Chapter 52
Computer Forensic Investigation in Cloud of Things

A. Surendar
Vignan's Foundation for Science, Technology and Research (Deemed to be University), India

ABSTRACT

Digital data transformation is most challenging in developing countries. In recent days, all the applications are functioning with the support of internet of things (IoT). Wearable devices involve the most insightful information, which includes individual healthcare data. Health records of patients must be protected. IoT devices could be hacked, and criminals use this information. Smart cities with IoT use information technology to collect, analyze, and integrate information. Smart reduces the network traffic using the ground sensors, micro-radars, and drones monitor traffic to the traffic controller based on that signals are designed. The data collected includes the images and convey information to smart vehicles, which in turn, if data are hacked, may affect many people. Smart city includes important features such as smart buildings, smart technology, smart governance, smart citizen, and smart security. Cyber threat is a challenging problem, and usage of apps may increase malware that affects various customers.

INTRODUCTION TO IoT

The issue of security is becoming more crucial as IoT devices are becoming more relevant in people's lives. IoT devices may not be as secured as other traditional devices connected to the internet because of their sizes and restrictions on power, the increasing number of connected devices is bound to create challenges that are new and will thus require innovative security approaches (Elmaghraby, & Losavio, 2014). From a legal point of view, there are legal issues associated with the IoT which are not clear and require interpretation, notable amongst them being the impact that location has on privacy regulation and issues associated with ownership of data in the cloud as the data on IoT is stored in the cloud (Fremantle & Scott, 2015). Other challenges that could be associated with IoT devices include authentication, integrity, access control and confidentiality (Marinescu, 2017). Physical threats like theft and tampering, logical threats like denial of service and viruses are threats that can be directed at IoT based devices (Bos

DOI: 10.4018/978-1-7998-2466-4.ch052

et al., 2009). As Data is kept on sites in the cloud, it is vulnerable to attacks such as SQL injection, side channel attacks and man in the middle attacks amongst others (Oriwoh et al., 2013). Today, discussions around IoT typically focus on applications, benefits and privacy, while there isn't much talk about incident response and forensic investigations. The need for an intelligent, adaptable forensic methodology to investigate IoT-related crimes, however, is becoming pertinent.

SMART CITY INFRA STRUCTURE DESIGN WITH SECURED INFORMATION TRANSFER

The security and privacy of information in a smart city has been interest of researchers. The reason behind it is that, in order to ensure the continuity of critical services like health care, governance and energy/utility issues in a smart city, the information security must be fool proof. The factors that are taken under consideration in order to identify the issues in information security in a smart city include governance factors, social/economic factors and most importantly economic factors. The researchers identify, explain and propose solutions to the information security issues by considering the mentioned factors. The IoT has been the key interest of the researchers as it is the core technology on which the smart cities are being developed and maintained (Mattern & Floerkemeier, 2010). For instance, in Marinescu (2017), the key hurdles and problems faced regarding security and privacy are discussed, keeping in the context of technological standards. This chapter particularly focuses on Machine to Machine (M2M) standard solutions that are helpful in better implementation of IoT in a smart city.

Though the mathematical and graphical model for the IoT, people and servers is given stating that it will help in locating the problems in security and privacy, but the methodology to do so is not discussed. Moreover, Mell and Grance (2011) propose a distributed framework for IoT applications, which promises security, trust and privacy in information delivery. As IoT applications play a key role on building the smarter city, so some information security issues in a smart city can be addressed through the distributive framework.

Data Security in Smart Cities: Challenges and Solutions

Trends as hyper connectivity, messy complexity, loss of boundary and industrialized hacking transform smart cities in complex environments in which the already-existing security analysis are not useful anymore. Specific data-security requirements and solutions are approached in a four-layer framework, with elements considered to be critical to the operation of a smart city: smart things, smart spaces, smart systems and smart citizens.

Data Vulnerabilities in a Smart City

Smart Things: In a smart city, objects are connected in order to provide seamless communication and contextual services. A large variety of things are used in a smart city. Data collected by smart things are at the heart of smart cities. The problem is that they are sensitive data, often gathered without our explicit consent. For example, messages, personal pictures, appointments, bank account information, contacts and others are stored in our smart phones in full awareness, with more or less security measures put in place.