Logs are widely used by large and complex software-intensive systems for troubleshooting. There have been a lot of studies on log-based anomaly detection. To detect the anomalies, the existing methods mainly construct a detection model using log event data extracted from historical logs. However, we find that the existing methods do not work well in practice. These methods have the close-world assumption, which assumes that the log data is stable over time and the set of distinct log events is known. However, our empirical study shows that in practice, log data often contains previously unseen log events or log sequences. The instability of log data comes from two sources: 1) the evolution of logging statements, and 2) the processing noise in log data. In this paper, we propose a new log-based anomaly detection approach, called LoRobust. LogRobust extracts semantic information of log events and represents them as semantic vectors. It then detects anomalies by utilizing an attention-based Bi-LSTM model, which has the ability to capture the contextual information in the log sequences and automatically learn the importance of different log events. In this way, LogRobust is able to identify and handle unstable log events and sequences. We have evaluated LogRobust using logs collected from the Hadoop system and an actual online service system of Microsoft. The experimental results show that the proposed approach can well address the problem of log instability and achieve accurate and robust results on real-world, ever-changing log data.