Chapter 11
Computer Forensic Investigation in Cloud of Things

A. Surendar

https://orcid.org/0000-0002-2421-9192

Vignan's Foundation for Science, Technology & 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 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.

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/computer-forensic-investigation-in-cloud-of-things/224452

Related Content

High Performance Scheduling Mechanism for Mobile Computing Based on Self-Ranking Algorithm

Hesham A. Aliand Tamer Ahmed Farrag (2006). *International Journal of Information Technology and Web Engineering (pp. 43-59).*

www.irma-international.org/article/high-performance-scheduling-mechanism-mobile/2607

Multi-Disciplinary Research Issues in Cloud Computing

Jitendra Singhand Vikas Kumar (2016). *Web-Based Services: Concepts, Methodologies, Tools, and Applications (pp. 2197-2220).*

www.irma-international.org/chapter/multi-disciplinary-research-issues-in-cloud-computing/140895

Image Mining: A Case for Clustering Shoe prints

Wei Sun, David Taniarand Torab Torabi (2008). *International Journal of Information Technology and Web Engineering (pp. 70-84).*

www.irma-international.org/article/image-mining-case-clustering-shoe/2642

An Improved Multilinear Map and its Applications

Chunsheng Gu (2015). *International Journal of Information Technology and Web Engineering (pp. 64-81).*

www.irma-international.org/article/an-improved-multilinear-map-and-its-applications/145841

Semantic Web in Ubiquitous Mobile Communications

Anna V. Zhdanova, Ning Liand Klaus Moessner (2010). *Web Technologies: Concepts, Methodologies, Tools, and Applications (pp. 41-62).*

www.irma-international.org/chapter/semantic-web-ubiquitous-mobile-communications/37624