**INTRODUCTION**

**Internet of Things (IoT) enables convergence and implementations between the real-world objects irrespective of their geographical locations. Implementation of such network management and control make privacy and protection strategies utmost important and challenging in such an environment. IoT applications need to protect data privacy to fix security issues such as intrusions, spoofing attacks, DoS attacks, DoS attacks, jamming, eavesdropping, spam, and malware. The safety measures of IoT devices depends upon the size and type of organization in which it is imposed.**

**The behavior of users forces the security gateways to cooperate. In other words, we can say that the location, nature, application of IoT devices decides the security measures [1]. For instance, the smart IoT security cameras in the smart organization can capture the different parameters for analysis and intelligent decision making [2]. The maximum care to be taken is with web based devices as maximum number of IoT devices are web dependent. It is common at the workplace that the IoT devices installed in an organization can be used to implement security and privacy features efficiently.**

**For example, wearable devices collect and send user’s health data to a connected smartphone should prevent leakage of information to ensure privacy. It has been found in the market that 25-30% of working employees connect theirpersonal IoT devices with the organizational network. The expanding nature of IoT attracts both the audience, i.e., the users and the attackers. However, with the emergence of ML in various attacks scenarios, IoT devices choose a defensive strategy and decide the key parameters in the security protocols for trade-off between security, privacy and computation. This job is challenging as it is usually difficult for an IoT system with limited resources toestimate the current network and timely attack status.**

**A. Contributions Based upon the above discussions, following contributions are presented in this paper. 1) The proposed scheme of spam detection is validated using five different machine learning models. 2) An algorithm is proposed to compute the spamicity score of each model which is then used for detection and intelligent decision making. 3) Based upon the spamicity score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics.** **B. Organization Rest of the paper is structured as follows. Section II discussed the related work. Section III illustrated the proposedscheme. Results are discussed and analyzed in Section IV. Finally, the paper is concluded in Section V.**