INTISARI

Autentikasi Mesin ke Mesin Berbasis Risiko pada Kasus *Fast Health Interoperability Resources* Menggunakan *Random Forest*

Oleh

Damar Arba Pramuditya
22/501365/PPA/06386

Studi ini menggunakan pendekatan berbasis risiko untuk mengidentifikasi dan menilai potensi risiko terkait otentikasi *Machine-to-Machine* (M2M). Analisis pelaku ancaman, kerentanan, dan dampak serangan dilakukan, serta evaluasi metode otentikasi M2M saat ini. Penelitian ini mengembangkan strategi peningkatan otentikasi guna mengurangi risiko serangan. Peningkatan perangkat IoT dalam teknologi perawatan kesehatan menekankan pentingnya otentikasi yang aman antar perangkat. Berbagai pendekatan seperti model enkripsi dan protokol otentikasi telah diusulkan, namun kurang dalam pendekatan berbasis risiko yang mengintegrasikan analisis ancaman dengan evaluasi efektivitas metode otentikasi.

Penelitian ini memanfaatkan algoritma *Random Forest* untuk mengklasifikasikan akses dan menilai efektivitas metode otentikasi saat ini. Temuan penting termasuk identifikasi risiko akses perangkat tidak sah seperti *replay attack*. Dalam konteks *Fast Healthcare Interoperability Resources* (FHIR), studi ini mencapai akurasi 0,708, presisi 0,701, recall 0,968, dan skor F1 0,813 dengan algoritma *Random Forest*.

Sebagai perbandingan, studi menggunakan *Local Outlier Factor* (LOF) untuk autentikasi berbasis data swipe pengguna smartphone menunjukkan bahwa meskipun model belum dioptimalkan mampu mencapai tingkat keberhasilan lebih dari 90% bahkan dengan FAR hingga 40%. Ini menunjukkan bahwa LOF dapat memberikan metrik autentikasi kompetitif dengan model kompleks seperti Random Forest.

Penelitian ini memberikan wawasan berharga bagi organisasi yang menerapkan perangkat IoT, khususnya di sektor teknologi perawatan kesehatan, untuk mengurangi risiko terkait otentikasi M2M.

Kata kunci: Otentikasi Machine-to-Machine (M2M), Fast Healthcare Interoperability Resources (FHIR), Random Forest, Local Outlier Factor (LOF), Perbaikan Autentikasi

ABSTRACT

Risk Based Machine to Machine Authentication in Fast Health Interoperability Resources Case Using Random Forest

By

Damar Arba Pramuditya
22/501365/PPA/06386

This study employs a risk-based approach to identify and assess potential risks associated with Machine-to-Machine (M2M) authentication. Threat actor analysis, vulnerability assessment, and evaluation of the impact of attacks are conducted, along with an evaluation of current M2M authentication methods. The research develops strategies to enhance authentication to mitigate attack risks. The increase in IoT devices in healthcare technology emphasizes the importance of secure inter-device authentication. Various approaches such as encryption models and authentication protocols have been proposed, but they fall short of a risk-based approach that integrates threat analysis with the evaluation of authentication effectiveness.

This study utilizes the Random Forest algorithm to classify access and assess the effectiveness of current authentication methods. Key findings include the identification of risks such as unauthorized device access like replay attacks. In the context of Fast Healthcare Interoperability Resources (FHIR), this study achieves an accuracy of 0.708, a precision of 0.701, a recall of 0.968, and an F1 score of 0.813 using the Random Forest algorithm.

For comparison, a study using the Local Outlier Factor (LOF) for swipe-based user authentication on smartphones showed that even without optimization, the model could achieve success rates of over 90% with a FAR of up to 40%. This indicates that LOF can provide competitive authentication metrics with complex models like Random Forest.

This research offers valuable insights for organizations implementing IoT devices, particularly in the healthcare technology sector, to reduce risks associated with M2M authentication.

Keywords: Machine-to-Machine (M2M) Authentication, Fast Healthcare Interoperability Resources (FHIR), Random Forest, Local Outlier Factor (LOF), Authentication Improvement