Monitoring and Analysing Anomaly Activities in a Network using Packetbeat

Bayana Raja, K Ravindranath, B Jayanag

Abstract: The primary intention of any organization is to provide security for their information because they are sensitive to different types of threats that might cause damage to providing services to their customers which will lead to disaster. This paper will draw more attention to protecting the client's systems from various network attacks by monitoring and analyzing the network traffic. Packet analysis can help us to identify the malicious network traffic, which is going to harm the entire systems connected to that network so that we can have some knowledge from the information extracted by analyzing network packets that will help us to get aware of the vulnerabilities and to resolve them before we become victims. Once we install the Packetbeat in our client's system it will collect and send all the network data in that organization, which can be used to analyze them in order to find out the abnormal network traffic. Using ELK at server side, we can store, monitor and analyze the network data for identifying malicious network packets that are going to infect our client's systems. This process can be helpful in small-scale SIEM services.

Keywords: Threats, Vulnerabilities, Malicious network traffic, Packet analysis, Packetbeat, ELK Stack.

I. INTRODUCTION

Today almost all the companies and organizations are depended on the Internet for accessing all the services as part of their business. As the number of companies with computers accessing internet increases, correspondingly the increase in external threats can be noticed. Mostly the network-based attacks that are occurring by accessing the global internet show a major impact on the business computers over the past several years. Due to the increasing of network-based attacks, it is very critical for companies to store and secure their sensitive data. When a security breach occurs, the companies may lose business and finally become bankrupt because of one successful attack.

In order to prevent the client's systems from various network attacks by detecting the malicious network traffic passing through the network, Packetbeat is used as a source in packet analysis which can be integrated into elk. Using the packetbeat we can collect all the network packet logs from the client's system, then perform packet analysis and detect the malicious network packets that are going to harm the systems in an organization. The data collected from the packet beat indicates all the events collected from users in that network. This will be helpful to find out the intrusions happening between the internal network and external network.

II. NEED FOR PACKET ANALYSIS

Packet analysis is a process used to log the network traffic that is passing over a network and it can be able to analyze the network traffic and to produce in detail report for assisting the organizations in maintaining their networks. Many organizations are planning to perform data logging and log analysis to enhance their security [1]. The capability to analyze logs effectively and accurately is critical to reduce system failure and to detect problems before or while they occur [5]. Packet analysis can help in reducing the time taken for problem diagnosis, resolution time, as well aseffective management of network infrastructure [13]. Packet analyzers can also be used by hackers to interfere on organizations networks and steal sensitive information from the network transmissions.

A packet analyzer can be referred as a data sniffer or network analyzer used for analyzing network data. A network analyst must be on alert to analyze the network traffic and to protect from threats. Analysts have to troubleshoot the network in order to provide an efficient and fast network traffic environment [13]. The main purpose of performing the packet analysis is to figure out the anomalies, monitoring or like a goal which is to not just to monitor and finding the anomalies but also to measure the ability for the safeguard to later on will help in enhancing the network security.

The packet analyzer can able to show all the details of network activities by presenting a complete picture of the bandwidth and resources utility. It can be helpful in generating a report of network data statistics in a tabular form, graphs or pie charts. When the resource is utilizing too much bandwidth, then the network analyst can release the resource by interrupting the process. By performing the packet analysis in real time, we can identify the network issues and as well as detect unauthorized attempts on the network.

III. EXISTING SOLUTION

Splunk

Splunk is one of the highly preferredtools in this field of monitoring and analyzing the data. It can able to collect, store, search, monitor and analyze the client's network logs in a dashboard. This is available in both open source and commercial plans, where the open source is a trial version

Revised Manuscript Received on April 12, 2019.

Bayana Raja, M Tech Student, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

K Ravindranath, Associate Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

B Jayanag, Assistant Professor, Department of CSE, VR Siddhartha Engineering College, Kanuru, Andhra Pradesh, India

and limited to 500 MB per day which is insufficient to implement in IT industries [1]. In the commercial edition, we should pay based on the amount of data we want to use. Even though it has many features but as any commercial products customization and scaling up could be considered as one of the biggest barriers.

According to the IDC report [2], we can observe that Splunk occupies the top market share and ranked number one in the worldwide Information Technology Operation Analytics (ITOA) for 2015. Splunk provides a very powerful user interface and the users can also apply their own user interface configuration. Rather than the financial issue in customizing the product, Splunk is more flexible and it can fulfil the need that would be a big demand for any organization.

IV. PROPOSED SOLUTION

There are many tools for performing the packet analysis each of them has certain advantages and disadvantages in solving network issues. Among them, opensource product packetbeat integrated into ELK Stack is more efficient for analysing network packets. ELK is the combination of three different projects like Elasticsearch, Logstash and Kibana. Elasticsearch, Logstash and Kibana when combined and used together, it forms a real-time data analytics tool that provides actionable insights from any type of structured and unstructured data source. Elasticsearch is like a database and a search engine, it can able to store a large volume of data. Logstash is used for processing the data and transporting events, logs through a pipeline to Elasticsearch. Kibana works on the top of Elasticsearch that can be helpful in analysing data in clear visualizations. We can customise our Kibana dashboards to fulfil our needs and also it can able to create new index patterns.

Beats

Beats are open source data shippers that we can install as agents in our client's system to collect the logs and send operational data directly to Elasticsearch or to transfer through Logstash to Elasticsearch [11]. Mainly, there are 5 types of beats that are helpful in collecting the logs.

- **Packetbeat:** Packetbeat is implemented to collect all the network data from the client's systems. Using this packetbeat we can monitor and analyse the network packets.
- **Winlogbeat:** winlogbeat is implemented to collect the windows event logs from the client's systems. It can deploy only in the Windows operating systems.
- **Metricbeat:** Metricbeat is implemented to collect various system level metrics for various system and platforms.
- **Filebeat:** filebeat is implemented to collect the log files. It has different modules for collecting, parsing and visualization of log files.
- **Auditbeat:** Auditbeat is implemented for auditing user and process activity on the Linux servers. It can be used to identify different security breaches and monitors the integrity of the data.

Each Beat is a separately installable product. Before installing Beats, we need to install and configure the ELK. Packetbeat is very much helpful to work and enhance network security.

Packetbeat

- Packetbeat is implemented to collect network data from client systems. And it is an opensource network datashipper and analyzer for network packets that can be integrated into ELK Stack.
- Packetbeat produces real-time monitoring of the various metrics on the web, database or any other protocol by monitoring the packets that are passing across the wire.
- Monitoring the data packets with ELK Stack can be useful to identify the harmful network traffic andthe network packet behavior, and to identify the packet source & destination and helpful in searching for specific data strings in the packets.
- Packetbeat can able to capture the network traffic between the servers and can be used for monitoring the performance of web applications.
- Packetbeat can be installed on the client system andcan be monitored on a dedicated server.
- Packetbeat tracks the network trafficand decodes the protocols finally records the data for the transaction.
- Protocol's supported by packetbeat includes DNS, HTTP, ICMP, etc.

V. PACKETBEAT ARCHITECTURE

The workflow conveys the performance of packetbeat in collecting the network data and helpful for performing packet analysis in ELK. When we deploy packetbeat in the client's system it will collect all the network data and sends to the Logstash. Logstash is responsible for processing the data. It consists of 3 parts INPUT, FILTER and OUTPUT [1]. The INPUT field describes the source of data i.e. from where it is getting the data. Here source is packetbeat it gets network data from packetbeat.

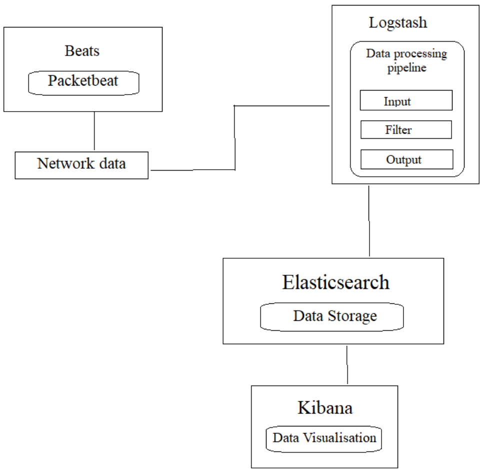


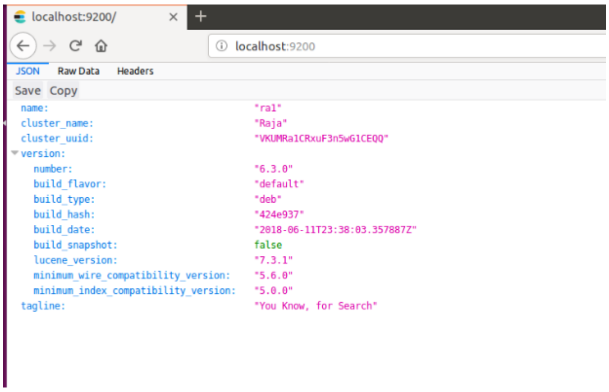
Fig. 1 Proposed workflow

FILTER is responsible for parsing the data and the OUTPUT field describes the output location i.e. to which location it has to forward the data.

Here we are forwarding the data to Elasticsearch. Elasticsearch receives the data from Logstash and stores the data. Kibana shows the visual representation of the data present in the Elasticsearch.

VI. RESULT ANALYSIS

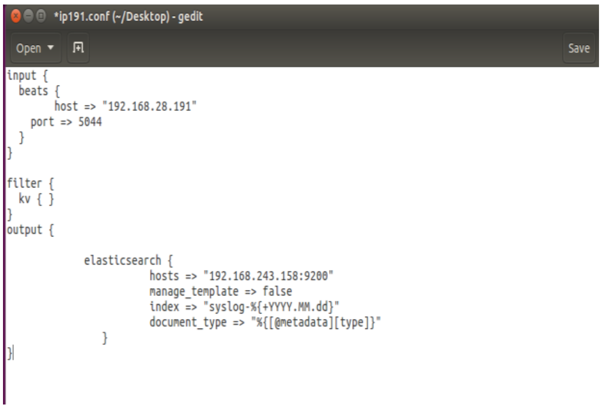
The scenario of our implementation is to monitor the network packets and to perform packet analysis using packetbeat in ELK stack. In order to deploy ELK in server-side systems, we need to install the pre-requisites like a web server and java version higher than 7. For my convenience, I installed apache server and Java 8 in my Ubuntu operating system. After that, we have to download the tools Elasticsearch, Logstash and Kibana from the official website of ELK stack [10] as I am using Ubuntu OS, so I have to download the DEB package. After installing Elasticsearch I need to configure it to send data to Kibana. During the configuration of Elasticsearch, we have to specify the destination IP address and default port number of Elasticsearch as 9200 in the Elasticsearch configuration. After configuring the Elasticsearch we can verify whether it is working or not (Fig 2).



```
name:                                   "ral"
cluster_name:                           "Raja"
cluster_uuid:                           "VKUMRa1CRxuF3n5wG1CEQQ"
version:
  number:                               "6.3.0"
  build_flavor:                         "default"
  build_type:                           "deb"
  build_hash:                           "424e937"
  build_date:                           "2018-06-11T23:38:03.357887Z"
  build_snapshot:                       false
  lucene_version:                       "7.3.1"
  minimum_wire_compatibility_version:   "5.6.0"
  minimum_index_compatibility_version:  "5.0.0"
tagline:                                "You Know, for Search"
```

Fig. 2 Elastic search service status

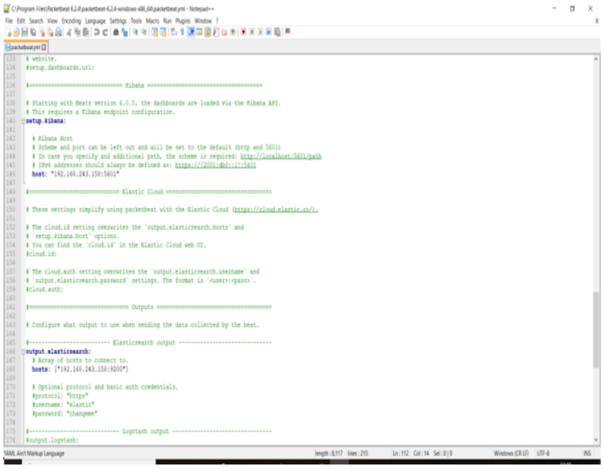
Kibana should be installed only after the successful installation of the Elasticsearch. After installing the Kibana we can configure it by specifying IP as the loopback IP address that is 0.0.0.0 and default port number of Kibana as 5601 in the Kibana configuration. Similarly, we will install and configure the Logstash. In the configuration file, INPUT section, we set our client IP address (source IP) and default port number 5044 for Logstash. In the OUTPUT section, we have to set the destination IP address of Elasticsearch along with Elasticsearch default port number (Fig 3).



```
input {
  beats {
        host => "192.168.28.191"
    port => 5044
  }
}

filter {
  kv { }
}
output {

             elasticsearch {
                        hosts => "192.168.243.158:9200"
                        manage_template => false
                        index => "syslog-%{+YYYY.MM.dd}"
                        document_type => "%{[@metadata][type]}"
             }
}
```

Fig. 3 Logstash configuration

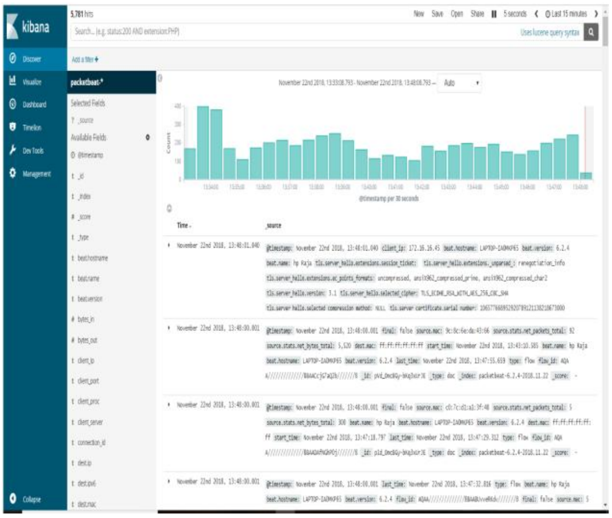
Now coming to the client side, we have to deploy packetbeat in our client system it will collect all the data about the network packets passing through the network. In order to install the packetbeat, we have to download the packetbeat file from ELK official website [10] and extract it to program files. Now we should open Windows PowerShell by running it as administrator and install the packetbeat. After the installation of packetbeat, we have to configure it to send data directly to Elasticsearch or to send data through Logstash. Here Fig 4 shows the packetbeat configuration file.


C:\Program Files\Packetbeat 6.2.4\packetbeat-6.2.4-windows-x86_64\packetbeat.yml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
packetbeat.yml
YAML Ain't Markup Language
length : 8,117 lines : 215
Ln : 112 Col : 14 Sel : 0 | 0
Windows (CR LF) UTF-8 INS

```
# website.
#setup.dashboards.url:

#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "192.168.243.158:5601"

#============================= Elastic Cloud ==================================

# These settings simplify using packetbeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.243.158:9200"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

#----------------------------- Logstash output --------------------------------
#output.logstash:
```

Fig. 4 Packetbeat configuration

After configuring the packetbeat in the client system we have to go to Task Manager and then check the status of packetbeat whether it is running or stopped. We have to set it to running state in order to collect the data. After that come to the server side and start the services of Elasticsearch, Logstash and Kibana. In the Kibana, we can visualize the graphical representation of our client's network traffic (Fig 5). It displaysthe overview of each and every packet by its source IP in that network along with its timestamp. Based on this we can monitor and analyze the network traffic.



```
November 22nd 2018, 13:48:01.040   @timestamp: November 22nd 2018, 13:48:01.040 client_ip: 172.16.16.45 beat.hostname: LAPTOP-IADMKP65 beat.version: 6.2.4
                                   beat.name: hp Raja tls.server_hello.extensions.session_ticket:  tls.server_hello.extensions._unparsed_: renegotiation_info
                                   tls.server_hello.extensions.ec_points_formats: uncompressed, ansiX962_compressed_prime, ansiX962_compressed_char2
                                   tls.server_hello.version: 3.1 tls.server_hello.selected_cipher: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
                                   tls.server_hello.selected_compression_method: NULL tls.server_certificate.serial_number: 106577668952920789121138218673000

November 22nd 2018, 13:48:00.001   @timestamp: November 22nd 2018, 13:48:00.001 final: false source.mac: 9c:8c:6e:da:43:66 source.stats.net_packets_total: 92
                                   source.stats.net_bytes_total: 5,520 dest.mac: ff:ff:ff:ff:ff:ff start_time: November 22nd 2018, 13:43:10.585 beat.name: hp Raja
                                   beat.hostname: LAPTOP-IADMKP65 beat.version: 6.2.4 last_time: November 22nd 2018, 13:47:55.659 type: flow flow_id: AQA
                                   A///////////////8AAACcjG7aQ2b//////8 _id: pVd_OmcBGy-bKq3xirJE _type: doc _index: packetbeat-6.2.4-2018.11.22 _score: -

November 22nd 2018, 13:48:00.001   @timestamp: November 22nd 2018, 13:48:00.001 final: false source.mac: c0:7c:d1:a1:3f:48 source.stats.net_packets_total: 5
                                   source.stats.net_bytes_total: 300 beat.name: hp Raja beat.hostname: LAPTOP-IADMKP65 beat.version: 6.2.4 dest.mac: ff:ff:ff:ff:ff:
                                   ff start_time: November 22nd 2018, 13:47:18.797 last_time: November 22nd 2018, 13:47:29.312 type: flow flow_id: AQA
                                   A///////////////8AAADAfNGkPOj//////8 _id: p1d_OmcBGy-bKq3xirJE _type: doc _index: packetbeat-6.2.4-2018.11.22 _score: -

November 22nd 2018, 13:48:00.001   @timestamp: November 22nd 2018, 13:48:00.001 last_time: November 22nd 2018, 13:47:32.816 type: flow beat.name: hp Raja
                                   beat.hostname: LAPTOP-IADMKP65 beat.version: 6.2.4 flow_id: AQAA///////////////8AAABUvveR6dv//////8 final: false source.mac: 5
```

Fig. 5 Network data visualization in Kibana

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

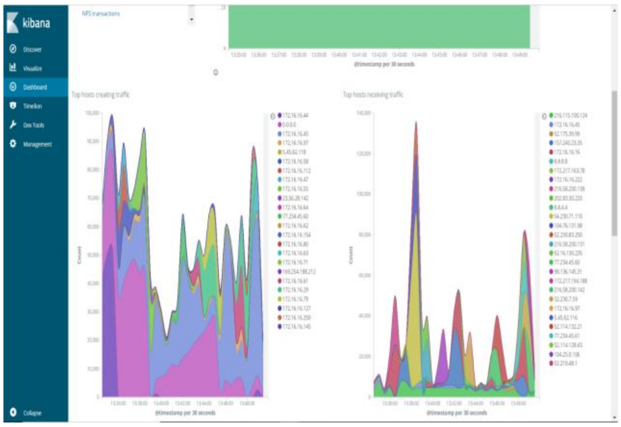

kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
NFS transactions
@timestamp per 30 seconds
Top hosts creating traffic
Top hosts receiving traffic
Count
@timestamp per 30 seconds

Fig. 6(a) Top hosts creating traffic

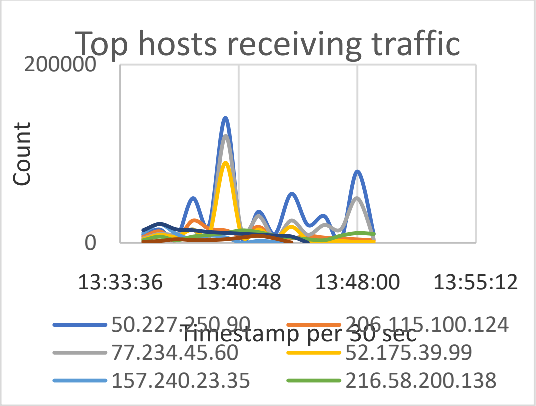
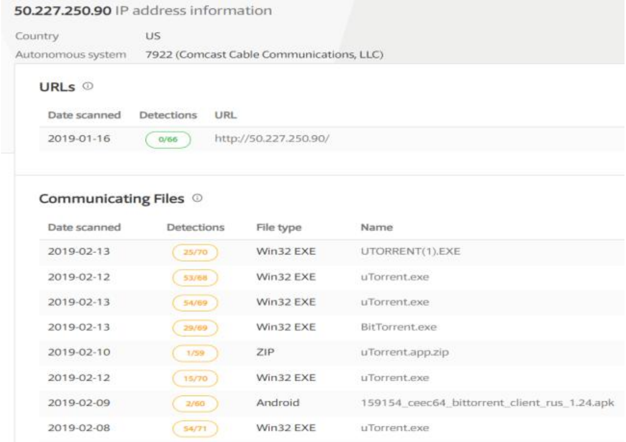


Fig. 6(b) Top hosts receiving traffic

In the Kibana dashboard, the graph displays the result of all the communicating hosts in that network along with their IP which can be identified by different colors for each host. We can see the top hosts creating traffic along with their IP address in one graph shown in fig 6a and top hosts receiving traffic in another graph shown in fig 6b. Top hosts creating traffic indicates all the communicating hosts in that network and top hosts receiving traffic indicates incoming traffic to that hosts in the network. Based on our analysis in incoming traffic we can identify the malicious traffic in that network by scanning the suspected source IP address in the virus total website [14]. Fig 7 illustrates the virus total report for a suspicious source IP. Based on this report we can detect the malicious activates that are performing on that network.



50.227.250.90 IP address information

Country	US
Autonomous system	7922 (Comcast Cable Communications, LLC)

URLs ⓘ

Date scanned	Detections	URL
2019-01-16	0/66	http://50.227.250.90/

Communicating Files ⓘ

Date scanned	Detections	File type	Name
2019-02-13	25/70	Win32 EXE	UTORRENT(1).EXE
2019-02-12	53/68	Win32 EXE	uTorrent.exe
2019-02-13	54/69	Win32 EXE	uTorrent.exe
2019-02-13	29/69	Win32 EXE	BitTorrent.exe
2019-02-10	1/59	ZIP	uTorrent.app.zip
2019-02-12	15/70	Win32 EXE	uTorrent.exe
2019-02-09	2/60	Android	159154_ceec64_bittorrent_client_rus_1.24.apk
2019-02-08	54/71	Win32 EXE	uTorrent.exe

Fig. 7 Virus total report for the malicious source in that network

VII. CONCLUSION AND FUTURE WORK

Now we successfully collected the client's network data into our Kibana dashboard and we can visualize and analyze them using elk stack. We can analyze each and every packet and its source and destination in order to detect the malicious attempts on that network by scanning the suspicious source IP in virustotal website. This shows that ELK is more efficient in protecting client’s systems from various network-based attacks. For small-scale industry’s it is better to use ELK stack open source tool rather than the commercial tool. For future work, I am going to do research on Kibana alerting system that will automatically detect the malicious network data and give alerts to the user.

REFERENCES

1. “Network Security Enhancement through Effective Log Analysis Using ELK” by Ibrahim Yahya Mohammed AL-Mahbashi, and Dr M. B. Potdar Bhaskaracharya Institute for Space Applications and Geo-informatics, Gandhinagar, Gujarat, India 382007.
2. “Performance of ELK Stack and Commercial System in Security Log Analysis” by Sung Jun son, and Youngmi Kowon, Dept. of Radio and Info. Communications Eng, Chungnam National University, Daejeon, South Korea.
3. “Real Time Distributed Analysis of MPLS Network Logs for Anomaly Detection” by Muhammet Macit, Emrullah Delibas, Tevfik Aytekin, Department of Computer Engineering, Bahçesehir University, Besiktas, 34353, ˙Istanbul, Turkey.
4. “A High Throughput Distributed Log Stream Processing System for Network Security Analysis” by Jingfen Zhao, Peng Zhang, Yong Sun, Institute of Information Engineering, Chinese Academy of Science, National Engineering Laboratory for Information Security Technologies, Beijing, China.
5. “LogLens: A Real-time Log Analysis System” by Biplob Debnath, Mohiuddin Solaimani, and Muhammad Ali Gulzar, CS Department, The University of Texas at Dallas, USA.
6. “Analysis of Log Files Intersections for Security Enhancement” by Kazimierz Kowalski, Mohsen Beheshti. Computer Science Department, California State University Dominguez Hills, 1000 Victoria Str., Carson, CA 90747.
7. “Event Log Analysis with the LogCluster Tool” by Risto Vaarandi, Markus Kont, and Mauno Pihelgas, TUT Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Tallinn, Estonia.
8. “Multidimensional Log Analysis” by Marcin Kubacki, Janusz Sosnowski, Institute of Computer science, Warsaw University of Technology, Warsaw, Poland.
9. “Massive Distributed and Parallel Log Analysis for Organizational Security” Xiaokui Shu, John Smiy, Danfeng (Daphne) Yao, and Heshan Lin Department of Computer Science Virginia Tech Blacksburg, Virginia 24060.
10. https://www.elastic.co/elk-stack
11. https://logz.io/learn/complete-guide-elk-stack/#beats
12. https://logz.io/blog/network-log-analysis-packetbeat-elk-stack/
13. https://www.techopedia.com/definition/25323/
14. www.virustotal.com
15. Yadlapati, A., Kakarla, H.K. An Advanced AXI Protocol Verification using Verilog HDL (2015) Wulfenia, 22 (4), pp. 307-314.
16. Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T “Review and Analysis of Promising Technologies with Respect to fifth Generation Networks”, 2014 First International Conference on Networks and Soft Computing,ISSN:978-1-4799-3486-7/14,pp.248-251,August 2014.
17. Bindu Bhargavi, K., Hari Kishore, K. Low Power Bist on Memory Interface Logic (2015) International Journal of Applied Engineering Research, 10 (8), pp. 21079-21090.

18. Charan, N.S., Kishore, K.H. Recognization of delay faults in cluster based FPGA using BIST (2016) Indian Journal of Science and Technology, 9 (28).
19. Hari Kishore, K., Aswin Kumar, C.V.R.N., Vijay Srinivas, T., Govardhan, G.V., Pavan Kumar, C.N., Venkatesh, R.V. Design and analysis of high efficient UART on spartan-6 and virtex-7 devices (2015) International Journal of Applied Engineering Research, 10 (9), pp. 23043-23052.
20. Kante, S., Kakarla, H.K., Yadlapati, A. Design and verification of AMBA AHB-lite protocol using Verilog HDL (2016) International Journal of Engineering and Technology, 8 (2), pp. 734-741.
21. Bandlamoodi, S., Hari Kishore, K. An FPGA implementation of phase-locked loop (PLL) with self-healing VCO (2015) International Journal of Applied Engineering Research, 10 (14), pp. 34137-34139.
22. Murali, A., Hari Kishore, K., Rama Krishna, C.P., Kumar, S., Trinadha Rao, A. Integrating the reconfigurable devices using slow-changing key technique to achieve high performance (2017) Proceedings - 7th IEEE International Advanced Computing Conference, IACC 2017, art. no. 7976849, pp. 530-534.
23. A. Surendar, K. H. Kishore, M. Kavitha, A. Z. Ibatova, V. Samavatian “Effects of Thermo-Mechanical Fatigue and Low Cycle Fatigue Interaction on Performance of Solder Joints” IEEE Transactions on Device and Materials Reliability, P-ISSN: 1530-4388, E-ISSN: 1558-2574, Vol No: 18, Issue No: 4, Page No: 606-612, December-2018.
24. N Bala Dastagiri K Hari Kishore “A 14-bit 10kS/s Power Efficient 65nm SAR ADC for Cardiac Implantable Medical Devices” International Journal of Engineering and Technology (UAE), ISSN No: 2227-524X, Vol No: 7, Issue No: 2.8, Page No: 34-39, March 2018.
25. N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.
26. N Bala Dastagiri, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.
27. Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.