SPELL & DEEPLOG

SOFTWARE
A cloud-based streaming method and neural network that provides real-time system log parsing with deep learning anomaly detection for information processing.

TECHNOLOGY SUMMARY
System event logs record system states at critical points to help debug failures and promote system stability. Analyzing system logs to detect irregularities establishes more secure and trustworthy systems. Typical log parsing software provides offline, batch processing of raw files, but many applications require constant monitoring not provided by offline methods. Additionally, current software requires end users to manually define parsing rules, which requires domain expertise and fails to identify less common patterns.

Spell, an online streaming method, parses system event logs to dynamically extract log patterns and maintain a set of discovered message types. DeepLog utilizes Long Short-Term Memory (LSTM) to model a system log as a natural language sequence that automatically learns log patterns. DeepLog detects anomalies when log patterns deviate from the model trained from log data under normal execution. When an anomaly is detected, users can diagnose and perform root cause analysis immediately, thereby increasing system security.

FEATURES AND BENEFITS
- Improves system security, efficiency, and effectiveness.
- Enables cloud-based, streamlined log parsing.
- Offers real-time analysis.
- Improves information processing.

RECENT PUBLICATIONS

INVENTOR PROFILE
Feifei Li, Ph.D., Associate Professor - School of Computing