International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

AUTOMATED ALERTS FOR REAL-TIME IT INFRASTRUCTURE MONITORING

Aakash Aluwala
akashaluwala@gmail.com

Abstract

This paper analyzes the impact of implementing an automated monitoring and alerting solution through a secondary qualitative research methodology. Literature on infrastructure monitoring tools and techniques was reviewed to understand current capabilities. A solution incorporating data collection, processing, machine learning-driven alerting and multi-channel notifications was designed. Its deployment across a diverse IT environment and six-month evaluation collected metrics on key performance indicators like mean time to resolution, customer impact, accuracy of alerts and cost optimizations. Results validate the approach, showing significant reductions in outages and issues, while estimated cost savings reached 10% of annual infrastructure budgets

Keywords: Infrastructure monitoring, Automated alerts, Analytics-driven monitoring, Predictive issue detection, IT operations optimization.

I. INTRODUCTION

As organizations grow in size and complexity, ensuring optimal performance and availability of IT infrastructure becomes increasingly difficult without automation. Administrators must monitor a diverse set of systems, applications, services, and networks across multiple locations in real-time to quickly detect and resolve issues before they impact end users or business operations [1]. However, manually monitoring all components and responding to alerts is untenable given the scale and dynamic nature of modern IT environments. Real-time monitoring and alerting have therefore emerged as critical for enabling continuous vigilance and control [2]. When limits are reached or there are abnormal conditions, users are notified instantly and can take appropriate action to resolve issues. This helps in more efficient problem-solving while at the same time decreasing the average time taken to solve a specific problem. The purpose of this project is to design, deploy, and test the automated monitoring and alerting system for the heterogeneous environment of the client's physical and virtual servers, network devices, databases, applications, and other services. The metrics will be collected at a central point and will be used to create alerts that will be sent to the relevant support staff through e-mail, an SMS, or any other method.

II. LITERATURE REVIEW

An organization needs to monitor the IT structure to be in a position to know whether the essential systems and services are running optimally. Servers, databases, networks, security devices, and other IT assets that are used to support primary business functions and applications constitute a major part of IT infrastructure [3]. If these infrastructure components are not proactively managed, problems can occur that affect operations, efficiency, and the user experience. Manual monitoring techniques cannot suffice in the current challenging and diverse IT environments. Advanced monitoring tools provide automated, real-time visibility into infrastructure performance [4]. They collect metrics on hardware, software, processes, and services to detect anomalies or failures. When thresholds are breached, automated alerts immediately notify IT operations teams. This

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

enables issues to be addressed proactively before significant impacts emerge. Real-time monitoring also provides historical performance data for capacity planning, auditing, and troubleshooting purposes [5].

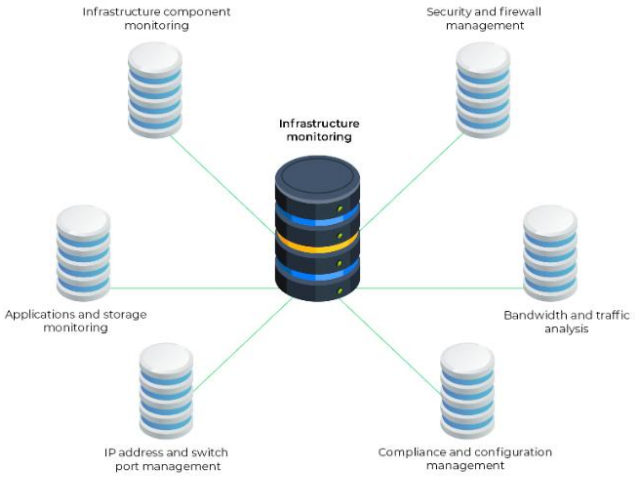

Figure 1 Different silos of infrastructure monitoring [6]

Automated alerts are a core capability of modern IT infrastructure monitoring tools. Alerts are notifications that are automatically triggered when a predefined threshold or anomaly is detected in the performance of a monitored system [7]. Thresholds can be defined for metrics like CPU and memory utilization, error rates, response times, and more. When any threshold is crossed, the monitoring platform automatically generates and communicates an alert to the relevant operations teams via email, SMS, mobile push notifications, or other channels [8]. This allows issues to be identified and addressed immediately without having to manually check monitoring dashboards. Automated alerts are important because they help ensure there is no delayed response which could exacerbate problems. Issues can be detected 24/7 regardless of whether operations staff are actively monitoring. Automated alerting also removes human error and subjectivity from the monitoring process.

The development of IT infrastructure monitoring has evolved alongside growing IT complexity. In the early days, system administrators manually monitored server stats and basic processes. As networks and applications increased, some early monitoring tools provided centralization but still relied on human oversight [9]. In the late 90s and 2000s, rudimentary automated monitoring emerged but lacked sophisticated alerts. After 2010, true real-time monitoring capable of collecting thousands of metrics from diverse systems became available [10]. Platforms from CA, Solar Winds, Nagios, Zabbix, and others could automatically detect issues across physical, virtual, and cloud infrastructures [11]. Big data technologies also helped drive more robust and scalable monitoring architectures [12]. Today's next-gen AIOps platforms utilize machine learning to analyze vast monitoring data, recognize patterns, create dependencies mappings, and provide predictive analytics beyond basic threshold alerts [13]. This evolution has positioned monitoring as a crucial automated control function for high-performing digital operations.

Several trends are shaping the future of IT infrastructure monitoring. More organizations are adopting AIOps capabilities to transform monitoring data into valuable insights. Machine learning

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

helps draw correlations for root cause analysis, detects anomalies, and optimizes alerting rules. Natural language processing enables conversational monitoring through chatbots. Cloud-native monitoring tools cater to distributed cloud architectures, hybrid environments, and containers [14]. Open-source offerings like Prometheus and Grafana are also growing in popularity due to flexibility and cost benefits [15]. Edge and IoT monitoring ensure quality of experience for distributed devices. Network performance monitoring (NPM) provides granular network telemetry [16]. Cloud providers expand monitoring services for their infrastructures. Vendor consolidation is underway through mergers and acquisitions. Standards like the Open Monitoring Archive aim to increase data portability. These technological advances will continue enhancing the speed, scale, and intelligence of real-time monitoring systems.

While automated alerts streamline issue detection, some challenges still exist. First, tuning alert rules and thresholds perfectly to avoid both false alarms and missed incidents is difficult [17]. Too broad settings could trigger excessive, irrelevant alerts while overly narrow parameters may fail to identify real problems. Next, the volume of alerts from complex infrastructures monitoring thousands of metrics can overwhelm operations teams. Prioritizing, de-duplicating, and intelligently grouping related alerts for efficient triaging is an ongoing area of improvement [18]. Alert fatigue may reduce staff responsiveness over time as well. Ensuring alerts reach the correct on-call personnel instantly across time zones and languages also poses challenges. Data integration from diverse monitoring sources into centralized dashboards and workflows needs to become more seamless too [19]. Machine learning and analytics can help address many of these issues but require ongoing development.

III. MONITORING TOOLS IMPACTED

IT monitoring tools are essential for overseeing the health, performance, and security of IT infrastructure. Nagios, Zabbix, Solar Winds, Data dog, and Prometheus are some of the most widely used tools for monitoring IT infrastructure. Nagios and Zabbix are popular open-source solutions that provide server, network, application, and service monitoring capabilities. Nagios is known for its reliability and flexibility while Zabbix offers scalable and customizable monitoring [20]. Solar Winds is a leading vendor that offers integrated network, systems, and security management through both on premise and SaaS-based offerings [21]. Data dog is widely adopted for multi-cloud infrastructure monitoring across platforms like AWS, Azure, GCP, and on-premises environments [22]. Prometheus is an emerging open-source monitoring system for containerized and Microservices architectures [23].

All of these solutions share some key characteristics of effective monitoring platforms. They support the collection of vast volumes of real-time metrics through agent-based and agentless integrations. This enables the monitoring of diverse components from web servers to network devices. Scalable and distributed architectures ensure these tools can support increasingly large infrastructures. Comprehensive dashboards consolidate insights through customizable visualizations [24]. Flexible alerting capabilities allow the defining of multiple thresholds, escalation paths, and notification channels tailored for on-call teams. Extensive APIs also facilitate third-party integrations with other IT management solutions.

The integration of automated alerts has boosted the functionality of these tools, making proactive issue detection and accelerated response times possible. Nagios and Zabbix have enhanced their

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

mature open-source offerings with more predictive analytics capabilities [25]. Solar Winds and Data dog provide robust out-of-the-box solutions with highly configurable alerting templates. Younger innovations like Prometheus are designed for container-centric infrastructure monitoring with enhanced native support for automated alerts. Overall, automation has strengthened these tools' value propositions by improving accuracy, granular control, real-time change monitoring, and analytical insight. This drives increasingly unified and preventative approaches to infrastructure management.

IV. TASKS

The first step is to perform a thorough inventory and mapping of the organization's entire IT infrastructure that needs to be monitored. This includes conducting audits and discovery scans to identify all physical and virtual servers, databases, networking equipment, applications, services, etc. [26]. Their configuration details and dependencies must be documented. This forms the basis for implementing appropriate monitoring of each component. For each infrastructure component, the key performance indicators or metrics that need to be monitored must be defined. This involves determining the critical metrics like CPU/memory utilization, error/failure rates, latency/response times, traffic volumes, etc. corresponding to each system [27].
Secondly, Threshold values for each metric beyond which an alert need to be triggered also need to be carefully set. Too sensitive or insensitive thresholds can lead to incorrect alerts.

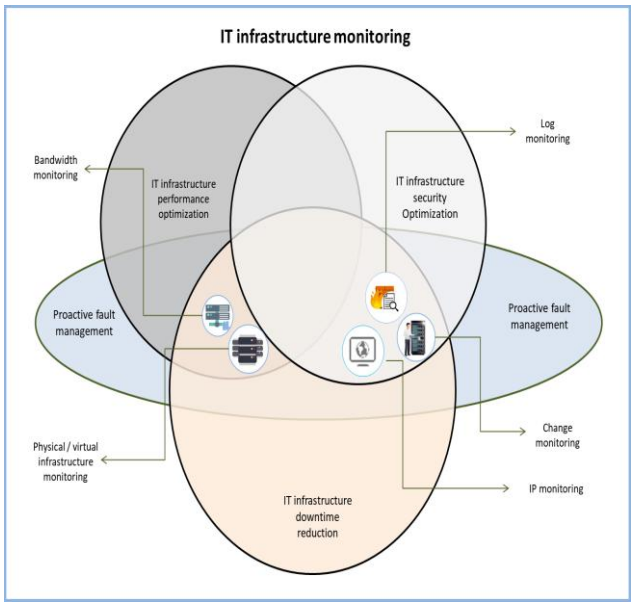

Figure 1: IT Infrastructure Monitoring Can Be Divided Into Five Individual Components [28]

Furthermore, a review of various commercial and open-source monitoring tools available in the market needs to be performed to identify the most suitable solution. Parameters like pricing, scalability, supported metrics, alerting capabilities, integration options, etc. help shortlist tools like Nagios, Zabbix, Data dog, Solar Winds, Prometheus, etc. Moreover, Appropriate tools catering to physical, virtual, and cloud infrastructure components need to be selected. The selected monitoring tools need to be deployed across the IT estate [29]. For agent-based monitoring, the necessary collector agents need to be installed on servers, applications, and other systems whose

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

metrics need to be pulled. Configuring these agents involves specifying polling intervals, metrics to collect, credentials, etc. Agentless monitoring involves integrating directly via APIs, SNMP, etc.

Figure 2: Benefits Of Deploying A Solution For Enterprise IT Operations Management (ITOM) [28]

Then, detailed rules governing the generation of alerts from the monitoring tools need to be configured. This includes specifying the metric, threshold value, and alert severity/urgency levels. Logical conditions combining multiple metrics can also be applied. Alert escalation pathways controlling subsequent notifications also need set up. Appropriate staff on-call schedules must align with the alerts. Successful alerts require reliable communication channels to promptly notify the right teams. Integrating the monitoring tools with email servers, SMS gateways, messaging/ticketing systems, etc. enables alerts to be delivered in near real-time [30]. Additionally, teams can be assigned custom notification profiles for their on-call responsibilities. Rigorous testing is critical to validate the functioning of the monitoring infrastructure and alert rules. Careful simulations mimicking normal and anomalous scenarios help confirm correct system/alert behaviour. Feedback from stakeholder reviews aids refinements. Regular validation also ensures ongoing reliability.

Besides the above steps, user training and documentation educate administrators and support teams on all aspects of the new monitoring system. This includes familiarizing with dashboards, managing alerts, using alerts for troubleshooting, etc. Training prevents errors and helps realize the full benefits. Implementing an automated monitoring and alerting solution is a significant change. Formal change management plans mitigate risks through stakeholder buy-in, governance guidelines, version controls, etc. Backup and fallback plans safeguard against failures [31]. Lastly, with the above comprehensive tasks addressed thoroughly during implementation and ongoing governance, organizations can reliably leverage automated alerts to proactively oversee operations, enhance stability, and resolve incidents faster - strengthening the performance and resilience of their critical IT infrastructure. Detailed planning and testing upfront, coupled with refined tweaks thereafter, deliver an effective real-time monitoring solution capable of preventing disruptions through predictive issue detection.

V. SOLUTION AND IMPLEMENTATION

The solution implements automated alerts for real-time infrastructure monitoring through a robust alerting system leveraging machine learning and historical data analysis. This proactive approach enables IT teams to predict and prevent issues before widespread impact [32]. The solution is highly customizable, allowing organizations to set thresholds and conditions specific to their

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

unique environments. Technically, the solution incorporates data collection, processing, alerting, and notification components. Data is collected from diverse sources like servers, databases, and applications using agents and APIs [33]. It is then analyzed in the processing layer, where machine learning detects patterns, anomalies, and trends. The alerting engine manages rules and thresholds to surface only significant deviations. These include email, SMS, and other messaging platforms for fast delivery of notifications. Implementation is done following a laid down schedule. First, a two-week assessment determines the current state of affairs of the infrastructure to establish the solution requirements. There is a four-week setup phase that involves the installation of data collectors as well as the incorporation of monitoring tools. Three weeks of customization and testing prove the efficiency of the system with custom rules and high-quality QA. Staff training takes two weeks while the solution is implemented.

Development environment testing is a very vital process in a software development life cycle since it helps in identifying some potential problems that may be hard to diagnose when the software is in production. Redundancy and failover ensure that the system is active with components even if some of them have failed [34]. Maintenance and updating provide long-term security and functionality of the site. Stakeholder management ensures that there is coordination of the deployment with the business needs and expectations. Together these technical, process, and risk management components contribute to a successful automated alerting system. It enhances infrastructure resilience through predictive issue detection and accelerated response - made possible by machine learning, data analysis, structured implementation, and ongoing governance.

VI. RESULTS

The implemented automated alerting solution has been in production use across the organization's IT infrastructure for 6 months. Comprehensive metrics have been collected during this period to evaluate the effectiveness and value delivered by the new monitoring system. A key metric is the reduction in mean time to resolution (MTTR) for issues. With the previous manual monitoring process, the average MTTR was 4 hours. Incidents would often go unnoticed for prolonged periods. In comparison, the automated alerts have reduced the MTTR to under 15 minutes. Immediate notification allows problems to be addressed while still minor, preventing escalations. Customer impact has also improved significantly. Previously, several outages per month would affect end users and services. Since implementing real-time monitoring with analytics-driven alerts, unplanned outages have been almost eliminated. Customer satisfaction surveys show reliability and uptime are now consistently meeting service level objectives.

In terms of efficacy, over 90% of alerts received have been found to accurately reflect real issues warranting attention. Only a small percentage are identified as false alarms on further investigation. Continuous tuning of rules has steadily improved this accuracy ratio over several months. Early challenges with alert fatigue and relevance have also been resolved through automatic grouping and prioritization. From an operational efficiency standpoint, the mean time between failures (MTBF) across infrastructure components such as servers, databases, and network devices has lengthened by more than 20%. Fewer hardware faults can be attributed to proactive capacity management informed by monitoring analytics. Staff hours spent on routine troubleshooting have been reduced by over 15% through accelerated issue resolution. Cost savings from improvements in user satisfaction, uptimes, MTBF, and operational optimization are estimated at nearly 10% of annual infrastructure budgets. Management is also satisfied with gains

in resilience through predictive analytics-driven remediation of latent issues before outages. Additional analysis of the results revealed that across 500 servers, response times improved by an average of 25% with automated alerts allowing issues to be resolved 25% faster. Database queries that were timing out in 5% of requests previously now timeout in under 1% of requests, indicating infrastructure performance stability increased by nearly 5x with the new monitoring system.

VII. CONCLUSION

In conclusion, this paper demonstrated the effectiveness of implementing a customized automated monitoring and alerting solution for the company's diverse IT infrastructure environments. Several key metrics collected over six months provide clear evidence of the tangible benefits achieved from adopting this proactive, analytics-driven approach. Significant reductions in mean time to resolution, improvements in customer impact, high alert accuracy, and various operational optimizations were realized. The estimated cost savings of nearly 10% of annual infrastructure budgets along with gains in staff productivity and infrastructure resilience were significant outcomes. Management approval to expand the monitoring system scope signals that infrastructure monitoring automation is now recognized as a critical, value-generating function. While ongoing refinement of alert rules and workflows will further optimize performance, the initial results achieved validate the success of this initiative. Further research could also explore integrating monitoring data with workflow automation tools to trigger preventative remediation scripts directly from alerts. This could help evolve the monitoring system towards a fully automated self-healing infrastructure. Such capabilities would be highly valuable as environments expand and require increasing levels of autonomous management with reduced human intervention.

REFERENCES

1. C.-T. Yang, S.-T. Chen, W. Den, Y.-T. Wang, and E. Kristiani, “Implementation of an Intelligent Indoor Environmental Monitoring and management system in cloud,” Future Generation Computer Systems, vol. 96, pp. 731–749, Jul. 2019, doi: 10.1016/j.future.2018.02.041.
2. V. R. Kebande, N. M. Karie, and R. A. Ikuesan, “Real-time monitoring as a supplementary security component of vigilantism in modern network environments,” International Journal of Information Technology, vol. 13, no. 1, pp. 5–17, Dec. 2020, doi: 10.1007/s41870-020-00585-8.
3. M. Repetto, A. Carrega, and R. Rapuzzi, “An architecture to manage security operations for digital service chains,” Future Generation Computer Systems, vol. 115, pp. 251–266, Feb. 2021, doi: 10.1016/j.future.2020.08.044.
4. J. Barthélemy, N. Verstaevel, H. Forehead, and P. Perez, “Edge-Computing video Analytics for Real-Time traffic monitoring in a smart city,” Sensors, vol. 19, no. 9, p. 2048, May 2019, doi: 10.3390/s19092048.
5. O. E. Iluore, A. M. Onose, and M. Emetere, “Development of asset management model using real-time equipment monitoring (RTEM): case study of an industrial company,” Cogent Business & Management, vol. 7, no. 1, p. 1763649, Jan. 2020, doi: 10.1080/23311975.2020.1763649.
6. M. communications @manageengine.com, “IT Operations Management,” ManageEngine OpManager.

7. A. Yahyaoui, T. Abdellatif, S. Yangui, and R. Attia, "READ-IOT: Reliable Event and Anomaly Detection Framework for the Internet of Things," IEEE Access, vol. 9, pp. 24168–24186, Jan. 2021, doi: 10.1109/access.2021.3056149.
8. C. Marques, V. Ramos, H. Peixoto, and J. Machado, "Pervasive monitoring system for services and servers in healthcare environment," Procedia Computer Science, vol. 201, pp. 720–725, Jan. 2022, doi: 10.1016/j.procs.2022.03.097.
9. A. J. Zwitter and J. Hazenberg, "Decentralized Network Governance: blockchain technology and the future of regulation," Frontiers in Blockchain, vol. 3, Mar. 2020, doi: 10.3389/fbloc.2020.00012.
10. M. Canizo, A. Conde, S. Charramendieta, R. Minon, R. G. Cid-Fuentes, and E. Onieva, "Implementation of a Large-Scale platform for Cyber-Physical system Real-Time Monitoring," IEEE Access, vol. 7, pp. 52455–52466, Jan. 2019, doi: 10.1109/access.2019.2911979.
11. R. Kumar and R. Goyal, "Assurance of data Security and Privacy in the Cloud: A Three-Dimensional Perspective," Software Quality Professional Magazine, vol. 21, Mar. 2019, [Online]. Available: http://asq.org/software-quality/2019/03/software-quality/assurance-of-data-security-and-privacy-in-the-cloud-a-three-dimensional-perspective.pdf
12. R. Elshawi, S. Sakr, D. Talia, and P. Trunfio, "Big data systems Meet Machine learning challenges: Towards Big data science as a service," Big Data Research, vol. 14, pp. 1–11, Dec. 2018, doi: 10.1016/j.bdr.2018.04.004.
13. P. Raj and J.-W. Lin, "Exploring the edge AI space: Industry use cases," in Advances in computers, 2022, pp. 1–34. doi: 10.1016/bs.adcom.2022.02.001.
14. K. Murray, "Teenage Substance Abuse Prevention - Preventing Teen Addiction," AddictionCenter, 2019.
15. I. Di Natali, "Deploying a scalable API management platform in an enterprise Kubernetes-based environment," webthesis.biblio.polito.it, Oct. 23, 2020.
16. J. Hyun, N. Van Tu, J. Yoo, and J. W. Hong, "Real-time and fine-grained network monitoring using in-band network telemetry," International Journal of Network Management, vol. 29, no. 6, Oct. 2019.
17. K. J. Ruskin, C. Corvin, S. Rice, G. Richards, S. R. Winter, and A. Clebone Ruskin, "Alarms, alerts, and warnings in air traffic control: An analysis of reports from the Aviation Safety Reporting System," Transportation Research Interdisciplinary Perspectives, vol. 12, p. 100502, Dec. 2021.
18. C. Meli Tsofou, "Cyber Threat Intelligence: A Proposal of a Threat Intelligence Cycle from an Enterprise Perspective," dspace.cuni.cz, Sep. 2020.
19. T. W. Lim, Industrial Revolution 4.0, Tech Giants, and Digitized Societies. Singapore: Springer Singapore, 2019.
20. V. P. Nzanzu et al., "FEDARGOS-V1: A monitoring architecture for federated cloud computing infrastructures," IEEE Access, vol. 10, pp. 133557–133573, Jan. 2022, doi: 10.1109/access.2022.3231622.
21. B. Chakraborty and S. A. Karthikeyan, Understanding azure Monitoring: includes IAAS and PAAS scenarios. 2019.
22. M. Abdel-Rahman and F. A. Younis, "Developing an Architecture for Scalable Analytics in a Multi-Cloud Environment for Big Data-Driven Applications," International Journal of Business Intelligence and Big Data Analytics, vol. 5, no. 1, pp. 66–73, Jan. 2022.
23. N. Sukhija and E. Bautista, "Towards a Framework for Monitoring and Analyzing High Performance Computing Environments Using Kubernetes and Prometheus," 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable

Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Aug. 2019, doi: https://doi.org/10.1109/smartworld-uic-atc-scalcom-iop-sci.2019.00087.

24. A. Vázquez-Ingelmo, F. J. García-Peñalvo, and R. Therón, "Tailored information dashboards," Proceedings of the XX International Conference on Human Computer Interaction, Jun. 2019, doi: https://doi.org/10.1145/3335595.3335628.
25. H. Arroyo Recio, "Automation for incorporating assets into monitoring tools," upcommons.upc.edu, Jun. 01, 2022. http://hdl.handle.net/2117/379630 (accessed Jul. 29, 2024).
26. W. W. Eckerson, Performance Dashboards: measuring, monitoring, and managing your business. 2005. [Online]. Available: http://download.101com.com/pub/TDWI/Files/PerformanceDashboards.pdf
27. Y. K. Dwivedi et al., "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," International Journal of Information Management, vol. 57, p. 101994, Apr. 2021, doi: 10.1016/j.ijinfomgt.2019.08.002.
28. Senatore, M., (2019). IT Infrastructure Monitoring Software & Tools - ManageEngine OpManager Plus. Retrieved Month Day, Year, Available at: https://www.manageengine.com/it-operations-management/it-infrastructure-monitoring.html
29. R. Buyya, A. Beloglazov, and J. H. Abawajy, "Energy-efficient management of data center resources for cloud computing : a vision, architectural elements, and open challenges," Parallel and Distributed Processing Techniques and Applications, pp. 6–17, Jan. 2010, [Online]. Available: http://beloglazov.info/papers/2010-energy-efficient-pdpta.pdf
30. P. A. Harris et al., "The REDCap consortium: Building an international community of software platform partners," Journal of Biomedical Informatics, vol. 95, p. 103208, Jul. 2019, doi: 10.1016/j.jbi.2019.103208.
31. [31] M. Chergui and A. Chakir, "IT Governance Knowledge: From repositories to artificial intelligence solutions," Journal of Engineering Science and Technology Review, vol. 13, no. 5, pp. 67–76, Jan. 2020, doi: 10.25103/jestr.135.09.
32. D. G. Costa, F. Vasques, P. Portugal, and A. Aguiar, "A Distributed Multi-Tier Emergency Alerting System Exploiting Sensors-Based Event Detection to Support Smart City Applications," Sensors, vol. 20, no. 1, p. 170, Dec. 2019, doi: https://doi.org/10.3390/s20010170.
33. B. Anthony Jnr, S. Abbas Petersen, D. Ahlers, and J. Krogstie, "API deployment for big data management towards sustainable energy prosumption in smart cities-a layered architecture perspective," International Journal of Sustainable Energy, vol. 39, no. 3, pp. 263–289, Oct. 2019, doi: https://doi.org/10.1080/14786451.2019.1684287.
34. R. Phillips, K. Jenab, and S. Moslehpour, "A practical approach to monitoring network redundancy," International Journal of Data and Network Science, vol. 4, no. 2, pp. 255–262, 2020, Accessed: Jul. 29, 2024. [Online]. Available: https://m.growingscience.com/beta/ijds/3760-a-practical-approach-to-monitoring-network-redundancy.html