# Chapter 14
# Securing the IoT System of Smart Cities by Interactive Layered Neuro-Fuzzy Inference Network Classifier With Asymmetric Cryptography

**B. Prakash**
*Computing Technologies, School of Computing, SRM Institute of Science and Technology, India*

**A. Saranya**
*School of Computing, SRM Institute of Science and Technology, India*

**P. Saravanan**
*Computing Technologies, School of Computing, SRM Institute of Science and Technology, India*

**P. Kirubanantham**
*Computing Technologies, School of Computing, SRM Institute of Science and Technology, India*

**V. Bibin Christopher**
*Computing Technologies, School of Computing, SRM Institute of Science and Technology, India*

## ABSTRACT

*Smart environments (SE) aim to improve daily comfort in the form of the internet of things (IoT). It starts many everyday services due to its stable and easy-to-use operations. Any real-world SE based on IoT architecture prioritises privacy and security. Internet of things systems are vulnerable to security flaws, affecting SE applications. To identify attacks on IoT smart cities, an IDS based on an iterative layered neuro-fuzzy inference network (ILNFIN) is presented. Initially the TON-IoT dataset was preprocessed, and the sparse wrapper head selection approach isolates attack-related features. The Iterative stacking neuro-fuzzy inference network classifies attacked data from the normal data. The asymmetric prime chaotic Rivest Shamir Adleman technique ensures the secure transmission of non-attacked data. To show the effectiveness of the suggested secure data transfer techniques, the authors compare their experimental results to existing approaches.*

DOI: 10.4018/979-8-3693-1642-9.ch014

## 1. INTRODUCTION

The Internet of Things (IoT) has gained significant popularity in several regions worldwide in recent times. The projected number of Internet of Things (IoT) devices by 2030 is predicted to reach 125 billion, with the current number of linked devices already surpassing 27 billion this year. Smart city apps facilitate the connection between many IoT devices and tangible items in the real world, resulting in a substantial influence on urban life. Administering IoT networks in the future will be a significant challenge due to the vast quantity of IoT devices spanning many technologies and protocols, including Wired/Wireless, Satellite/Cellular, Bluetooth/Wi-Fi, and more. As a result, the personal information of citizens is in danger owing to significant cyber security concerns and weaknesses that might be taken advantage of. Irrespective of the user or administrator's awareness, these cyber threats may gain entry to Internet of Things devices. Consequently, smart city applications are susceptible to two primary hazards. Detecting zero-day attacks in a smart city's cloud data centre poses an initial hurdle due to the diverse range of IoT protocols and the potential for large-scale attacks to be concealed inside IoT devices. By using a sophisticated method for detecting cyber-attacks, it is possible to identify IoT malware assaults in advance, hence preventing their impact on a smart city via the IoT networks. At now, Internet of Things (IoT) sensors are gathering the whole of the data that is being sent via the large volume of data currently being processed on cloud servers by the majority of the sensors currently in operation. Conventional intrusion detection systems (IDS) are unsuitable for devices with restricted resources and capabilities (Haseeb et al., 2020; Kolivand et al., 2021; Saba, 2020; Saba, Sadad, Rehman et al, 2021; Yar et al., 2021).

### 1.1 The internet of things (IoT)

Devices are linked to the internet via the Internet of Things in order to exchange information via authorised protocols. Consequently, all information may be retrieved at any given moment and from any place. Microscopic sensors integrated into common objects provide the fundamental infrastructure of an Internet of Things (IoT) network. IoT devices are capable of intercommunication without the need for human intervention. Figure 1 depicts the potential applications of IoT in several domains such as health monitoring, intelligent settings, residential automation, urban infrastructure, and wearable technology.

Smart cities use IoT-enabled technology communications to optimise operational efficiency, enhance the quality of services offered, and improve the overall quality of life for residents (Al-Hamar et al., 2021; Rehman Khan et al., 2022). With the increasing use of Internet of Things (IoT) technology, there is a rising number of expressed concerns. The issue of IoT security is of utmost importance and requires immediate attention, along with several other concerns. Massive cloud servers are connected to sensors.

Smart cities are vulnerable to attacks due to the presence of Internet of Things (IoT) devices. IoT devices may be accessed from any location via untrusted networks, such as the internet. In other words, the Internet of Things (IoT) is susceptible to a diverse range of risks. Figure 1 illustrates the many components of the Internet of Things.

### 1.2 The Smart City

"The smart city's technology, population, and infrastructure are all vital aspects of a city. Cities may be characterized as digital cities, omnipresent cities, or even as smart communities depending on their degree of functionality. Smart cities are those that have high levels of emphasis and operational effi-