ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 1 Issue 1, September, 2021 / Page No: 57-64
Paper Id: JETA-V1I1P109 / Doi: 10.56472/25832646/JETA-V1I1P109

Original Article

Utilizing Splunk for Proactive Issue Resolution in Full Stack Development Projects

Ranjit Kumar Gupta[1], Sagar Shukla[2], Anaswara Thekkan Rajan[3], Sneha Aravind[4]
[1,2,3,4]*Independent Researcher, USA.*

Received Date: 17 May 2021 Revised Date: 19 June 2021 Accepted Date: 17 July 2021

Abstract: *With the help of various sources of unstructured and structured data like system and application monitoring streams, open-source knowledge capture, and on-demand simulation output, exascale data environments are quickly approaching. With storage prices so low, the challenge today lies in turning massive data repositories into useful information. Any company, organisation, or agency can use log data as a definitive recording of what's happening, and it's frequently an underutilised resource for troubleshooting and supporting larger business goals. For the purpose of combining and indexing any type of log or machine-generated information, including complicated multi-line application logs that are complex and unstructured, Splunk offers the best software in the industry. Any machine-generated data can be gathered, stored, indexed, searched, correlated, visualised, analysed, and reported on in order to quickly, reliably, and affordably discover and address operational and security issues. Nowadays, most businesses and organisations use Information Technology (IT), which is the use of networked computers, and physical equipment to create, process, and share electronic information. While one significant danger to IT-based networks and systems is cyberattacks. Every firm has information security procedures in place since an attack that succeeds has the potential to result in significant financial loss. Logging and monitoring are crucial security measures that shield an organisation from potential threats. Specifically, threat identification is an important method for locating invaders. In this research, we examine the threat hunting utility of the Elastic stack tool and contrast it with four other tools of a similar nature. When used in a large-scale setting, the Elastic Stack tool has been shown to be both cost-effective and efficient in identifying threats and breaches of security.*

Keywords**:** *Data Environments, Splunk Provides, Elastic Stack, Important Security, Log Data, Logging And Monitoring, IT, Operational Momentum, Large-Scale Environment, Cost-Efficient, Maintaining Research, Open-Source, Cyberattacks.*

I. INTRODUCTION

For the purpose of combining and indexing any type of log or machine data, including complicated multi-line application log files that are complex and unstructured, Splunk offers the best software in this sector. It can gather, store, index, search, correspond, visualise, analyse, and report on any machine-generated data in order to more quickly, reliably, and economically discover and address operational and security issues. It's a fully integrated, enterprise-ready solution for gathering, storing, and visualising log management material. It is also possible to perform ad hoc searches and historical data generating without the use of third-party reporting tools [1].

By offering flexible access to databases with relational structure, field-delimited data in comma-separated value files, and other business data storage like Hadoop, Splunk software facilitates log data enhancement. Numerous log management use cases, including as log consolidating and retention, and security, IT operations problem-solving, application solving problems, and compliance reporting, are supported by Splunk software [1, 2].

Thus, when it comes to release, the operation group gets everything ready for it, and they have to return to the development team silo if the program doesn't function in the production atmosphere [2]. If this pattern is repeated, both sides could have to wait a long time and get quite irritated. When development and production are in sync, the goal of DevOps is to bring both sides together to work closely together. This speeds up the process as a whole. Everyone is happy and may go on to the next task if the software deploys correctly, as in [2, 3]. If not, they can work together to resolve every problem and discover a solution.

A. Log analysis can assist in resolving DevOps issues:

The goal of DevOps approaches is to shorten the time between a software lifecycle's creation and deployment of new features. Many DevOps strategies focus on system status monitoring in order to get the optimal outcome. The developer bears the responsibility of guaranteeing the proper operation of the system consistently [3, 4]. In addition, DevOps seeks to identify the root of issues and promptly resolve them in the event of a system malfunction. The primary source of data on

the system's present state is kept in files known as logs. Any software program that prints a message with some information about the system's current state is called a log [3, 4]. Depending on the kind of system that created it, each log may have a distinct format. A developer can also manually write logs to inform the system of a certain state or occurrence. As a result, DevOps techniques for examining a software system's state rely on log analysis [4].

The majority of the studies conducted in this field has been either general in nature, describing and/or implementing SOCs, or it has concentrated on a single issue that a SOC faces, such as staffing and issues with employees, big data integration and analysis, or cloud-based SOC infrastructure security. This study aims to synthesise pertinent research to determine the most prevalent issues that a typical SOC is currently facing, issues that they expect to face in the near future, solutions that SOCs are already using to address these issues, and future solutions that are planned.

This essay will concentrate on both the quantitative and the qualitative facets of the problems that SOCs are dealing with. The qualitative components are derived from scholarly and commercial literature on particular subjects. The SANS Institute's survey-based statistics, which gather and analyse responses from hundreds to thousands of SOC employees across various industries, will serve as the basis for the statistical analyses. These data points contribute to a comprehensive picture of the SOC community [5, 6]. To provide context for the challenge/solution conversation that follows, a general review of SOCs—including what they are, what makes them up, how they work, and what they can do—will be covered in the part that follows.

B. Middleware for EVpath:

A middleware layer for event transfer called EVpath allows collaborating processes to create any kind of dataflow graph. EVpath is based on the idea of stones—that is, "stepping stones"—that may be connected to create a path. In an EVpath, stones are small, light entities that roughly map to dataflow graph processor points. Different kinds of stones carry out the transformation of data, data filtering, data muxing and demuxing, and data transfer via network connections between processes [7].

An example dataflow network that could be implemented with EVpath is shown in Figure 1. Data is transmitted from the original location to the sinks via the network by connected stone. As each sink may wish to customise the event stream in a unique fashion (e.g., sink i customising its stream with a function Fi), it is illogical to assume that all sinks are interested in the same data [7, 8]. Placing these filter functions as close to the source as feasible would enable a successful implementation of event delivery, preventing the transmission of useless data that would only be rejected upon arrival at the intended destination Figure 1.

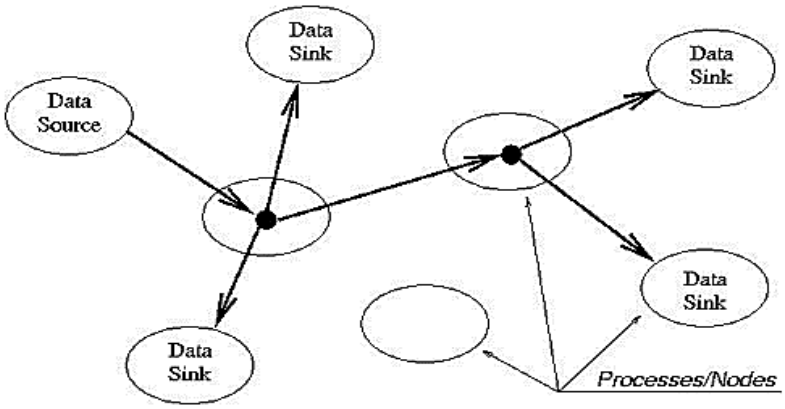

Figure 1: An Example of an Evpath-Implementable Dataflow Network. [8]

The world of technological innovation is changing quickly because to the use of cloud computing, automated processes, social networks, online transactions, and more [8, 9]. Though there is always a drawback to progress, for example, as technology advances, cybercrimes also rise. With the use of recently created tools, assaults, and strategies, attackers may be able to breach more secure, controlled, or sophisticated environments, causing significant harm that may be difficult to track. Cybercriminals have the power to jeopardise the accessibility, security, and reliability of data and resources.

As a result, in the modern world, cyber-threat hunting is crucial for spotting various dangers. The process of proactively and continuously searching networks to identify and isolate advanced threats that could evade detection by present security measures is known as "cyber-threat hunter" [8].

Reducing false positives, accelerating root cause analysis, and precisely and swiftly identifying issues are the main objectives. The following are the three main components of the ELK stack.

C. Elastic search:

This is the core of Elastic Stack; it acts as a search engine and log storage.

- Logstash: An intermediate element that enriches and parses the data to convert unorganised input into structured information [9].
- Kibana: This GUI-based visualisation application creates dashboards and other visual representations to enhance usage.

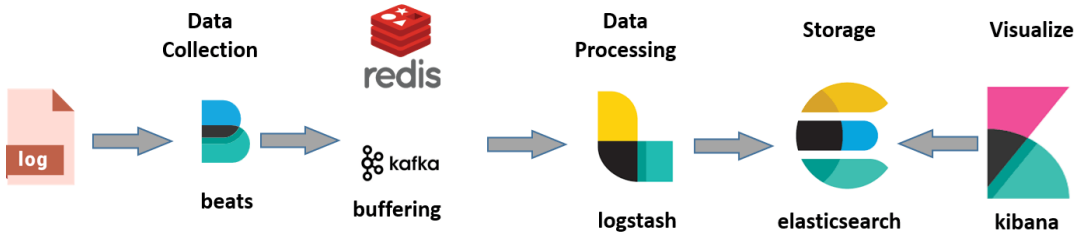

Figure 2: Methodology of Elastic Stack

II. LOG ORGANISATION AND ANALYSIS

A. The ELK Stack Approach:

Users can input data from any location in any format with ELK Stack, and it can be searched, analysed, and visualised in real time [8, 9]. It offers centralised logging, which is helpful for figuring out what's wrong with servers or apps.

B. Collection of Logs:

One crucial phase or procedure in the cyberthreat hunting process is log gathering. Logs from many sources can be gathered by ELK Stack and parsed into a usable manner. From there, it may be utilised for correlation and log analysis across several logs in one place [9]. In this work, we will explain below how to gather logs for various purposes and sources.

a) Netflow:

The Cisco router generates NetFlow logs, which offer an effective means of monitoring connection establishment, disconnection, and denials [9]. In order to accomplish this, binary data is sent over UDP packets rather than ASCII-based Syslog statements.

b) Windows Logs:

This kind of log collecting takes place on the control server (an Active Directory (AD) network). Since this server is secret, we created another one where the Winlogbeat agent may be installed to forward all Windows event logs to Kibana [9, 10].

c) SharePoint Logs:

The following procedures can be used to retrieve the SharePoint logs from the office admin centre.

- Select times in the audit log search under Admin Centre > Security and Standards.
- With this functionality, we can also set alert policies. The fact that it must be individually uploaded is the problem. The creation of an Azure active directory is required in order to automate a basic API connector [9], which queries the Office 365 Management API and sends audit records via TCP to the Elastic Stack (Logstash). [10, 11].

d) Antivirus Logs:

We utilised the Kaspersky antivirus software logs for this job, and the admin-center server has a feature that allows you to transfer data to Kibana in that syslog format at the necessary frequency [11].

C. Parsing Logs:

Parsing is essentially the process of dividing the log signal into smaller data segments and putting each one into a named field with its own specifics by adhering to pre-established guidelines [11, 12]. Data analysis, querying, and visualisation can be made easier by parsing logs.

D. Analysing Logs:

In this study, [13], we visualised the logs using Kibana, an open-source analytical and visualisation platform with a browser-based interface. It has the ability to track, look up, examine, and display the supplied data in a range of visualisations, including tables and diagrams. Kibana is the final location for all of the gathered logs, as seen in Figure 2.

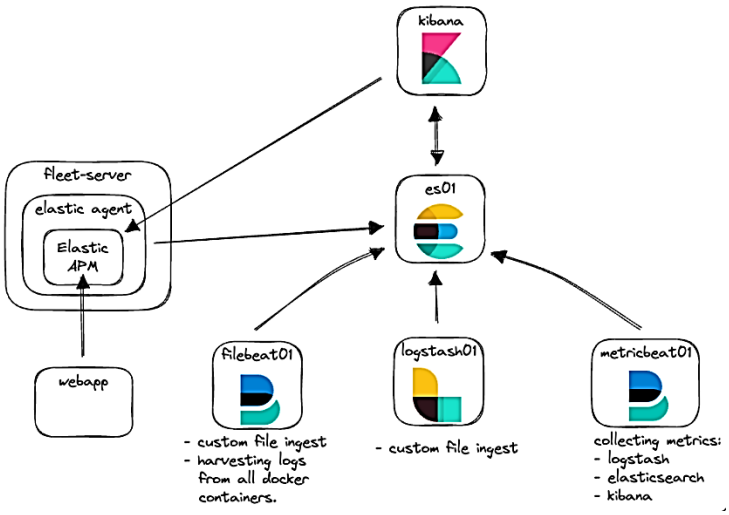

Figure 3: Agent of the Elastic Stack

III. ASSESSMENT AND ATTACK DEVELOPMENT

To assess the efficacy of ELK Stack, we develop attacks during the review process. We can monitor or identify those assaults by making the warning or suspicious activities apparent in our visualisation tool based on these attacks [12, 13]. We employed some light-weight shipper for this task by employing Winlogbeat, File beat, Audit beat, [13], Metricbeat, and Packet beat in important machinery, where the attacks have been recorded, in order to make this possible. We then deployed some agents to transport the logs to our visualisation tool.

A. All-Out Attack:

In every organisation when someone has access to the system and credentials, a brute force assault is a common way to breach it.

a) Hydra tool:

In actuality, the majority of security researchers utilise the Hydra tool to find vulnerability because it can quickly generate a basic assault using brute force and run a large number of password combinations. Since Hydra is an open-source program, attackers are always able to design additional modules.

b) Attack Implementation:

Using SSH and hydra, an attack with brute force on a distant server can crack the password. Hydra -l test -P '/root/Desktop/pass.txt' is the command that is used. Both internal and exterior attacks are possible [14].

- **Internal Attack:** Employees within a company can quickly guess passwords if they know the IP address and username.
- **External Attack:** If an attacker from outside the organisation has access to a user list and password list that is already available, they can crack the passwords and usernames [15].

B. Dictionary Attack:

In Kali Linux, the Dictionary attack is carried out via the X-Hydra tool. Using this program, one can demonstrate how to hack an SSH password on a distant server [15]. The procedures for carrying out a dictionary attack to break the password are as follows:

- **Step 1:** Identifying the destination and the SSH protocol that must be broken.
- **Step 2:** Naming the user whose password has to be broken and providing a link to the dictionary's whole list of probable passwords [15, 16].

C. DDoS Attack:

DDoS attacks are malevolent attempts by an attacker to render a network inaccessible to users by flooding it with traffic from many sources and keeping it active for an extended period of time [16, 17]. When other users attempt to access the network, it has the ability to immediately deny them service.

D. Social Engineering:

We used Setoolkit to develop phoney websites on a Kali machine, including Twitter, Instagram, and LinkedIn. We can see the username and password from the Kali terminal once users have logged in to the website [18]. We can keep an eye out for these assaults using website logs in Kibana. Figure 3 provides an illustration of a spoof Facebook page.

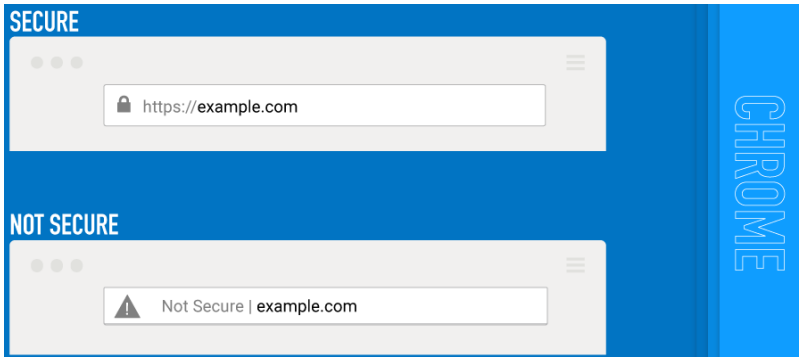

Figure 4: A Model of a Fictitious Website [18]

E. Injecting Payload:

The goal of payload injecting is to inject a chosen payload into the target, such as a computer running Windows, which can be started in the manner described below.

- To produce a dangerous file.
- To completely evade detection of the executable file [18, 19].

Table 1: A list of the tools, assaults, and logs. [19]

Attacks	Tools	Implemantation	Agent	Logs
Brute force attack	Hydra	Tried using SSH to break the password on a distant server.	Audit beat	Audit logs
Dictionary attack	Xhydra	Attempted to use SSH to crack the password on a distant server.	Audit beat	Audit logs
DDos attack social engineering	Creating servers	Reconstructed multiple 404 error in the web service.	Winlogbeat	Webserver logs
Payload injection	Metasploit	To replicate malevolent files on Windows systems.	Winlogbeat	Webserver logs
Social engineering	Setoolkit	Bogus login page was made in order to get the user name and password.	Winlogbeat	Windows/Antivirus logs

Table 2: An overview of the attacks' outcomes. [17, 18]

Attacks	Kibana Resuls
Brunte force attack	There are more login events than there are genuine login occurrences.
Dictionary attack	There are more login events than there are actual log-ins.
DDoS attack	The 404 error page may indicate the beginning of a DDoS attack.
Social engineering	Keep an eye out for unusual processes that users aren't supposed to be handling.
Payload injection	Use Kibana to track harmful activity and produce an alarm.

F. Office 365 Monitoring:

Office 365 is a useful tool for most structure users. Kibana helps us monitor every Office 365 log [19]. To access all Office 365 app logs and operations using Kibana, such as file a page activities, folder operation, SharePoint list actions, synchronisation actions, exchange the mailbox procedures, etc., we need to install the Metricbeat agent in the Azure Active Directory (AD) [20].

G. Outcomes and Instantaneous Threat Intelligence:

Real-time intelligence on threats can identify malicious and suspicious activity to a local network by analysing Packetbeat data, often known as network traffic. The original or destination IPs gathered by Packetbeat are compared with the malicious IP [21, 22]. Netflow data in a wider network (such as an enterprise network) can be used for this. The results of this research have been tested and visualised using Packetbeat on Kibana logs. Additionally, it offers IP and location-based results [23].

IV. EFFICIENCY COMPARISON

Given the information, log files are essential for determining the cause of a system's failure. The knowledge is easier to access with the first two tools, which are both IBM and HP. The history of Splunk and LogPoint is primarily presented below [23, 24].

A. LogPoint:

A Scandinavian business that specialises in SIEM created LogPoint. By using this technology, we may intercept events on both proprietary and standard systems before they endanger a company's core operations. In addition, the solution makes it possible for:

- *To acquire a current summary of network data [25, 26.*
- *To use data enrichment to identify unwanted network activities and look into incidents.*
- *To simply adhere to regulatory compliance standards like ISO2700x, GDPR, SOX, HIPAA, PCI, and GPG13.*

B. Splunk:

Users may sort through a lot of data and retrieve the pertinent facts with the aid of Splunk. Splunk gathers, correlates, and indexes current information before storing it in a search repository from which it creates dashboards, reports, alerts, diagrams, and visualisations [26, 27]. The three primary parts of Splunk are the search head of flesh, which is the main component of the online user interface and allows all of these components to be combined or distributed across the servers; the indexer, which stores and catalogues data and reacts to search queries; and the forwarder, or forwarder, which encourages data to remote indexers.

- To build a plexiglass table to monitor threat behaviour: To compile threat activity into distinct categories, sources, and matches [27, 28].
- To handle the metrics visually: We utilise editing software to upload photos, create shapes, add text and icons, and create linkages for the glass table that show how the danger metrics relate to one another.
- To keep track of unique metrics using the glass table: The APT (Advanced Persistent Threat) group, for example, can track individual threat groups using custom search methods to track their bespoke threat activity statistics.

C. Discussion:

ELK Stack is a useful security tool for analysing logs and spotting harmful occurrences, according to the study above. In actuality, a few more security features, such traffic purification, trust leadership, systems for intrusion detection [29, 30], and more, can be included to offer an improved level of security protection.

V. CONCLUSION

Despite this is not what we were hoping for in our scenario, Splunk offers a very finished engine search and indexed optimisation for the log the information. The system generates enormous amounts of log files, making it possible to see searching through and indexing the data as a full-time job that will becoming harder to manage over time.

For any company to detect security breaches before they have an opportunity to proliferate and result in grave, irreversible harm, log monitoring is essential. In this paper, we compare the efficiency of ELK Stack with four similar apps and assess its effectiveness against various assaults. It is found that ELK Stack is an effective and cost-efficient a solution for cyber-threat hunting. Log management provides a vital component of protection against uninvited intrusions and data theft.

VI. REFERENCES

[1] Janos and N. Dai, “Security concerns towards Security Operations Centers”, in 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), IEEE, 2018, pp. 000273–000278.

[2] A. Crowley and J. Pescatore, “The Definition of SOC-cess? SANS 2018 Security Operations Center Survey”, SANS Institute Reading Room, SANS Institute, 2018.

[3] (ISC) 2, “Cybersecurity Professionals Stand Up to a Pandemic”, (ISC) 2 Cybersecurity Workforce Study 2020, (ISC)2 , 2020.

[4] J. Pescatore and B. Filkins, “Closing the Critical Skills Gap for Modern and Effective Security Operations Centers (SOCs)”, SANS Institute Reading Room, SANS Institute, 2021.

[5] B. Filkins, “2019 SANS Automation and Integration Survey”, SANS Institute Reading Room, SANS Institute, 2019.

[6] S. Sundaramurthy, et al., “A Human Capital Model for Mitigating Security Analyst Burnout”, Eleventh Symposium On Usable Privacy and Security (SOUPS), 2015, pp. 347–359. [16] D. Murdoch, “2020 SANS Automation and Integration Survey Integration Survey”, SANS Institute Reading Room, SANS Institute, 2021.

[7] A. Cole, “SOC Automation - Deliverance or Disaster", SANS Institute Reading Room, SANS Institute, 2017.

[8] Fay Chang, Jeffrey Dean, Sanjay Ghemawat, Wilson C. Hsieh, Deborah A. Wallach, Mike Burrows, Tushar Chandra, Andrew Fikes, and Robert E. Gruber. Bigtable: A distributed storage system for structured data. In Proc. 7th USENIX Symposium on Operating Systems Design and Implementation (OSDI), pages 205–218, 2006.

[9] Greg Eisenhauer, Hasan Abbasi, Matthew Wolf, and Karsten Schwan. Event-based systems: opportunities and challenges at exascale. In Proc. Third ACM International Conference on Distributed Event-Based Systems, Nashville, Tennessee, July 2009. ACM.

[10] Greg Eisenhauer, Matthew Wolf, Hasan Abbasi, Scott Klasky, and Karsten Schwan. A type system for high performance communication and computation. In Proc. 2011 D3 science Workshop, Stockholm, Sweden, December 2011. IEEE. Associated with the 7th IEEE International Conference on e-Science.

[11] Susanne Busse et al. Federated Information Systems: Concepts, Terminology, and Architectures. Technische Universitat Berlin, 1999.¨
[12] Simon Garfunkel, Paul Farrell, Vassil Roussev, and George Dinolt. Bringing science to digital forensics with standardized forensic corpora. In Proc. Digital Forensic Research Workshop, Montreal, Canada, 2009. Elsevier.
[13] N. Bosch and J. Bosch, “Software logs for machine learning in a devops environment,” in 2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), pp. 29–33, 2020.
[14] M. Kersten, “A cambrian explosion of devops tools,” IEEE Software, vol. 35, no. 2, pp. 14–17, 2018.
[15] P. Agrawal and N. Rawat, “Devops, a new approach to cloud development testing,” in 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), vol. 1, pp. 1–4, 2019.
[16] J. Henkel, C. Bird, S. K. Lahiri, and T. Reps, “Learning from, understanding, and supporting devops artifacts for docker,” in 2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE), pp. 38–49, 2020.
[17] J. Rufino, M. Alam, and J. Ferreira, “Monitoring v2x applications using devops and docker,” in 2017 International Smart Cities Conference (ISC2), pp. 1–5, 2017.
[18] C. Ebert, G. Gallardo, J. Hernantes, and N. Serrano, “Devops,” IEEE Software, vol. 33, no. 3, pp. 94–100, 2016.
[19] R. K. Pratibha Jha, “A review paper on devops: Beginning and more to know,” pp. 1–5, 06 2018.
[20] K. Yao, M. Sayagh, W. Shang, and A. E. Hassan, “Improving state-of-the-art compression techniques for log management tools,” IEEE Transactions on Software Engineering, pp. 1–1, 2021.
[21] C.-T. Yang, E. Kristiani, Y.T. Wang, G. Min, C.H. Lai, and W.J. Jiang, “On construction of a network log management system using ELK Stack with Ceph,” J. Supercomput. 76(8), pp. 6344-6360, 2020.
[22] M. Beechey, K.G. Kyriakopoulos, and S. Lambotharan, “Evidential classification and feature selection for cyber-threat hunting,” Knowl. Based Syst. 226, 107120, 2021.
[23] W. Meng, W. Li, and L.F. Kwok, “Towards Effective Trust-based Packet Filtering in Collaborative Network Environments,” IEEE Transactions on Network and Service Management, vol. 14, no. 1, pp. 233-245, 2017.
[24] S.J. Son and Y. Kwon, “Performance of ELK stack and commercial system in security log analysis,” in Proc. IEEE Malaysia International Conference on Communications (MICC), 2017.
[25] I.Y.M. Al-Mahbashi, M.B. Potdar, and P. Chauhan, “Network security enhancement through effective log analysis using ELK,” in Proc. ICCMC, pp. 566-570, 2018.
[26] Al-Mohannadi, I. Awan, J.A. Hamar, A.J. Cullen, J.P. Disso, and L. Armitage, “Cyber Threat Intelligence from Honeypot Data Using Elastic search,” in Proc. AINA, pp. 900-906, 2018.
[27] P. P. I. Langi, Widyawan, W. Najib, and T. B. Aji, “An evaluation of twitter river and logstash performances as elasticsearch inputs for social media analysis of twitter,” in 2015 International Conference on Information Communication Technology and Systems (ICTS), pp. 181–186, 2015.
[28] O. Andreassen, C. CharrondiA¨re, and A. De Dios Fuente, “Monitoring Mixed- ˜ Language Applications with Elastic Search, Logstash and Kibana (ELK),” p. WEPGF041. 4 p, 2015.
[29] B. Purnachandra Rao and N. Nagamalleswara Rao, HDFS Logfile Analysis Using ElasticSearch, LogStash and Kibana, pp. 185–191. Singapore: Springer Singapore, 2019.
[30] C. He, “Using logstash and elasticsearch to achieve real-time statistical analysis of dspace logs,” Data Analysis and Knowledge.
[31] Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). AI Applications in Smart Cities: Experiences from Deploying ML Algorithms for Urban Planning and Resource Optimization. Tuijin Jishu/Journal of Propulsion Technology, 40(4), 50-56.
[32] Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service . (2019). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98
[33] Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service. International Journal
[34] ofTranscontinental Discoveries, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98
[35] Choppadandi, A., Kaur, J., Chenchala, P. K., Kanungo, S., & Pandian, P. K. K. G. (2019). AI-Driven Customer Relationship Management in PK Salon Management System. International Journal of Open Publication and Exploration, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128
[36] AI-Driven Customer Relationship Management in PK Salon Management System. (2019). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128
[37] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
[38] Ashok : "Choppadandi, A., Kaur, J.,Chenchala, P. K., Nakra, V., & Pandian, P. K. K. G. (2020). Automating ERP Applications for Taxation Compliance using Machine Learning at SAP Labs. International Journal of Computer Science and Mobile Computing, 9(12), 103-112. https://doi.org/10.47760/ijcsmc.2020.v09i12.014
[39] Chenchala, P. K., Choppadandi, A., Kaur, J., Nakra, V., & Pandian, P. K. G. (2020). Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. International Journal of Open Publication and Exploration, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127
[40] Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. International Journal of Open Publication and Exploration, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127

[41] AI-Driven Customer Relationship Management in PK Salon Management System. (2019). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128

[42] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76

[43] Fadnavis, N. S., Patil, G. B., Padyana, U. K., Rai, H. P., & Ogeti, P. (2020). Machine learning applications in climate modeling and weather forecasting. NeuroQuantology, 18(6), 135-145. https://doi.org/10.48047/nq.2020.18.6.NQ20194

[44] Tilala, Mitul, and Abhip Dilip Chawda. "Evaluation of Compliance Requirements for Annual Reports in Pharmaceutical Industries." NeuroQuantology 18, no. 11 (November 2020): 138-145. https://doi.org/10.48047/nq.2020.18.11.NQ20244.