

Patent Draft

Title: IT SYATEM LOG ANALYZER

List of Inventors:

Name in Full	Nationality	Country of Residence	Address of the Applicant
MRIDUL SHARMA	INDIAN	INDIA	KIET GROUP OF INSTITUTIONS, DELHI NCR, GHAZIABAD
MAYANK KUMAR	INDIAN	INDIA	KIET GROUP OF INSTITUTIONS, DELHI NCR, GHAZIABAD
VIKAS YADAV	INDIAN	INDIA	KIET GROUP OF INSTITUTIONS, DELHI NCR, GHAZIABAD

IT SYSTEM LOG ANALYZER

- Log analysis is the process of analyzing computer-generated log events to get insight into the health and performance of IT environments and applications.
- Log analytics takes log monitoring one step further, allowing observability teams to discover patterns across an organization.
- This can help them resolve application and system issues quickly and provide operational insights to get ahead of future problems.
- Since the inception of computer-generated records, organizations have been trying to review logs, at scale.
- But logs are generated across your entire IT ecosystem. Many do not contain all the information required, and are usually not in a consistent format.

- In modern tools, the process of log analysis centralizes this information and translates it for easier consumption.

FIELD INNOVATION

- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. Business runs on information.
- The faster information is received and the more accurate it is, the better.
- Blockchain is ideal for delivering that information because it provides immediate, shared, and observable information that is stored on an immutable ledger that only permissioned network members can access.
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransomware normal business processes.
- Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

BACKGROUND







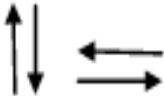
- Logs are crucial records of events or actions performed by software applications are tools or software systems used to monitor, collect, parse, and analyze logs generated by various components of an IT infrastructure., servers, devices, and other system components.
- These logs can contain a wealth of information, such as error messages, status updates, user actions, security events, and system performance metrics.
- The primary goal of log analyzers is to help organizations gain insights from these logs, ensuring the smooth functioning, security, and optimization of their IT systems.

OBJECTIVES

- The objective of an IT system log analyzer is to systematically examine and interpret log data from various IT systems and applications to achieve several key goals.
- **Troubleshooting and Diagnostics** Identify and diagnose issues, errors, or anomalies in IT systems and applications. Analyzing logs helps in pinpointing the root cause of problems and resolving them efficiently.
- **Performance Monitoring** Assess the performance of systems and applications by analyzing log data.

- This includes identifying performance bottlenecks, slow response times, and resource utilization issues. **Security and Compliance** Monitor and detect potential security threats or breaches.
- Log analysis helps in identifying unauthorized access, suspicious activities, and compliance with regulatory requirements. **Operational Insights:** Gain insights into the operational behavior of IT systems. This includes understanding usage patterns, system load, and overall health, which can inform capacity planning and optimization efforts.

FIGURES

Symbol	Name	Function
	Process	Indicates any type of internal operation inside the Processor or Memory
	input/output	Used for any Input / Output (I/O) operation. Indicates that the computer is to obtain data or output results
	Decision	Used to ask a question that can be answered in a binary format (Yes/No, True/False)
	Connector	Allows the flowchart to be drawn without intersecting lines or without a reverse flow.
	Predefined Process	Used to invoke a subroutine or an Interrupt program.
	Terminal	Indicates the starting or ending of the program, process, or interrupt program
	Flow Lines	Shows direction of flow.

CLAIMS

- The claims of IT system log analyzers are core benefits and functionalities these tools offer, positioning them as essential components in modern IT infrastructure management, security, and compliance.
- These claims highlight the value log analyzers provide across various domains, such as real-time monitoring, operational efficiency, security, and data-driven decision-making.

TECHNOLOGY USED

- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. Business runs on information.
- The faster information is received and the more accurate it is, the better.
- Blockchain is ideal for delivering that information because it provides immediate, shared, and observable information that is stored on an immutable ledger that only permissioned network members can access.
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

ABSTRACT

- In the digital age, the effective management and analysis of IT system logs are crucial for maintaining operational efficiency, ensuring security, and meeting compliance requirements.
- The IT System Log Analyzer project addresses these needs by developing a comprehensive tool designed to aggregate, analyze, and visualize log data from diverse IT systems.
- This project aims to provide organizations with an advanced solution to streamline their log management processes, enhance threat detection, and improve system performance.
- The IT System Log Analyzer integrates with various log sources, including servers, network devices, and applications, to centralize log data into a unified platform.
- By employing sophisticated parsing and normalization techniques, the system standardizes log entries, making them easier to search and analyze. Real-time data collection and advanced querying capabilities enable users to perform in-depth analysis and quickly identify patterns, anomalies, and potential security threats.
- Key features of the IT System Log Analyzer include automated alerting and notification systems, customizable dashboards, and detailed reporting tools.

END USERS

- The **end users** for an **IT system log analyzer** span a variety of roles within an organization, ranging from technical professionals responsible for infrastructure management to executives focused on compliance and business performance.
- Each end user utilizes log analyzers for different purposes based on their role in maintaining, securing, and optimizing IT systems.
- System Administrators
- Network Administrators
- Security AnalystsDevOps Engineers
- IT Operations Teams
- Incident Response Teams
- IT Support Team
- Database Administrators (DBAs)

ADVANTAGES

- An IT system log analyzer offers numerous advantages that enhance the management, security, and optimization of IT infrastructures.
- These tools help organizations gain actionable insights from log data, enabling efficient troubleshooting, monitoring, and decision-making.

CONCLUSION WITH RESULT

The IT System Log Analyzer serves as a critical tool for maintaining and improving the security, performance, and reliability of IT systems. By effectively processing and analyzing logs, the analyzer provides several key benefits and results. Improved detection and response to security threats. The analyzer aggregates and correlates log data from various sources to identify patterns and anomalies indicative of potential security breaches. By analyzing logs from firewalls, servers, and applications, the system can detect suspicious activities, unauthorized access attempts, and malware infections to security incidents. . This proactive detection helps in mitigating risks and responding quickly Streamlined IT operations and reduced downtime. By analyzing performance logs and system events, the log analyzer helps in identifying and diagnosing system issues, performance bottlenecks, and configuration errors. This allows IT teams to address problems before they escalate into major outages, thereby improving overall system uptime and operational efficiency. Adherence to industry regulations and standards. Many industries have specific regulations regarding data logging and audit trails. The log analyzer assists in ensuring compliance by maintaining detailed logs of all critical system activities. Automated reports and alerts generated by the analyzer help organizations meet regulatory requirements and provide necessary documentation during audits. Informed decision-making and strategic planning. The analyzer provides valuable insights by visualizing log data and generating actionable reports. IT administrators and managers can leverage these insights to make informed decisions regarding system improvements, capacity planning, and resource allocation. Historical log data also helps in understanding trends and predicting future needs.