



THE BUSINESS PARTNER
FOR YOUR IDEAS



SPELL & DEEPLUG

COMPUTING

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

TECHNOLOGY TYPE

Cyber Security
Machine Learning

STAGE OF DEVELOPMENT

- Tests demonstrate efficacy of developed software.

- Further refinement of user interface required.

IP PROTECTION

PCTs Pending

FUNDING TO DATE

Received nearly \$3M in NSF grants through 2021.

LEARN MORE

Reference Numbers: U-6423, U-6424

Dean Gallagher

Technology Manager
dean.gallagher@tvc.utah.edu
801-585-0396

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

Du, M., Li, F. (2016). Spell: streaming parsing of system event logs. *2016 IEEE 16th International Conference on Data Mining (ICDM)*, Barcelona. 859-864. doi: [10.1109/ICDM.2016.0103](https://doi.org/10.1109/ICDM.2016.0103)

Du, M., Li, F., Zheng, G., Srikumar, V. DeepLog: anomaly detection and diagnosis from system logs through deep learning. *2017 ACM Conference on Computer and Communications Security (CCS)*. Dallas. 1285-1298. doi: [10.1145/3133956.3134015](https://doi.org/10.1145/3133956.3134015)

INVENTOR PROFILE

Feifei Li, Ph.D., [Professor - School of Computing](#)

DATE UPDATED: 7/25/2019