ABSTRACT (ITALIANO)

I Software Bill of Materials (SBOM) e gli Artificial Intelligence Bill of Materials (AIBOM) stanno emergendo come un supporto fondamentale per la gestione della supply chain dei sistemi software e di Intelligenza Artificiale (IA), migliorando la trasparenza, la tracciabilità, la conformità e altro. Mentre gli SBOM offrono inventari dei componenti software strutturati e leggibili dalle macchine, gli AIBOM estendono questi principi ai sistemi di IA, documentando modelli e dataset. Tuttavia, conosciamo ancora poco sull'adozione e sull'uso pratico sia degli SBOM che degli AIBOM.

Questa tesi esplora lo stato attuale della pratica degli SBOM e degli AIBOM per supportare la gestione della supply chain dei sistemi software e di IA, contribuendo al miglioramento degli strumenti per la generazione di SBOM e AIBOM. Attraverso una combinazione di metodi qualitativi e quantitativi—comprendenti interviste semi-strutturate con professionisti, mining di repository open-source e una revisione multivocale della letteratura—questa ricerca identifica una bassa consapevolezza e una limitata adozione di SBOM e AIBOM, nonché significative limitazioni tecniche negli attuali generatori di SBOM e AIBOM.

Per migliorare il supporto alla generazione degli SBOM e degli AIBOM, sono stati sviluppati e valutati empiricamente due strumenti. AIRBORNE arricchisce gli SBOM con dati di provenienza a grana fine, collegando artefatti software ai contenuti riutilizzati da Stack Overflow. ALOHA genera AIBOM estraendo e strutturando informazioni da Hugging Face, una piattaforma importante per la condivisione di modelli e dataset di IA. Entrambi gli strumenti hanno dimostrato la fattibilità di arricchire gli SBOM e gli AIBOM attraverso un'analisi più approfondita della composizione software.

I risultati di questa tesi offrono implicazioni pratiche e orientate alla ricerca. Per i professionisti—specialmente fornitori, acquirenti e operatori software—l'adozione di SBOM e AIBOM è

essenziale per la gestione della software supply chain. I fornitori dovrebbero integrare la generazione automatizzata di SBOM/AIBOM nelle loro pipeline, garantendo la conformità a linee guida, standard e normative. Gli acquirenti dovrebbero richiedere SBOM/AIBOM completi e accurati durante il processo di approvvigionamento, mentre gli operatori dovrebbero integrarli nelle pipeline di Continuous Integration/Continuous Delivery per il monitoraggio continuo dei rischi. Per i ricercatori, i futuri lavori dovrebbero concentrarsi sul miglioramento del supporto per la generazione di SBOM e AIBOM, migliorando la loro accuratezza e copertura, così come la qualità delle fonti di dati a supporto, e tracciando più efficacemente la provenienza del software.

ABSTRACT (ENGLISH)

Software Bills of Materials (SBOMs) and Artificial Intelligence Bills of Materials (AIBOMs) are emerging as critical support for managing the supply chain of software and Artificial Intelligence (AI) systems by improving transparency, traceability, compliance, and more. While SBOMs offer structured, machine-readable inventories of software components, AIBOMs extend these principles to AI and AI-enabled systems by documenting models and datasets. However, we still know little about the adoption and practical usage of both SBOM and AIBOM.

This thesis investigates the current state of practice of SBOM and AIBOM to support the management of the supply chain of software and AI systems, and contributes to improving the tooling of SBOM and AIBOM. Through a combination of qualitative and quantitative methods—including semi-structured interviews with practitioners, mining of open-source repositories, and a multivocal literature review—this research identifies low awareness and limited adoption of SBOM and AIBOM, and significant technical limitations in existing SBOM and AIBOM generators.

To improve support for the generation of SBOM and AIBOM, two tools were developed and empirically evaluated. AIRBORNE enhances SBOMs with fine-grained provenance data by linking software artifacts to reused content from Stack Overflow. ALOHA generates AIBOMs by extracting and structuring information from Hugging Face, a major platform for sharing AI models and datasets. Both tools demonstrated the feasibility of enriching SBOMs and AIBOMs through deeper software composition analysis.

The findings of this thesis offer practical and research-oriented implications. For practitioners—especially software suppliers, choosers, and operators—adopting SBOMs and AIBOMs is essential for managing the software supply chain. Suppliers should integrate automated SBOM/AIBOM generation into their pipelines, ensuring compliance with guidelines, standards, and regulations. Choosers should demand complete and accurate SBOMs/AI-

BOMs during procurement, while operators should incorporate them into CI/CD pipelines for continuous risk monitoring. For researchers, future work should focus on improving the support for the generation of SBOM and AIBOM, enhancing their accuracy and coverage, improving the quality of supporting data sources, and tracking software provenance more effectively.