

**CHENNAI – PONDICHERRY**

**Robust Malware Detection for Internet Of (Battlefield) Things Devices Using Deep Eigenspace Learning**

**Abstract**

Internet of Things (IoT) in military setting generally consists of a diverse range of Internet-connected devices and nodes (e.g. medical devices to wearable combat uniforms), which are a valuable target for cyber criminals, particularly state-sponsored or nation state actors. A common attack vector is the use of malware. In this paper, we present a deep learning based method to detect Internet Of Battlefield Things (IoBT) malware via the device's Operational Code (OpCode) sequence. We transmute OpCodes into a vector space and apply a deep Eigenspace learning approach to classify malicious and bening application. We also demonstrate the robustness of our proposed approach in malware detection and its sustainability against junk code insertion attacks. Lastly, we make available our malware sample on Github, which hopefully will benefit future research efforts (e.g. for evaluation of proposed malware detection approaches).