CLAIMS:

1. A computer implemented system (100) for performing electromotive force analysis of a storage device (142) comprising:

a storage device (142) configured to utilize a predefined protocol;

an AI Co-processor chipset (120);

a thin coil inductor (110) positioned in proximity to a portion of the surface of the storage device (142) for capturing data associated to electromotive force energy generated by the storage device (142);

an analog-to-digital-converter (140); and

at least one probe for communicating the captured data to an analog-to-digital converter (140);

wherein the data is captured by the thin coil inductor (110) and communicated to the analog-to-digital-converter (140) via the at least one probe;

wherein the analog-to-digital-converter (140) digitizes the voltage level of the captured data and communicates the results of the digitization and amplification to the AI Co-processor chipset (120);

wherein the AI Co-processor chipset (120) performs analysis of the data to detect any anomalies caused by malware in the operation of the storage device (142) and outputs those result for further processing; and

wherein to perform analysis of the data for detection of anomalies, the AI Co-processor chipset (120) is configured to calculate a correlation between command values of the predefined protocol and the electromotive force energy generated by the storage device (142).

2. The computer implemented system (100) for performing electromotive force analysis of a storage device (142) of claim l wherein the storage device (142) is a solid state drive.

3. The computer implemented system (100) for performing electromotive force analysis of a storage device (142) of claim 2 further comprising:

a solid state drive SoC controller; and

a circuit chipset in communication with the solid state drive SoC controller;

wherein the solid state drive SoC controller monitors the hardware performance of the solid state drive by measuring electromotive force of the solid state drive and communicates the measured electromotive force data to the AI Co-processor chipset (120).

4. The computer implemented system (100) for performing electromotive force analysis of a storage device (142) of claim 3 wherein the AI Co-processor chipset (120) performs analysis to provide real time protection against any anomalies in the operation of the solid state drive.

5. The computer implemented system (100) for performing electromotive force analysis of a storage device (142) of claim 4 wherein the predefined protocol comprises (i) a NVMe protocol or (ii) an AHCI protocol.

6. The computer implemented system (100) for performing electromotive force analysis of a storage device (142) of claim 4 wherein the further processing interrupts the operation of the solid state drive.

7. The computer implemented system (100) for performing electromotive force analysis of a storage device (142) of claim 4 wherein the AI Co-processor chipset (120) applies artificial intelligence algorithms to detect ransomware activities, and wherein when the ransomware activities are detected, the operation of the solid state drive is interrupted.

8. A computer implemented method for performing electromotive force analysis of a storage device (142) comprising the steps of:

capturing data associated to electromotive force energy generated by a storage device (142) using a thin coil inductor (110) positioned in proximity to a portion of a surface of a storage device (142), the storage device (142) utilizing a predefined protocol;

communicating the captured data to an analog-to-digital-converter (140) via at least one probe;

digitizing the voltage level of the captured data using the analog-to-digital converter (140);

communicating the voltage level to an AI-Coprocessor (120);

analyzing the voltage level using the AI-Coprocessor (120) to detect any anomalies caused by malware in the operation of the storage device (142);

outputting the result for further processing, and

wherein the analyzing the voltage level for the detection of anomalies comprises calculating a correlation between command values of the predefined protocol and the electromotive force energy generated by the storage device (142).

9. The computer implemented method for performing electromotive force analysis of a storage device (142) of claim 8 wherein the storage device (142) is a solid state drive.

10. The computer implemented method for performing electromotive force analysis of a storage device (142) of claim 9 further comprising the step of:

monitoring the hardware performance of the solid state drive by measuring electromotive force of the solid state drive with a solid state drive SoC controller and a circuit chipset in communication with the solid state drive SoC controller;

communicating the measured electromotive force data to the AI-Coprocessor (120);

using the AI-Coprocessor (120) to analyze the measured electromotive force data; and

outputting the results of the analysis to provide real time protection against any anomalies in the operation of the solid state drive.

11. The computer implemented method for performing electromotive force analysis of a storage device (142) of claim 10 wherein the AI-Coprocessor (120) performs analysis to provide real time protection against any anomalies in the operation of the solid state drive.

12. The computer implemented method for performing electromotive force analysis of a storage device (142) of claim 9 wherein the predefined protocol comprises (i) a NVMe protocol; or (ii) an AHCI protocol.

13. The computer implemented method for performing electromotive force analysis of a storage device (142) of claim 9 further comprising the step of:

interrupting the operation of the solid state drive when an anomaly caused by malware is detected.

14. The computer implemented method for performing electromotive force analysis of a storage device (142) of claim 10 wherein the AI-Coprocessor (120) utilizes artificial intelligence algorithms to detect ransomware activities.

15. The computer implemented method for performing electromotive force analysis of a storage device (142) of claim 14 further comprising the step of:

interrupting the operation of the solid state drive when the ransomware activities are detected by the AI-Coprocessor (120).

16. The computer implemented system (100) for performing electromotive force analysis of a storage device (142) of claim l, wherein the one or more actions comprise limiting access to the stored data, sending one or more alert beams through an external wireless connection or a wired connection or both, locking the storage device (142) or a component within the storage device (142) or a component external to the storage device (142), and/or allowing read only mode without the ability to overwrite any stored data.

17. The computer implemented method for performing electromotive force analysis of a storage device (142) of claim 8, wherein the one or more actions comprise limiting access to the stored data, sending one or more alert beams through an external wireless connection or a wired connection or both, locking the storage device (142) or a component within the storage device (142) or a component external to the storage device (142), and/or allowing read only mode without the ability to overwrite any stored data.