# Chapter 10
# KK Approach to Increase Resilience in Internet of Things
## A T-Cell Security Concept

**Kutubuddin Sayyad Liyakat Kazi**
https://orcid.org/0000-0001-5623-9211
*Brahmdevdada Mane Institute of Technology, Solapur, India*

## ABSTRACT

*This technique for identifying malicious nodes is known by the inventor as the "KK approach." We compare the throughput and delay of the system with the proposed KK Approach, and the results are superior compared to the earlier techniques. Its abilities to learn, adapt, collaborate, and act independently make it a potent weapon in fighting against cyber threats. It is also capable of learning. However, additional research and development are required to overcome the limitations and challenges associated with its deployment. It is essential to continue investigating and financing state-of-the-art solutions in order to guarantee the security and privacy of these networks. This is because we rely more and more on gadgets connected to the IoT for our everyday needs.*

## INTRODUCTION

The Internet of Things (IoT) is a growing network of interconnected devices. Among these gadgets are wearable technologies, industrial devices, and smart home systems. The continuous data exchange and networking of these gadgets is making our daily activities more convenient and efficient. This interconnectedness

DOI: 10.4018/979-8-3693-8014-7.ch010

does, however, come with a serious security risk that needs to be addressed. The probability of cyberattacks and data breaches has also increased due to the growing number of devices connected to the internet. Liyakat (2024) has thus raised grave worries about the privacy on our own private data and the security of IoT devices.

IoT technology, whose continues to progressively gaining pace, is currently being used in a wide range of sectors and applications. As a result, there are several instances of IoT application use. Among IoT application scenarios, smart home applications are among the most well-known. As virtual assistants likes Google Home and Amazon's Alexa gain popularity, more and more people are making their houses "smart homes" by Gund (2023). Owing to Internet of Things devices, homeowners can monitor and operate their properties remotely. Among these devices are smart thermostats, smart lighting, and smart security systems. For example, individuals may regulate the temperature and lighting in their houses and get notifications if something strange happens. Liyakat Kazi (2024) and Neeraja (2024) observe that by including this, things become safer and more energy-efficient in addition to being more convenient.

Moreover, K S (2022) describes a noteworthy Internet of Things application situation in the healthcare industry. Patients may now monitor their health in real time thanks to IoT gadgets. Thanks to Veena (2023) and Megha (2024), they may also provide this information to their healthcare practitioners. For instance, a diabetic patient can utilize an ongoing glucose monitoring device that uses K S to send data to their doctor (2023b). This gives the doctor the chance to adjust the treatment plan as necessary. In a same vein, hospitals can employ IoT devices to remotely monitor patient vitals, automate some procedures, and track the whereabouts of medical equipment—all of which will enhance patient care and efficiency by Priya (2023).

The change that IoT is bringing about in the transportation industry has caused us to travel in a different way. Cars can now speak with intelligent traffic systems and with one another, thanks to the growing usage of IoT devices like sensors and GPS trackers. This makes it possible to monitor traffic in real-time, which helps to lessen traffic bottlenecks and raises overall road safety. The logistics sector is also using IoT technology to track shipments and improve delivery routes, which finally results in more timely and effective delivery of goods.

Another area where IoT is becoming well-known is in the manufacturing industry, where it is referred to as the Industrial-Internet of Things, or IIoT. Manufacturers can connect machines, equipment, and networks to collect data in real time and remotely monitor processes. This makes predictive maintenance possible, boosting output while decreasing downtime. The IIoT enables businesses to optimize their supply chain and inventory, increasing efficiency and reducing expenses.

Design and Development of Hybrid Algorithms to Improve Cyber Security and Provide Securing Data Using Image Steganography With Internet of Things

Abhishek Rajeshkumar Mehtaand Trupti Pravinsinh Rathod (2021). *Multidisciplinary Approach to Modern Digital Steganography (pp. 326-338).*

www.irma-international.org/chapter/design-and-development-of-hybrid-algorithms-to-improve-cyber-security-and-provide-securing-data-using-image-steganography-with-internet-of-things/280009