

# **Ransomware Readiness Assessment Tool**

**Dr. Nandini S<sup>1</sup>, D P Sai Manohar<sup>2</sup>, Darshan D<sup>3</sup>, G Shivaram Gowda<sup>4</sup>, Nisarga S<sup>5</sup>**

Associate Professor, Department of Information Science and Engineering<sup>1</sup>

Under Graduate Student, Department of Information Science and Engineering<sup>2,3,4,5</sup>

S J C Institute of Technology, Chikkaballapur, India

**Abstract:** *Ransomware attacks have been increasingly concerning in times. The situation is only getting worse. They have shed light on a category of software that demands a ransom, for releasing a hostage asset. The majority of ransomware strains rely on encrypting data. Essentially, they lock up files on the victims' devices and network drives before demanding payment to decrypt them. In this study, we first introduce a classification system for ransomware. Then drawing from this taxonomy and identifying a present in highly resilient ransomware during the key exchange process we propose an innovative method for detecting and thwarting these resilient strains to prevent them from encrypting victims' data. Through testing our model shows promising results, in identifying variations of dangerous ransomware strains.*

**Keywords:** ransomware, crypto virology, prevention; high survivable ransomware