Foreword and Editorial

International Journal of Security Technology for Smart Device

We are very happy to publish this issue of an International Journal of Security Technology for Smart Device 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 "A Survey on Comparison of Various Protocols and Key Management Issues in Manet", remote Network incorporates a bigger favorable position in the present correspondence application like ecological, movement, military and wellbeing perception. To understand these applications it's important to have a solid directing convention. The self-sorting out nature of MANETs makes them appropriate for some applications and henceforth, extensive exertion has been put into anchoring this kind of systems. Secure correspondence in a system is dictated by the unwavering quality of the key administration conspire, which is in charge of creating, circulating and looking after encryption/decoding keys among the hubs. In this paper different key administration plans for MANETs are talked about. This examination work proposes a novel secure Identity-Based Key Management convention making utilization of cryptographic and Information Theoretic Security.

In the research paper "A Detailed Review about Attacks on WSNs", remote sensor systems have an arrangement of calculations and conventions with self-building up abilities. The current sensors or the sensors used in these sensor networks will work wirelessly by locating at various locations of the actual requirement. The major advantage of these sensor networks are that these network nodes can be placed at various locations where it will be more difficult for the human beings or persons to enter and collect data. In such dangerous places also these nodes can be placed and can collect the data from time to time. As a result of such important facilities, the utilization such node sin these networks are becoming very high and the usage of such networks had grown a lot. In these current days, the networks which were built with the combination of such nodes and networks are built and the attackers always are ready to tap or attack such networks and hack the data. Once the data had collected and can be used for various other benefits and the actual user or the network established person or the company had to lose the data and also can be used such important data for various other anti social issues. Hence, the attacks on these nodes and networks can be treated seriously and can be considered with various preventive measures. In the current paper an attempt has been made to present some important points and issues to be noted for the establishment and working of the network. Different assaults are performed in this system, for example, inactive and dynamic assaults or insider and outcast assaults. The remotely arrange required continuously security as information respectability, secrecy, legitimacy and so forth.

November 2019

Editors of the November Issue on
International Journal of Security Technology for Smart Device