International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 2, Mar-Apr-2020, ISSN (Online): 2395-566X

Iot in Oil & Gas: Exploring Technology &Firmware Security Techniques

Daniel Ekpah
Department of Electrical Engineering
METI
University of Port Harcourt

Kamalu .A. Ugochukwu
Department of Electrical Engineering
METI
University of Port Harcourt

Prince .O. Asagba
Department of Computer Science
METI
University of Port Harcourt

daniel.ekpah@uniport.edu.nginfo@metiuniport.com.ng

Abstract **- The Oil and Gas industry remains the hope of future energy mix and the engine that drives the clean gas initiative. The output of today's industry now rest on the geometrical change in the technological advancement such as artificial intelligence and IoT. This paper explored IoT applications and solutions that could be applied in the oil and gas industry in creating new value information generated from integrated sensors and actuators, communication channels and data analytics. Large variety of IoT deployments and protocols raises the IoT security assurance way. In this approach, the paper examines security solutions and cases capable of improving the quality and quantity of oil production.**

Keywords– **IoT, IoT Cloud Service, Security , Firmware, Cryptographic Security.**

I. BACKGROUND STUDY

The Internet of Things (IoT) in the oil & gas industry is the network of physical objects connected to the Internet. Wearable devices, vehicles, equipment, buildings, and just about any other thing can be embedded with electronics, software, sensors, and network connectivity. The ability to transfer data without requiring human interaction enables previously unprecedented amounts of data to be collected and exchanged with other devices, or through a central platform. Increasingly, forward-thinking oil & gas organizations are focusing their IoT initiatives less on underlying sensors, devices, and "smart" things and more on developing bold approaches for managing data, leveraging "brownfield" IoT infrastructure, and developing new business models.

II. ROLES OF IOT IN THE OIL AND GAS

In the oil & gas industry, sensors that monitor inventory levels of onshore oil tanks automatically dispatch trucks when the tanks need to be emptied. Sensors also monitor the performance of above-ground pumps to alert maintenance teams of potential and actual issues, and provide employees with early warning signs of possible safety issues to help prevent injuries and fatalities. Real-time oil tank sensor notifications enable continuous pumping while optimizing inventory transportation and minimizing downtime costs. Cloud-based digital dashboard visualizations convey information in an insightful manner that drives improved decision-making.
Modest IoT acoustic sensors in the oil field persistently break down oil organization (oil, water, gas, and so on.) inside pipelines, while research center tests from recreated field conditions and chose sensors showing ideal oil stream execution upgrade the readings. What's more, measurable models gauge the synthesis and stream rates to consistently improve getting ready for resulting tasks and decrease costly gear use.A fully loaded digital twin–a digital replica of an actual asset being constructed–gives oil & gas companies the ability to drill down virtually to obtain project progress updates (e.g., outstanding issues, bottleneck constraints) increasing knowledge-gathering efficiency. The digital twin also provides a 3D status report that allows management to "look around the platform" and understand the status of each component from design, to build, to assembly.
Information is fed into a dashboard that tracks real-time actuals at the part and component level and compares outputs against historical performance. Constructing a digital twin can improve project speed and quality, and provide insights into process and design improvement opportunities in the oil & gas industry.Maintaining the digital twin developed during asset construction (upgrades, equipment changes, etc.) can improve asset management and performance for oil & gas companies [3].
A digital twin predicts potential maintenance issues and optimizes operating parameters to elongate asset life and reduce downtime. Problems can be resolved quickly by drilling down into the digital twin to understand the issue and formulate a repair plan. In addition, comparing performance across assets and executing root-cause analyses helps to improve evidence-based asset management. These benefits can be expanded by using a visual- or virtual reality-based digital twin.Individual IoT sensors connected by fiber optic cables aid oil exploration by mapping subsurface drilling sites to determine new drilling locations and optimize output of operational sites. An Internet-connected seismic sensor network collects

data (over a million readings per site) and transfers it to servers to provide an image of the subsurface
new and existing drilling rig productivity and reduces the time required for site-selection data analysis.A Midstream Company was struggling with asset management lifecycle challenges as its aging infrastructure created competing investment priorities. They wanted to refocus their program on leveraging data to improve information management, predictive asset management, asset risk management, and asset management planning [5].

III. FIRMWARE SECURITY IMPROVEMENTS FOR IoTS

The techniques adopted for data collection in this paper incorporated those from hypothetical investigation of scientifically reproduced instances of the issue and essential information from a reason fabricated FPGA with PUF circuit configuration utilizing a coordinated firmware. Every technique will be configured to deliver information about certain parts of the work as abridged beneath:

1. Mathematical models that dependably exemplify the association and relative commitment of every one of the contributing factors that will be engaged with the input signals will be developed.
2. Appropriate input control calculations which permit information for recovery from the numerical models will be detailed.
3. A test circuit and programming will be created and developed for analyze approval of the numerical models and control calculations. Diverse hacking assaults which will reproduce the various dangers conduct of programmers will be tried so as to assess framework reaction and conduct.
4. The test information will be dissected to created trademark profiles which would be contrasted and the reenacted models.
5. The information will likewise be PC supported accomplished and later recovered to recreate the Hardware framework.
6. The output will be completed with two decoupling arrangement for the force dispersion system of the FPGA center, that the PUF circuit is to be executed utilizing the new firmware.
7. A lightweight social occasion based confirmation encryption framework for Web of things MTC utilizing FPGA crypto and PUF as significant gadget. Actualizing PUF innovation in a FPGA necessitates that the gadgets remember worked for cryptographic abilities, for example, equipment quickening agents SHA and elliptic bend cryptography (ECC). Additionally required is a cryptographic-grade genuine arbitrary piece generator. With these capacities, it is conceivable to make a client open key framework with the client's own testament authority by allowing each real machine in the system. This guarantees each machine has a chain-of-trust broadening right from the client's well-ensured root-CA keys on to the high-affirmation, nuclear level character that has been set up by the FPGA's PUF. Together, the PUF and PKI guarantees that each machine and their correspondence are ensured and can be securely, safely and unquestionably utilized in M2M, IoT and other hyper associated applications. In this section, we presented the methodology taken by the researcher whose work we plan to enhance to verify IoT gadgets dependent on Catalog traversal Powerlessness in IP Camera and DSL-N12E_C1 of the regular vulnerabilities exposures as appeared in Table 1 and accessible vindictive datasets in table 2 for implementation. Besides, Figure 1 portrayed the Systematization of equipment security and counter measures around the assault strategy utilized by the author including an arrangement of threat models, best in class resistances, and assessment measurements for significant equipment based assaults.

Table I: Publicly Available Common Vulnerabilities Exposures(Source:www.cvemitre.org)

Dataset	Short description
CVE-2018-995	Able to extract account credentials of DVR devices
CVE-2017-6780	Vulnerability for Cisco IoT Field Network Detector
CVE 2017-7911	Insufficient encapsulation Vulnerabilities
CVE-2017-7243	IoT Vulnerability which allow denial of services
CVE-2017-14913	IoT Vulnerability at Qualcomm
CVE 2016 0866	Xss Vulnerability in Tollgrade Light House Sensor
CVE-2015-0739	Vulnerability in Cisco FireSight System
CVE—2018-2361	Directory traversal Vulnerability in D-Link IP Camera
CVE 2018 9231	ASUS DSL-N12E_C1

Table II: Freely Available Datasets (source:www.freecodecamp.org/news)

Dataset	No. packets	No. files	Format	Short description
Contagiodump	988898pkt	1154	p-cap zipped	Collect malicious and exploit pcaps from various devices resources (2017–2018)
Virus-traffic analysis	2445211pkt	1291	p-cap zipped	Malicious network traffic (2017–2018)
GTISK-PANDA malrec	100201pkt	373	p-cap	Malware samples run in PANDA (2018)

IV. SECURITY KEY MIXTURE CALCULATION

Key generation process in AES is utilized to make a key to give constant insurance. As a matter of first importance, two 4 x 4 lattices, which are called remain and key were utilized to deliver key for encryption. A

spot was looked over the state framework and a key from the key grid arbitrarily and produce open key of H by sender in XOR activity. This progression of joining the HAN calculation was drawn from AEC calculation. We noticed that the key of h was created based on hexadecimal. At that point open key h is delivered. The point was to send a concealed message from sender. Making the received encryption procedure to be a tight security. This implies the scrambled message by the sender will be sent to the collector stealthily and security. In this manner, NTRU uneven encryption was utilized to improve the security. At the point when the sent message by the sender is scrambled, it ought not be recognizable by any individual other than planned beneficiary. Accept that a message is sent from the sender to the recipient. This message is in a multinomial called message. In the wake of making a multinomial message, the sender haphazardly picks a multi ostensible like r from the assortment like Lr. We noticed the hugeness of having a message by multi ostensible r. Along these lines, it can't be uncovered by the sender.

Encryption pr * h message 1.1

To pick a right parameter, coefficients of the polynomial equation somewhere in the range of q2 and p2 are chosen. So as p3, at that point it radically lessens and doesn't have any impact on the procedure, so we can finish up the accompanying connection. In the subsequent stage, parameter b will be determined. Simply increase private key f in introductory message which has been sent by the sender. At whatever point Decoding Message, we will be certain that the message will arrive at security to the beneficiary with no turmoil. D. Advanced Mark It is smarter to utilize computerized signature in gave HAN half and half encryption calculation to keep ID credit in this examination. It is only for message legitimacy and verification of personality and security. It ought to be noticed that for advanced mark, we should go from the sender to the collector, so the beneficiary of the previous advance goes about as the sender now, and the sender of the previous advance goes about as the recipient.

V. PUF-BASED IP CONFIRMATION FOR FPGAS

Here, we presented conventions dependent on PK encryption for security of IP squares. We contrasted our convention with past conventions in the writing and break down the preferences that PK cryptography gives in this setting. In the examined conventions, we just arrangement with the accompanying gatherings: the framework integrator or originator (SYS), the equipment IP-Supplier or center merchant (IPP), the equipment/FPGA producer (HWM) or seller, and a Confided in Outsider (TTP). We gave a point by point portrayal of all gatherings in the IP insurance chain. Notice that in the convention proposed in this segment just as in the work exhibited, it is expected that there exists an inside security module with access to the PUF circuit and either an AES module or elliptic bend (EC) and hash modules. The accompanying advances were taken to guarantee free spread of parcels across two specialized gadgets designed to work on powerful host setup convention (dhcp):
Discover - The PC conveys a communicate message on the system, planning to find a DHCP specialist organization. Offer - Each DHCP supplier hears the message, perceives the remarkable equipment address of the PC, and communicates something specific back contribution its administrations to that PC.
Request - The PC chooses a DHCP supplier from its contributions and afterward sends a solicitation to that supplier requesting an IP address task. Acknowledge - The focused on DHCP supplier recognizes the solicitation and issues an IP address to the PC that doesn't coordinate some other IP tends to at present dynamic on the system.

The PUF IP and FPGA verification gave the stage to the new firmware reconciliation. After the mix, we mimicked the new firmware to create information that was utilized in the following Section to investigate the realness of the coordinated firmware. The aftereffects of the Vulnerabilities in the two understood IoT gadgets that permitted the remote execution of self-assertive order fit for getting to the arrangement settings of the item were additionally broke down: Index traversal Helplessness in IP Camera and ADSL Switch DSL_N12E_C1. The following section additionally displayed the trial convention consequences of our work and estimated the effect of the structured incorporated firmware on the exhibition of IoT gadgets. The yield aftereffects of sets of IP addresses in the set tables were additionally disclosed utilizing Ping plotter to discover the fitness of the item preceding organization. So as to create worthy quality parcel circulations that depicted the conduct of powerlessness misuse, we understood the need of a huge bundle database for reproduction purposes. Luckily, Cisco frameworks conceded access to the openly downloaded dataset as appeared in table 2. From the datasets gave, we assembled a guarded code utilizing Linux as stated earlier in this work to guarantee that in hostile system demands are not caught by the planned firmware arrangements.

The found Powerlessness on the D-Lnk IP Camera as caught in table 3.1 permitted remote code execution by accomplishing a reverseshell association while exploiting the Uniform asset locator(URL) used to thumbnail the client pictures. We utilized the Wireshark as implicit application in our new firmware abuse form to produce a pcap document catching the assaults. The new firmware (NFW) involves a three-organize activity. The initial step plan the separating condition to identify the bundles, and the subsequent advance channel with a lot of parcels caught in a pcap channel and set of ordinary parcels. The

third step transformed the cross breed arrangement into IP table principles.

1. Discover - The PC conveys a communicate message on the system, planning to find a DHCP specialist organization. Offer - Each DHCP supplier hears the message, perceives the remarkable equipment address of the PC, and communicates something specific back contribution its administrations to that PC.
2. Request - The PC chooses a DHCP supplier from its contributions and afterward sends a solicitation to that supplier requesting an IP address task. Acknowledge - The focused on DHCP supplier recognizes the solicitation and issues an IP address to the PC that doesn't coordinate some other IP tends to at present dynamic on the system.

The PUF IP and FPGA verification gave the stage to the new firmware reconciliation. After the mix, we mimicked the new firmware to create information that was utilized in the following Section to investigate the realness of the coordinated firmware. The aftereffects of the Vulnerabilities in the two understood IoT gadgets that permitted the remote execution of self-assertive order fit for getting to the arrangement settings of the item were additionally broke down: Index traversal Helplessness in IP Camera and ADSL Switch DSL_N12E_C1.

The following section additionally displayed the trial convention consequences of our work and estimated the effect of the structured incorporated firmware on the exhibition of IoT gadgets. The yield aftereffects of sets of IP addresses in the set tables were additionally disclosed utilizing Ping plotter to discover the fitness of the item preceding organization. So as to create worthy quality parcel circulations that depicted the conduct of powerlessness misuse, we understood the need of a huge bundle database for reproduction purposes. Luckily, Cisco frameworks conceded access to the openly downloaded dataset as appeared in table 2.
From the datasets gave, we assembled a guarded code utilizing Linux as stated earlier in this work to guarantee that in hostile system demands are not caught by the planned firmware arrangements. The found Powerlessness on the D-Lnk IP Camera as caught in table 3.1 permitted remote code execution by accomplishing a reverseshell association while exploiting the Uniform asset locator(URL) used to thumbnail the client pictures. We utilized the Wireshark as implicit application in our new firmware abuse form to produce a pcap document catching the assaults. The new firmware (NFW) involves a three-organize activity. The initial step plan the separating condition to identify the bundles, and the subsequent advance channel with a lot of parcels caught in a pcap channel and set of ordinary parcels. The third

step transformed the cross breed arrangement into IP table principles.

Table III: Virus Traffic-Analysis scan Result on Internet Protocol address 94.100.0.100.

Severity	Cvss	Plugins	Name
Medium	6.4	51192	SSL cannot be trusted
Medium	5.0	11213	HTTP Trace/Track Methods allowed
Medium	4.3	65582	Web Application Potentially Vulnerable to clickjacking
Low	2.6	65821	SSL RC4 Cipher Suits Supported
Low	2.6	70658	SSH Server CBC Mode Cipher Enabled
Low	2.6	71049	SSH Weak MAC Algorithms enabled

Table IV: Virus Traffic-Analysis scan output on Internet Protocol address 94.101.0.102.

Severity	Cvss	Plugins	Name
Medium	6.4	51192	SSL cannot be trusted
Medium	5.0	42873	HTTP Trace/Track Methods allowed
Medium	4.3	10815	Web Application Potentially Vulnerable to clickjacking
Low	2.6	70658	SSH Server CBC Mode Cipher Enabled
Low	2.6	71049	SSH Weak MAC Algorithm Enabled

Table V: Intergated NFW Scan Result on Internet Protocol address 94.101.0.100.

Severity	Cvss	Plugins	Name
Info	N/A	10114	ICMP Timestamp Request
Info	N/A	10223	RPC Port mapper Service detection
Info	N/A	10267	SSH Server type and Version Information
Info	N/A	10287	Trace Route Information
Info	N/A	70658	Nessus TCP Scanner
Info	N/A	71049	SSH Protocol Versions Supported

Table VI: Intergated NFW Scan Result on Internet Protocol address 94.101.0.102

Severity	Cvss	Plugins	Name
Info	N/A	11111	RPC Service Enumeration
Info	N/A	11936	OS Identification
Info	N/A	12053	Host Fully Qualified Domain Name
Info	N/A	20094	VMware Virtual Machine Detection
Info	N/A	22964	Service Detection

Table VII: Throughput before new firmware Integration.

IP Route	Packet Speed	Packet Loss	Hop
154.68.195.129	5.2	0.0	1.0
154.68.196.17	14.4	4.0	2.0
154.68.196.37	78.1	4.0	3.0
154.68.196.42	48.1	4.0	4.0
212.187.136.145	187.9	4.0	5.0
213.248.96.37	137.6	4.0	6.0
62.115.138.150	198.7	32.0	7.0
80.91.249.9	194.6	4.0	8.0
80.91.246.85	188.2	8.0	9.0
62.115.143.85	174.7	8.0	10.0
141.208.192.138	201.7	32.0	11.0

Table VIII: Performance Throughput After firmware Integration.

IP Route	Packet Speed	Packet Loss	Hop
154.68.195.129	5.2	0.0	1.0
154.68.196.17	14.4	4.0	2.0
154.68.196.37	78.1	4.0	3.0
154.68.196.42	48.1	4.0	4.0
212.187.136.145	187.9	4.0	5.0
213.248.96.37	137.6	4.0	6.0
62.115.138.150	198.7	30.0	7.0
80.91.249.9	194.6	4.0	8.0
80.91.246.85	188.2	8.0	9.0
62.115.143.85	174.7	6.0	10.0
141.208.192.138	201.7	26.0	11.0

Table IX: Performance behaviour with the new integrated firmware.

?	No guard	New firmware
Hyper Text transferred (bytes)	207010000	207010000
Synchronised time perrequest (ms)	2.9345	2.937
Event per request (ms)	29.3465	29.367
Duration taken for investigations (seconds)	29.3465	29.367
Over-all transferred (bytes)	2097500000	2097500000
Transmission rate (Kb/sec)	2539.905	6534.1

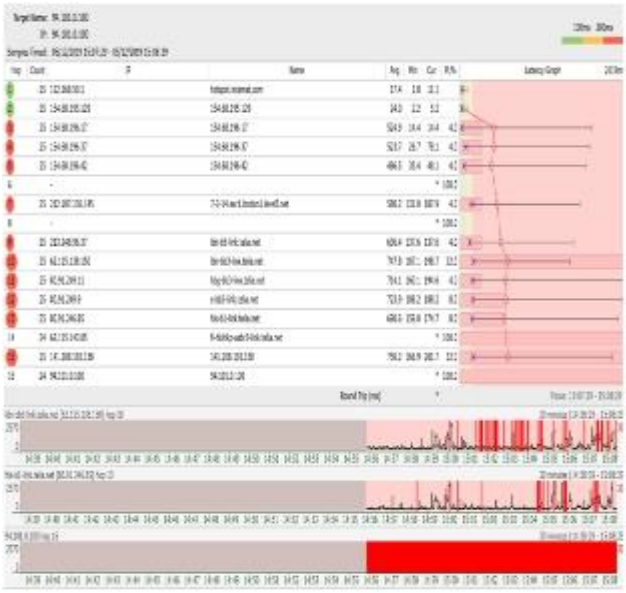

Fig.1. Round trip performance of IoT device on IP Address 94.101.0.100 before NFW.

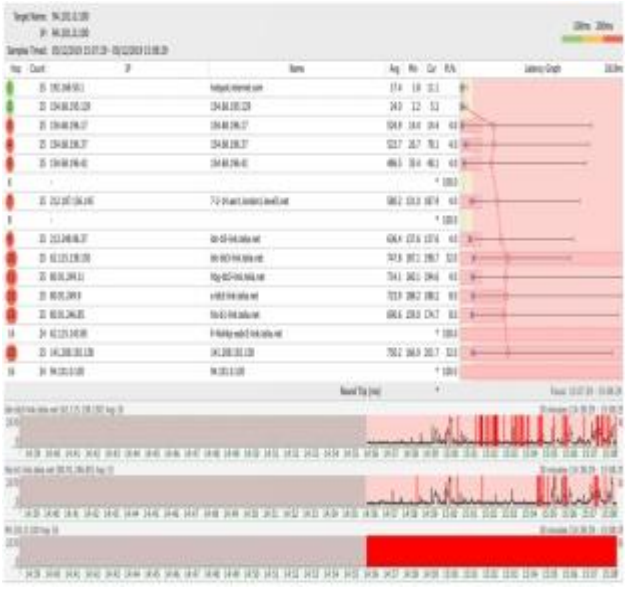

Fig.2. Round trip performance of IoT device on IP Address 94.101.0.100 after NFW

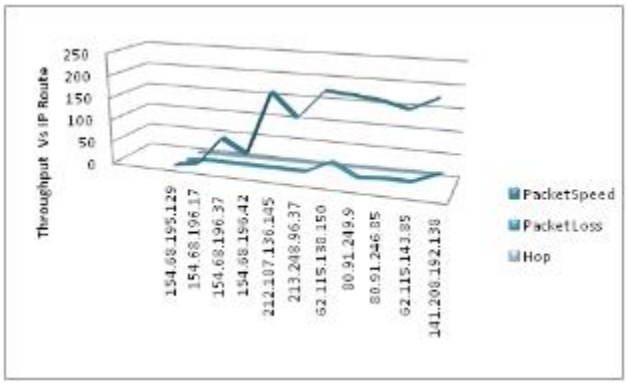

Fig.3. Throughput of the Operating System prior to Firmware Integration.

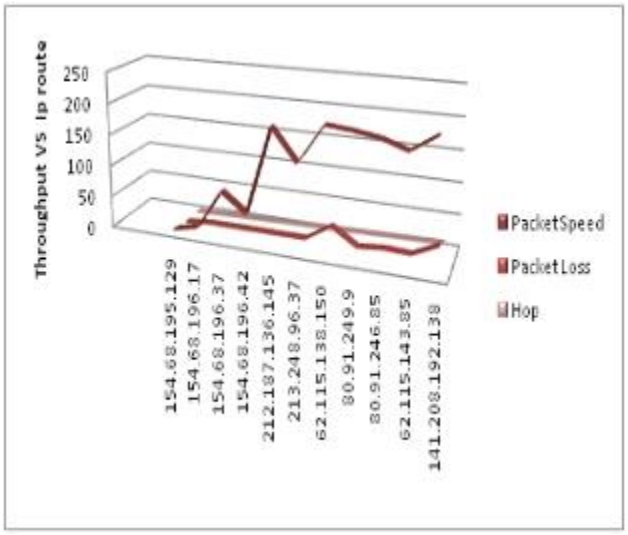

Fig.4. Throughput of the Operating System after the new firmware Integration.

VI. DISCUSSION OF EXPERIMENTAL RESULTS

Table1 uncovered generated packet expression. These new produced expressions were straightforwardly implanted in WebOs to ensure the end gadget. The subsequent investigation is about remote code helplessness in DSL_N12E_C1 switch, explicitly in firmware version of 1.1.2.3345. The defenselessness was considered as severe because it permitted the execution of odd codes utilizing obscure capacity of the record 'Main_Analysis_Content.asp'. A remote assailant would then be able to get to the switch as an advantaged client through telnet application and run Working framework directions. The new firmware had the option to channel this kind of assault by exemplifying the passage IP address as showed in table 3.6 utilizing wireshark. The created parcel is appeared in table 3.7 with increasingly cautious capacities.

The outcomes in Table 3 and Table 4 with the allocated IP delivered the option to distinguish three medium arranged vulnerabilities and the remainder of the discoveries was low and data kind of information. The key point here is that for these gadgets, the main discovering was identified with the SSL convention while Web Server finding was identified with the conceivably malevolent JavaScript. The coordinated propelled check gave fascinating outcomes from nature gave by frameworks to dissect Malware assaults. The primary observation was that, it had the option to distinguish a few Medium level arranged vulnerabilities from the application. These vulnerabilities need an increasingly indicated examination. Furthermore, propelled examine had the option to recognize numerous data ordered kind of vulnerabilities from the application has. Vulnerabilities with classification data commonly needn't bother with any further investigations. The vulnerabilities with class Medium were investigated all the more explicitly in light of the fact that they were potential dangers for offensives by vulnerabilities. Table 3.5 and 3.6 dependent on our new firmware filtering, all highlighted vulnerabilities were delegated data kind of information, making it liberated from malignant dangers. Table 3.7 expressed the exhibition between the nonattendance of assault assurances and the use of two NFW sifting rules. We evaluated the effect of utilizing our coordinated new firmware channels on IoT gadgets so as to decide whether they could be effectively used to ensure IoT gadgets against organize defenselessness abuse. To play out this reproduction, we utilized an Apache web server introduced on a Raspberry Pi 4 Model B. We utilized the functionalities of Apache HTTP server benchmarking and GNU parallel instruments to assess the effect of utilizing NFW firewalls in IoT equipment. Utilizing these apparatuses, we benchmarked the execution of two parallel tests making 10000 HTTP demands dispersed in 10 strings, with 1000 solicitations for each string. The normal of estimations made for parallelized tests is given as result. For correlation purposes, we utilized the produced NFW articulations for the two contextual analyses referred to in table 1. The outcomes arranged in

Table 5 shows that the exhibition sway when utilizing NFW channels is very constrained and won't seriously influences the general activity of IoT gadgets. We investigated the effect continuously by adding NFW rules to the channel and signifying 100 new standards and estimated the exchange rate after each NFW articulation was included. For whatever length of time that the exhibition is exceptionally impacted by the nearness of extra traffic in arrange and different procedures expending CPU, we plotted a pattern line to watch the components behaviour on resource allocations. As found in Figure 2, the throughput performace is near zero when utilizing something like 50 (nonfitting) NFW rules. In any case, the consideration of excess of 50 principles

unmistakably harms the presentation of GNU/Linux firewalling framework and would require the utilization of extra iptables speedup procedures, for example, the making of extra chains and counters-based enhancements

VII. CONCLUSION

IoT span over a huge range of industries and use cases by implementing a large number of devices and network communication protocols. Hence, applying security best practices during IoT deployments has become a critical requirement of IoT environments and infrastructures. The challenge is to synchronize the multitude of protocols used by IoT deployments related to infrastructure, device discovery and organization, data protocols and semantic representations,communication / TCP layer, infrastructure and data security.Possible solutions to achieve secure IoT deployments include JavaCard technology and investigations on those are part of future researches. One reason to choose JavaCard is its maturity to support security requirements within IoT and Industry 4.0 field.

VIII. ACKNOWLEDGEMENT

This paper acknowledges the great contribution of Deliotte and groups for promoting the fusion Oil and Gas to industry 4.0.

REFERENCES

[1]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies protocols and applications”, Proc. IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347 – 2376, 4th Quart. 2015, https://ieeexplore.ieee.org/document/712 3563/

[2]. I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulner abilities and challenges", Proc. IEEE Symp.Comput.Commun. (ISCC), Jul. 2015, pp. 180-187.

[3]. M. Doinea, C. Boja, L. Batagan, C. Toma, and M. Popa, “Internet of Things Based Systems for Food Safety Management”, InformaticaEconomică, vol. 19, no. 1, 2015, pp. 87-97

[4]. D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, J. Henry, IoT Fundamentals:Networking Technologies, Protocols, and Use Cases for the Internet of Things, Cisco Press, 2017, http://www.ciscopress.com

[5]. A. Minteer, Analytics for the Internet ofThings (IoT): Intelligent analytics for your intelligent devices, Packt Publishing,2017, http://www.packtpub.com

[6]. M. Popa, C. Toma, C. Boja, and A. Zamfiroiu, “Privacy and Security in ConnectedVehiclesEcosystems”, InformaticaEconomică, vol. 21, no. 4, 2017, pp. 29-40.

[7]. B. Russell, and D. van Duren, PracticalInternet of Things Security, Packt Publishing, 2016, http://www.packtpub.com

[8]. D. Slama, F. Puhlmann, J. Morrish and R. M. Bhatnagar. Enterprise IoT, O’Reilly Inc. Publishing House, 2016

[9]. Wikipedia Industry 4.0: https://en.wikipedia.org/wiki/Industry_4. 0

[10].Gems Sensors & Controls – Oil and Gas Applications: http://www.gemssensors.com/ Markets/Oil-and-Gas

[11].Oracle IoT CS libraries: http://www.oracle.com/technet work/indexes/downloads/iot-client-libraries-2705514.html

[12].Understanding REST from Spring: https://spring.io/understanding/REST

[13].RESTful API and Taxonomy: http://searchmicroservices.techtarget.com /definition /RESTful-APIOWASP Security Cheat Sheet.