Pengembangan Kerangka Kerja Forensik Digital dan Metode Baru berbasis Machine Learning untuk Investigasi Insiden Kebocoran Data = Development of a Digital Forensics Framework and New Machine Learning-based Methods for Investigating Data Leak Incidents

Arif Rahman Hakim, author

Abstrak

Salah satu tantangan utama investigasi insiden kebocoran data adalah tidak tersedianya kerangka kerja spesifik yang sesuai dengan karakteristik insiden kebocoran, disertai langkah-langkah yang jelas dan memberikan hasil investigasi yang komprehensif. Tantangan lain berupa proses analisis terhadap logs berjumlah besar akan menghabiskan waktu dan berpotensi terjadi human-error bila dilakukan secara manual. Pendekatan machine learning (ML) dapat dijadikan solusi, namun kinerja ML seringkali tidak optimal dikarenakan kondisi ketidakseimbangan dataset. Untuk itu, pada penelitian ini dikembangkan kerangka kerja forensik digital baru yang bernama KARAFFE (Kalamullah Ramli–Arif Rahman Hakim–Forensic Framework for Exfiltration), yang bersifat spesifik sesuai dengan karakteristik kebocoran data. Tahapan dan komponen pada KARAFFE mampu menghasilkan jawaban atas pertanyaan investigatif berupa What, When, Who, Where, Why dan How (5WH) dari insiden yang diinvestigasi. Berdasarkan karakteristik pembanding yang ditetapkan, KARAFFE memenuhi enam indikator karakteristik mengungguli kerangka kerja existing lainnya. Lebih lanjut, analisis studi kasus menunjukkan bahwa KARAFFE mampu menginvestigasi insiden secara utuh disertai jawaban 5WH yang lengkap atas insiden yang diuji. Metode lain yang dikembangkan adalah ARKAIV (Arif Rahman Hakim-Kalamullah Ramli-Advanced Investigation). Metode ARKAIV berbasis ML mampu memprediksi terjadinya exfilration berdasarkan event logs yang dipetakan ke adversarial tactics. Untuk prediksi tersebut dilakukan modifikasi dataset berupa rangkain tactics dengan exfiltration sebagai target dan didesain skema resampling untuk mengatasi kondisi ketidakseimbangan dataset. SMOTEENN menghasilkan kinerja terbaik mengungguli empat teknik resampling lainnya, dengan meningkatkan nilai geometric-mean 0 pada initial dataset menjadi 0.99 pada resampled dataset. Selain itu, model ML pada metode ARKAIV dipilih dengan kinerja paling optimal berdasarkan lima teknik feature selection, menerapkan lima classifiers ML, dan dua teknik validasi model. Hasil ML-ARKAIV menunjukkan bahwa Random Forest melampaui kinerja empat classifiers lainnya (XGBoost, Logistic Regression, Naive Bayes, dan Support Vector Machine), dengan mean accuracy sebesar 99.1% (5-folds), 99.8% (10-folds), 99.7% (5-folds 5-repetitions), dan 99.74% (10-folds 10-repetitions). Selain itu, analisis studi kasus menunjukkan bahwa ARKAIV mampu memprediksi secara akurat dua insiden exfiltration dan satu insiden non-exfiltration. Dengan demikian, ARKAIV menunjukkan konsistensi kinerja dan efektifitasnya dalam memprediksi terjadinya exfiltration dalam berbagai skenario.

......One of the primary challenges in investigating data breach incidents is the lack of a specific framework tailored to the characteristics of such incidents, accompanied by clear steps to ensure comprehensive investigative results. Another challenge lies in the analysis of large volumes of logs, which is time-consuming and prone to human error when performed manually. Machine learning (ML) approaches offer a potential solution; however, their performance is often suboptimal due to the imbalance in datasets. This study proposes a novel digital forensic framework named KARAFFE, designed specifically to address the unique characteristics of data breach incidents. The stages and components of KARAFFE are structured to answer investigative questions encompassing What, When, Who, Where, Why, and How (5WH) of the incidents under investigation. Case study analysis demonstrates that KARAFFE provides a complete investigation of incidents, delivering comprehensive 5WH responses for the examined cases. Based on the established comparative characteristics, KARAFFE meets six key indicators, outperforming other existing frameworks. Furthermore, the case study analysis demonstrates that KARAFFE enables comprehensive incident investigation, providing complete 5WH answers for the tested incidents. Additionally, this study introduces the ARKAIV method. ARKAIV is an ML-based approach capable of predicting exfiltration attacks based on event logs mapped to adversarial tactics. To facilitate these predictions, the dataset was modified to include a sequence of tactics with exfiltration as the target, and a resampling scheme was designed to address dataset imbalance. SMOTEENN achieved the best performance, surpassing four other resampling techniques by improving the geometric mean value from 0 on the initial dataset to 0.99 on the resampled dataset. Furthermore, the ML models in ARKAIV were selected for optimal performance through the application of five feature selection techniques, five ML classifiers, and two model validation methods. The results of ML-ARKAIV indicate that Random Forest outperformed four other classifiers (XGBoost, Logistic Regression, Naive Bayes, and Support Vector Machine), with mean accuracy rates of 99.1% (5-folds), 99.8% (10-folds), 99.7% (5-folds with 5 repetitions), and 99.74% (10-folds with 10 repetitions). Additionally, the case study analysis demonstrated that ARKAIV accurately predicted two exfiltration incidents and one non-exfiltration incident. These findings underscore ARKAIV's consistent performance and effectiveness in predicting exfiltration across various scenarios.