

**CYBER BREACH DIAGNOSTICS SYSTEM FOR USE IN DIAGNOSING
WHETHER TARGET NETWORK SYSTEM IS BREACHED BY CYBER ATTACK**

ABSTRACT OF DISCLOSURE

A cyber breach diagnostics system includes: an activity records collection device arranged to operably collect multiple suspicious activities records related to multiple computing devices in a target network and corresponding multiple time stamps and multiple attribute tags, and to operably process the multiple suspicious activities records, the multiple time stamps, and the multiple attribute tags to generate a return data; and a suspicious event analysis device arranged to operably conduct a suspicious event sequence diagram generating operation to identify multiple suspicious events related to the target network as well as multiple time records corresponding to the multiple suspicious events, and to operably generate and display a suspicious event sequence diagram corresponding to the multiple suspicious events according to the multiple suspicious events and the multiple time records.

FIG. 1