International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Analyzing Real-Time Application Logs for Informed Decision Making

Ramasankar Molleti

Submitted: 16/01/2021 **Revised**: 15/02/2021 **Accepted**: 21/02/2021

Abstract: This technical report explains how the key control of real-time application log analysis has been dismantled in present day software development and activities. It looks at the definition, types, and importance of the real-time log and the tools and techniques for driving the analysis. Looking at the benefits and challenges of real-time log analysis, the report also provides recommendations for implementation and use cases as well as the best practices of using log data for decision-making processes. As real-life examples demonstrate, real-time log analysis can also foster application execution, update security, and redesign clients' experience according to this report.

Keywords: *Log Data, Real Time monitoring, Decision Making*

1. Introduction

1.1 Overview

In the present rapidly evolving digital environment, applications generate massive amounts of log data consistently. These logs hold massive information about application runs, client direct, security incidents, and system health. Real-time application log analysis has emerged as a core process that any affiliation attempting to leverage this wealth of information for better decision-making cannot do without.

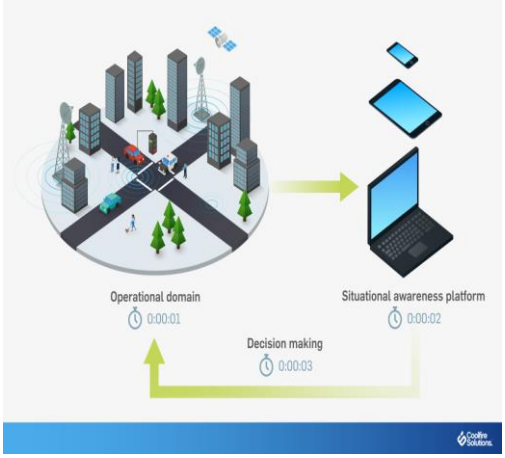

Fig 1: Real-time decision making

(Source: https://i0.wp.com/coolfiresolutions.com)

Real-time log analysis combines the steady procurement, management, and awareness of log information as it is created. This approach provides relationship to get quick experiences into their applications' way to deal with acting, watch issues as they happen, and chase data-driven choices in close to real-time. By taking separated logs in real-time, affiliations can preemptively sort out issues, moreover advance execution, and redesign client experience without holding some sort of control for occasional reports or post-scenario appraisals.

1.2 Background

Historically, it can be noted that log analysis was always a reactive action, which was carried out as often as possible after incidents had occurred that affected users or business processes recently. It is only natural that system administrators would truly filter through log archives to isolate the concern or look at security incidents. This was a time-consuming approach which was error prone and very often it produced conceded responses to critical issues.

Meanwhile, as applications turned out to be more complex and distributed, the volume and arrangement of log data increased significantly [1]. Old methods of log analysis were insufficient to handle the scope and velocity of the modern applications. This resulted in the creation of clear log leaders and analysis tools that were capable of handling large volumes of log data in real-time.

The method of cloud computing, microservices designs, and containerization enhanced the need for real-time log analysis even more. These technologies introduced new challenges with respects to log aggregation, gathering, and association across the distributed systems. While they limited the higher level monitoring and analysis, they provided chances to the more detailed ones.

Today, real-time log analysis has become one of the basic components of DevOps, Site Reliability Engineering (SRE), and Information Technology Operations Analytics (ITOA).

Independent Researcher, Illinois, USA
Email: Ramasankar.molleti@gmail.com

It anticipates a crucial role in guaranteeing the application reliability, execution, and security in a rather complex and ever-evolving technological environment.

2. Understanding Real-Time Application Logs

2.1 Definition and types

Real-time application logs are then defined as documents containing records of events, activities, and states that are generated by an application as they occur. These logs provide a detailed, timed account of an application's approach to acting and performance. It is not at all like conventional logging, which may include cluster processing or delayed analysis, real-time logs are collected, processed, and examined in real-time, with regard to rapid interactions and activities.

Fig 2: Decision Making Process

(Source: servintegrales.com.co)

Types of real-time application logs include:

Error logs: Document exceptional circumstances, disappointments, and innovative ways of performing in the application.

Transaction logs: Capture details of business transactions and the client collaborative efforts.

Performance logs: Keep track of the resource usage and response times other required performance estimations.

Security logs: Record the number of check attempts, the access control decisions made, and any possible security threats.

Audit logs: Alter data for system game plans and changes for the purpose of making them more consistence.

Application logs: It used to feed bits of information into within operations of the application such as capability calls and state changes.

Such logs can be planned (according to the certain schedule) and unplanned (the free-text message), and each type has its unique challenges and possibilities for research.

2.2 Importance of real-time log analysis in modern applications

Real-time log analysis has become crucial in modern application management for several reasons:

Rapid problem detection and resolution: Real-time log analysis allows affiliations to identify problems and determine them, therefore reducing the time and effect on users.

Performance optimization: Performance logs are continually monitored and think about brief area of bottlenecks or resource goals to allow early smoothing out.

Security threat identification: The analysis of logs in real-time is useful in perceiving and noting the security breaks or abnormal activities in the shortest time possible.

User behavior insights: Transaction and application logs provide brief interaction with client direct, including real-time personalization and enhancing client experience.

Compliance and auditing: Real time log analysis guarantees that consistency encroachment or doubtful exercises are raised right away, meeting the guidelines and organization procedures [2].

Capacity planning: It will be possible to come to informed end results about scaling and resource designation by separating resource utilization logs in real-time.

Continuous improvement: Real-time encounters relate to perpetuate and also develop their applications incessantly based on certified usage models and performance data.

In the context of the modern period, conveyed applications, real-time log analysis becomes strikingly more important. It assists in connecting events in different organizations, owners, or microservices to provide a broad view of the application environment. This total perspective is principal for being informed of the reliability and performance of complex, integrated systems.

3. Tools and Techniques

Real-time log analysis has recently become a rapidly developing field, and there is now a vast array of tools and

techniques available to assist with eliminating large chunks of information from an application's logs. This part investigates the most widely used tools, effective approaches, and innovative technologies in the sphere of real-time log analysis.

3.1 Overview of popular log analysis tools and platforms

One of the most thoroughly implemented open-source solutions used for log analysis is the ELK stack, which includes Elastic search, Log stash, and Kibana. Elasticsearch provides areas of strength for an examination engine, Logstash is answerable for log ingestion and managing, and Kibana brings perception limits. Thus, things being what they are, this stack's flexibility and flexibility go with it making it a popular choice for affiliations.

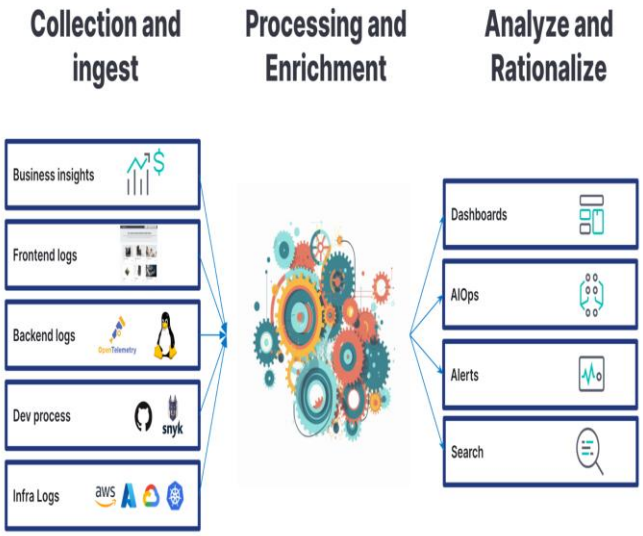

Figure 3: Tools and Techniques

(Source: www.elastic.co)

For ventures looking for business outcomes, Splunk has for quite a long time been a market pioneer. The establishment of Splunk also provides rich real time log analysis limits, large number level pursuit functionalities and a vast amount of consolidations [5]. It is prevalent with respect to handling enormous measures of different information sorts, which makes it reasonable for intricate undertaking circumstances.

Recently, the solutions of the cloud-logging are gaining forward speed. AWS CloudWatch and Google Cloud Logging provide a reliable mix their respective cloud platforms, providing integrated log aggregation, storage, and analysis features. These services are especially desirable for affiliations that for the most part contribute into cloud structure.

Other prominent competitors in the log analysis market are Datadog, Sumo Logic, and Loggly. These stages give clear interfaces, including pre-configured compromises with basic applications and administrations, as well as high-quality assessment instruments. They typically provide a correlation between the convenience and the advanced analysis limits, which makes them suitable for a wide range of direction applications.

3.2 Techniques for real-time log monitoring and analysis

Effective real-time log analysis relies on several key techniques. Log aggregate and centralization form the basis of any good log analysis technique. When social event logs from different assets are stored in an incorporated storage facility, affiliations get a broad perspective on the application environment. This centralization involves cross-part analysis and association, which is colossal for perceiving intricate issues that span different systems.

Real-time logs analysis uses pattern recognition, as well as anomaly detection, as two of the most basic methods. When the benchmark patterns of regular approach to acting are dispersed, affiliations can rapidly identify disparities that may demonstrate issues or security risks. This can use sharp edge based alerts or more refined actual analysis to identify subtle anomalies.

Visualization and dashboarding therefore expect an essential role in making log data open and valuable. Real-time dashboards are initial approaches to viewpoints on key metrics and system health indicators [3]. By integrating the visual components, the specialists are allowed to analyze data more efficiently and come up with patterns and relations that are presumably not distinguishable from raw log entries.

Issue objective alerting and notification systems are critical for the proactive issue objective. The affiliations can guarantee that the right group of people is informed of critical issues in real-time by creating smart alerting rules. This much of the time involves the use of the layered alerting, whereby the differing degrees of reality elicit the differing degree of response shows.

Another vast methodology is log enrichment, which includes the addition of setting focused data to the log segments. It can sum up the experiences regarding the application environment, clients' data or other business data. Additional developed logs provide more pieces of information and require more complex analysis.

3.3 Automation and machine learning in log analysis

The amount and frequency of logs created in today's applications have led to the need to adopt the automation and machine learning approaches in log analysis. Log analysis with the help of Artificial Intelligence can in essence operate on the rate and reliability of issue identification and goal.

Log data can be analyzed using machine learning algorithm beyond simple rules that can be used for detection of pattern and irregularities in logs. Such algorithms can adhere to the shift in application methods to acting for a very long time, reducing false positives, and detecting problems that are quite subtle and could easily be averted by human analysts.

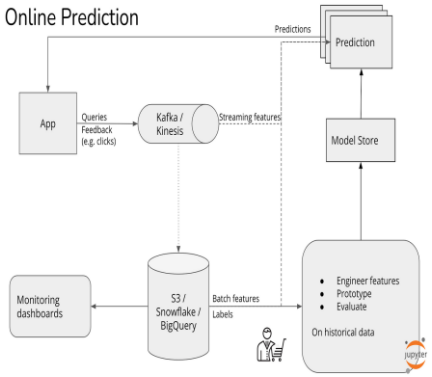

Figure 4: Real-time machine learning

(Source: bootcampai.medium.com)

Log analysis is another comforting use of machine learning where predictive analytics is another application of the same. Thus, by dividing log data from the rest of the recent things, predictive models can predict likely problems before they escalate [4]. This allows relationship to undertake a preliminary action to prevent power blackouts and performance compromization.

The analysis of root sources is another district where there is tremendous progress in the application of machine learning. Expressing log information crosswise over various segments and dismantling the strategy of occasions going toward an issue, AI frameworks can rapidly distinguish the concealed reason for issues. This unambiguously reduces the time and energy anticipated for studying multifaceted problems.

In the same way, NLP is also being used in log analysis especially for the unstructured log data. The problem of extracting crucial information from the free-text log segments can be solved with NLP, it becomes much easier to search and analyze the logs that do not follow any standard format.

the field of real-time log analysis can be considered full of amazing resources and creative approaches. Starting with the established platforms such as the ELK stack and Splunk to the new-age AI-based plans and strategies, affiliations have various options for managing the force of their log data. Thus, with the help of the presented tools, it is possible to unite feasible techniques and with the help of the capabilities of machine learning, transform the log data into an immense resource for route and proactive IT the leaders of businesses.

4. Benefits, Challenges and Considerations

4.1 Advantage

Real-time log analysis has become the tool for associations that want to sustain the optimal performance of the systems, improve security, and make decisions based on data. One of the principal advantages is the possibility of the identification of the system's specific features and security threats at the initial stage. In this way, affiliations can identify fantastic patterns or ways to behave that might indicate a future system failure or security break. This proactive methodology takes into account the fast intervention, the restriction of the time that the system is out of order and the reduction of the effects of the security episodes.

The other important advantage is the enhancement of the system efficiency and utilization of the available resources. Live log analysis provides encounters with information about the system's congestion, resource critical time, and deficiency[7]. Thus, IT aggregations can modify system plans, distribute resources more realistically, and implement performance transformations. Such prompts additionally grew by and large performance, decreased practical costs, and updated client experience.

Figure 5: Real-time decision-making strategies

(Source: Self-created in MS-Word)

Also, real-time log analysis actively involves data-driven self-direction of course with master experiences. This way, affiliations can rapidly come to vital decisions depending on current system estimations and client direct data. This agility is especially important for fast pace environments where the financial position or clients' requirements can shift quickly. Live interactions can inform as far as product creation and the progression of systems, enabling organizations to sustain competition and respond to propulsive pressures.

4.2 Disadvantage

Despite its benefits, real-time log analysis comes with its own set of challenges which are outlined in the following plan. Among the primary ones, there is the regulating of the amount and the clustering of logs. Today's systems generate huge volumes of log data from a wide range of sources, thus it becomes challenging to collect, analyze and decompose this information as such. To this effect, affiliations should implement charitable log the chiefs systems that can handle large volumes of data and sponsorship various log formats. Thus, managing the data storm can also be helped by applying the data pressure techniques and implementing the useful data amassing plans.

Real-time monitoring is another test, which also entails data accuracy and its integrity. It means that log data can be divided, debased or clashing, and such information leads to mixed up analysis and flawed free heading. To address this, affiliations ought to apply severe data affirmation and purging processes [8]. Traditional log source and data pipeline reviews can assist in perceiving and reviewing data quality problems. Also, performing plain repetitiveness in log combination and applying data compromise techniques can enhance data integrity even more.

Issues of scale and resource availability are therefore enormous problems in log analysis, especially for affiliations that are growing fast or that manage constantly changing status. The volume of log data is likely to increase over time and hence the computational resources expected for analysis can be humongous. To this end, affiliations ought to consider assuming cloud-based log analysis game plans that are elastic in nature. High-quality log parsing and requesting implementation can moreover additionally enhance the speed of processing. Additionally, applying machine learning algorithms for the irregularity area and model identification can also assist to automate and optimize the analysis process, thus, minimizing the burden on human analysts?

Benefits	Disadvantages
Early detection of anomalies and threats	High computational resource requirements
Increased efficiency of the system	Complex in dealing with large volumes of logs that are of different types
Real-time insights for fast decision-making	Potential for data overload and analysis
Enhanced security posture	Challenges in ensuring data accuracy and integrity
Proactive issue resolution	Initial setup and training costs
Improved user experience	Potential privacy and compliance concerns
Efficient resource allocation	Ongoing maintenance and updates required
Competitive advantage through data-driven strategies	Risk of false positives in automat

Comparative Table 1: Benefits vs. Disadvantages of Real-Time Log Analysis

4.3 Recommendations

To maximize the benefits of real-time log analysis:

The third strategy is to establish a clear plan of managing logs that will be coherent with business goals.

Apply the correct methods of sorting out the logs and harmonizing them in the applications.

Develop underlying infrastructure for log analysis that will allow it to grow as the data volumes grow.

However, do not let real-time analysis overpower you by providing fake data, while outside context and trends give you the real picture.

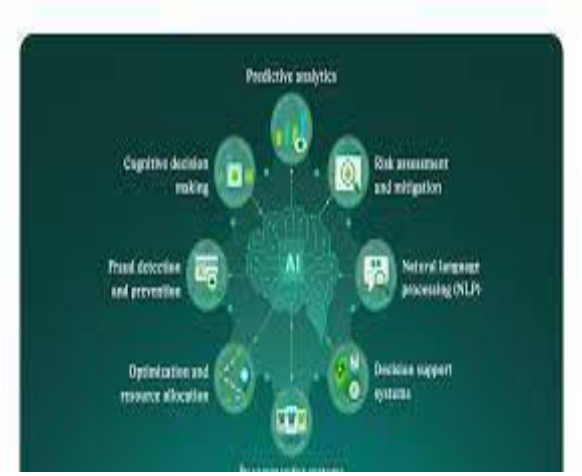

Fig 6: AI in Decision-Making

(Source: https://www.upwork.com)

Continuously improve the thresholds and rules used in alerting to minimize false alarms [10].

Ensure proper handling and protection of log data by putting in place proper data governance and security measures.

Arrange training sessions for the concerned teams regarding the tools and methods of log analysis.

It is also good practice to review the collection of logs and refine them for relevance and effectiveness on a frequent basis.

5. Best Practices

5.1 Real-world examples showcasing the impact of real-time log analysis

E-commerce platform optimization:

The largest e-commerce connection to date used real-time log analysis to monitor user activities and application throughout the peak of shopping seasons. Analyzing transaction logs in real time, they found the source of a database problem that slowed down the checkout process. This led to an enhanced rate of successful transactions by 15% and a dramatic satisfaction of consumers.

Financial fraud detection:

A large bank used real-time log analysis to increase the effectiveness of misrepresentation detection. By synchronizing user authentication records, transaction records, and users' behaviors in real-time, they were able to effectively prevent fraud transactions with the rate of 99%. Nine percent precision and millions in potential losses were saved [14].

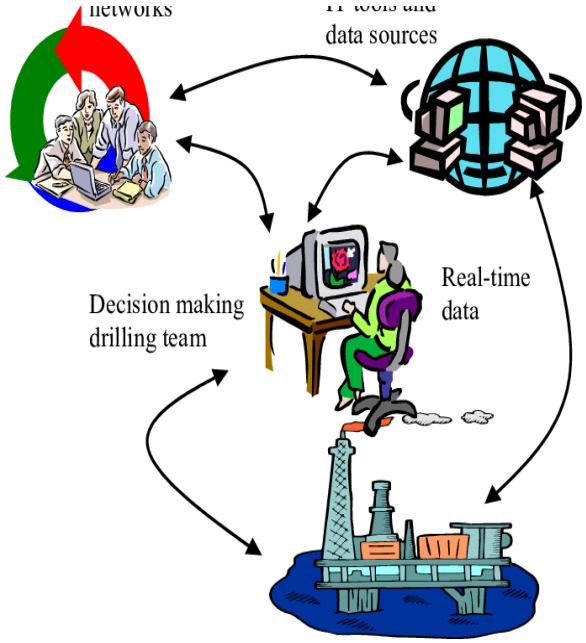

Fig 7: Decision Support and Real-time Management

(Source: https://www.researchgate.net)

Cloud service reliability improvement:

The cloud service provider in this case had a means of performing real-time log analysis to check the health and performance of distributed infrastructure. By applying automated irregularity detection on system logs, they cut down their mean time to resolution (MTTR) for basic problems by 60 per cent; thus, they only improved service reliability and customer satisfaction.

Application performance optimization:

A SaaS firm adopted real-time log analysis for tracking the Programming interface in the microservices setup. They were able to map performance logs to user movement and determine that some of the Programming interface endpoints were slow and were able to rectify this by increasing application response time by 30 percent.

These cases show how real-time log analysis can help in decision making in a variety of contexts and achieve tangible positive results for a business, its security, and the users.

6. Conclusion

Real-time application log monitoring has turned into a necessity for affiliations that aim at having high performing, secure, and reliable applications in the current fast-paced digital world. Due to the fact that log analysis provides real-time pieces of knowledge about application behavior, user interactions, and system health, it becomes possible to address issues before they appear, enhance the performance, and make data-driven decisions.

Log analysis is relevant as applications become more complex and large and as applications continue to extend into these areas, the need for good log analysis will only grow. Those partners that embrace and implement robust log analysis solutions and adopt best practices will be more prepared for the realities of today's application development and deployment, and provide better experiences to their users and shareholders.

The future of real-time log analysis is in the enhancement of machine learning and artificial intelligence to provide more sophisticated methods of anomaly detection, predictive analysis, and even automatic solving of the problem. With these technologies, the process of finding useful bits of knowledge from the database of log data will only improve and propel the development and progress of applications and their management forward.

7. Reference List

Journals

[1] Franklin, A., Gantela, S., Shifarraw, S., Johnson, T.R., Robinson, D.J., King, B.R., Mehta, A.M., Maddow, C.L., Hoot, N.R., Nguyen, V. and Rubio, A., 2017. Dashboard visualizations: Supporting real-time throughput decision-making. Journal of biomedical informatics, 71, pp.211-221.

[2] Tien, J.M., 2017. Internet of things, real-time decision making, and artificial intelligence. Annals of Data Science, 4, pp.149-178.

[3] Vera-Baquero, A., Colomo-Palacios, R. and Molloy, O., 2016. Real-time business activity monitoring and analysis of process performance on big-data domains. Telematics and Informatics, 33(3), pp.793-807.

[4] Sieverink, F., Kelders, S., Poel, M. and van Gemert-Pijnen, L., 2017. Opening the black box of electronic health: collecting, analyzing, and interpreting log data. JMIR research protocols, 6(8), p.e6452.

[5] Ismail, A., Truong, H.L. and Kastner, W., 2019. Manufacturing process data analysis pipelines: a requirements analysis and survey. Journal of Big Data, 6(1), pp.1-26.

[6] Wong, B.P. and Kerkez, B., 2016. Real-time environmental sensor data: An application to water quality using web services. Environmental Modelling & Software, 84, pp.505-517.

[7] He, S., Zhu, J., He, P. and Lyu, M.R., 2016, October. Experience report: System log analysis for anomaly detection. In 2016 IEEE 27th international symposium on software reliability engineering (ISSRE) (pp. 207-218). IEEE.

[8] Wise, A.F. and Jung, Y., 2019. Teaching with analytics: Towards a situated model of instructional decision-making. Journal of Learning Analytics, 6(2), pp.53-69.

[9] Narkhede, N., Shapira, G. and Palino, T., 2017. Kafka: the definitive guide: real-time data and stream processing at scale. " O'Reilly Media, Inc.".

[10] Du, J., Zou, Z., Shi, Y. and Zhao, D., 2018. Zero latency: Real-time synchronization of BIM data in virtual reality for collaborative decision-making. Automation in construction, 85, pp.51-64.

[11] Saggi, M.K. and Jain, S., 2018. A survey towards an integration of big data analytics to big insights for value-creation. Information Processing & Management, 54(5), pp.758-790.

[12] Oliveira, M.P.V.D. and Handfield, R., 2019. Analytical foundations for development of real-time supply chain capabilities. International Journal of Production Research, 57(5), pp.1571-1589.

[13] Jeble, S., Kumari, S. and Patil, Y., 2017. Role of big data in decision making. Operations and Supply Chain Management: An International Journal, 11(1), pp.36-44.

[14] Ghasemi, M. and Amyot, D., 2020. From event logs to goals: a systematic literature review of goal-oriented process mining. Requirements Engineering, 25(1), pp.67-93.

[15] [Hassan, W.U., Noureddine, M.A., Datta, P. and Bates, A., 2020, January. OmegaLog: High-fidelity attack investigation via transparent multi-layer log analysis. In Network and distributed system security symposium.

[16] Zur Mühlen, M. and Shapiro, R., 2015. Business process analytics. Handbook on business process management 2: strategic alignment, governance, people and culture, pp.243-263.

[17] Polyvyanyy, A., Ouyang, C., Barros, A. and van der Aalst, W.M., 2017. Process querying: Enabling business intelligence through query-based process analytics. Decision Support Systems, 100, pp.41-56.

[18] Zhu, J., He, S., Liu, J., He, P., Xie, Q., Zheng, Z. and Lyu, M.R., 2019, May. Tools and benchmarks for automated log parsing. In 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP) (pp. 121-130). IEEE.