In today’s world, smartphones and mobile devices are playing an important role in most of the people lives’ for all the requirements such as internet banking, social media, gaming etc. Smartphones use has been expected to rise 84% to 859m by 2022 as reported by The Economic times [1]. There has been a huge difference in the usage of Smartphones, Desktops and Tablets based on the requirement and convenience provided by each. As a result we can see difference in market share between mobiles and Desktops and tablets in present world as reported by statcounter GlobalStats[2] presenting mobiles covers 49.56% of world market shares in comparison to desktop which holds 46.53% and tablets holds 3.91%. Smartphones uses types such as Android, IOS, Windows, Blackberry, etc. Android covers mainly the mobile share in the due to affordable prices and more features in less price. Android has 75.48% of MOS market share worldwide, IOS has 21.77% and so on as reference [3]. There are 2.3 billion android smartphones in use as reported by Newszoo[4]. Android Smartphones provides facilities and fulfils requirement of the user by providing various apps. In Android Smartphones, apps are provided by official application Google Play’s Store in which free as well as paid apps can be downloaded as per the user requirement on their android smartphones. App developers built the apps and publish it in the Google Play’s Store. Android users can choose from 2.1 million apps as reference [5] provided by the android.

In the past years due to growing usage of android smartphones and the android apps, the android users has been facing many issues due to the introduction of malware apps among the android app collection. Due to the lack of suitable security features in the android system, malware apps can cause various threats to the user such as Information leakage, System Damage, Financial Loss. As per the report presented by AV-TEST[6] the development of malware apps in 2018 is 5.52m and in 2019 till June 1.54m.Many users are affected by malwares such as 25m Android Smartphones by Agent Smith android malware around the world as reported by 91mobiles[7]. So there is excessive need for malware apps to be detected and removed from the Google Play’s Store and third party app markets which is done by Android Malware Detection. Malware can be detected either by Analyzing Permission, Static Analysis or Dynamic Analysis.

Permission control is one of the Android Security Mechanism by limiting the actions the system can perform. The purpose of permissions is to protect the privacy of user. App developers must declare the request for permissions to access sensitive data of users (Reading contacts, messages, etc.) and various system features. Every app have a group of permissions requesting the access to system data and various other system features. Depending on the permission it may be granted automatically either by the system or it is passed to the user to request the approval. The central design point of android security architecture is that no app by default has permissions to perform such operations which would affect the system or the user. There is a pattern in permissions which tells about the behavior of the app whether it is malicious or normal app. In these paper the challenge is to analyze the permissions and find the particular set of permissions which together differentiates between the malicious apps and the normal apps. Various machine learning algorithm like Naïve Bayes Test, SVM Test, etc. are used to find the particular pattern of permissions in the apps to identify the difference between the malware and the normal apps. Through this paper, our objective is to determine the set of permissions so as to detect the malware precisely and accurately.

Our work can be classified into, first to strategically extract all the permissions from the manifest file in all the training apps including malware apps and normal apps. To rank and arrange the permissions based on their level of riskiness from top to bottom using Information Gain, Chi-Square Test applying on both normal apps and malware apps. To analyze the permissions ranking from each test with the help of machine learning Naïve Bayes Algorithm or SVM Test and find the set of permissions common to all malware apps and normal apps. Finally to check our result on the testing dataset and find the accuracy of our result.

In summary, our paper makes the following contributions to the analyzing pattern of permissions:

1. We applied Entropy mechanism to rank the permissions with an aim to find the distinguishing features.

2. We further ranked the permissions using the Chi-Square test to find the significant permissions present in normal and malicious apps.

3. We proposed an algorithm, to find the best set of permissions amongst the different permissions’ ranking, which can give the best detection accuracy based on Naïve Bayes’ classifier.

[1]= <https://economictimes.indiatimes.com/tech/hardware/smartphone-users-expected-to-rise-84-to-859m-by-2022-assocham-pwc-study/articleshow/69260487.cms?from=mdr>

[2]= <http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide/#monthly-201806-201906-bar>

[3]= <http://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-201806-201906-bar>

[4]=( Newszoo) <https://newzoo.com/insights/articles/insights-into-the-2-3-billion-android-smartphones-in-use-around-the-world/>

[5]= (Statista)<https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>

[6]= (AV-TEST) <https://www.av-test.org/en/statistics/malware/>

[7]= (91mobiles) <https://www.91mobiles.com/hub/agent-smith-android-malware-infected-india-disguised-as-google-app/>