling scenarios involving six unsupervised machine learning algorithms are compared for performance validations. These include: K-Nearest Neighborhood with Isolated Forest (KNN +IF), Load Prediction with Regression (LPBSVR), Support vector machine (SVM), Load Prediction with Neural Network (LPBNN), Local Outlier Factor (LOF) and Lightweight On-line Detector of Anomaly (LODA). These are discussed in the next Section. SG-IoT-CI AMI grid metrics such tampering system latency profile, network service rate, queuing length, end-to-end throughput hits and prediction accuracy were carefully selected and investigated in order to understudy the impact of tampering in SG-IoT-CI ecosystems.

3.3 Secure SG-IoT-CI_AMI Latency

As depicted in Fig. 9, the SG-IoT-CI-AMI latency response under tampering scenario and SG AMI traffic model is evaluated for LPBSVR, Proposed KNN +IF, SVM, LPBNN, LOF and LODA respectively. The tampering latency responses were 20.96%, 11.98%, 19.31%, 19.76%, 19.01% and 8.98% respectively. This shows that KNN+IF is relatively optimal for reactive latency response.

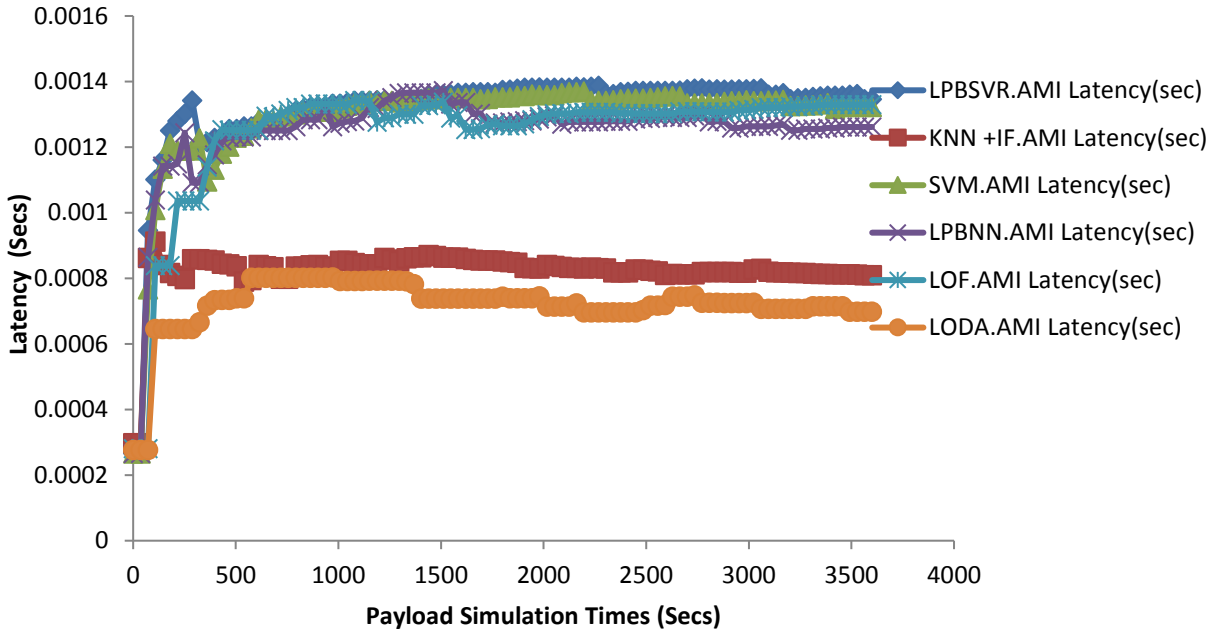

Figure 9: Secure SG-IOTCI_AMI Latency (Secs)

3.4 Secure SG-IoT-CI _AMI Service Rate

In the proposed SG-IoT-AMI Infrastructure, service rate refers to the pace at which clients end-users are served in a system, particularly in queuing theory. It is equal to the service time multiplied by itself. As depicted in Fig. 10, the SGIoT-AMI network service rate response under tampering scenario and SG AMI traffic model is evaluated for LPBSVR, Proposed KNN +IF, SVM, LPBNN, LOF and LODA respectively. The major contributing factor are the AMI SG gateway and control Load Balancer Docker Agent with Binomial sink and the SG AMI Network packet processing Scheme. The tampering service rates responses were 14.03%, 35.09%, 5.26%, 8.77%, 15.79% and 21.05% respectively. This shows that KNN+IF guarantees very high and optimal service response. The implication is that tampering incidences will be processed optimally. Appendix VI shows the SG-IoTCI_AMI tampering system network service rate datasets.

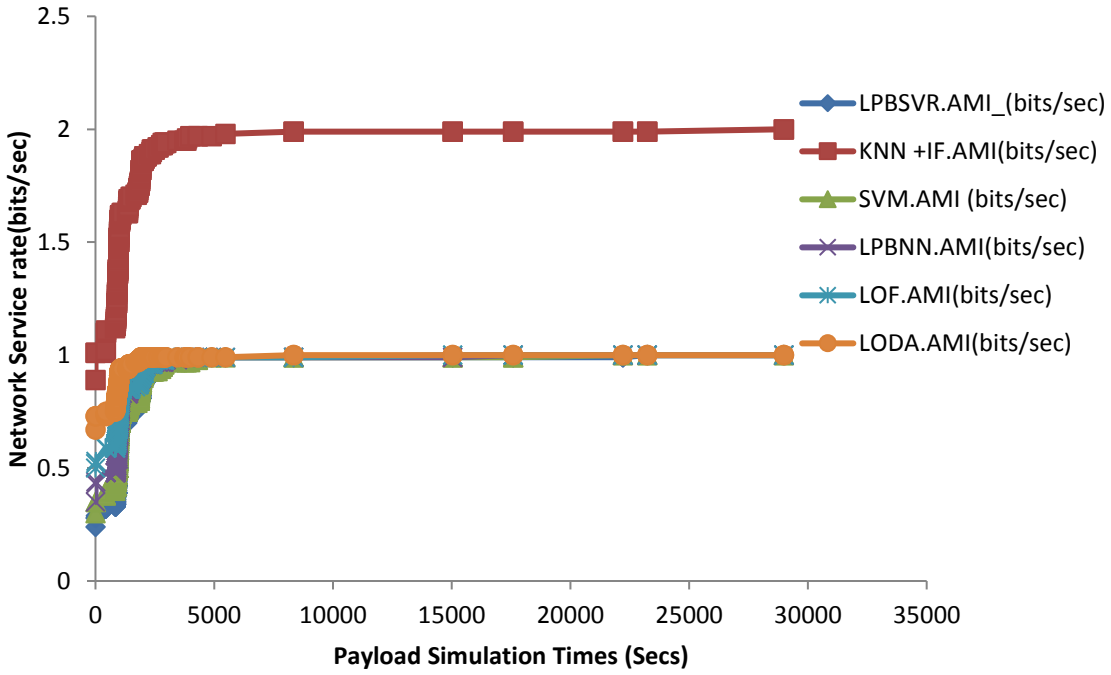

Figure 10: Secure SG-IOTCI_AMI Service Rate

3.5 Secure SG-IoT-CI_AMI Queuing Workload

In real systems, tampering service demands can be very difficult to measure. However, an optimization-based technique such as KNN+IF, this was addressed as a peak robust linear parameter estimation. This is used to aggregate measurements such as throughput and utilization during tampering instances. For service demands, network packet processing Scheme alongside the dynamic resource allocation and load balancing/scheduling sets up a queue. From Fig. 11, it was observed that AMI SG gateway and control Load Balancer Docker Agent with Binomial sink offers isolated queue length behaviour for the traffic processing Scheme. For dynamic resource allocation and load balancing/scheduling, KNN+IF offers very negligible queuing profile thereby allowing for efficiency network performance.

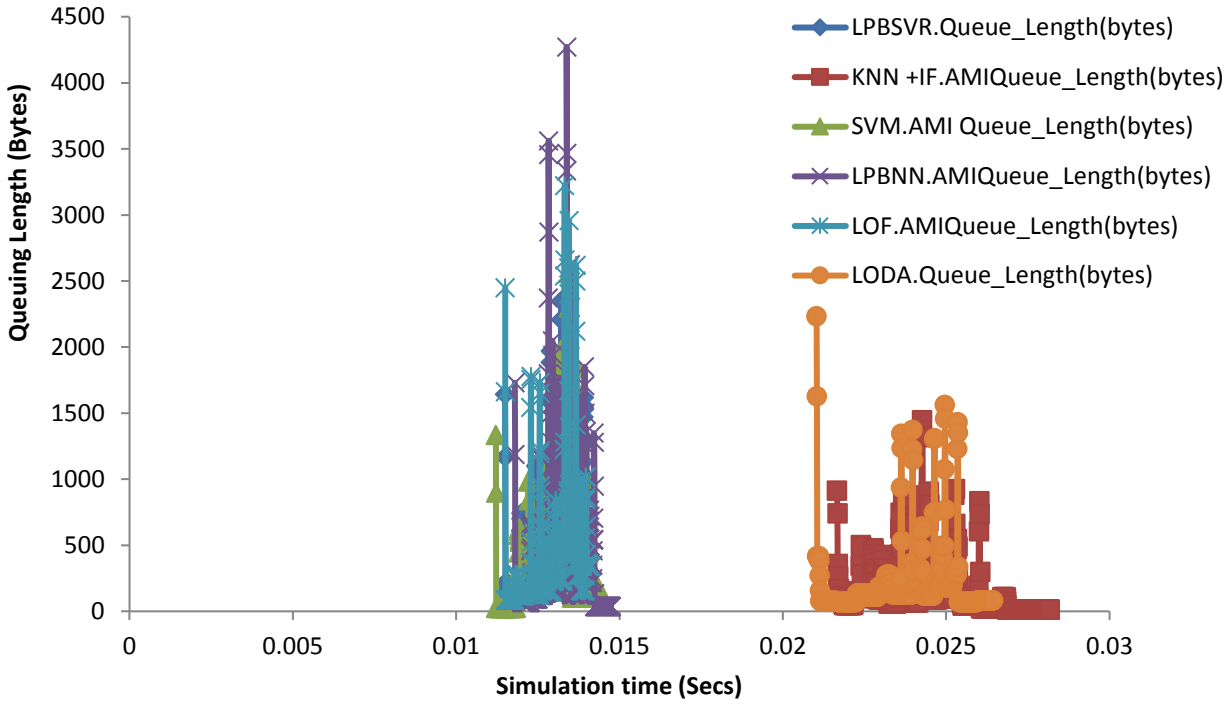

Figure 11: Secure SG-IoT-CI_AMI Queuing Workload Validation

3.6 Secure SG-IoT-CI AMI Throughput

The rate of successful data transfer over the network communication channel is measured by SGIoT throughput hit. The data in these messages is supplied through a network node via a logical link. The system's throughput under tampering attack vector is influenced by a number of factors, including the constraints of the underlying analog physical medium, the system components' available computing capacity, and end-user behaviour. When protocol overheads are included in, the practical rate of sent data might be much lower than the maximum attainable throughput; this is referred to as good put.

As depicted in Fig. 12, the SGIoT-AMI network throughput response under tampering scenario and SG AMI traffic model is evaluated for LPBSVR, Proposed KNN +IF, SVM, LPBNN, LOF and LODA respectively. The gateway and control load balancer docker agent with binomial sink and the SG AMI Network packet processing Scheme. The tampering throughput responses were 19.13%, 25.04%, 19.27%, 15.47%, 18.28% and 28.12% respectively. This shows that KNN+IF guarantees optimal throughput response. The implication is that tampering incidences will be processed optimally.

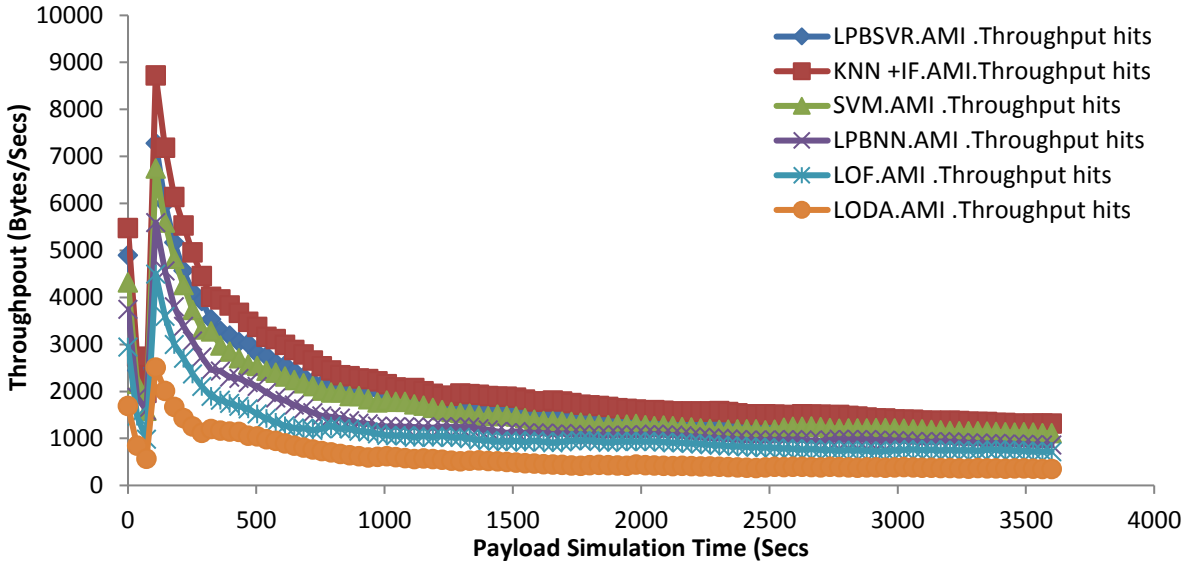

Figure 12: Secure SG-IOT_AMI Throughput Validation

So far, the metrics implications of SG-IoT-CI _AMI SG gateway and control Load Balancer Docker Agent with Binomial sink, SG-IoT-CI _AMI Network packet processing Scheme, SG-IoT AMI docker Orchestration as well as SG-IoT-CI dynamic resource allocation and load balancing/scheduling has been evaluated.

3.7 Secure SG-IoT-CI _AMI Accuracy Response

In this Section, the calculation of machine learning model performance metrics such as for assessing the performance of the classification model is presented using Python Sklearn. Accuracy/Precision was chosen due to its lightweight compared with Recall and F1-Score. The predicted data results could be read in the following manner: True Positive (TP) representing the value of correct predictions of positives out of actual positive cases. From the plot, false positive which represents the value of incorrect positive predictions was not visible. True Negative (TN) which represents the value of correct predictions of negatives out of actual negative cases was not visible. False Negative (FN) which represents the value of incorrect negative predictions was not visible. Given that SG-IoT AMI metrics on full scale subscription is vulnerable to errors, tampering on the AMI network from the riverbed statistics engine impacted various throughput shits LPBSVR, Proposed KNN +IF, SVM, LPBNN, LOF and LODA respectively. These gave 26.66%, 31.11%, 15.55%, 0.00%, 22.22% and 4.46% respectively. This implies that as users transact with the SG-IoT-AMI in the peak periods, the proposed KNN+IF offered best True Positive (TP) optimum response when compared to other schemes. This will make the objective of protecting the grid from attack vectors and payloads very feasible.

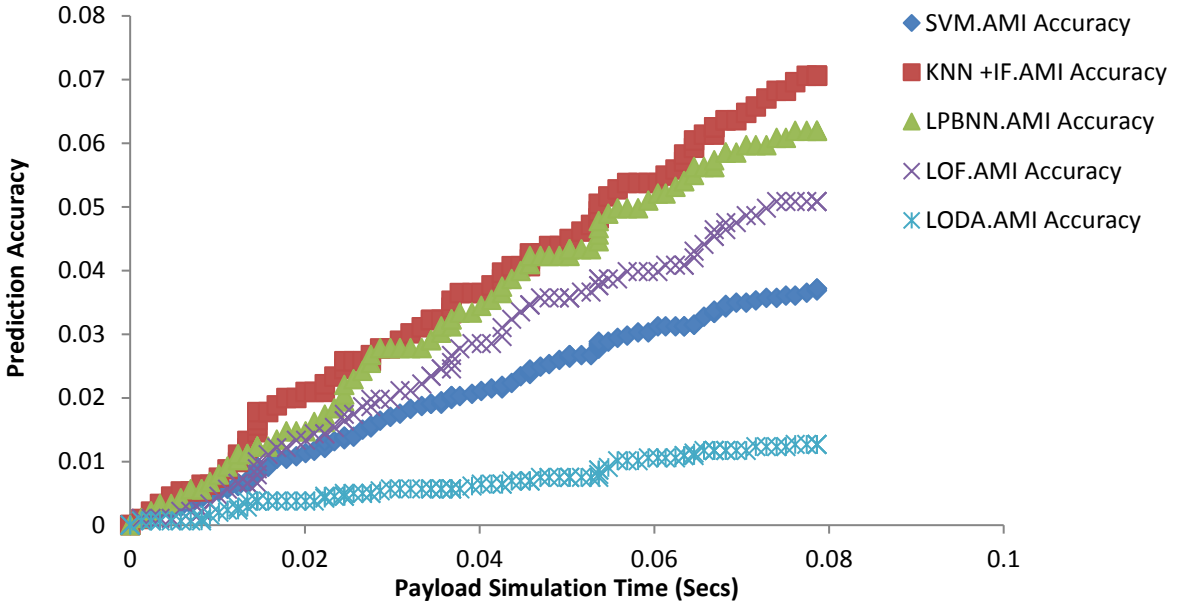

Figure 13: Secure SG-IoTCI _AMI Accuracy Validation

4.0. Conclusion

This paper developed a computational technique to achieve SG-IoT-CI automation for tampering mitigation suitable for Nigerian power grid. SG AMI hardware, SG hardware neural network and load management with tracking attributions were covered. First, computation models were introduced while exploring RNN with IF optimization model (RRN-IF) in the SG-IoT-CI. This was implemented to satisfy SG AMI load consumption tracking as well as Quality-of-Service (QoS) requirements. The system offers a reliable method for managing load demand using a combined symmetry of DISCO and Cloud optimization techniques. To characterize the system for efficient demand side monitoring in Nigeria, a formulation was developed for monitoring the tampered and non-untampered energy consumption via the SG probability models (Bernoulli and expanded Binomial distribution).

Using SG AMI design programming, the work developed an automated SG design algorithm for energy consumption. Also, for efficient load management and consumption tracking, neural network control was achieved using C++ and embedded designs on the SG system. In context, a functional AMI hardware was built to demonstrate SG coordination while linking its processes into the Cloud for peak and off-peak demand side management for energy tampering. tampering load control of end-user services, DSM, security and QoS optimization were achieved within SG-IoTCI to satisfy the requirement of real time SG automation. SG computational process model achieved in Minitab. In this case, a computation controller for SG architecture was used for learning/training accuracy for tampered and untampered status.

Also, various integration algorithms were developed and implemented from the edge to cloud. SG-IoTCI Webhook REST APIs were introduced alongside with OpenFlow (2-layer Datacenter model to solve highly complex problems of SG network supports. So far, the metrics implications of SG-IoTCI _AMI SG gateway and control Load Balancer Docker Agent with Binomial sink, SG-IoTCI _AMI Network packet processing Scheme, SGIoT AMI docker Orchestration as well as SG-IoTCI dynamic resource allocation and load balancing/scheduling has been evaluated.

In the SG network validation, six schemes were used for validation on a simulated on layered architecture. In all instances of load tampering for demand side management (DSM) strategy, the unsupervised algorithm was used to enhance SG AMI transaction considering the peak load demand. Also, the algorithm provided computational matrix for prediction and isolating tampered AMIs in SG-IoTCI. Essentially, K-Nearest Neighbourhood with Isolated Forest (KNN +IF) was compared with Load Prediction with Regression (LPBSVR), Support vector machine (SVM), Load Prediction with Neural Network (LPBNN), Local Outlier Factor (LOF) and Lightweight On-line Detector of Anomaly (LODA) algorithms. S-GIoTCI Metrics such as Service delays, throughput payload, energy data received,

cryptographic overhead, and Service traffic availability were carefully selected and investigated in order to understudy the impact of load scheduling on smart-grid ecosystems. The results showed that the proposed K-Nearest Neighborhood with Isolated Forest (KNN +IF) algorithm offered significant improvements.

References

Depuru, S., Wang, L., and Devabhaktuni, V., 2011. Support vector machine-based data classification for detection of electricity theft, *Proceedings of the. 2011 IEEE/PES Power Systems Conference and Exposition (PSCE)*, **p**p. 1-8.

Depuru, S., Wang, L., and Devabhaktuni, V., 2012 , Enhanced encoding technique for identifying abnormal energy usage pattern, *Proceedings of the. IEEE North American Power Symposium (NAPS)*, pp. 1-6.

Depuru, S., Wang, L., and Devabhaktuni, V., 2013 , High performance computing for detection of electricity theft, *International Journal of Electrical Power & Energy Systems*, vol. 47, pp. 21-30**.**

Hearst, M.,Dumais, S., and Scholkopf, B., 1998. Support vector machines, *IEEE Intelligent Systems and their Applications*, vol. 13, no. 4, pp. 18-28.

Nagi, J., Yap, k., Tiong, S. and Ahmed, K., 2011. Improving SVM-based nontechnical loss detection in power utility using the fuzzy inference system, *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 1284-1285.

Nagi, J.,Yap, k., Tiong, S. and Ahmed, k., 2018. Detection of abnormalities and electricity theft using genetic support vector machines, Proceedings of the *IEEE Region 10 Conference*, pp. 1-6.

Nagi, J., Yap, K., Tiong, S. and Ahmed, K., 2018. Nontechnical loss detection for metered customers in power utility using support vector machines, *IEEE Transactions on Power Delivery*, vol. 25, no. 2, pp.1162-1171**.**

Rong J., 2014. Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid, *Tsinghua Science and Technology,* 19 (2), pp. 105-120