International Journal of Engineering & Technology, 7 (4.29) (2018) 119-123

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cloud Based Intrusion Detection Conceptual Model for IoT Objects

Abdulaziz Aborujilah[1], Rasheed Mohammad Nassr [2], Abdul Rauf Bin Johari [3]

[1]Malaysian Institute of Information Technology, University Kuala Lumpur, Kuala Lumpur, Malaysia
[2]Malaysian Institute of Information Technology, University Kuala Lumpur, Kuala Lumpur, Malaysia
[3]Malaysian Institute of Information Technology, University Kuala Lumpur, Kuala Lumpur, Malaysia
**Corresponding author E-mail: Abdulazizsaleh@unikl.edu.my*

Abstract

IoT is a new paradigm that link the physical objects with Internet. Many of vehicles, home appliances, human health and environmental monitoring and other objects are able to be connected to each other through the IoT network. IoT objects have the ability to sense and exchanging data with each other. However, IoT paradigm brings new challenges related to security issues. Intrusion Detection Systems (IDS) is widely used to monitor and secure networks. It is very beneficial applying IDS in IoT environment. This paper suggests a conceptual model to integrate IDS with IoT networks. Initial experiments have been conducted to test the possibility of applying SNORT IDS in IoT environment. The results were very encouraging.

Keywords*: IoT , IDS integration , cloud computing , visualization, ML*

1. Introduction

Recently, there has been renewed interest in the Internet of Things (IoT) technology which has increased the potential of integrating smart objects into our daily life. Different technologies such as embedded computing, sensors, automatic identification and tracking, wireless communications, broadband internet access and distributed services have contributed to spreading IoT applications in verity domains [1]. IoT is frequently prescribed as one of the most important paradigms in the Information and Communication Technology (ICT) industry for next year's [2]. According to Gartner Inc., IoT units will reach 26 billion by 2020. Many companies are investing in IoT industry, for example, Cisco company expected to get $ 14.4 trillion as a revenue from IoT industry from 2013 to 2022 [3-6]. IoT applications are used in many application domains such as home automation, and healthcare industrial process, logistic, public safety, environmental monitoring [7].

However, one of the greatest challenges of IoT technology is how to communicate with Internet in a secure way.

Connecting IoT objects with Internet is a new security vulnerability which may threat the human being life. And may make some critical infrastructures such as power plants and transportation of cities and countries in danger.

IoT based home appliance also can be the main target for attackers who aims to violent family's security and privacy [1]. Lack of privacy and encryption and authentication methods have caused different vulnerabilities in the popular smart home devices [8]. So, smart home privacy demands more concentration because of the current security countermeasures are inadequate [8]. So, improving IoT network privacy and data confidentiality and authentication, access control trust among users and things is the main the main focus for numerous ongoing research projects [9].

Though, even with all IoT security mechanisms, IoT networks are still vulnerable to multiple kinds of attacks. So, IDSs can play an important role in securing IoT network [1]. Despite the traditional IDS methods have reached very high performance but they still suffer from some drawbacks because of IoT limited resources capacity and the different protocols are being used [1].

In legacy commuter networks, IDS is hosted on a higher computing capacity nodes but IDSs in IoT networks are constrained with very limited computing resources. Also in the traditional networks, end systems are directly connected to centre nodes (e.g., wireless access points, switches, and routers) to pass the packets to their destination. In contrast, IoT networks usually depend on different kinds of multi-hops based communication protocols which means one node may simultaneously works as front and back end of network packets [10-12].

Very little is known about the development of IDSs which consider the IoT constraints. In this research, we propose a conceptual IDS model which is more specific for IoT nodes considering their limited computing resources.

The rest of this paper is organized as follows. First, we discuss relevant studies that have surveyed the existed IDS placement strategies. Then, we present our proposed IoT IDS architecture Next, we show our initial experiments results of testing SNORT IDS with smart TV appliance. Finally, we present our concluding remarks.

2. Related Works

Internet of Things (IoT) and cloud computing are two technologies that have become part of the daily life [18]. They have remarkable effects on several aspects of our life such as (e.g. logistics, industrial automation, transportation of goods, security and etc) [18]. several studies suggested methods to integrate IDS techniques with IoT paradigm. They mainly focus on IDS place-

ment strategies, detection methods, security threats, validation strategies.

IDS can be placed in different positions in IoT environment. For example, IDSs can be hosted in every physical object of IoT network. This placement strategy need more computing resources [1]. Oh, et al. [13] have suggested distributed lightweight placement method. It uses auxiliary shifting and early decision techniques to decrees number of attacks signature matching. Lee et al. [14] similarly have suggested a low computational resources IDS method to detect the attack in every single IoT nodes. This IDS method depends on comparing the node energy consumption in the normal usage with the consumption under attacks. In contrast, Cervantes et al. [15] have proposed a solution called INTI (Intrusion detection of Sinkhole attacks on 6LoWPAN for the Internet of ThIngs) which divided IoT nodes into masters and slaves nodes. The master nodes are responsible on monitoring their neighbours' nodes(slaves). These detection methods associate concepts of trust and reputation in a hierarchical structure to detect and mitigate the attacks. In this method, one node works as leader and the rest are as members. Each node monitors its superior's node by calculating their inbound and outbound network packets and this role may change according to the network reconfiguration or attacks behaviour. The role of the master node to alert another node in case of the attack is detected and to disconnect the malicious node. The authors did not discuss the performance of this detection method on IoT low capacity nodes.

Raza et al. [16] present a centralized IDS placement method which the border router operates as the main gate for inbound and outbound network traffic. This IDS monitor and analysis the traffic which are being exchanged between IoT nodes and Internet [1]. The serious drawback this placement method is that the traffic which traverses in IoT network is not observed. It is obvious that more research need to done on how to monitor the traffic which are being exchanged between IoT nodes with taking into the consideration the impact of this step on IoT nodes processing capacity. In addition, the centralized IDS methods face a difficulty in minoring nodes in case of a particular of IoT network is collapsed [1].

Another method for IDS placement in IoT network is Hybrid IDS placement which combine the advantages of the both previous strategies and avoid their weakness points [1]. Amaral et al. [17] have proposed to host IDS in some selected nodes(watchdogs). The watchdog's node task is to capture the traffic that are being exchanged between IoT nodes to identify intrusions. Than watchdog's node decides whether a node is compromised or not according to a set of rules. Then each node may have different detection rules according to its position in IoT network and traffic behaviour in that particular segment of IoT network. This strategy differs from Cervantes et al.'s work [15] strategy which divide IoT networks into clusters of nodes and any man is able to monitor its neighbour. The main weakness of hybrid approach is that only the robust node can host IDS instances and monitor its neighbour [1]. Local hosted strategies are more preference than centralized IDS placement methods but they consume more computing resources than the distributed placement strategies [1].

Cloud computing technology is very common network model of remote servers to deliver IT service to the end user. It seems that these two technologies are very different from each other and but in reality their characteristics are often complementary [18]. Therefore, many researchers have proposed IoT and cloud computing integration models which have very high impact on many application scenarios [19-21].

Integrating cloud with IoT may extend the scope of dealing with real world things in more efficient manner. cloud offer intermediate layer between IoT objects and their application and it hid the complexity of IoT application development. In addition, it reduces IoT applications development challenges such as information gathering, processing, and data transmission [22].

Data mining(DL) and Machin learning (ML) are common techniques used in intrusion detection. Cannady [24] Artificial neural networks(ANN) technique has been used multi-category classification to detect the intrusions. Several ML techniques have been used in anomaly and misused IDSs such as association rules [24-27], Bayasin network [28-30], clustering technique [31-33], Hidden markov Model(HMM)[34-35], SVM[36-37] and other techniques mentioned in [38].

The current IoT IDS methods are not taking the advances of other technologies such cloud computing and visualization technologies and such technologies can improve the performance and availability of IDSs and show IDS alerts in more understandable from.

3. Proposed IDS Architecture

According to the above-related studies, it can be concluded that supporting IDS approach with matching ML and cloud computing services will have high impact overcoming the complexity of applying IDS in IoT limited resources nodes. For aims of associating the end users with IDS report, visualization techniques and mobile applications can be used to show the IDS alerts in more understandable and portable manner. Since Virtualization techniques are widely used in many IT industries such as management, education, and training [39-41]. However, it is not wildly used in security applications.

The proposed IDS model consists of five layers: IoT objects which form the data source. It may include smart things such as smart phone, smart TV, smart devices for better health and fitness, smart vehicle and so on. The second layer contain cloud computing based services for example PaaS, SaaS and IaaS which are able to host IDS in cloud and provide SNORT developers with numerous of development and testing tools. Thirdly, ML layer which is responsible on receiving IDS events and loges then feed such data to ML methods for classification, clustering or production purposes. Fourthly and in order to show the minded data in more understandable and readable form, IDS output is send to visualization process such as heat maps doubles charts, scatter plot and others. Finally, the summarized report my disabled to end user through mobile applications.

Figure 1 present the model layers which are namely IoT devices, cloud computing, machine learning, visualization and mobile applications layers.

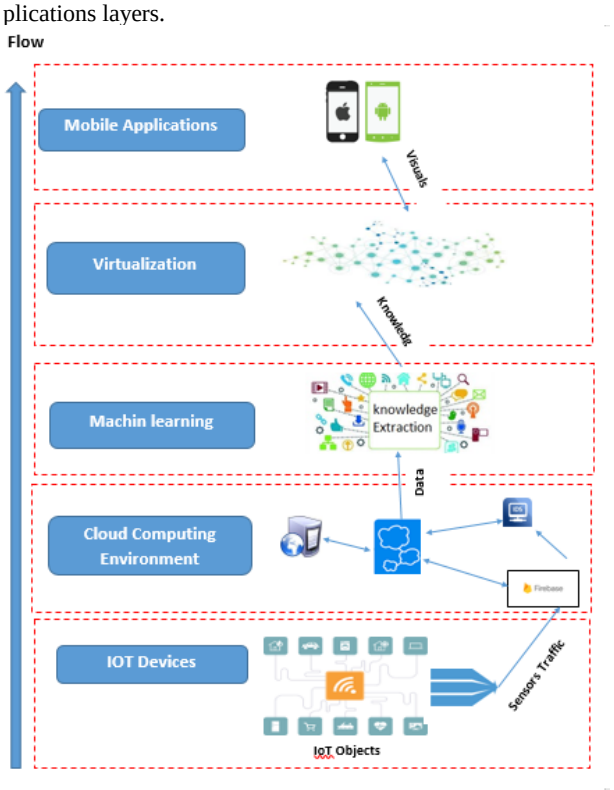

Fig.1: Conceptual illustration of IoT IDS architecture

4. Experiments

In this study, Initial experiments have been conducted to test the applicability of using SNORT to detect Brute Force attack in IoT platform. Brute Force attacks are commonly attacks that target the TCP/IP network and 6LOWPAN network as well. a simulation for SMART TV devices under Brute Force attacks has been implemented. In this line SNORT [42] has been used to detect this attacks in this IoT appliance. The tools required to implement this experiments are VMware Workstation, and SNORT, smart TV emulator 5.1 [43] Kali Linux and Wireshark.

4.1. Environment Configuration

The experiments environment requires installing and running both Kali Linux and smart TV emulator in NAT environment. Also it needs bridging the virtual machine to the physical adapter by setting up NAT on network adapter. Prior to generating Brute Force attacks, we need to investigate the undertaking SMART TV network vulnerabilities by scanning the target device on SMART TV Network using netdiscover command. Figure 2 show SMART TV network scanning information.

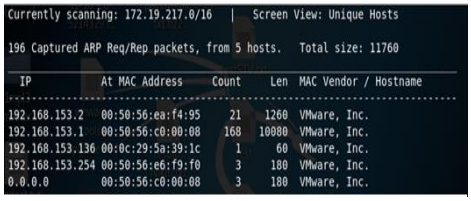

Fig2: network scanning information

Once IP address of the Smart TV is detected which is 192.168.153.13 in this case. We run nmap command using nmap -sV <ip address> to know which port and services are open as it shows in Figure 3.

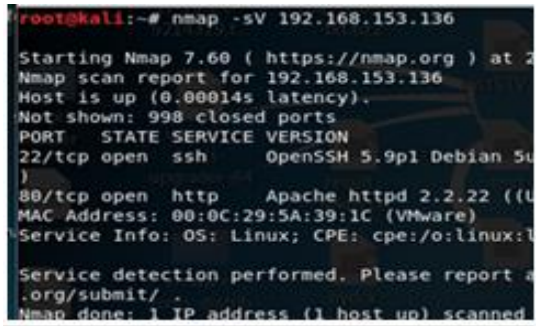

Fig3: show ports scan information

From above nmap scan result, it is noticeable that SSH services are open on port 22. It also it shows the version of the kernel used. Next nikto commands is used to check the vulnerabilities exist on the system using nikto -h <ip address> as it is showed in Figure 4.

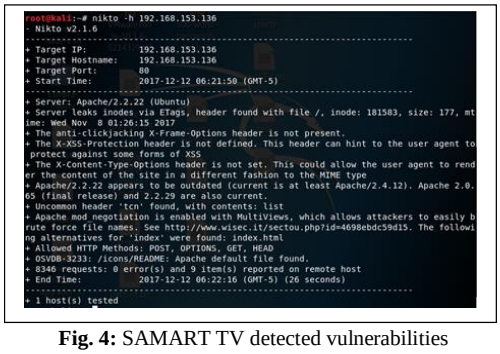

Fig. 4: SAMART TV detected vulnerabilities

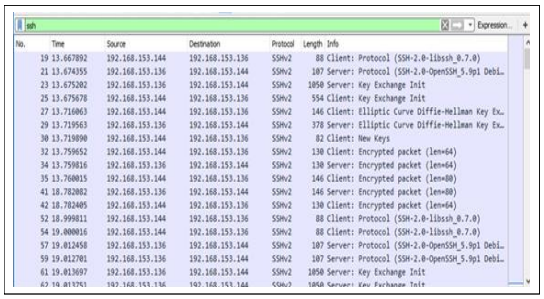

Fig 5: Brute force attack pcap file

In this simulation, Hydra in Kali Linux is used to generate the Brute Force attack. To know the password list Hydra command crunch is used with the this crunch syntax <number of desired password length> <number of desired password length> <password attributes> -o <location to save the password and create a new name file> as it is showed in Figure 6

Fig.6: custom made password list

We can also use another password list available on the internet such as Rockyou password list that available in Kali Linux. Next is to run Hydra command on Kali Linux as it showed in Figure7

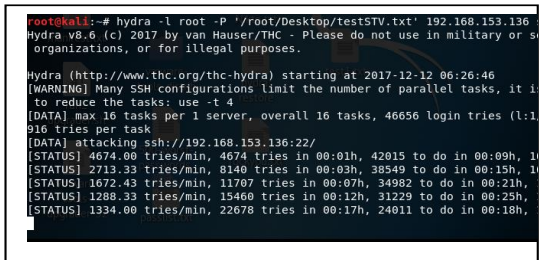

Fig.7: haydra password attacks

During Brute Force attack Wireshark capture all the packet network during attack simulation and save it as PCAP file as Figure 5 shows.

In this simulation, we use hydra -l -P <destination of passlist> <target IP> <services/port> command. This attack takes quite a long time to complete due to big list of pass list. Upon completion, the result will be displayed as it shows in Figure8.

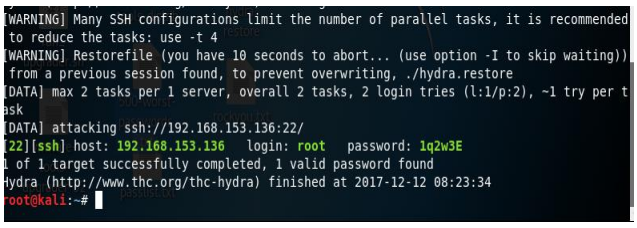

Fig8: shows results of Brute Force attack

Then, the ssh port accessibility is checked. Figure 9 show result of ran ssh command on SMART TV IP address (168.153.136).

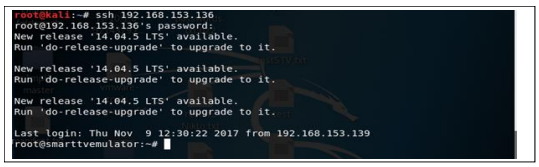

Fig. 9: result of ran ssh command on SMART TV IP address

4.2. Brute Force Detection

4.2.1. SNORT Configuration

In this scenario, we are focusing on SSH protocol to create the Snort rule. To test the Snort alert, we use the rules that specify flow to the server on port 22. as it shows in Figure 10.

```
alert tcp any any -> $EXTERNAL_NET 22 (msg:"Potential SSH Brute Force Attack"; \
flow:to_server; \
flags:S; \
threshold:type threshold, track by_src, count 3, seconds 60; \
classtype:attempted-dos; \
sid:2001219; \
rev:4; resp:rst_all; \
)
```

Fig. 10: SNORT rule of Brute Force attack

4.2.2 Brute Force attacks Detection

Based on this analysis , Brute Force attacks is detected and its log data was generated as it shows in Figure 11.

```
[**] [1:2001219:4] Potential SSH Brute Force Attack [**]
[Classification: Attempted Denial of Service] [Priority: 2]
12/12-21:26:25.295607 192.168.153.144:35418 -> 192.168.153.136:22
TCP TTL:64 TOS:0x0 ID:30289 IpLen:20 DgmLen:60 DF
******S* Seq: 0x38E32B71  Ack: 0x0  Win: 0x7210  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1457876823 0 NOP WS: 7

[**] [1:2001219:4] Potential SSH Brute Force Attack [**]
[Classification: Attempted Denial of Service] [Priority: 2]
12/12-21:32:46.611321 192.168.153.144:35430 -> 192.168.153.136:22
TCP TTL:64 TOS:0x0 ID:61104 IpLen:20 DgmLen:60 DF
******S* Seq: 0xBB393F36  Ack: 0x0  Win: 0x7210  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1458258138 0 NOP WS: 7
```

Fig11: log data of Brut Force attack

5. Conclusions and Future Work

IoT technology is a new form of physical objects networks. It has generated verity of applications in different domains in our delay life such as smart home appliances, e-health, smart cities and environment applications. However, The main concern with this technology is related to the security issues. The present research aims to examine the main weakness of IoT IDS systems and propose a new security model to improve the security level of IoT networks. The integration between machine learning techniques, cloud-based services, mobile applications and virtualization technology are suggested to improve IoT nodes security. The Initial experiments have confirmed that SNORT IDS is effective security technique that can be used to detect the attacks in IoT environment. overall, This research identifies a scope to explore new methods on IoT IDSs. Further studies need to be carried out in order to validate the performance of the proposed model in real smart objects networks.

Acknowledgements

This work is supported by UniKL MIIT STRG grant number 16008.

References

[1] Zarpelão, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C., 2017. A Survey of Intrusion Detection in I nternet of Things. Journal of Network and Computer Applications.

[2] Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I., 2012. Internet of things: vision, applications and research challenges. Ad Hoc Netw. 10 (7), 1497–1516.Mishra, A., Nadkarni, K., Patcha, A.,2004. Intrusion detection in wireless ad hoc networks. IEEE Wirel. Commun. 11 (1), 48–60

[3] Lee, I., Lee, K., 2015. The internet of things (IoT): applications, investments, and challenges for enterprises. Bus. Horiz. 58 (4), 431–440.

[4] Bradley, J., Barbier, J., Handler, D., 2013. Embracing the Internet of Everything to capture your share of $14.4 trillion, Tech. rep., Cisco White Paper

[5] Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A., 2015. Security, privacy and trust in internet of Things: the road ahead. Comput. Netw. 76 (0), 146–164.

[6] Singh, D., Tripathi, G., Jara, A.J., 2014. A survey of Internet-of-things: future vision, architecture, challenges and services. In: Internet of Things (WF-IoT), 2014 IEEE

[7] Borgia, E., 2014. The Internet of Things vision: key features, applications and open issues. Comput. Commun. 54, 1–31.

[8] Notra, S., Siddiqi, M., Gharakheili, H., Sivaraman, V., Boreli, R., 2014. An experimental study of security and privacy risks with emerging household appliances. In: Communications and Network Security (CNS), 2014 IEEE Conference on, pp. 79–84.

[9] Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A., 2015. Security, privacy and trust in internet of Things: the road ahead. Comput. Netw. 76 (0), 146–164

[10] Pantoni, R., Fonseca, C., Brandão, D., 2012. Street lighting system based on wireless

[11] Elejoste, P., Angulo, I., Perallos, A., Chertudi, A., Zuazola, I.J.G., Moreno, A., Azpilicueta, L., Astrain, J.J., Falcone, F., Villadangos, J., 2013. an easy to deploy street light control system based on wireless communication and LED technology. Sensors 13 (5), 6492–6523.

[12] Shahzad, G., Yang, H., Ahmad, A.W., Lee, C., 2016. Energy-efficient intelligent street lighting system using traffic-adaptive control. IEEE Sens. J. 16 (13), 5397–5405.

[13] Oh, D., Kim, D., Ro, W.W., 2014. A malicious pattern detection engine for embedded security systems in the Internet of Things. Sensors 14 (12), 24188–24211. Pantoni, R., Fonseca, C., Brandão, D., 2012. Street lighting system based on wireless

[14] Lee, T.-H., Wen, C.-H., Chang, L.-H., Chiang, H.-S., Hsieh, M.-C., 2014. A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN. In:

[15] Cervantes, C., Poplade, D., Nogueira, M., Santos, A., 2015. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In: 2015 IFIP/ IEEE International Symposium on Integrated Network Management (IM), pp. 606– 611

[16] Raza, S., Wallgren, L., Voigt, T., 2013. SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. 11 (8), 2661–2674.

[17] Amaral, J., Oliveira, L., Rodrigues, J., Han, G., Shu, L., 2014. Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks. In: Communications (ICC), 2014 IEEE International Conference on, pp. 1796–1801

[18] Botta, Alessio, et al. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016): 684-700.

[19] Alamri, A., Ansari, W. S., Hassan, M. M., Hossain, M. S., Alelaiwi, A., Hossain, M. A., 2013. A survey on sensor-cloud: architecture, applications, and approaches. International Journal of Distributed Sensor Networks 2013.

[20] Aitken, R., Chandra, V., Myers, J., Sandhu, B., Shifren, L., Yeric, G., 2014. Device and technology implications of the internet of things. In: VLSI Technology (VLSI-Technology): Digest of Technical Papers, 2014 Symposium on. pp. 1{4.

[21] Gomes, M. M., Righi, R. d. R., da Costa, C. A., 2014. Future directions for providing better iot infrastructure. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication. UbiComp '14 Adjunct. pp. 51{54.

[22] European Commission, 2013. De_nition of a research and innovation policy leveraging Cloud Computing and IoT combination. Tender specifications, SMART 2013/0037.

[23] J. Cannady, "Artificial neural networks for misuse detection," in Proc. 1998 Nat. Inf. Syst. Secur. Conf., Arlington, VA, USA, 1998, pp. 443– 456

[24] A. Bivens, C. Palagiri, R. Smith, B. Szymanski, and M. Embrechts, "Network-based intrusion detection using neural networks," Intell. Eng. Syst. Artif. Neural Netw., vol. 12, no. 1, pp. 579–584, 2002.

[25] H. Brahmi, B. Imen, and B. Sadok, "OMC-IDS: At the cross-roads of OLAP mining and intrusion detection," in Advances in Knowledge Discovery and Data Mining. New York, NY, USA: Springer, 2012, pp. 13–24.

[26] H. Zhengbing, L. Zhitang, and W. Junqi, "A novel network intrusion detection system (NIDS) based on signatures search of data

mining," in Proc. 1st Int. Conf. Forensic Appl. Techn. Telecommun. Inf. Multimedia Workshop (e-Forensics '08), 2008, pp. 10–16.
[27] D. Apiletti, E. Baralis, T. Cerquitelli, and V. D'Elia, "Characterizing network traffic by means of the NetMine framework," Comput. Netw., vol. 53, no. 6, pp. 774–789, Apr. 2009.
[28] C. Livadas, R.Walsh, D. Lapsley, andW. Strayer, "Usingmachine learning techniques to identify botnet traffic," in Proc 31st IEEE Conf. Local Comput. Netw., 2006, pp. 967–974.
[29] F. Jemili, M. Zaghdoud, and A. Ben, "A model for an adaptive intrusion detection system using Bayesian network," in Proc. IEEE Intell. Secur. Informat., 2007, pp. 66–70.
[30] C. Kruegel, D. Mutz,W. Robertson, and F. Valeur, "Bayesian event classification for intrusion detection," in Proc. IEEE 19th Annu. Comput. Secur. Appl. Conf., 2003, pp. 14–23.
[31] R. Hendry and S. J. Yang, "Intrusion signature creation via clustering anomalies," in Proc. SPIE Defense Secur. Symp. Int. Soc. Opt. Photonics, 2008, pp. 69730C–69730C.
[32] M. Blowers and J. Williams, "Machine learning applied to cyber operations," in Network Science and Cybersecurity. New York, NY, USA: Springer, 2014, pp. 55–175.
[33] K. Sequeira and M. Zaki, "ADMIT: Anomaly-based data mining for intrusions," in Proc 8th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., 2002, pp. 386–395.
[34] D. Ariu, R. Tronci, and G. Giacinto, "HMMPayl: An intrusion detection system based on hiddenMarkov models," Comput. Secur., vol. 30, no. 4, pp. 221–241, 2011.
[35] S. S. Joshi and V. V. Phoha, "Investigating hidden Markov models capabilities in anomaly detection," in Proc. ACM 43rd Annu. Southeast Reg. Conf., 2005, vol. 1, pp. 98–103.
[36] Z. Li, A. Zhang, J. Lei, and L. Wang, "Real-time correlation of network security alerts," in Proc. IEEE Int. Conf. e-Business Eng., 2007, pp. 73– 80
[37] [37] Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, "An effìcient intrusion detection system based on support vector machines and gradually feature removal method," Expert Syst. Appl., vol. 39, no. 1, pp. 424–430,2012.
[38] Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications Surveys & Tutorials 18.2 (2016): 1153-1176.
[39] Cayirci, Erdal, et al. "Snow leopard cloud: a multi-national education training and experimentation cloud and its security challenges." Cloud Computing (2009): 57-68.
[40] Stewart, Kyle E., Jeffrey W. Humphries, and Todd R. Andel. "Developing a virtualization platform for courses in networking, systems administration and cyber security education." Proceedings of the 2009 spring simulation multiconference. Society for Computer Simulation International, 2009.
[41] Gaspar, Alessio, et al. "The role of virtualization in computing education." ACM sIGCsE bulletin. Vol. 40. No. 1. ACM, 2008.
[42] Roesch, Martin. "Snort: Lightweight intrusion detection for networks."Lisa.Vol.99.No.1.1999.
[43] http://developer.samsung.com/tv/develop/tools/tv-extension/archive/),