Centralized Information Security Log-Collection facility

T. Veda Reddy[1], Adithi Rudrangi[2], A. Thanmai[3], Chinnam Bharath[4]

[1]*Assistant Professor, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.*
[2,3,4]*UG Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.*

Abstract. This paper extensively develops and thoroughly creates a highly centralized and extremely efficient log collection system utilizing and leveraging the robust syslog server and comprehensively collects and gathers log data from the numerous hosts residing within the network, meticulously analyses and scrutinizes the detailed log files and promptly sends and transmits a critical alert message to the central host through secure and reliable SMS. This paper thoroughly and comprehensively addresses and tackles the increasingly growing and rapidly expanding need for extremely robust and highly reliable cybersecurity measures and solutions in the vulnerable and sensitive power sector.

Keywords. Cybersecurity, Power Sector, Log collection, Syslog server, Alert system.

I. INTRODUCTION

Computer logs are very useful, as security device logs trace possible attacks from the attackers and records the activity of the system users. A log is evidence of what events occurring in an organization and networks. In most of the organizations, logs play an important role in cybersecurity [1]. It is widely recognized by the government and industry that it is both beneficial and desirable to share logs for the purpose of security research [2]. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. The logs contain descriptions of notable events such as crashes of system programs, failed login attempts. Event logging and event logs play an important role in modern IT systems. Today, many applications, operating systems, network devices, and other system components are able to log their events to a local or remote log server [3]. For this reason, event logs are an excellent source for determining the health status of the system, log management refers to the process of generating, storing and analysis of the log data. As logs contain records of system and network security, they need to be protected from breaches of their confidentiality and integrity.

The problem becomes much more challenging when log messages are generated by many sources. It might not be feasible to understand the meaning of all messages, so analysis might be limited to keyword and pattern searches [3]. Hence log management is very essential for any organization, as it is a helping hand to combat cyber security by protecting the log files from the attackers, who are trying to alter/erase the log files in order to wipe out evidence of his trespass out of those files. Syslog provides a simple framework for log entry generation, storage and transfer. Many log sources either use syslog as their native logging format or offer features that allow their logging formats can be converted to syslog format. In syslog-based logging infrastructure each log generator uses the same high-level format for its logs and the same basic mechanism for transferring its log entries to a syslog server running on another host.

Syslog uses message priorities to determine which messages should be handled more quickly, such as forwarding higher-priority messages more quickly than lower-priority ones. With the development of the computer technology, the virtual machine has been become the main research topic. By using the virtual technology, the computer system can aggregate all kinds of data resources, software resources and hardware resources and make these resources to provide service for different tasks. Moreover, the virtualization technology can separate hardware and software management and provide useful features including performance isolation [4], server consolidation and live migration [5]. In addition, the virtual technology can also provide portable environments for the modern computing systems [6]. Therefore, the new computing theorem and model that the virtualization technology embodies has very widespread use. The NXLog Enterprise Edition and its Support Services enabled Atmosera to implement a scalable logging system by making sure that all their log data is collected in an efficient, secure, and reliable way, at the same time allowing them to structure, format, and filter the data so it can be forwarded in a unified format to their SIEM to ingest. Atmosera, a US- based company partnered with NXLog to deliver log collection and centralization solutions along with their Security Information and Event Management platform. As an NXLog MSSP Partner, Atmosera continues to build customer trust with solutions that provide tangible results maximizing their security and ensuring compliance.

NXLog Enterprise Edition became one of their core applications within their Managed Detection and

Response (MDR), platform, designed to support environments with advanced security and compliance requirements. In general, log files – or simply ›logs‹ – are automatically generated text files that record specific technical information of a broad range of events taking place in a computer system or software application such as date, time, and type of event or executed action. In relation to Internet use, those events or actions are data exchanges between computers; and log files are the metadata of these data exchanges. Whenever we refer to ›log files‹ or ›log data‹ below, we mean this metadata of Internet tra c. Other types of log files, such as application or message logs, as well as keyboard, mouse or screen logging data, are not considered. The analysis of log files originates from technical hardware and software monitoring. In the past years, however, Internet-related log data in particular has increasingly gained a political dimension as it is used by companies and states for extensive tracking of Internet users on a large scale.

II. LITERATURE SURVEY

Early Research (2000s)

1. "Syslog: The Standard for Logging" by Rysavy (2001) - Introduced syslog protocol and its applications.
2. "Syslog Server Implementation" by Kuhn et al. (2002) - Discussed design and implementation of syslog servers.

Security and Compliance (2005-2010)

1. "Syslog-based Intrusion Detection" by Wang et al. (2005) - Proposed using syslog for intrusion detection.
2. "Compliance Management using Syslog" by Taylor et al. (2007)

- Explored syslog's role in regulatory compliance.

3. "Syslog Security Analysis" by Sailer et al. (2008) - Analyzed syslog security vulnerabilities.

Scalability and Performance (2010-2015)

METHODOLOGY

1. "Distributed Syslog Architecture" by Lee et al. (2010) - Proposed scalable syslog architecture.
2. "High-Performance Syslog Server" by Kim et al. (2012) - Optimized syslog server performance.
3. "Cloud-based Syslog Solutions" by Zhang et al. (2013) - Explored cloud-based syslog solutions.

Big Data and Analytics (2015-present)

1. "Syslog Data Analytics" by Singh et al. (2015) - Applied big data analytics to syslog data.
2. "Machine Learning for Syslog Analysis" by Wang et al. (2017) - Used machine learning for syslog anomaly detection.
3. "Real-time Syslog Analytics" by Kumar et al. (2019) - Developed real-time syslog analytics framework.

Recent Advances (2020-present)

1. "AI-powered Syslog Analysis" by Li et al. (2020) - Integrated AI for intelligent syslog analysis.
2. "Syslog-based Threat Hunting" by Kim et al. (2020) - Proposed syslog-based threat hunting framework.
3. "Cloud-native Syslog Solutions" by Patel et al. (2022) - Explored cloud-native syslog solution

Cloud-Based Virtual Desktops (2010s)

1. "Cloud-Based Virtual Desktop Infrastructure" by Amazon Web Services (2011) – Introduced cloud-based VDI.
2. "Cloud Desktop as a Service" by Citrix (2012) - Proposed cloud- based desktop-as-a-service.

Performance Optimization (2010s)

1. "Optimizing Virtual Desktop Performance" by Zhang et al. (2013) - Investigated performance optimization.
2. "Virtual Desktop Resource Allocation" by Li et al. (2015) - Explored resource allocation.

Security and Management (2010s)

1. "Secure Virtual Desktops" by Chen et al. (2014) - Investigated security measures.
2. "Virtual Desktop Management" by Kumar et al. (2016) - Proposed management frameworks.

Recent Advances (2020s)

1. "Container-Based Virtual Desktops" by Docker (2020) - Explored container-based virtual desktops.
2. "AI-Optimized Virtual Desktops" by NVIDIA (2022) - Investigated AI-optimized virtual desktops

Machine Learning and Log Analysis (2015-2020)

1. "Log Analysis with Machine Learning" by IEEE (2015) - Applied ML to log analysis.
2. "Python Log Analysis with Scikit-learn" by Data Camp (2018)- Used Scikit-learn for log analysis.

Deep Learning and Log Analysis (2020-present)

1. "Log Analysis with Deep Learning" by ResearchGate (2020) - Explored DL techniques.
2. "Python Log Analysis with TensorFlow" by towards data science (2022) - Used TensorFlow for log analysis.

Logs are also used widely in digital communication where data transaction is in need of high technologies and good management, log are used to provide more optimized and better solutions for data transaction in this technology and are also used for many other tasks that are usual and are used also in other platforms and technologies.[7] The architectural model proposed below in figure 1 used to centralize the storage and interpretation of the logs of an organization's system or networks and to protect the logs from the attacker. Centralization of the interpretation of the logs, serves to protect critical audit data from attackers by removing it immediately from the host, on which it is generated. The first tier of this architecture contains the hosts that generate the log data. The Syslog Server receives the log files from the individual log generating hosts such as routers, Switches, and local servers. This research paper implements the Winsyslog as the central Syslog Server. The central server then writes the log data into the database as per the rules specified in the Winsyslog configuration. The Syslog Server receives Syslog messages, processes them via the rule base and stores them in a database. Then the log files are stored separately on a data base server (Central Storage) for a period of time. Each host generating logs uses the same standard log format and forwards its log files to the Centralized storage. Windows can be configured to implement Syslog protocol.

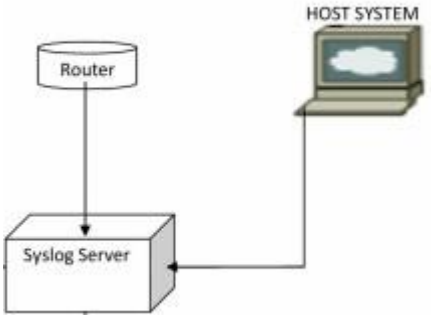


FIGURE 1. shows the Architectural diagram of the proposed work

1. Devices send Syslog messages to the Syslog Server.
2. Syslog Server forwards messages to the Message Queue.
3. Processing Script consumes messages from the Message Queue.
4. Script analyzes and processes messages in real-time.
5. Script triggers alerts based on message severity or content.

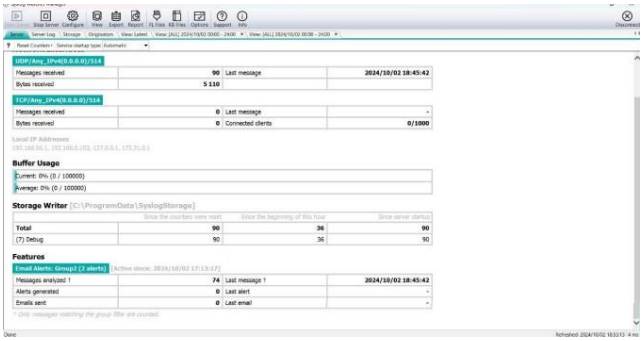


FIGURE 2. shows Syslog manager using TCP and UDP

We need 'n' number of guest systems in the network so that their logs are monitored by our system which is acting as host. Instead of installing many desktops in the network we tend to use the virtual desktop which solves our hardware constraints. Our model gets simplified and compacted to project. We use Oracle VM VirtualBox for installing virtual machine on the host which is shown in the Fig. 3.

Download and Install VirtualBox

1. Download VirtualBox from the official website.
2. Run the installer and follow the prompts.
3. Choose the installation location and components.
4. Install the VirtualBox Extension Pack (optional).

Create a New Virtual Machine

1. Launch VirtualBox.
2. Click "New" to create a new VM.
3. Enter VM name, type, and version.
4. Allocate memory (RAM) and CPU resources.
5. Create a virtual hard disk (VDI, VMDK, or VHD).

Configure VM Settings

1. Network: Select NAT, Bridged, or Host-only.
2. Storage: Add ISO file or installation media.
3. Audio: Select audio controller.
4. Display: Select graphics controller.

Install Guest Operating System

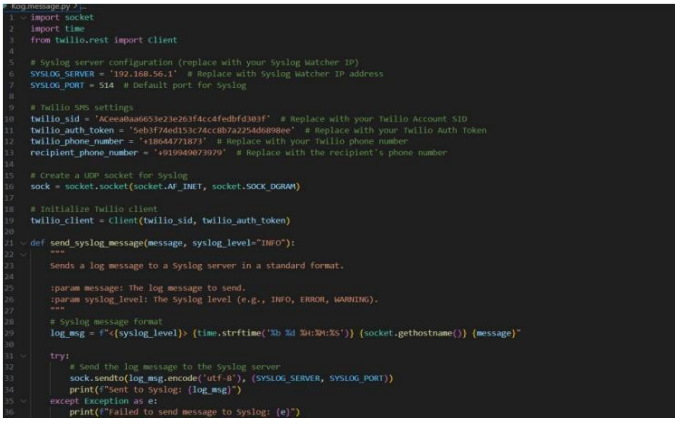
1. Start the VM.
2. Follow the installation prompts for the guest OS.
3. Install necessary drivers and software.

Configure Guest OS

1. Set up network connections.
2. Install VirtualBox Guest Additions.
3. Configure display and audio settings.

FIGURE 3. shows virtual machine on the host system

Log analysis script should run on all the guest os/virtual machines that automates the process of examining and interpreting log data from various sources to the host. Fig. 4 shows the log analysis script.



```
log_message.py
import socket
import time
from twilio.rest import Client

# Syslog server configuration (replace with your Syslog Watcher IP)
SYSLOG_SERVER = '192.168.56.1'  # Replace with Syslog Watcher IP address
SYSLOG_PORT = 514  # Default port for Syslog

# Twilio SMS settings
twilio_sid = 'ACeea0aa6653e23e263f4cc4fedbfd303f'  # Replace with your Twilio Account SID
twilio_auth_token = 'eb3f74ed153c74cc8b7a2254d6898ee'  # Replace with your Twilio Auth Token
twilio_phone_number = '+18644771873'  # Replace with your Twilio phone number
recipient_phone_number = '+919949073979'  # Replace with the recipient's phone number

# Create a UDP socket for Syslog
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

# Initialize Twilio client
twilio_client = Client(twilio_sid, twilio_auth_token)

def send_syslog_message(message, syslog_level="INFO"):
    """
    Sends a log message to a Syslog server in a standard format.

    :param message: The log message to send.
    :param syslog_level: The Syslog level (e.g., INFO, ERROR, WARNING).
    """
    # Syslog message format
    log_msg = f"<{syslog_level}> {time.strftime('%b %d %H:%M:%S')} {socket.gethostname()} {message}"

    try:
        # Send the log message to the Syslog server
        sock.sendto(log_msg.encode('utf-8'), (SYSLOG_SERVER, SYSLOG_PORT))
        print(f"Sent to Syslog: {log_msg}")
    except Exception as e:
        print(f"Failed to send message to Syslog: {e}")
```

FIGURE 4. shows Log analysis python script

Step 1: Importing Libraries

import socket import datetime import logging import re

- socket: for creating a network socket to connect to the Syslog server.
- datetime: for handling dates and times.
- logging: for logging purposes (not used extensively in this script).
- re: for regular expression pattern matching.

Step 2: Defining Syslog Server Settings

# Define Syslog server settings SYSLOG_SERVER = '192.168.1.100'
SYSLOG_PORT = 514

- Replace '192.168.1.100' with your Syslog server's IP address.
- 514 is the default Syslog port.

Step 3: Defining Log File Path and Name

# Define log file path and name LOG_FILE_PATH = 'C:\\SyslogLogs\\'
LOG_FILE_NAME = 'syslog_log_{}.log'.format(datetime.date.today())

- Define the directory path where logs will be saved.
- The log file name includes the current date.

Step 4: Creating Log File Directory (if needed)

Create log file directory if it doesn't exist import os
if not os.path.exists(LOG_FILE_PATH): os.makedirs(LOG_FILE_PATH)

- Check if the log file directory exists.
- If not, create the directory using os.makedirs().

Step 5: Defining Log Analysis Parameters # Define log analysis parameters
START_TIME = datetime.datetime.now() - datetime.timedelta(hours=1)
END_TIME = datetime.datetime.now()

- Define the time range for log analysis (last hour).

Step 6: Creating a Syslog Socket # Create a Syslog socket
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

- Create a UDP socket for Syslog communication.

Step 7: Binding the Socket to the Syslog Server # Bind the socket to the Syslog server
sock.bind((SYSLOG_SERVER, SYSLOG_PORT))

- Bind the socket to the Syslog server's IP address and port.

Step 8: Collecting Syslog Logs # Collect Syslog logs
logs = [] while True:
data, addr = sock.recvfrom(1024)

log_message = data.decode('utf-8') logs.append(log_message)

Break the loop if 1000 logs are collected if len(logs) >= 1000:
break

- Receive Syslog logs from the server.
- Decode the logs from bytes to UTF-8 string.
- Append each log to the logs list.
- Break the loop after collecting 1000 logs.

Step 9: Saving Logs to File # Save logs to file
with open(LOG_FILE_PATH + LOG_FILE_NAME, 'w') as f: for log in logs:
f.write(log + '\n')

- Open the log file in write mode.
- Write each log message to the file followed by a newline.

Step 10: Analyzing Logs # Analyze logs
error_logs = [log for log in logs if re.search(r'ERROR', log)]
warning_logs = [log for log in logs if re.search(r'WARNING', log)]

NXlogger

We use nxlogger as a comprehensive logging solution to collect and store log data from the network devices. We integrate nxlogger with syslog server where we get in detail information of the syslogs.

Installation:

1. Download the NXLogger installer from the official website.
2. Run the installer and follow the prompts.
3. Choose the installation location and components.

Configuration:

1. Launch NXLogger.
2. Configure the logging settings:

- Log sources (e.g., Windows Event Logs, Syslog).
- Log formats (e.g., CSV, JSON).
- Log filters (e.g., event ID, severity).

3. Set up log storage:

- Local file storage.
- Remote storage (e.g., Syslog server, database).

4. Configure alerting and notification options.

Setting up local file enables to store the log in .txt files.

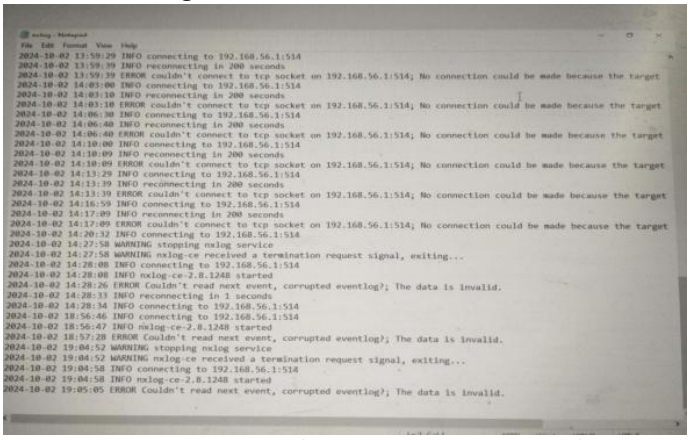


FIGURE 5. shows local file collecting syslogs in .txt format

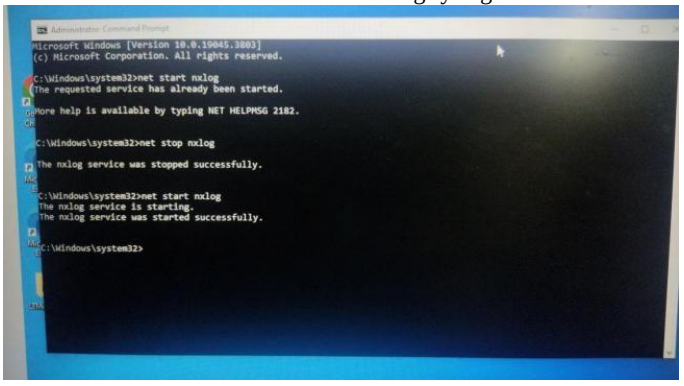


FIGURE 6. shows running nxlog in command prompt of the guest system

After running the nxlog we can see that our syslog server analysis our collected and stored logs and visualizes the information in the form of table with clear arguments mentioned in it.

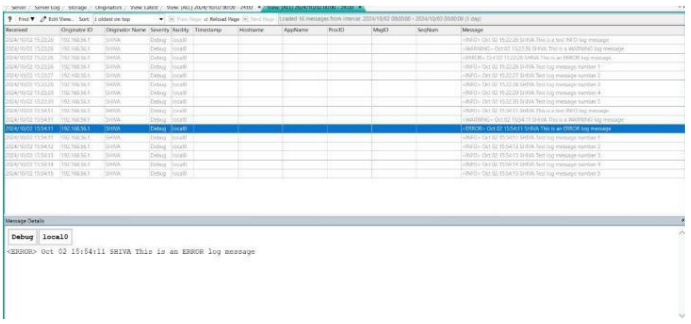


FIGURE 7. shows syslog server analyzed and visualized the syslogs

III. RESULT

We write a python script to integrate with syslog server to send alerts to the host through SMS

Create a Python script that:

1. Connects to your Syslog server.
2. Parses logs for specific events.
3. Sends SMS alerts using Twilio.

Example script:

```
import sys import logging
from twilio.rest import Client

# Twilio account settings account_sid = 'your_account_sid' auth_token = 'your_auth_token'
client = Client(account_sid, auth_token)

# Syslog server settings syslog_server = 'your_syslog_server' syslog_port = 514

# Define SMS settings
sms_from = 'your_twilio_phone_number' sms_to = 'recipient_phone_number'

# Define log filtering rules log_filter = 'your_log_filter'

# Connect to Syslog server import pySyslog
syslog = pySyslog.Client(syslog_server, syslog_port)
# Parse logs and send SMS alerts for log in syslog:
if log_filter in log:
message = client.messages.create( body=log,
from_=sms_from, to=sms_to
)
print(f'SMS sent: {message.sid}')
```

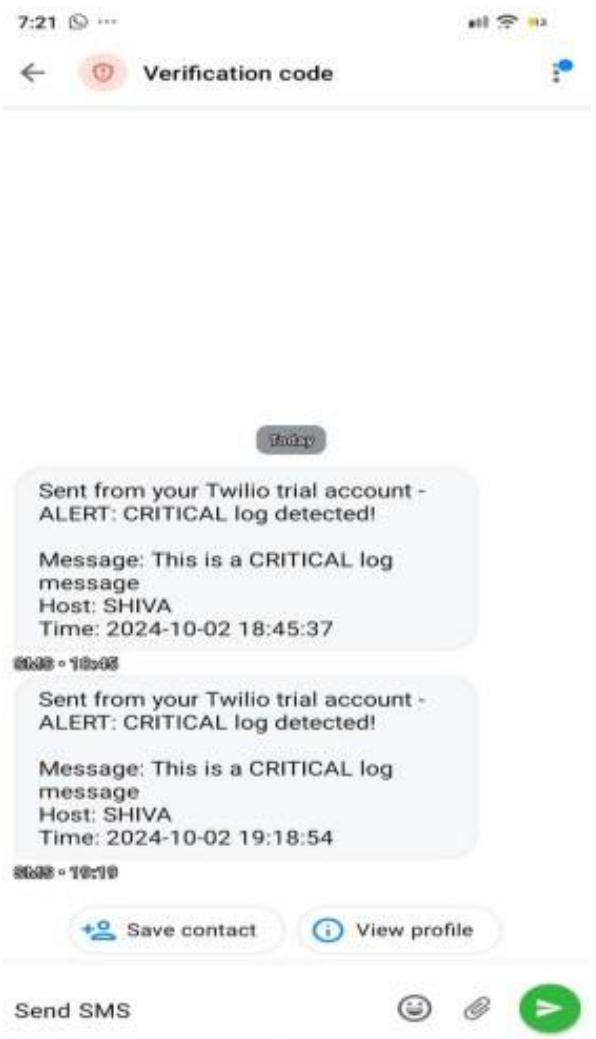


FIGURE 8. shows the SMS alert is sent to the host

IV. CONCLUSION

This paper develops a centralized log collection system using the syslog server and collects log from the hosts in the network, analyses the log files and sends an alert message to the central host through SMS. This paper addresses the growing need for robust cybersecurity in the power sector.

REFERENCES

1. Raj, R. S., & Raju, G. P. (2014, December). An approach for optimization of resource management in Hadoop. In *International Conference on Computing and Communication Technologies* (pp. 1-5). IEEE.
2. Ujwala, B., & Reddy, P. R. S. (2016). An effective mechanism for integrity of data sanitization process in the cloud. *European Journal of Advances in Engineering and Technology*, *3*(8), 82-84.
3. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, *30*(3).
4. Reddy, A. V. B., & Ujwala, B. Answering Xml Query Using Tree Based Association Rules.
5. Reddy, P. R. S., Reddy, A. M., & Ujwala, B. IDENTITY PRESERVING IN DYNAMIC GROUPS FOR DATA SHARING AND AUDITING IN CLOUD.
6. CHITHANURU, V. A review on the use of English language as an important factor in academic writing.
7. Mahammad, F. S., Viswanatham, V. M., Tahseen, A., Devi, M. S., & Kumar, M. A. (2024, July). Key distribution scheme for preventing key reinstallation attack in wireless networks. In *AIP Conference Proceedings* (Vol. 3028, No. 1). AIP Publishing.
8. Tahseen, A., Shailaja, S. R., & Ashwini, Y. (2023, December). Security-Aware Information Classification Using Attributes Extraction for Big Data Cyber Security Analytics. In *International*

Conference on Advances in Computational Intelligence and Informatics (pp. 365-373). Singapore: Springer Nature Singapore.

9. Tahseen, A., Shailaja, S. R., & Ashwini, Y. Extraction for Big Data Cyber Security Analytics. *Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2023*, *993*, 365.
10. Keshamma, E., Rohini, S., Rao, K. S., Madhusudhan, B., & Kumar, M. U. (2008). Molecular biology and physiology tissue culture-independent In Planta transformation strategy: an Agrobacterium tumefaciens-mediated gene transfer method to overcome recalcitrance in cotton (Gossypium hirsutum L.). *J Cotton Sci*, *12*, 264-272.
11. Sreevathsa, R., Sharma, P. D., Keshamma, E., & Kumar, U. (2008). In planta transformation of pigeon pea: a method to overcome recalcitrancy of the crop to regeneration in vitro. *Physiology and Molecular Biology of Plants: an International Journal of Functional Plant Biology*, *14*(4), 321-328.
12. Keshamma, E., Sreevathsa, R., Kumar, A. M., Reddy, K. N., Manjulatha, M., Shanmugam, N. B., ... & Udayakumar, M. (2012). Agrobacterium-mediated in planta transformation of field bean (Lablab purpureus L.) and recovery of stable transgenic plants expressing the cry 1AcF gene. *Plant Molecular Biology Reporter*, *30*, 67-78.
13. Gopinandhan, T. N., Keshamma, E., Velmourougane, K., & Raghuramulu, Y. (2006). Coffee husk-a potential source of ochratoxin A contamination.
14. Kumar, J. P., Rao, C. M. P., Singh, R. K., Garg, A., & Rajeswari, T. (2024). A comprehensive review on blood brain delivery methods using nanotechnology. *Tropical Journal of Pharmaceutical and Life Sciences*, *11*(3), 43-52.
15. Jeslin, D., Prema, S., Ismail, Y., Panigrahy, U. P., Vijayamma, G., RS, C., ... & Kumar, J. P. (2022). ANALYTICAL METHOD VALIDATION OF DISSOLUTION METHOD FOR THE DETERMINATION OF% DRUG RELEASE IN DASATINIB TABLETS 20MG, 50MG AND 70MG BY HPLC. *Journal of Pharmaceutical Negative Results*, 2722-2732.
16. Kumar, J., Dutta, S., Sundaram, V., Saini, S. S., Sharma, R. R., & Varma, N. (2019). intraventricular hemorrhage compared with 9.1% in the restrictive group (P=. 034).". *Pediatrics*, *144*(2), 1.
17. Kumar, J. P., Rao, C. M. P., Singh, R. K., Garg, A., & Rajeswari, T. A brief review on encapsulation of natural poly-phenolic compounds.
18. KP, A., & John, J. (2021). The Impact Of COVID-19 On Children And Adolescents: An Indianperspectives And Reminiscent Model. *Int. J. of Aquatic Science*, *12*(2), 472-482.
19. John, J., & Akhila, K. P. (2019). Deprivation of Social Justice among Sexually Abused Girls: A Background Study.
20. Akhila, K. P., & John, J. Deliberate democracy and the MeToo movement: Examining the impact of social media feminist discourses in India. In *The Routledge International Handbook of Feminisms in Social Work* (pp. 513-525). Routledge.
21. Akhila, K. P., & John, J. Impact of Pandemic on Child Protection-A Response to COVID-19.
22. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2012). Reliability improvement of radial distribution system with distributed generation. *International Journal of Engineering Science and Technology (IJEST)*, *4*(09), 4003-4011.
23. Gowda, B. M. V., Murthy, G. V. K., Upadhye, A. S., & Raghavan, R. (1996). Serotypes of Escherichia coli from pathological conditions in poultry and their antibiogram.
24. Balasubbareddy, M., Murthy, G. V. K., & Kumar, K. S. (2021). Performance evaluation of different structures of power system stabilizers. *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(1), 114-123.
25. Murthy, G. V. K., & Sivanagaraju, S. (2012). S. Satyana rayana, B. Hanumantha Rao," Voltage stability index of radial distribution networks with distributed generation,". *Int. J. Electr. Eng*, *5*(6), 791-803.
26. Anuja, P. S., Kiran, V. U., Kalavathi, C., Murthy, G. N., & Kumari, G. S. (2015). Design of elliptical patch antenna with single & double U-slot for wireless applications: a comparative approach. *International Journal of Computer Science and Network Security (IJCSNS)*, *15*(2), 60.
27. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2015). Voltage stability enhancement of distribution system using network reconfiguration in the presence of DG. *Distributed Generation & Alternative Energy Journal*, *30*(4), 37-54.
28. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.
29. Madhavi, M., & Murthy, G. V. (2020). Role of certifications in improving the quality of Education in Outcome Based Education. *Journal of Engineering Education Transformations*, *33*(Special Issue).
30. Varaprasad Rao, M., Srujan Raju, K., Vishnu Murthy, G., & Kavitha Rani, B. (2020). Configure and management of internet of things. In *Data Engineering and Communication Technology: Proceedings of 3rd ICDECT-2K19* (pp. 163-172). Springer Singapore.
31. Murthy, G. V. K., Suresh, C. H. V., Sowjankumar, K., & Hanumantharao, B. (2019). Impact of distributed generation on unbalanced radial distribution system. *International Journal of Scientific and Technology Research*, *8*(9), 539-542.
32. Siva Prasad, B. V. V., Mandapati, S., Kumar Ramasamy, L., Boddu, R., Reddy, P., & Suresh Kumar, B. (2023). Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc

networks. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *64*(3), 658-671.

33. Siva Prasad, B. V. V., Sucharitha, G., Venkatesan, K. G. S., Patnala, T. R., Murari, T., & Karanam, S. R. (2022). Optimisation of the execution time using hadoop-based parallel machine learning on computing clusters. In *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021* (pp. 233-244). Singapore: Springer Nature Singapore.
34. Prasad, B. V., & Ali, S. S. (2017). Software–defined networking based secure rout-ing in mobile ad hoc network. *International Journal of Engineering & Technology*, *7*(1.2), 229.
35. Elechi, P., & Onu, K. E. (2022). Unmanned Aerial Vehicle Cellular Communication Operating in Non-terrestrial Networks. In *Unmanned Aerial Vehicle Cellular Communications* (pp. 225-251). Cham: Springer International Publishing.
36. Prasad, B. V. V. S., Mandapati, S., Haritha, B., & Begum, M. J. (2020, August). Enhanced Security for the authentication of Digital Signature from the key generated by the CSTRNG method. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1088-1093). IEEE.
37. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Veeneetha, S. V., Srivalli, N., ... & Sahitya, D. (2022, November). Prediction of Flight-fare using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 134-138). IEEE.
38. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Bhargavi, P. J., Alekhya, A., ... & Nandini, K. (2022, November). Cardiovascular Disease Prediction using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 60-66). IEEE.
39. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*.
40. Rao, B. T., Prasad, B. V. V. S., & Peram, S. R. (2019). Elegant Energy Competent Lighting in Green Buildings Based on Energetic Power Control Using IoT Design. In *Smart Intelligent Computing and Applications: Proceedings of the Second International Conference on SCI 2018, Volume 1* (pp. 247-257). Springer Singapore.
41. Someswar, G. M., & Prasad, B. V. V. S. (2017, October). USVGM protocol with two layer architecture for efficient network management in MANET'S. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 738-741). IEEE.
42. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
43. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
44. Balram, G., Poornachandrarao, N., Ganesh, D., Nagesh, B., Basi, R. A., & Kumar, M. S. (2024, September). Application of Machine Learning Techniques for Heavy Rainfall Prediction using Satellite Data. In *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1081-1087). IEEE.
45. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
46. KATIKA, R., & BALRAM, G. (2013). Video Multicasting Framework for Extended Wireless Mesh Networks Environment. *pp-427-434*, *IJSRET*, *2*(7).
47. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
48. Prasad, P. S., & Rao, S. K. M. (2017). A Survey on Performance Analysis of ManetsUnder Security Attacks. *network*, *6*(7).
49. Sheta, S. V. (2021). Investigating Open-Source Contributions to Software Innovation and Collaboration. *International Journal of Computer Science and Engineering Research and Development (IJCSERD)*, *11*(1), 46-54.
50. Sheta, S. V. (2021). Artificial Intelligence Applications in Behavioral Analysis for Advancing User Experience Design. *ISCSITR-INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE (ISCSITR-IJAI)*, *2*(1), 1-16.
51. Ingle, S. D., & Tohare, S. P. (2022). Geological investigation in the Bhuleshwari River Basin, Amravati District, Maharashtra. *World Journal of Advanced Research and Reviews*, *16*(3), 757-766.
52. Ingle, S. D. Hydrogeological Investingations in the Bhuleshwari River Basin with Emphasis on Groundwater Management Amravati District Maharashtra.
53. Ingle, S. D., & Jadhav, K. A. Evaluating The Performance of Artificial Recharge Structures Towards Ground Water Recharge in Amravati District, Maharashtra.

54. Ingle, S. D. GEOPHYSICAL INVESTIGATION IN THE BHULESHWARI RIVER BASIN, AMRAVATI DISTRICT, MAHARASHTRA.
55. Vaddadi, S. A., Thatikonda, R., Padthe, A., & Arnepalli, P. R. R. (2023). Shift left testing paradigm process implementation for quality of software based on fuzzy. *Soft Computing*, 1-13.
56. Vaddadi, S., Arnepalli, P. R., Thatikonda, R., & Padthe, A. (2022). Effective malware detection approach based on deep learning in Cyber-Physical Systems. *International Journal of Computer Science and Information Technology*, *14*(6), 01-12.
57. Yendluri, D. K., Ponnala, J., Thatikonda, R., Kempanna, M., Tatikonda, R., & Bhuvanesh, A. (2023, November). Impact of Robotic Process Automation on Enterprise Resource Planning Systems. In *2023 International Conference on the Confluence of Advancements in Robotics, Vision and Interdisciplinary Technology Management (IC-RVITM)* (pp. 1-6). IEEE.
58. Yendluri, D. K., Tatikonda, R., Thatikonda, R., Ponnala, J., Kempanna, M., & Bhuvanesh, A. (2023, December). Integration of SAP and Intelligent Robotic Process Automation. In *2023 International Conference on Next Generation Electronics (NEleX)* (pp. 1-6). IEEE.
59. Rao, P. R., Kumar, K. H., & Reddy, P. R. S. (2012). Query decomposition and data localization issues in cloud computing. *International Journal*, *2*(9).
60. Reddy, P. R. S., & Ravindranath, K. (2024). Enhancing Secure and Reliable Data Transfer through Robust Integrity. *Journal of Electrical Systems*, *20*(1s), 900-910.
61. REDDY, P. R. S., & RAVINDRANATH, K. (2022). A HYBRID VERIFIED RE-ENCRYPTION INVOLVED PROXY SERVER TO ORGANIZE THE GROUP DYNAMICS: SHARING AND REVOCATION. *Journal of Theoretical and Applied Information Technology*, *100*(13).
62. Reddy, P. R. S., Ram, V. S. S., Greshma, V., & Kumar, K. S. Prediction of Heart Healthiness.
63. Reddy, P. R. S., Reddy, A. M., & Ujwala, B. IDENTITY PRESERVING IN DYNAMIC GROUPS FOR DATA SHARING AND AUDITING IN CLOUD.
64. Madhuri, K., Viswanath, N. K., & Gayatri, P. U. (2016, November). Performance evaluation of AODV under Black hole attack in MANET using NS2. In *2016 international conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-3). IEEE.
65. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
66. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7 S).
67. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, 255.
68. Madhuri, K. (2022). A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network. *Journal of Algebraic Statistics*, *13*(1), 159-168.
69. Selvan, M. A. (2021). Robust Cyber Attack Detection with Support Vector Machines: Tackling Both Established and Novel Threats.
70. Selvan, M. A. (2023). INDUSTRY-SPECIFIC INTELLIGENT FIRE MANAGEMENT SYSTEM.
71. Selvan, M. Arul. "PHISHING CONTENT CLASSIFICATION USING DYNAMIC WEIGHTING AND GENETIC RANKING OPTIMIZATION ALGORITHM." (2024).
72. Selvan, M. Arul. "Innovative Approaches in Cardiovascular Disease Prediction Through Machine Learning Optimization." (2024).
73. FELIX, ARUL SELVAN M. Mr D., and XAVIER DHAS Mr S. KALAIVANAN. "Averting Eavesdrop Intrusion in Industrial Wireless Sensor Networks."
74. Yakoob, S., Krishna Reddy, V., & Dastagiraiah, C. (2017). Multi User Authentication in Reliable Data Storage in Cloud. In *Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016* (pp. 531-539). Springer Singapore.
75. DASTAGIRAIAH, D. (2024). A SYSTEM FOR ANALYSING CALL DROP DYNAMICS IN THE TELECOM INDUSTRY USING MACHINE LEARNING AND FEATURE SELECTION. *Journal of Theoretical and Applied Information Technology*, *102*(22).
76. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
77. Sudhakar, R. V., Dastagiraiah, C., Pattem, S., & Bhukya, S. (2024). Multi-Objective Reinforcement Learning Based Algorithm for Dynamic Workflow Scheduling in Cloud Computing. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *12*(3), 640-649.
78. PushpaRani, K., Roja, G., Anusha, R., Dastagiraiah, C., Srilatha, B., & Manjusha, B. (2024, June). Geological Information Extraction from Satellite Imagery Using Deep Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
79. Tambi, V. K., & Singh, N. A Comprehensive Empirical Study Determining Practitioners' Views on Docker Development Difficulties: Stack Overflow Analysis.

80. Tambi, V. K., & Singh, N. Evaluation of Web Services using Various Metrics for Mobile Environments and Multimedia Conferences based on SOAP and REST Principles.
81. Tambi, V. K., & Singh, N. Developments and Uses of Generative Artificial Intelligence and Present Experimental Data on the Impact on Productivity Applying Artificial Intelligence that is Generative.
82. Tambi, V. K., & Singh, N. A New Framework and Performance Assessment Method for Distributed Deep Neural Network-Based Middleware for Cyberattack Detection in the Smart IoT Ecosystem.
83. Tambi, Varun Kumar, and Nishan Singh. "Creating J2EE Application Development Using a Pattern-based Environment."
84. Tambi, Varun Kumar, and Nishan Singh. "New Applications of Machine Learning and Artificial Intelligence in Cybersecurity Vulnerability Management."
85. Tambi, V. K., & Singh, N. Assessment of Possible REST Web Service Description for Hypermedia-Focused Graph-Based Service Discovery.
86. Tambi, V. K., & Singh, N. Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
87. Tambi, V. K., & Singh, N. Analysing Methods for Classification and Feature Extraction in AI-based Threat Detection.
88. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
89. Arora, P., & Bhardwaj, S. Using Knowledge Discovery and Data Mining Techniques in Cloud Computing to Advance Security.
90. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector. *Methods*, *8*(2).
91. Arora, P., & Bhardwaj, S. A Thorough Examination of Privacy Issues using Self-Service Paradigms in the Cloud Computing Context.
92. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.
93. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
94. Arora, P., & Bhardwaj, S. (2019). Safe and Dependable Intrusion Detection Method Designs Created with Artificial Intelligence Techniques. *machine learning*, *8*(7).
95. Arora, Pankit, and Sachin Bhardwaj. "A Very Effective and Safe Method for Preserving Privacy in Cloud Data Storage Settings."
96. Arora, P., & Bhardwaj, S. (2017). A Very Safe and Effective Way to Protect Privacy in Cloud Data Storage Configurations.
97. Arora, P., & Bhardwaj, S. The Applicability of Various Cybersecurity Services to Prevent Attacks on Smart Homes.
98. Arora, P., & Bhardwaj, S. Designs for Secure and Reliable Intrusion Detection Systems using Artificial Intelligence Techniques.
99. Abbas, S. A., Khan, A., Kalusalingam, A., Menon, B., Siang, T., & Mohammed, J. S. (2023). Pharmacological Screening Of Polyherbal Formulation For Hepatoprotective Effect Against Anti Tuberculosis Drugs Induced Hepatotoxicity On Albino Rats. *Journal of Survey in Fisheries Sciences*, 4313-4318.
100. Kumar, A., Ravishankar, K., Varma, A. K., Prashar, D., Mohammed, J. S., & Billah, A. M. Liposome Nano-particles for Therapeutic and Diagnostic Applications.
101. Samya, B., Archana, M., Ramana, T. V., Raju, K. B., & Ramineni, K. (2024, February). Automated Student Assignment Evaluation Based on Information Retrieval and Statistical Techniques. In *Congress on Control, Robotics, and Mechatronics* (pp. 157-167). Singapore: Springer Nature Singapore.
102. Sravan, K., Rao, L. G., Ramineni, K., Rachapalli, A., & Mohmmad, S. (2024). Analyze the Quality of Wine Based on Machine Learning Approach Check for updates. *Data Science and Applications: Proceedings of ICDSA 2023, Volume 3*, *820*, 351.
103. Chandhar, K., Ramineni, K., Ramakrishna, E., Ramana, T. V., Sandeep, A., & Kalyan, K. (2023, December). Enhancing Crop Yield Prediction in India: A Comparative Analysis of Machine Learning Models. In *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)* (pp. 1-4). IEEE.
104. Ramineni, K., Shankar, K., Shabana, Mahender, A., & Mohmmad, S. (2023, June). Detecting of Tree Cutting Sound in the Forest by Machine Learning Intelligence. In *International Conference on Power Engineering and Intelligent Systems (PEIS)* (pp. 303-314). Singapore: Springer Nature Singapore.
105. Ashok, J., RAMINENI, K., & Rajan, E. G. (2010). BEYOND INFORMATION RETRIEVAL: A SURVEY. *Journal of Theoretical & Applied Information Technology*, *15*.
106. Selvan, M. Arul, and S. Miruna Joe Amali. "RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE." (2024).
107. Selvan, M. Arul. "Fire Management System For Indutrial Safety Applications." (2023).
108. Selvan, M. A. (2023). A PBL REPORT FOR CONTAINMENT ZONE ALERTING APPLICATION.

109. Selvan, M. A. (2023). CONTAINMENT ZONE ALERTING APPLICATION A PROJECT BASED LEARNING REPORT.
110. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
111. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
112. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*(Special Issue 1).
113. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
114. Amarnadh, V., & Moparthi, N. R. (2024). Prediction and assessment of credit risk using an adaptive Binarized spiking marine predators' neural network in financial sector. *Multimedia Tools and Applications*, *83*(16), 48761-48797.
115. Amarnadh, V., & Moparthi, N. R. (2024). Range control-based class imbalance and optimized granular elastic net regression feature selection for credit risk assessment. *Knowledge and Information Systems*, 1-30.
116. Amarnadh, V., & Akhila, M. (2019, May). RETRACTED: Big Data Analytics in E-Commerce User Interest Patterns. In *Journal of Physics: Conference Series* (Vol. 1228, No. 1, p. 012052). IOP Publishing.
117. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.
118. Rao, K. R., & Amarnadh, V. QoS Support for Cross-Layer Scheduling Algorithm in Wireless Networks.
119. Gowda, P., & Gowda, A. N. (2024). Best Practices in REST API Design for Enhanced Scalability and Security. *Journal of Artificial Intelligence, Machine Learning and Data Science*, *2*(1), 827-830.
120. Gowda, P. G. A. N. (2024). Benefits and Risks of Generative AI in FinTech. *Journal of Scientific and Engineering Research*, *11*(5), 267-275.