

New integrated risk analysis framework enhances cybersecurity for small- and medium-sized enterprises

July 31 2024

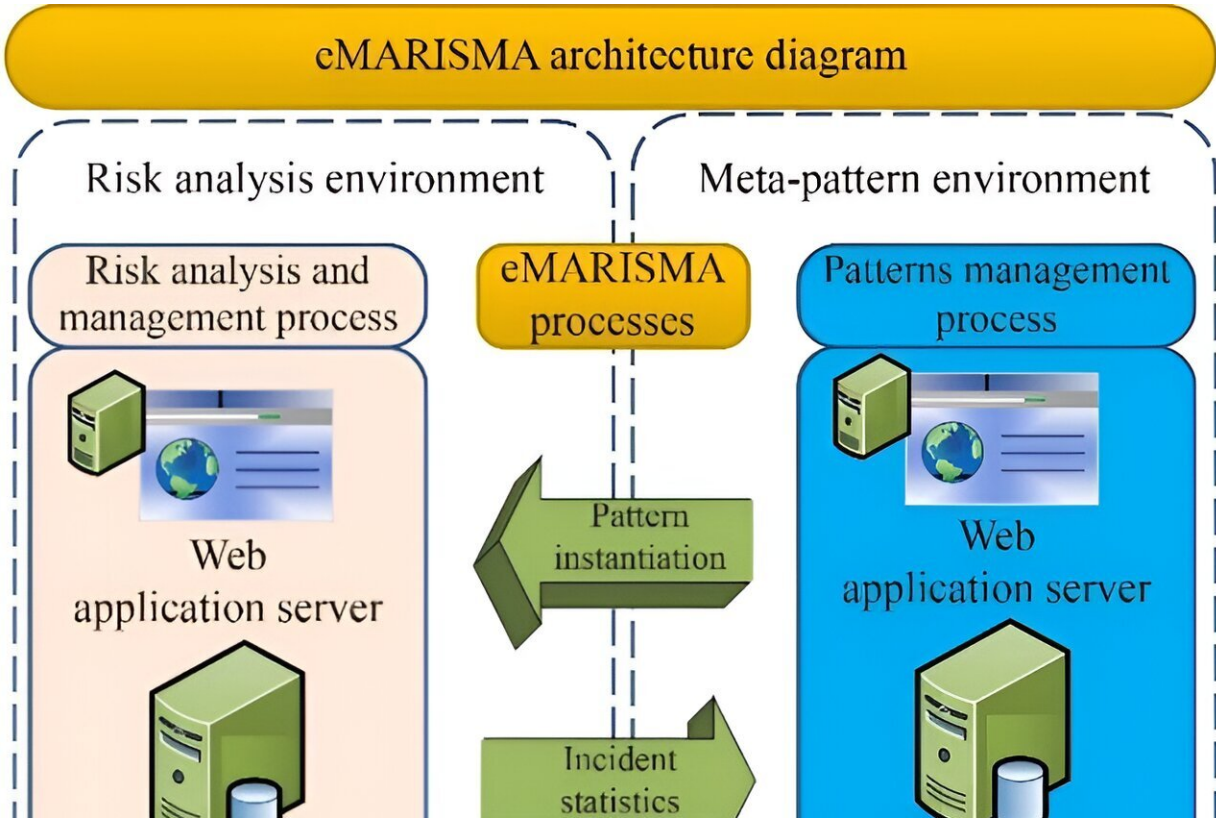


Diagram of eMARISMA architecture. Credit: Antonio Santos-Olmo

A recent study introduces MARISMA, a new framework developed to address limitations in existing risk analysis models for cybersecurity.

The study conducted by Prof. Antonio Santos-Olmo and his team identifies 10 major weaknesses in current models, leading to the development of MARISMA.

MARISMA aims to improve [cybersecurity](#) for companies, particularly small and medium-sized enterprises (SMEs), by providing a dynamic and adaptable risk management approach that evolves with new threats. "In today's digital age, companies must be proactive in cybersecurity. MARISMA provides the tools needed to stay ahead of potential threats," says Prof. Santos-Olmo.

The need for this framework arises from the rapid evolution of technology and the increasing interconnectivity of businesses. Traditional models often fail to account for new risks associated with technologies like Cloud Computing, the Internet of Things (IoT), and Big Data, necessitating a more robust and adaptive approach to risk management.

The study, [published](#) in *Frontiers of Computer Science*, utilized a systematic review protocol to analyze existing [risk analysis](#) and management literature, ensuring a comprehensive understanding of current limitations.

The review revealed that current models often lack the flexibility to adapt to new risks in real time, resulting in outdated risk assessments. MARISMA addresses this issue by incorporating a risk data management module, a systematic application methodology, and an automation tool.

MARISMA's dynamic approach allows companies to maintain up-to-date risk assessments without incurring significant additional costs, making it particularly beneficial for SMEs. "Our framework is already being applied by customers in several European and American countries,

showing its practical effectiveness and adaptability," noted Prof. Santos-Olmo.

Looking ahead, the research team plans to further refine the MARISMA framework by integrating artificial intelligence techniques, which will enhance its ability to predict and respond to emerging threats. This study and the development of the MARISMA framework contribute to the advancement of cybersecurity risk [management](#) by offering a dynamic, adaptable solution.

More information: Antonio Santos-Olmo et al, Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals, *Frontiers of Computer Science* (2023). [DOI: 10.1007/s11704-023-1582-6](#)

Provided by Higher Education Press

Citation: New integrated risk analysis framework enhances cybersecurity for small- and medium-sized enterprises (2024, July 31) retrieved 15 August 2024 from <https://techxplore.com/news/2024-07-analysis-framework-cybersecurity-small-medium.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.