# Foreword and Editorial

## International Journal of Advanced Research in Computer and Information Security (IJACIS)

We are very happy to publish this issue of an International Journal of Advanced Research in Computer and Information Security by Global Vision Press.

This issue contains 2 articles. Achieving such a high quality of papers would have been impossible without the huge work that was undertaken by the Editorial Board members and External Reviewers. We take this opportunity to thank them for their great support and cooperation.

In the paper “Applications of Machine Learning in Cyber Security”, Machine learning is one of the latest trends models and methods that can be implemented and the users can get the good results. The growth of this area was developing day to day by almost all areas of applications and research. The other important area to be considered was the cyber security. The most of the common people also being trapped by these technologies and the people are losing their valuable data in some cases and in some other cases the people or losing their valuable money also. In some other cases, the people are losing their lives due to the sharing of their personal data to the public domain. Hence, people need to think of these problems in a different manner and also to solve these technical problems by using these advanced technologies. In the current article, some of the cyber security issues and threats that were being occurring in these days were highlighted and how the utilization of these machine learning techniques will be used to identify such threats and can be avoided or can be protected from these sorts of attacks.

The paper entitled “Analysis of Black Hole Attacks on Wireless Sensor Networks” explored that Wireless sensing element networks contains of assorted variety of freelance sensing element units and nodes that were accustomed monitor and live the physical properties of assorted devices and conjointly the temperature and its connected measurements etc. The key applications of those units square measure the military, setting, unsafe places wherever it's troublesome for the masses to enter. A number of the necessary restrictions or the bounds of a sensing element network which is able to play a significant role on the performance of those kinds of networks. By considering these drawbacks, the sensing element networks is simply attacked by different devices or the different set of users within the same networks or other set of networks. This type of attacks within the wireless sensing element networks was thought of here and therefore the performance of the networks below these attacks was simulated by victimization the NS2 machine. When simulation, the result shows that the performance of the network may well be influenced by the presence of assorted set of attacks within the networks. Conjointly the importance was given to the amount of nodes being attacked during a single network.

December 2019

**Editors of the December Issue on**
**International Journal of Advanced Research in Computer and Information Security**