3rd International Congress on Scientific Research May 1-2 2024 by IKSAD Institute

**USB-port risk analysis to protect user data**

Zoltán Lehrer (<https://orcid.org/0009-0002-4978-7492>),

László Pitlik (Jr.) (<https://orcid.org/0000-0002-8058-9577>)

Dr. László Pitlik (<https://orcid.org/0000-0001-5819-0319>),

e-Mails: [lehrerzoltan@gmail.com](mailto:nayyaraadi@gmail.com), [ptlklszl@my-x.hu](mailto:ptlklszl@my-x.hu), [pitlik@my-x.hu](mailto:pitlik@my-x.hu)

Kodolányi János University and MY-X research team Hungary

*Keywords: AI, security, automation, similarity- and risk-analysis*

**Abstract**

History: The topic of my thesis was inspired by the presentation of a USB device that is capable of running a short line of code hidden on it on a computer, and the executed line of code can even endanger our personal data. This is a simple data/charging cable that can cause huge damage to the unsuspecting user. Its users can abuse our personal data, break into computer networks, steal our identity, commit financial fraud, spread malware and viruses, and carry out various types of Internet abuse, harassment, or blackmail.

Background and benchmarks: Risk analysis is an important step in the development and implementation of any project plan. The application of the object-attribute matrix (OAM) enables a structured and comprehensive analysis of risks, which helps to identify, evaluate, and manage potential hazards and uncertainties. OAM is a tool that allows you to link objects (such as project phases, business processes, assets, etc.) and their associated attributes (such as risk factors, hazards, impacts, etc.) in a structured form. As a result, it is easier to identify and assess potential risks and design appropriate risk management strategies.

Highlighted details: The USB-port risk analysis enables detailed monitoring and analysis of the activity of USB-ports. The data required for the analysis is collected manually from the performance measurement program of the operating system, thereby guaranteeing reliable and accurate results. The process can be automated later. Measured values include maximum paging file utilization, disk drive write rate, and CPU and memory utilization.

The data is recorded in an object attribute matrix, where the rows show the measured values, while the columns show the elapsed time. All measurements are made in two-second time intervals, thus ensuring a detailed and timely analysis. With the help of OAM, we rank and evaluate the various risk factors related to each object. This enables the prioritization of risks and the extent of their effects. During the analysis, we use the COCO Y0 model, which can be found in <https://miau.my-x.hu/myx-free/coco/beker_y0.php> site. At the end of the analysis, we carry out an authenticity test, which is carried out with the inverse version of the original (direct) OAM. If t analysis is successful, we get the inverse result of the original analysis.

Future aspects: Automating the entire process and creating an independent software in the form of a thesis, which provides the user with real data in real time.