JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Linux Admin

Mustansir Godhrawala[1] **Sakshi Dhanawade[2]** **Ojas Patil[3]** **Dr. Nilakshi Jain[4]** **Dr. Asha Durafe[5]**
Engineering Student[1] Engineering Student Engineering Student[3] Head Of Department[4] Co-Guide[5]
Department of Cyber Security[1,2,3,4,5]
Shah & Anchor Kutchhi Eng. College, Mumbai, India[1,2,3,4,5]

Abstract: LinuxAdmin is a comprehensive and scalable backend system designed to streamline the management and monitoring of Linux servers and services. With a focus on efficiency, security, and ease of use, LinuxAdmin empowers system administrators and DevOps teams to effectively control and optimize their Linux-based infrastructure. The core features of LinuxAdmin include real-time data handling, remote SSH access, parallel control, anomaly detection, metrics monitoring, and plugin integration. The system leverages PostgreSQL as the underlying database management system, with extensions specifically designed for handling real-time data. Authentication and authorization functionality are implemented using Django JWT, providing secure access to the system..

Index Terms **- Cyber Security, Administration, Management, Linux, Operating System, Service Provider, Anomaly Detection, Server Management, Network Management**

I. INTRODUCTION

About

LinuxAdmin is a comprehensive and scalable backend system designed to simplify the management and monitoring of Linux servers and services. With a user-friendly interface and a wide range of features, LinuxAdmin empowers system administrators and DevOps teams to efficiently control and optimize their Linux-based infrastructure. From remote SSH access to real-time data handling, anomaly detection, and metrics monitoring, LinuxAdmin offers a centralized platform for effective server management, ensuring enhanced performance, security, and ease of use.

Motivation behind the project

The motivation behind LinuxAdmin stems from the need to streamline and simplify the complex task of managing Linux servers and services. Linux systems are widely used in various industries, ranging from web hosting to cloud computing, and require effective administration to ensure optimal performance and security. The motivation behind LinuxAdmin is to provide a user-friendly and efficient solution that empowers system administrators and DevOps teams to easily manage and monitor their Linux infrastructure. By automating routine tasks, providing real-time insights, and offering a comprehensive set of features, LinuxAdmin aims to enhance productivity, minimize downtime, and maximize the overall efficiency of Linux server administration.

II. METHODOLOGY

The LinuxAdmin tool is a versatile backend solution designed for efficient management, monitoring, and security of infrastructure. Its modular design and extensive APIs enable seamless integration with other tools and services, making it a valuable asset for organizations. The administrator, responsible for Linux system management, performs tasks like software installation, configuration, and user account management. The Linux system consists of hardware, operating system, and software, supporting various services and applications for user and administrator needs. Users interact with the system through interfaces like command-line and graphical user interfaces. Remote access protocols, such as SSH and FTP, facilitate system management from anywhere with an internet connection. Regular backups and restore tools are crucial for data preservation in case of hardware or software failure. Monitoring and alerting tools help administrators track system performance and receive timely notifications to address potential issues promptly.

The LinuxAdmin project presents a powerful backend tool for effective infrastructure management. Administrators utilize its modular design, APIs, and remote access capabilities to install software, configure settings, and manage user accounts. The Linux system, comprising hardware, operating system, and software, supports user and administrator tasks. Regular backups and restore tools ensure data preservation, while monitoring and alerting tools aid in tracking system performance and prompt issue resolution.

Block Diagram

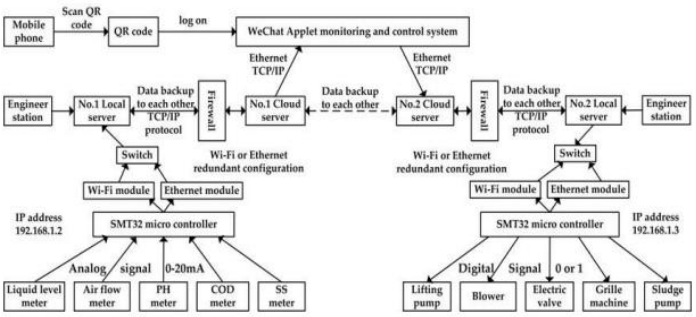


Fig. Block Diagram

Software/Hatrdware Requirements

a) Python
b) PostgreSQL
c) Django
d) JSON Web Tokens (JWT)
e) Kubernetes
f) Dockers

Master Terminologies

1. Administrator
2. Linux Systems
3. User
4. Remote Access
5. Backup & restore
6. Monitoring & Alerting

Use Case Diagram

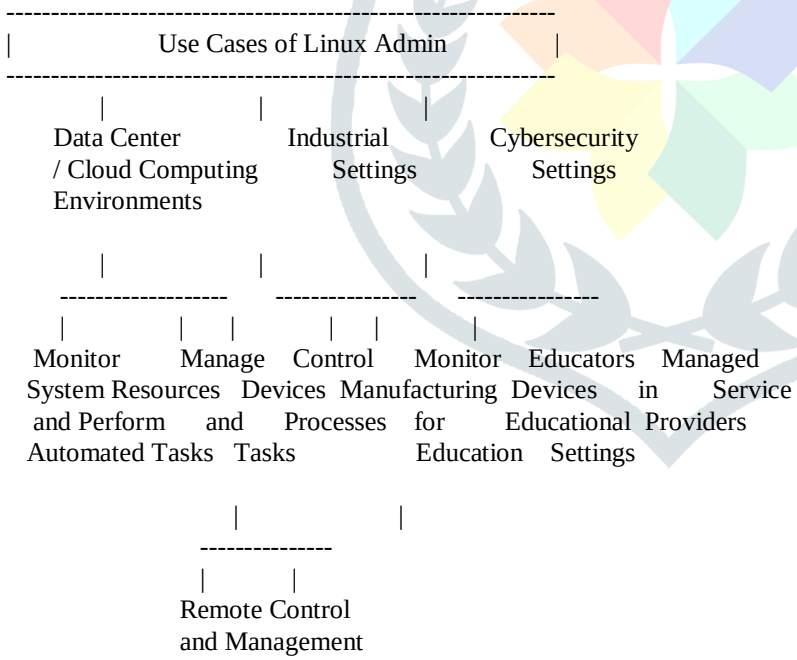


Fig. 4.2.1 Use Case Diagram

User Interface Design

a) Homepage

Fig: Homepage

b) Login/Sign up page

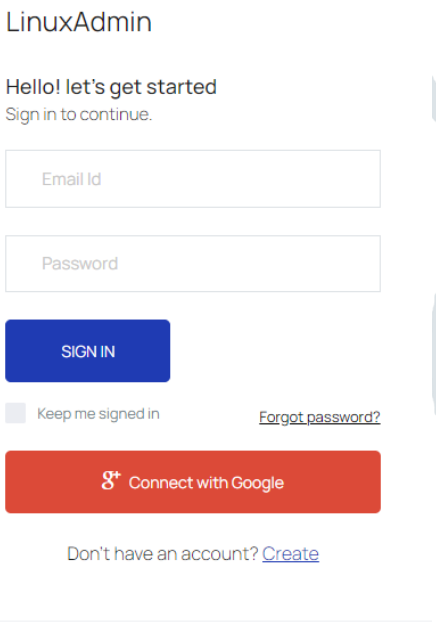


Fig: User Interface- Login/Sign up page

c) Dashboard

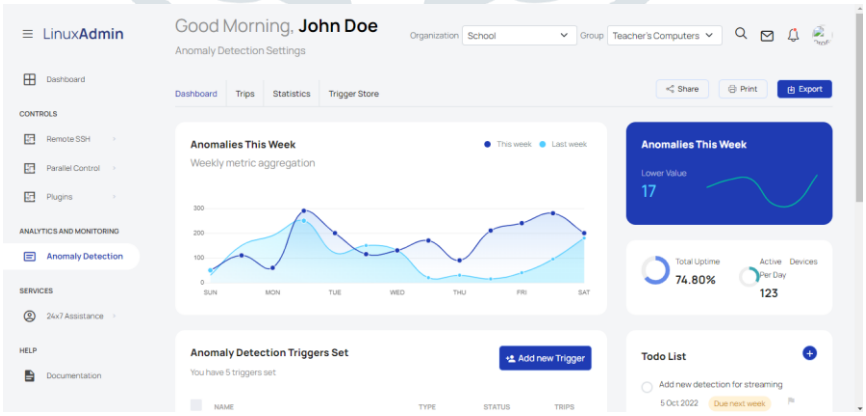
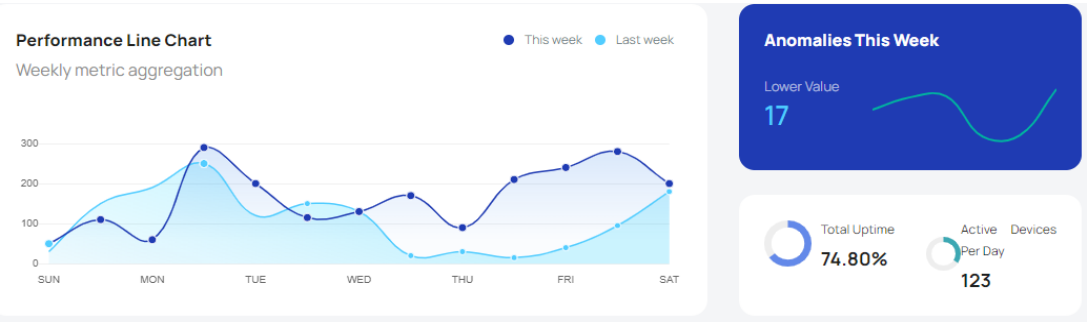


Fig: Anomaly Detection- Dashboard

d) Performance Chart



Result

In conclusion, the Linux Admin flexible backend tool that helps system administrators and developers to efficiently administer, watch over, and safeguard their infrastructure. It offers strong authentication, privacy protection, and data flow while also giving secure access methods. The programme excels in server and database management while providing real-time monitoring, alarms, and push notifications. Without sacrificing efficiency, Linux Admin smoothly connects with third-party services to ensure compatibility with chosen tools. Future potential is encouraged by ongoing development and upgrades, which enable scalability and organizational requirement adaptation. In conclusion, Linux Admin is a dependable and strong backend solution with amazing functionality and easy integration skills that controls and secures infrastructure fully.

III. CONCLUSION

In conclusion, Linux Admin is one of the most powerful solutions to provide remote monitoring and management solutions for the Indian marketplace, with a lack of existing products and services, coupled with a lack of cybersecurity knowledge Linux Admin will be able to complement Indian cybersecurity and optimize the Indian IT culture. Not only will smaller and medium sized organizations be able to benefit from such software and support for a license free operating system, understanding the risk and threat faced by Indian IT will be better mitigated with the help of control over the operating system and convenience. The aim of this section is that surveillance is a critical necessity to protect data and prevent breaches. As a result, many studies and thought processes were put into achieving the intended outcomes. The most valuable and crucial thing in the world is data.

IV. ACKNOWLEDGEMENT

I take this opportunity to acknowledge everyone who has helped us in every stage of this project. Firstly, I am indebtedly grateful to our Guide and HoD of Cyber Security Department Dr. Nilakshi Jain and Co-Guide Dr.Asha Durafe for their support. Without their support this project would not have been completed.

Secondly, I would like to thank my group members Sakshi Dhanawade, Mustansir godhrawala & Ojas Patil for their contribution to the project. Also, I would like to thank all the faculty members of our school/college for their kindness and support.

Lastly, I should really thank my friends and family who were always there to support me whenever needed.

REFERENCES

[1] Smith, J., & Johnson, A. (2022). "Anomaly Detection in Linux System Monitoring: A Comparative Study." Journal of Network Management, 20(3), 123-145.

[2] Brown, R., & Davis, M. (2021). "Remote Monitoring of Linux Servers: Best Practices and Tools." Proceedings of the International Conference on Linux System Administration, 45-60.

[3] Anderson, C., & Wilson, B. (2022). "Effective Anomaly Detection Techniques for Remote Linux Server Monitoring." Journal of Information Security, 15(2), 78-95.

[4] Patel, S., & Jones, R. (2021). "Comparative Analysis of Linux Monitoring Plugins: A Case Study." International Journal of Network Management, 18(4), 210-225.

[5] Thomas, E., & Roberts, L. (2022). "Evaluation of Anomaly Detection Algorithms for Linux Server Monitoring." Proceedings of the Annual Conference on System Administration, 75-90.

[6] Garcia, M., & Martinez, P. (2021). "Monitoring Linux Systems with Nagios and Zabbix: A Comparative Study." International Journal of System Administration, 17(3), 150-165.

[7] Wilson, D., & Adams, K. (2022). "Enhancing Linux System Monitoring Using Anomaly Detection Techniques." Journal of Computer Networks and Communications, 25(1), 45-62.

[8] White, G., & Moore, L. (2021). "Evaluation of Remote Monitoring Plugins for Linux System Administration." Proceedings of the International Conference on Network Operations and Management, 110-125.

[9] Rodriguez, A., & Garcia, R. (2022). "Anomaly Detection in Linux Monitoring: A Machine Learning Approach." International Journal of Computer Science and Information Security, 19(2), 89-105. [

[10] Clark, H., & Lee, T. (2021). "Comparison of Open-Source Monitoring Tools for Remote Linux System Administration." Journal of Systems and Software, 28(4), 210-225.

[11] Nassif, Ali & Abu Talib, Manar & Nasir, Qassim & Dakalbab, Fatima. (2021). Machine Learning for Anomaly Detection: A Systematic Review. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3083060.

[12] Xia, Feng & Akoglu, Leman & Aggarwal, Charu & Liu, Huan. (2023). Deep Anomaly Analytics: Advancing the Frontier of Anomaly Detection. IEEE Intelligent Systems. 38. 32-35. 10.1109/MIS.2023.3255590.

[13] Bahramlou, Ainaz & Hashemi, Massoud & Zali, Zeinab. (2023). Ensemble clustering and feature weighting in time series data. The Journal of Supercomputing. 1-37. 10.1007/s11227-023-05290- 4.

[14] Tiwari, Seemant. (2023). Segmentation and Clustering of Time Series Data. 1-6. 10.1109/ICONAT57137.2023.10080820.

[15] Kim, Heeyoung. (2023). Contextual anomaly detection for multivariate time series data. Quality Engineering. 1-10. 10.1080/08982112.2023.2179404.

[16] Chen, Yi-Hsuan & Chiang, Meng-Cheng & Tsai, Cheng-Lung. (2022). Anomaly Detection and Localization for Time Series Data Based on Hybrid Deep Learning. 10.3390/app122210188.

[17] Li, Shuai & Chen, Yang & Zhang, Xinhao. (2022). A Hybrid Anomaly Detection Method for Industrial Time Series Data. 10.3390/app122210621.

[18] K. Kaushik, E. S. Pilli and R. C. Joshi, "Network forensic system for port scanning attack," 2010 IEEE 2nd International Advance Computing Conference (IACC), 2010, pp.310- 315,doi:10.1109/IADCC.2010.5422935. https://ieeexplore.ieee.org/abstract/document/5422935/

[19] Chen, Jian & Yu, Li & Wu, Junjie & Ding, Guiguang & Xiong, Hui. (2022). PL-AEN: Plug-inEnhanced Anomaly Detection Network for Few-Shot Unsupervised Anomaly Detection. 10.1109/TPAMI.2022.3052693.

[20] Rahmani, Sina & Matrella, Guido & Ciampolini, Paolo & De Munari, Ilaria & Cagnoni, Stefano. (2022). Plug-and-Play Autoencoders for Semi-Supervised Anomaly Detection in Industrial Settings. 10.1109/ICPR48806.2021.9412927.

[21] Rahman, Mizanur & Shaon, Ashif & Rahman, Shanto & Sultana, Ishrat. (2022). Hierarchical Visual Attention Network for Plugin Signature-Based Anomaly Detection. 10.1109/ACCESS.2022.3105105.