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

Intrusion Detection System (IDS) in Internet of Things (IoT) Devices for Smart Home

M.D. Shakhawat Shafaet Romeo, Nor Azlina Abd Rahman and
Yusnita Yusof

Abstract--- *The Internet of Things (IoT) is an emerging technology where smart devices are flawlessly connected to the world using the internet to provide common goals and objectives such as aiding home automation service. Research on the usage of IoT devices being done and based on statistics showed that this technology is demanding nowadays and it shows increasing trends over the years. Influence factors towards IoT usage are also being discussed in terms of available infrastructure such as network connectivity, IoT devices and security technology to protect the environment. Other influence factors such as ease of use, social impact and trust are also being considered. Several Intrusion Detection systems such as Snort, Suricata, Bro and security Onion are being analyzed to identify the best services to be implemented for the proposed system. A survey is taken for the purpose of this research in order to obtain the public's concern and opinions on IoT security that critically examined with supporting evidences. The outcome of this paper is by proposing a framework of Intrusion Detection System for IoT Devices in Smart Home based on research and survey conducted.*

Keywords--- *Internet of Thing (IoT), Intrusion Detection System (IDS), IoT Devices, Smart Home, HIDS, NIDS.*

I. INTRODUCTION

Internet of Thing (IoT) is a technology emerging Internet based technical architecture where everyday devices are connected to each other and to the user. This technology is rapidly increasing and getting cheaper and cheaper to use and more available for everyone. As there is no stop for this technology to rise there are many concerns which can affect society in a security perspective.

Intrusions Detection System, which is basically software that can detect unusual activity in a network and report the user. This technology can be used along with Internet of thing (IoT) devices to connect all the IoT devices in a smart home. The user will be able to monitor and also detect if the devices have been breached by any hackers when all of these devices are connected to the intrusion detection system (IDS). Internet of Things Devices are increasing in demand day by day, especially in the normal households where people make use of IoT devices to ease daily task and operation, the global smart home market is expected to grow to USD 119.26 billion by 2022 [1], this huge investment in IoT smart home technology is proof that the demand from the customer side is increasing drastically.

M.D. Shakhawat Shafaet Romeo, Asia Pacific University of Technology & Innovation Technology Park Malaysia, Bukit Jalil, Kuala Lumpur. E-mail: romeoshakawat@gmail.com

Nor Azlina Abd Rahman, Asia Pacific University of Technology & Innovation Technology Park Malaysia, Bukit Jalil, Kuala Lumpur. E-mail: nor_azlina@apu.edu.my

Yusnita Yusof, Asia Pacific University of Technology & Innovation Technology Park Malaysia, Bukit Jalil, Kuala Lumpur. E-mail: yusnita@apu.edu.my

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

Figure 1 illustrates the general idea of how the system works, all the IOT devices in the house are protected by the “Green shield” made by the IDS in the computer metaphorically. This shield will protect the house; if the shield is “touched” by an intruder the IDS will alert the owner of the house.

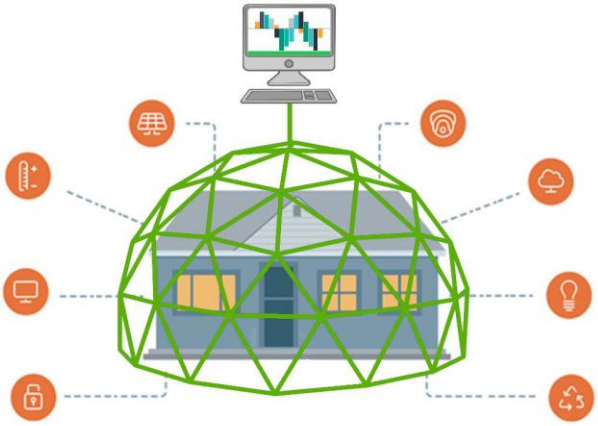


Figure 1: IDS System for Smart Home with IoT devices

According to a recent forecast by market research firm Gartner [2], our homes will become a whole IoT smarter over the next few years. Gartner expects the so-called Internet of Things to break through to the mainstream, predicting the number of smart objects in use worldwide to reach 25 billion by 2020. This revolution expansion of IoT devices will bring security issues where at this point an Intrusion Detection System is needed to protect all the IoT devices from being compromise or attack by intruders.

The Internet of Things covers a wide range of products: from consumer products such as Nest's smart thermostats (Nest was recently acquired by Google for $3.2 billion) to intelligent street lighting that could help governments save energy - the potential for connected objects is basically limitless. Gartner expects a certain degree of connectivity to become the standard for everyday products, meaning that smartphones might soon become even smarter, as they turn into a remote control for everything from refrigerators to lamps and washing machines. Figure 2 shows statistics of the growth of IoT devices for smart homes [3]. Based on Figure 2, the green bar represents the IoT for smart home consumers, yellow represents IoT for corporate offices consumers and the blue represents IoT installed in cars. It shows increasing trends of IoT devices used in different area across the years. This statistics shows the growth of IoT devices usage among the users around the world.

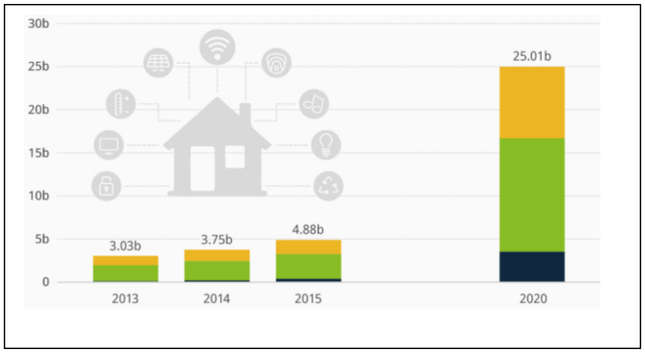


Figure 2: The IoT Usage Worldwide [3]

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

II. Materials and Methods

The statistic below show the number of Internet of Things (IoT) usage among Asia Pacific users from the year 2013 to 2020. In 2018, 7.02 billion IoT units were in use in the Asia Pacific Region [4].

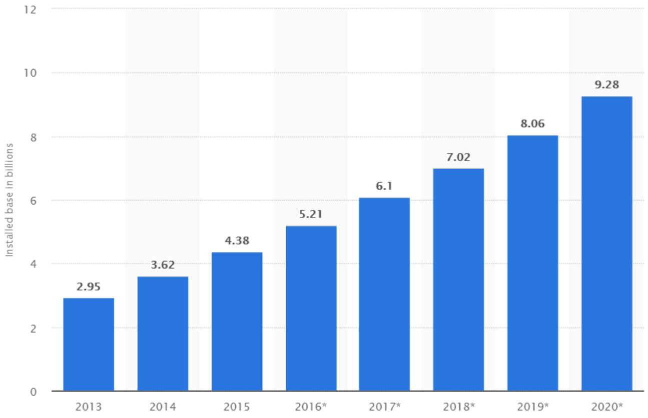


Figure 3: The IoT Usage in Asia Pacific region [4]

Figure 3 shows the statistic of IoT Users in Asia Pacific region [4]. The graph shows the growth trend of IoT usage among Asia Pacific user from the year 2013 to 2020.

2.1. Influence Factor towards IoT Usage in Household

Recently, IoT is one of the latest technologies, which have revolutionized in various fields and the most important developments in household that led to the adopting this type of technology. The initial smart home service was promoted through the automation of the domestic system, aiming for convenience, comfort, stability, amenity, health, reduction of household labor, and energy efficiency.

Since then, developments of the wireless Internet and smart phones have extended the concept of a smart home to services that can be remotely controlled anytime and anywhere. In the IoT era, household electrical appliances and information and communication devices are interconnected, and the smart home is developing into a form of an artificial intelligence service that operates by self-understanding the behaviors of the residents. Therefore, the smart home in the IoT era is a concept that adds interconnectedness to the traditional characteristics of automation and remote controllability [5].

Service stability, security, and privacy also have been suggested as important factors that may hinder user acceptance. These factors can be summarized as the reliability of the service. The smart home environment is a factor that must be considered because it is closely related to the user’s life and can cause serious damage in the case of a dangerous situation. Thus, automation, remote controllability, interconnectedness, and reliability can be summarized as crucial factors for accepting a smart home service.

What people wants in a smart home is the ability to control IoT devices remotely. This is a core feature of a smart home system since users prefer to instantly control smart home services such as controlling lamps, curtains, and information appliances [5]. However, to design an intelligent and remote-controllable smart home system, a network connection is essential. Many networks exist with a variety of features such as Bluetooth IEEE 802.15.4, Z-

Wave, and Wi-Fi. To enable remote control, networks should be standardized and interconnected to expand the use of smart home services. Most electronic devices support the Wi-Fi protocol, which allows home devices to be controlled by mobile devices. When remote control is possible, the general concept of smart, anywhere and anytime, can actually be implemented [5].

Many researchers tried to determine the factors that affect the acceptance of IoT by customers. As according to LinglingGao et al worked to investigate factors that might affecting on accepting IoT in daily lives in China, where they used Technology Acceptance Model (TAM) as a theory accepting model, and their investigation included around 368 respondents. However, the results indicate that the most important factors that may affect the behaviour of users are perceived ease of use, social impact, and trust.

All perceived behaviours played a significant impact on user intent [6]. While, in UK the researcher, Bushra Alolayan et al attempted to discover the factors that affect the consumer through the adoption of the smart refrigerator by students. Thus, the results indicated that the most important factors that had a huge impact on consumer intent were the social factors such as cost, concern of this technology, as well as Perceived usefulness, and perceived ease of use as technical factors [7].

Since the concept of IoT is still new, researchers have attempted to conduct qualitative studies in order to determine the factors that have high influence the user's intention to use this new technology. Such as the research that conducted by Acquity Group, that examined the concerns of customers in adoption of IoT, where they conducted a survey which involved around 2000 customers in the United States, and through that they found that the awareness of technology, interest , as well as its cost , linking with security and privacy issues were the most important concerns of customers and the most factors that hinder their desire to adopt such technology [8]. However, as the IoT industry continues to grow, there is a need to develop a framework that enhance the security of IoT devices in the household and that is the main purpose of this paper.

III. A REVIEW ON INTRUSION DETECTION SYSTEM

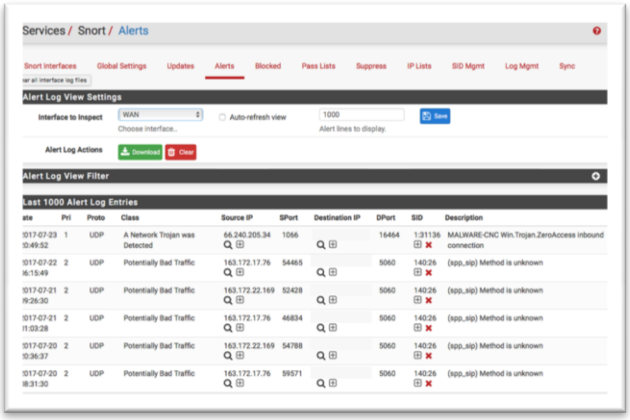
There are several Intrusion Detections System that available and can be used in any kind of networks depending on the configurations from the user. Some of that system is as discussed below.

3.1. Snort

Snort is an open source network intrusion detection system (IDS) and prevention system developed by Marin Reosch. It has multiple core features which makes it stand out from most of the other IDS such as real time traffic monitoring and analysis, detect malicious payloads or suspicious activities in the network.

Snort is dependent on "libpcap" which is a library used to capture packet in the network, this tool is used in TCP/IP traffic analyzers and sniffers. Snort can detect a variety of attacks such as buffer overflow, common gateway interface (CGI), denial of service attacks, SMB probes and stealth port scan. When an attack is detected snort alerts the user with a pop up windows and saves logs in the "syslog" which is a separate file for alerts in linux for Snort [9].Figure 4 below shows the alert page for Snort.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019



Interface to Inspect: WAN
Choose interface..

□ Auto-refresh view

1000
Alert lines to display.

Alert Log Actions

Last 1000 Alert Log Entries

ate	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
:017-07-23 :0:49:52	1	UDP	A Network Trojan was Detected	66.240.205.34	1066		16464	1:31136	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
:017-07-22 :6:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465		5060	140:26	(spp_sip) Method is unknown
:017-07-21 :9:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428		5060	140:26	(spp_sip) Method is unknown
:017-07-21 :1:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834		5060	140:26	(spp_sip) Method is unknown
:017-07-20 :0:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788		5060	140:26	(spp_sip) Method is unknown
:017-07-20 :8:31:30	2	UDP	Potentially Bad Traffic	163.172.17.76	59571		5060	140:26	(spp_sip) Method is unknown

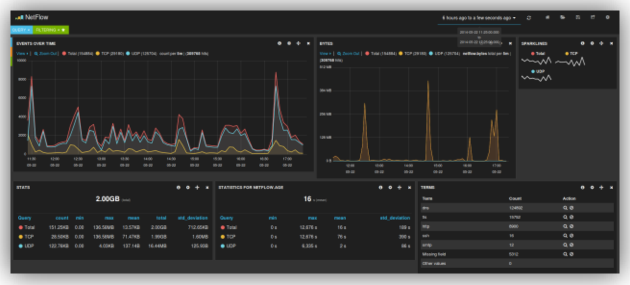
Figure 4: Alert Section of Snort [10]

Snort was tested by the "European network security testing organizations" also known as NSS group, it was tested along with 15 other Intrusion Detections Systems developed by many different big shot companies such as Cisco, Symantec, Computer Associates and many more, Snort incredibly enough out-performed all the competitions and still remains one of the most powerful open source IDS [9].

3.2. *Suricata*

Suricata is an open source Intrusion Detection System (IDS). It is an Inline Intrusion Prevention system (IPS) and a Network Security Monitoring systems (NSM) and it can perform offline pcap processing.

The complexity of this software is really high, which makes it very powerful and an extensive signature-based IDS, it has powerful Lua scripting support which can be used to detect complex and sophisticated signatures in the network. It is developed using standard input and output formats like JSON and YAML integrations which makes database reading effortless, fluid and fast. Suricata is developed from a fast-paced community which highly focuses on security, usability and efficiency. The Suricata project is owned by Open Information Security Foundation (OISF) which is a non-profit organization. Figure 5 shows Suricata in the network flow monitoring page.



2.00GB (total)

Query	count	min	max	mean	total	std_deviation
● Total	151.25KB	0.00	136.58MB	13.57KB	2.00GB	712.65KB
● TCP	28.50KB	0.00	136.58MB	71.47KB	1.99GB	1.60MB
● UDP	122.76KB	0.00	4.03KB	137.14B	16.44MB	125.93B

16 s (mean)

Query	min	max	mean	std_deviation
● Total	0 s	12,676 s	16 s	189 s
● TCP	0 s	12,676 s	76 s	390 s
● UDP	0 s	6,335 s	2 s	86 s

Term	Count	Action
dns	124602	
tls	15752	
http	6980	
ssh	16	
smtp	12	
Missing field	5312	
Other values	0	

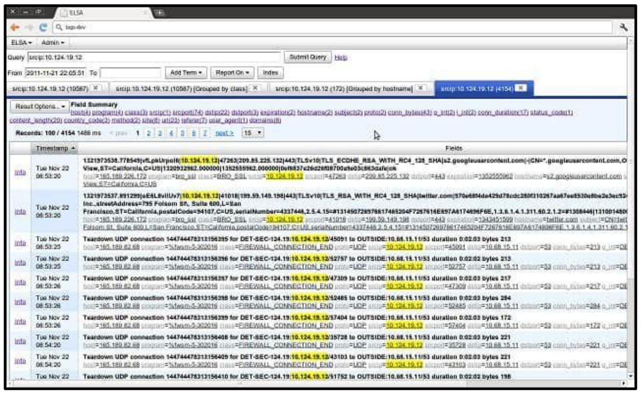
Figure 5: Suricata network flow [11]

3.3. *Bro*

Bro is another great free IDS and Intrusion Prevention System (IPS). This software supports Linux, Unix, and Mac OS. Bro uses network-based intrusion detection methods. While tracking the network for malicious activity, Bro also gives statistics on the performance of your network devices and traffic analysis.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

The detection rules of Bro operate at the Application Layer, which means that it is able to detect for signatures across packets. Bro also has a database of anomaly-related detection rules. The detection stage of Bro's work is conducted by the 'event engine.' This writes packets and suspicious events to file. Policy scripts search through the stored records for signs of intruder activity. The user can also write its own policy scripts, but they are also included with the Bro software [12]. As well as looking at network traffic, Bro will keep an eye on device configurations. Network anomalies and irregular behavior of network devices are tracked through the monitoring of SNMP traps. As well as regular network traffic, Bro pays attention to HTTP, DNS, and FTP activity. The tool will also alert the user if it detects port scanning, which a hacker method is used to gain unauthorized access to a network. Figure 6 shows a screenshot of the application [12].



Query srcip:10.124.19.12

From 2011-11-21 22:05:51 To

srcip:10.124.19.12 (10587) | srcip:10.124.19.12 (10587) [Grouped by class] | srcip:10.124.19.12 (172) [Grouped by hostname] | srcip:10.124.19.12 (4154)

Field Summary
host(4) program(4) class(3) srcip(1) srcport(74) dstip(22) dstport(3) expiration(2) hostname(2) subject(2) proto(2) conn_bytes(43) o_int(2) i_int(2) conn_duration(17) status_code(1) content_length(20) country_code(3) method(2) site(8) uri(23) referer(7) user_agent(1) domains(8)

Records: 100 / 4154 1486 ms

```
Tue Nov 22 08:53:20  1321973538.778549|vfLpkUrpoI6|10.124.19.12|47263|209.85.225.132|443|TLSv10|TLS_ECDHE_RSA_WITH_RC4_128_SHA|s2.googleusercontent.com|-|CN=*.googleusercontent.com,O
                     View,ST=California,C=US|1320932962.000000|1352555962.000000|0ef6837e26d26f08700a9e03c863dafe|ok
                     host=165.189.226.172 program=bro_ssl class=BRO_SSL srcip=10.124.19.12 srcport=47263 dstip=209.85.225.132 dstport=443 expiration=1352555962 hostname=s2.googleusercontent.com
                     View,ST=California,C=US
Tue Nov 22 08:53:20  1321973537.891299|oE6L8vIIUv7|10.124.19.12|41018|199.59.149.198|443|TLSv10|TLS_RSA_WITH_RC4_128_SHA|twitter.com|570e6854de429d78cdc280f310267aa67ee8530a8be2e3ec52
                     Inc.,streetAddress=795 Folsom St, Suite 600,L=San
                     Francisco,ST=California,postalCode=94107,C=US,serialNumber=4337446,2.5.4.15=#131450726976617465204F7267616E697A6174696F6E,1.3.6.1.4.1.311.60.2.1.2=#1308446|131001450
                     host=165.189.226.172 program=bro_ssl class=BRO_SSL srcip=10.124.19.12 srcport=41018 dstip=199.59.149.198 dstport=443 expiration=1343451599 hostname=twitter.com subject=CN=twit
                     Folsom St, Suite 600,L=San Francisco,ST=California,postalCode=94107,C=US,serialNumber=4337446,2.5.4.15=#131450726976617465204F7267616E697A6174696F6E,1.3.6.1.4.1.311.60.2.1
Tue Nov 22 08:53:25  Teardown UDP connection 1447444783131156395 for DET-SEC-124.19:10.124.19.12/45091 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 213
                     host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=45091 dstip=10.68.15.11 dstport=53 conn_bytes=213 o_int=OE
Tue Nov 22 08:53:25  Teardown UDP connection 1447444783131156396 for DET-SEC-124.19:10.124.19.12/52757 to OUTSIDE:10.68.15.11/53 duration 0:02:02 bytes 213
                     host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=52757 dstip=10.68.15.11 dstport=53 conn_bytes=213 o_int=OE
Tue Nov 22 08:53:26  Teardown UDP connection 1447444783131156397 for DET-SEC-124.19:10.124.19.12/47309 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 217
                     host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=47309 dstip=10.68.15.11 dstport=53 conn_bytes=217 o_int=OE
Tue Nov 22 08:53:26  Teardown UDP connection 1447444783131156398 for DET-SEC-124.19:10.124.19.12/52465 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 284
                     host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=52465 dstip=10.68.15.11 dstport=53 conn_bytes=284 o_int=OE
Tue Nov 22 08:53:26  Teardown UDP connection 1447444783131156399 for DET-SEC-124.19:10.124.19.12/57404 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 172
                     host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=57404 dstip=10.68.15.11 dstport=53 conn_bytes=172 o_int=OE
Tue Nov 22 08:54:20  Teardown UDP connection 1447444783131156408 for DET-SEC-124.19:10.124.19.12/35728 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 221
                     host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=35728 dstip=10.68.15.11 dstport=53 conn_bytes=221 o_int=OE
Tue Nov 22 08:54:20  Teardown UDP connection 1447444783131156409 for DET-SEC-124.19:10.124.19.12/43103 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 221
                     host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=43103 dstip=10.68.15.11 dstport=53 conn_bytes=221 o_int=OE
Tue Nov 22           Teardown UDP connection 1447444783131156410 for DET-SEC-124.19:10.124.19.12/51752 to OUTSIDE:10.68.15.11/53 duration 0:02:02 bytes 198
```

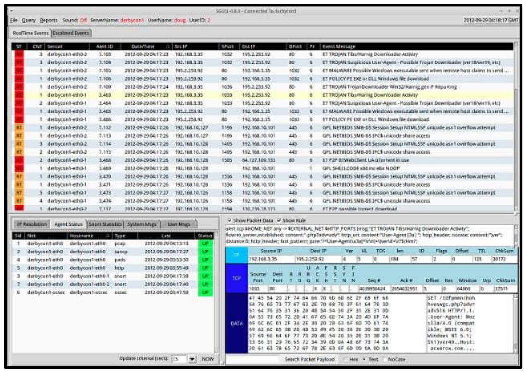
Figure 6: BRO Screenshot [12]

3.4. Security Onion

It is a mixture of IDS solutions, and anyone can get Security Onion system for free. The developers took elements from the source code of Snort, Suricata, and Bro and stitched them together to make this free Linux-based NIDS/HIDS hybrid. Security Onion is written to run on Ubuntu and it also integrates elements from front-end systems and analysis tools including Snorby, Sguil, Squert, Kibana, ELSA, Xplico, and NetworkMiner [13]. Although Security Onion is classified as a NIDS, it does include HIDS functions as well. It will monitor your log and config files for suspicious activities and check on the checksums of those files for any unexpected changes.

One downside of the Security Onion's comprehensive approach to network monitoring is its complexity. It has several different operating structures and there isn't really sufficient learning material online or bundled in to help the network administrator get to grips with the full capabilities of the tool [13]. Network analysis is conducted by a packet sniffer, which can display passing data on a screen and also write to a file. The analysis engine of Security Onion is where things get complicated because there are so many different tools with different operating procedures that you may well end up ignoring most of them. The interface of Kibana provides the dashboard for Security Onion and it does include some nice graphs and charts to ease status recognition [13].

Both signature-based and anomaly-based alert rules are included in this system. The user can get information on device status as well as traffic patterns. Figure 7 shows a screen shot on how Security Onion capturing and display the information to the users.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	3	derbycon1-eth0-2	7.103	2012-09-29 04:17:23	192.168.3.35	1032	195.2.253.92	80	6	ET TROJAN Tibs/Harnig Downloader Activity
RT	3	derbycon1-eth0-2	7.104	2012-09-29 04:17:23	192.168.3.35	1032	195.2.253.92	80	6	ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19, etc)
RT	1	derbycon1-eth0-2	7.105	2012-09-29 04:17:23	195.2.253.92	80	192.168.3.35	1032	6	ET MALWARE Possible Windows executable sent when remote host claims to send ...
RT	1	derbycon1-eth0-2	7.106	2012-09-29 04:17:23	195.2.253.92	80	192.168.3.35	1032	6	ET POLICY PE EXE or DLL Windows file download
RT	1	derbycon1-eth0-2	7.109	2012-09-29 04:17:24	192.168.3.35	1036	195.2.253.92	80	6	ET TROJAN TrojanDownloader Win32/Harnig.gen-P Reporting
RT	1	derbycon1-eth0-1	3.463	2012-09-29 04:17:23	192.168.3.35	1033	195.2.253.92	80	6	ET TROJAN Tibs/Harnig Downloader Activity
RT	2	derbycon1-eth0-1	3.464	2012-09-29 04:17:23	192.168.3.35	1033	195.2.253.92	80	6	ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19, etc)
RT	1	derbycon1-eth0-1	3.465	2012-09-29 04:17:23	195.2.253.92	80	192.168.3.35	1033	6	ET MALWARE Possible Windows executable sent when remote host claims to send ...
RT	1	derbycon1-eth0-1	3.466	2012-09-29 04:17:23	195.2.253.92	80	192.168.3.35	1033	6	ET POLICY PE EXE or DLL Windows file download
RT	1	derbycon1-eth0-2	7.112	2012-09-29 04:17:26	192.168.10.127	1196	192.168.10.101	445	6	GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt
RT	1	derbycon1-eth0-2	7.113	2012-09-29 04:17:26	192.168.10.127	1196	192.168.10.101	445	6	GPL NETBIOS SMB-DS IPC$ unicode share access
RT	3	derbycon1-eth0-2	7.114	2012-09-29 04:17:26	192.168.10.128	1495	192.168.10.101	445	6	GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt
RT	2	derbycon1-eth0-2	7.115	2012-09-29 04:17:26	192.168.10.128	1495	192.168.10.101	445	6	GPL NETBIOS SMB-DS IPC$ unicode share access
RT	2	derbycon1-eth0-1	3.468	2012-09-29 04:17:26	192.168.10.128	1505	64.127.109.133	80	6	ET P2P BTWebClient UA uTorrent in use
RT	1	derbycon1-eth0-1	3.469	2012-09-29 04:17:26	192.168.10.128		192.168.10.101		1	GPL SHELLCODE x86 inc ebx NOOP
RT	1	derbycon1-eth0-1	3.470	2012-09-29 04:17:26	192.168.10.128	1536	192.168.10.101	445	6	GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt
RT	1	derbycon1-eth0-1	3.471	2012-09-29 04:17:26	192.168.10.128	1536	192.168.10.101	445	6	GPL NETBIOS SMB-DS IPC$ unicode share access
RT	5	derbycon1-eth0-1	3.473	2012-09-29 04:17:27	192.168.10.126	1158	192.168.10.101	445	6	GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt
RT	4	derbycon1-eth0-1	3.474	2012-09-29 04:17:27	192.168.10.126	1158	192.168.10.101	445	6	GPL NETBIOS SMB-DS IPC$ unicode share access
RT	1	derbycon1-eth0-2	7.117	2012-09-29 04:17:27	192.168.10.128	1594	130.239.18.173	80	6	ET P2P possible torrent download

Sid	Net	Hostname	Type	Last	Status
1	derbycon1-eth0	derbycon1-eth0	pcap	2012-09-29 04:13:13	UP
2	derbycon1-eth0	derbycon1-eth0	sancp	2012-09-29 04:17:27	UP
4	derbycon1-eth0	derbycon1-eth0	pads	2012-09-29 03:53:30	UP
5	derbycon1-eth0	derbycon1-eth0	http	2012-09-29 03:55:49	UP
3	derbycon1-eth0	derbycon1-eth0-1	snort	2012-09-29 04:17:39	UP
7	derbycon1-eth0	derbycon1-eth0-2	snort	2012-09-29 04:17:40	UP
6	derbycon1-ossec	derbycon1-ossec	ossec	2012-09-29 03:47:59	UP

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Tibs/Harnig Downloader Activity";
flow:to_server,established; content:".php?adv=adv"; http_uri; content:"User-Agent|3a| "; http_header; nocase; content:"ver";
distance:0; http_header; fast_pattern; pcre:"/^User-Agent\x3a[^\r\n]+\)ver\d+\r?$/Hmi";
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.3.35	195.2.253.92	4	5	0	184	57	2	0	128	30172

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	1033	80	.	.	.	X	X	.	.	.	4039956624	2654632951	5	0	64860	0	37571

```
DATA
47 45 54 20 2F 74 64 66 70 6D 6D 6E 2F 68 6F 68    GET /tdfpmmn/hoh
68 76 65 73 77 67 63 2E 70 68 70 3F 61 64 76 3D    hveswgc.php?adv=
61 64 76 35 31 36 20 48 54 54 50 2F 31 2E 31 0D    adv516 HTTP/1.1.
0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A    .User-Agent: Moz
69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61 74    illa/4.0 (compat
69 62 6C 65 3B 20 4D 53 49 45 20 36 2E 30 3B 20    ible; MSIE 6.0;
57 69 6E 64 6F 77 73 20 4E 54 20 35 2E 31 3B 20    Windows NT 5.1;
53 56 31 29 76 65 72 34 39 0D 0A 48 6F 73 74 3A    SV1)ver49..Host:
20 61 63 78 65 72 6F 78 2E 63 6F 6D 0D 0A 0D 0A     acxerox.com....
```

Figure 7: Security Onion Screenshot [13]

IV. Users Requirement Analysis

Questionnaire were successfully distributed to people with more than average technical knowledge to ensure high quality answers from the respondents, a number of 49 responds were taken and analyzed in this section.

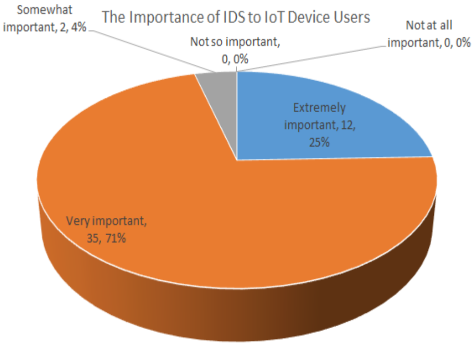


Figure 8: The Importance of IDS to IoT Device Users

Based on figure 8, the researcher can clearly understand the importance of using an Intrusion Detection System for Internet of Things devices in smart home is "Very Important" as a 71% of the respondents clearly have stated. This result further confirms the impact that the proposed system will make if it is released as a product to the real world. Furthermore, the researcher Philokypros [14] has mentioned the risks and raise the importance of using IoT devices without an IDS installed in their home, because most of the IoT devices are build unsecured.

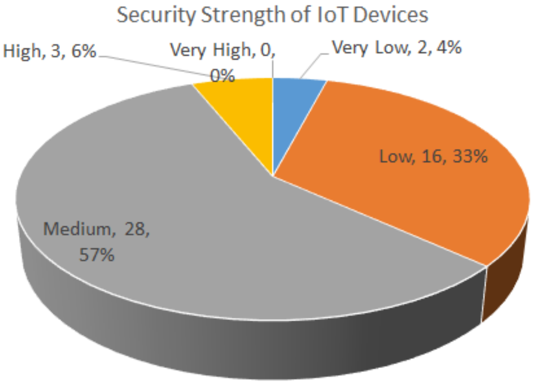


Figure 9: The Security Strength of IoT Devices

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

Figure 9 shows that 57% responds thinks that the security for IoT devices in homes is moderate (Medium), this further proves that security for IoT devices is not being taken seriously by industries and application/system like the researcher is proposing must be used to increase the strength of security. It has been mentioned by Affinity Security Service [15] that "the security of these newly interconnected devices is often weak or non-existent", this means that IoT devices have weak security furthermore supporting the results collected by this question from the respondents.

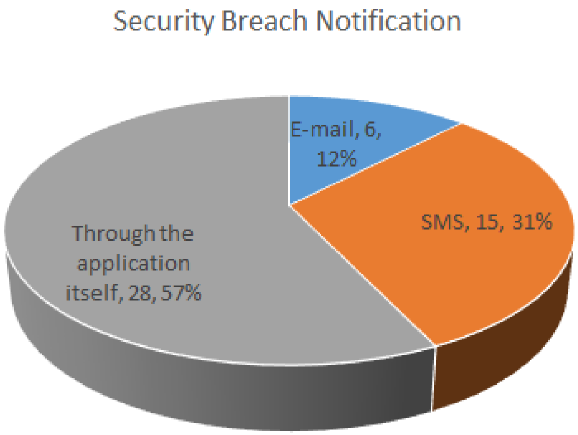
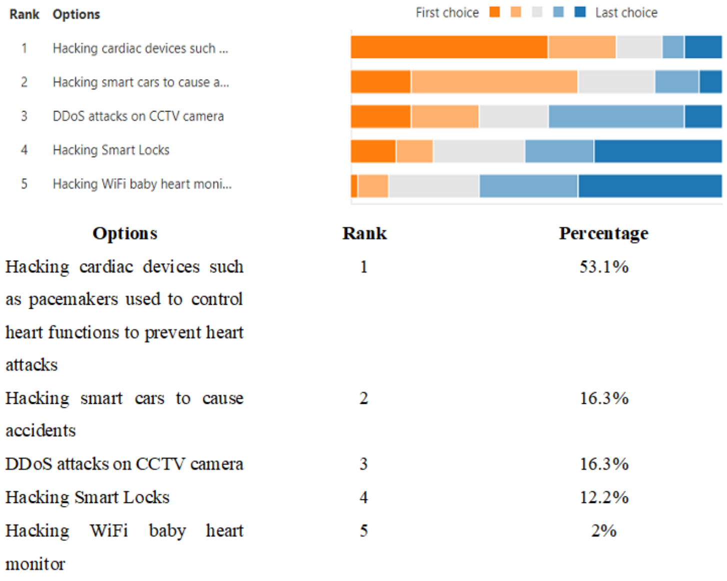


Figure 10: Security Breach Notification

The highest vote to notify the users if there is any security breach is "Through the application itself" with a percentage of 57% from 28 respondents. The responds from this question has a high impact on the development of the system as the researcher will implement the "notify" feature depending on the highest voted answer or highest demand from the end user/future user. This concludes that the researcher will be developing the system in such a way that the notifications will be sent through the application itself. Most of the other IDS in the market or open source alerts/notify the user thought the application itself as explained in Intrusion Detection Review section.



Options	Rank	Percentage
Hacking cardiac devices such as pacemakers used to control heart functions to prevent heart attacks	1	53.1%
Hacking smart cars to cause accidents	2	16.3%
DDoS attacks on CCTV camera	3	16.3%
Hacking Smart Locks	4	12.2%
Hacking WiFi baby heart monitor	5	2%

Figure 11: Attacks for IoT Devices

Based on figure 11, the highest rank with a percentage of 53.1% is the attacks regarding health care, which is a critical factor regarding health of a person. The second in rank is the hacking related to cars that causes accidents with a voting percentage of 16.3% which is not really that high or concerning. The researcher and author Michael Peters [16] has mention in his article that medical IoT devices are the most targeted devices from hackers.

Table 1: Information needed for log file or report generated

Options	Responds	Percentage
Time of when the detection occurs	39	31%
Graphical view of the bandwidth	21	17%
Type of attack attempted by the hacker	40	31%
Graphical view of types of traffic, e.g. TCP, UDP, ICMP and Postscan	25	19%
Others: 1. “Source IP, physical location, attacker's details” 2. “All possible details”	2	2%

Table 1 shows the information that needed in the log file or report that generated by the system. Information such as “Time of when the detection occurs”, “Type of attack attempted by the hacker” and “Graphical view of types of traffic, e.g. TCP, UDP, ICMP and Posts can” have the highest votes with 31%, 31% and 19% respectively, which shows the importance for the system to provide/generate these reports to the user. The demanded report from the IDS also matches with several other IDS system that discussed in IDS system review section of this paper.

V. Proposed System Framework

Figure 12 shows the framework of IDS for IoT devices in smart home.

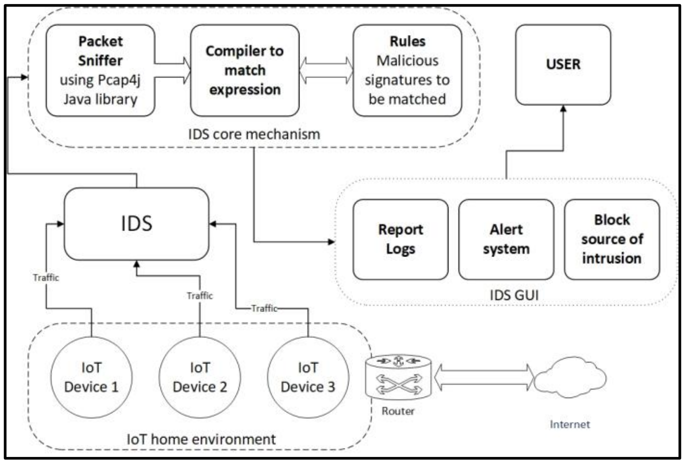


Figure 12: Framework of IDS for IOT devices in smart home

There are 3 samples of IoT devices which are placed in the “IoT home environment” as shown the in framework. All the traffic from all the IoT devices that connected to the system will travels through the IDS which is the proposed system. The IDS core mechanism consist of a packet sniffer which uses Pcap4J Java library to capture packets in the IoT home environment, then a compiler is used to match the packets with the rules given by the user to identify any suspicious network activity. If there is any suspicious network activity identified by the system, alert will be displayed and the system will block the unwanted or suspicious packet. All the data captured by the system will be tabulated to generate the log file and the report which is in graphical view.

VI. Conclusion

The Intrusion Detections System (IDS) for Internet of Things (IoT) application is highly recommended for specific individual that owns IoT devices in their homes. Nowadays this technology's popularity is growing exponentially. It is predicted that the number of IoT devices connected to the internet will grow at rate of 23.1% from 2014 to 2020 annually, reaching 50.1 billion IoT devices by 2020. (Press, 2016). The global growth of in economy of IOT for smart homes shows that demand will increase a lot and companies are following the trend, which leaves millions of target customers for the use of the system proposed in this paper, the Intrusion Detection System for Smart Home IoT devices.

The literary review on several Intrusion Detection System were contributed to the construction of a new conceptual framework of Intrusion Detection System for IoT devices in Smart Home System. User requirements being gathered through the online questionnaire. All the 49 respondents' feedbacks were analysedin considering services and system features that needed to protect the IoT devices in Smart Home System.

The proposed framework is integrated with the hybrid intrusion detection system with anomaly-based intrusion detection technique. This techniques is comparing normal data pattern created based on data from normal users and current data patterns in an online manner to detect anomalies. Any phenomenon that probably being created by hacking tools will be alert by the system and log file is generated. The suspicious packet will be blocked based on the rules created to match with the malicious signature stored in database in IDS core mechanism.

Acknowledgments

The authors wish to express gratitude to the management of Asia Pacific University of Technology and Innovation (APU) for their support in this work.

References

[1] Intelligence, M (2018). Mordor Intelligence. Retrieved March *12, 2019*, from https://www.mordorintelligence.com/industry-reports/global-smart-homes-market-industry?gclid=CIjd6MXjydYCFYYDKgod4ZQFaw

[2] Gartnet, (2019). *gartner.* Retrieved March 12, 2019, from https://www.gartner.com/en/newsroom

[3] Richter, F., (2018). Internet of Things to Hit the Mainstream by 2020. *Statistica.*

[4] Statista, (2018). *Statista.* Retrieved March 15, 2019, from https://www.statista.com/statistics/510780/iot-installed-base-asia-pacific/

[5] Heetae Yang, W. L. H. L. (2018). IoT Smart Home Adoption: The Importance of Proper Level Automation. *Journal of Sensors. Doi:* https://doi.org/10.1155/2018/6464036

[6] Gao, L. & Ba, X. (2014). A unified perspective on the factors influencingconsumer acceptance ofinternet of things technology. *Asia Pacific Journal of Marketing and Logistics,* 26(2), pp. 211-231.

[7] Alolayan, B., 2014. Do I Really Have to Accept Smart Fridges?. *The Seventh International Conference on Advances in Computer-Human Interactions,* pp. 186-191.

[8] Al-Momani, A. M., Mahmoud, M. A. & SharifuddinAhmad, M., 2016. Modeling the adoption of internet of things services: A conceptual framework. *International Journal of Applied Research,* 2(5), pp. 361-367

[9] Rouse, M. (2018). Snort. Search Midmarket Security.

[10] NetGate, (2019). NetGate Documentations. Retrieved March 15, 2019, from at: https://docs.netgate.com/pfsense/en/latest/ids-ips/snort-alerts.html

[11] Inliniac (2014). Suricata Flow Logging. *Inliniac everything inline.*

[12] Cooper, S. (2018). 7 best intrusion prevention systems (IPSs). *comparitech.*

[13] Onion, S. (2019). Security Onion. Retrieved March 20, 2019, from https://securityonion.net/

[14] Philokypros, I. (2018). A Signature-based Intrusion Detection System. *Univeristy of York.*

[15] Service, A. S. (2018). A Security Rating Model for the Internet of Things (IoT). *Internet of Things.*

[16] Peters, M. (2016). IoT Security: Medical Devices Are the Next Target for Hackers. *Proactive Cyber Security.*

[17] P. Mary Jeyanthi, Santosh Shrivastava Kumar "The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region", *Theoretical Economics Letters,* 2019, 9, 752-760,

[18] P. Mary Jeyanthi, "An Empirical Study of Fraudulent and Bankruptcy in Indian Banking Sectors", The Empirical Economics Letters, Vol.18; No. 3, March 2019, ISSN: 1681-8997.

[19] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Hybrid Metaheuristic techniques", *International Journal of Business Intelligence Research,* - Volume 5, Issue 1, April-2014.

[20] P. Mary Jeyanthi, "INDUSTRY 4.O: The combination of the Internet of Things (IoT)and the Internet of People (IoP)", *Journal of Contemporary Research in Management,* Vol.13; No. 4 Oct-Dec, 2018, ISSN: 0973-9785.

[21] P. Mary Jeyanthi, "The transformation of Social media information systems leads to Global business: An Empirical Survey", *International Journal of Technology and Science (IJTS),* issue 3, volume 5.

[22] P. Mary Jeyanthi," An Empirical Study of Fraud Control Techniques using Business Intelligence in Financial Institutions", *Vivekananda Journal of Researc,* Vol. 7, Special Issue 1, May 2018, Page no: 159-164.

[23] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Artificial bear Optimization Approach", *International Journal of Scientific & Engineering Research,* Volume 4, Issue 8, August-2013.

[24] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Optimization techniques for Decision Making", *International Journal of Engineering Research and Technology,* Volume 2, Issue 8, August-2013.

[25] Mary Jeyanthi, S and Karnan, M.: "A New Implementation of Mathematical Models with metaheuristic Algorithms for Business Intelligence", *International Journal of Advanced Research in Computer and Communication Engineering,* Volume 3, Issue 3, March-2014.

[26] Dr. Mary Jeyanthi: "Partial Image Retrieval Systems in Luminance and Color Invariants: An Empirical Study", *International Journal of Web Technology* (ISSN: 2278-2389) – Volume-4, Issue-2.

[27] Dr. Mary Jeyanthi: "CipherText Policy attribute-based Encryption for Patients Health Information in Cloud Platform", *Journal of Information Science and Engineering* (ISSN: 1016-2364)

[28] Mary Jeyanthi, P, Adarsh Sharma, Purva Verma: "Sustainability of the business and employment generation in the field of UPVC widows" (ICSMS2019).

[29] Mary Jeyanthi, P: "An Empirical Survey of Sustainability in Social Media and Information Systems across emerging countries", *International Conference on Sustainability Management and Strategy"* (ICSMS2018).

[30] Mary Jeyanthi, P: "Agile Analytics in Business Decision Making: An Empirical Study", *International Conference on Business Management and Information Systems"* (ICBMIS2015).

[31] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence – soft computing Techniques", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).

[32] Mary Jeyanthi, S and Karnan, M.: "A Comparative Study of Genetic algorithm and Artificial Bear Optimization algorithm in Business Intelligence", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).

[33] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Optimization for Decision Making ", *2011 IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).

[34] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Decision making to overcome the Financial Risk", *2011 IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).

[35] Dr. Mary Jeyanthi, S: "Pervasive Computing in Business Intelligence", *State level seminar on Computing and Communication Technologies.* (SCCT-2015)

[36] Dr.P.Mary Jeyanthi, "Artificial Bear Optimization (ABO) – A new approach of Metaheuristic algorithm for Business Intelligence", ISBN no: 978-93-87862-65-4, *Bonfring Publication.* Issue Date: 01-Apr-2019

[37] Dr.P.Mary Jeyanthi , "Customer Value Management (CVM) – Thinking Inside the box" – ISBN : 978-93-87862-94-4, *Bonfring Publication,* Issue Date: 16-Oct-2019.

[38] Jeyanthi, P. M., & Shrivastava, S. K. (2019). The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region. *Theoretical Economics Letters,* 9(4), 752-760.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019