Dear Reviewer,

Thank you very much for your valuable comments and the acceptance of the article in doctoral symposium. We have effectively addressed all the comments to improve the quality of the article.

The individual response for the comments of reviewers are mentioned below.

**Comment 1:**

First, introduce briefly each type of attack that is discussed in the proposal.

**Response 1:**

Thank you for your comment. All types of attacks are introduced and discussed in the introduction section.

Please see section 1 as –

“The prominent threats in cybersecurity are malware, fileless malware, botnet, and intrusions. The malware is a malicious program that do things which any programs are not supposed to do in the system. It comprises all sort of malware like Adware, Trojans, Bots, Worm, Backdoor, and fileless malware [12]. Bot is a small malicious program that can target the vulnerable system to compromise and make it a part of larger botnet (Ro**bot** **net**work) controlled by a bot-master. A bot-master can launch a cyberattack using the botnet like sending spam, data theft, compromising confidential info, and distributed denial of service (DDoS) [11]. The fileless malware can compromise a system without making any changes or minor changes in the file system living entirely in the main memory, rootkit, or registry. The malware still has all the capabilities like traditional malware making it hard to detect and more harmful [10]. Further, intrusion can be classified into any kind of unauthorised or malicious activities in the network like network flood attack, malware attached with messages, and man-in-middle attack [11]. In our work, we have classify the above cyberthreats using ML and DL techniques. The contribution of the thesis is shown in figure 1.”

**Comment 2:**

Figure 1 is not explained.

**Response 2:**

Thank you for your comment. We have removed the figure and added a block diagram comprising all the work proposed in the thesis.

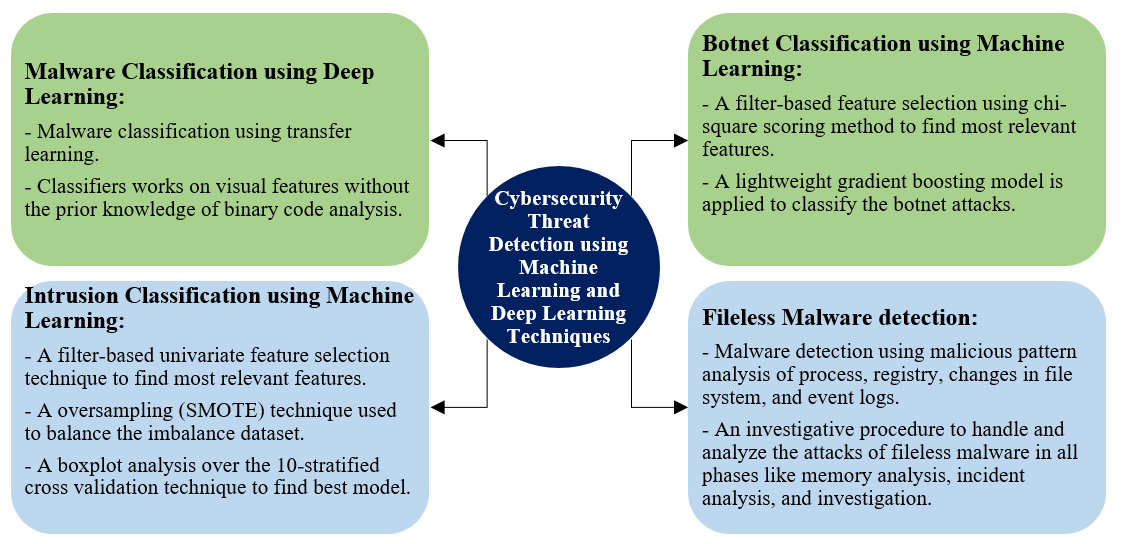


Figure 1: Thesis contributions.

**Comment 3:**

The main contributions of the thesis can be presented with the help of a diagram. So, instead of Figure 1, an architecture describing the key contributions of the thesis should be presented.

**Response 3:**

Thank you for your comment. We have removed the figure and added a block diagram comprising all the work proposed in the thesis. The key contributions of each model is also presented in the architecture.

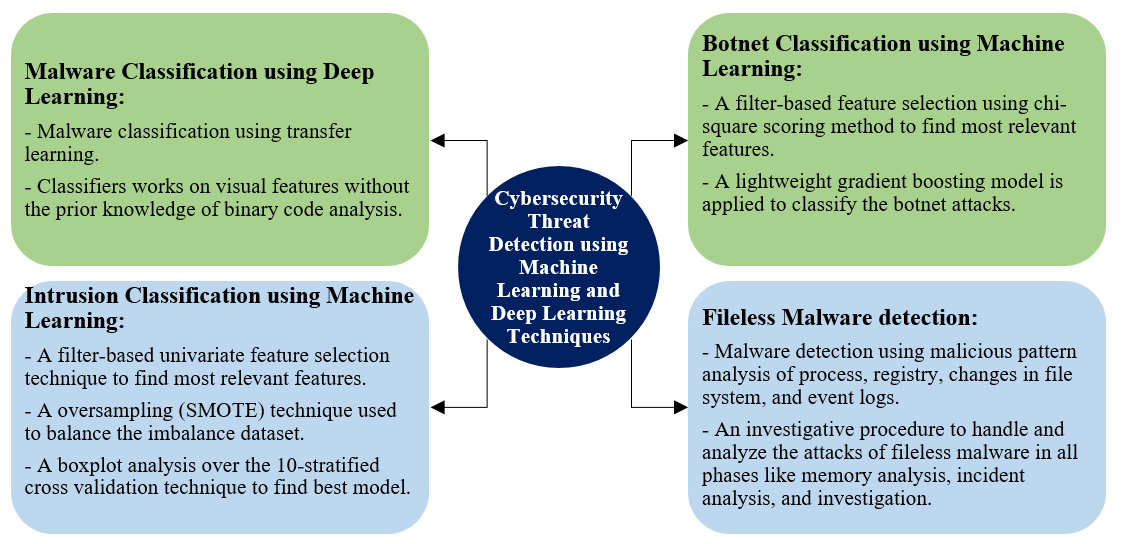


Figure 1: Thesis contributions.

**Comment 4:**

Does the proposed model MCFT-CNN use both the visual and textual features and only the visual features to classify malware? Please clarify. If it only uses visual features, then please explain how it is better than the already existing models which also use visual features.

**Response 4:**

Thank you for your comment. The proposed model only trained with visual features to classify the malware. The model also performs better in terms of accuracy and prediction time than already existed state-of-art models.

Please see section 2, 3rd paragraph as –

“Thus, we propose a novel MCFT-CNN model to address the above issues and trained with only visual features. We have achieved 99.18% accuracy and 5.14ms prediction time on the MalImg dataset [6]. The model shows significant improvement over a larger dataset (Microsoft Malware Challenge [8]) with 98.63% accuracy and 5.15ms prediction time. Our model performs significantly better than the existed state-of-art [14]. Similarly, in intrusion detection and botnet detection, we have used machine learning algorithms to efficiently classify intrusions and botnet attacks. We have also proposed an incident handling and response process in case of a fileless malware attack to analyze the attack and behavior of the fileless malware. The proposed models perform significantly better than other models available in the literature [1–5, 7, 9, 10, 15, 16].”

**Comment 5:**

Please explain the intuition (at a high level) why your model performs better than the state-of-the-art for the task of fileless malware detection, intrusion, and botnet detection. What challenges were faced while trying to solve these problems, and why could they not be solved using state-of-the-art techniques?

**Response 5:**

Thank you for your comment. We have explained the performance of our model, how it is better than state-of-art and challenges faced in solving the problem?

Please see section 1, 2nd paragraph as –

“It is very crucial for any network to neutralize the cyberthreats in order to safeguard their infrastructure. We have used machine learning and deep learning techniques to detect and classify the cyberthreats. We required benchmark datasets and its attributes like diversified attacks and imbalance distribution of classes to train our models. Each models required fine-tuning of hyper-parameters to train efficiently. Our models have successfully classify the above cyberthreats. The contribution of the thesis is shown in figure 1.”