Chapter 5
Cross-Layer Learning:
A Deep Learning-Based Forensic Framework for IoT Systems

Tushar Mane
Symbiosis Institute of Technology, Symbiosis International University (Deemed), India

Ambika Pawar
Symbiosis Institute of Technology, Symbiosis International University (Deemed), India

ABSTRACT

Deep learning-based investigation mechanisms are available for conventional forensics, but not for IoT forensics. Dividing the system into different layers according to their functionalities, collecting data from each layer, finding the correlating factor, and using it for pattern detection is the fundamental concept behind the proposed intelligent system. The authors utilize this notion for embedding intelligence in forensics and speed up the investigation process by providing hints to the examiner. They propose a novel cross-layer learning architecture (CCLA) for IoT forensics. To the best of their knowledge, this is the first attempt to incorporate deep learning into the forensics of the IoT ecosystem.

INTRODUCTION

Along with the exponential growth of the IoT, there has been a surge in security and privacy breaches as well. A survey conducted by Hewlett Packard depicts 70% of the investigated IoT applications contain security and privacy breaches (Rawlinson,

DOI: 10.4018/978-1-7998-8386-9.ch005

2014). The well-known Mirai botnet attack, which caused severe Denial- of- Service (DoS) for thousands of IoT devices in America is another notable case (*Mirai (malware) - Wikipedia*, n.d.). As the IoT systems are being deployed rapidly, it is quite clear that there is a need for research in the IoT forensics. Although existing forensic techniques and tools are still found to be useful in some phases of the IoT forensics, there is still a desperate need to upgrade existing tools, methodologies, and legislation to tackle the characteristics of IoT. IoT security altogether a different type of security approach, as it deals with the light-weight computing devices which are connected to the cloud. IoT security architecture and communication standards are discussed thoroughly in (Silva et al., 2019). Challenges and research opportunities for IoT security are highlighted in (Ryan & Watson, 2017) . Traditional security methodologies are not sufficient to secure IoT security (Fernandes et al., 2017). IoT security understanding is unquestionably valuable in the field of IoT forensics, nevertheless, tracing the root cause, collecting evidence, and correlating it in the end to end IoT system entails aid of the machine intelligence.

Deep learning is proving to be more robust and accurate in comparison with the rest of the machine learning techniques due to the support of larger datasets (Q. Zhang et al., 2018). Deep linking in IoT environments is achievable with the help of deep learning (Fadlullah et al., 2017). Deep Linking Protocol enables IoT objects and applications to interact involuntarily with each other. Smart home example (Li et al., 2018) gives an idea of how things in a smart home can collaborate to form a system. As of now, deep learning has been applied in Network Forensics only. We believe Deep learning assisted investigation of end-to-end IoT applications will certainly help speed up the investigation process with fewer errors and leftovers. Notable contributions of our study are as follows:

- We provide a compact description of prerequisite areas of deep learning assisted IoT forensics, such as- IoT, IoT security, digital forensics, deep learning, and its application in the aforementioned area.
- Further, we do a comparative study of existing IoT Forensic models and highlight the uniqueness of the proposed model.
- A Comprehensive study on contributions which inspired us to device Deep Learning assisted IoT Forensics.
- We coin Cross-Layer Learning Architecture (CLLA) for IoT Forensics. It studies the correlation between the layers to analyze the attacks. By establishing links it hints probability and priority value of each layer to the investigator.
- Thorough research directions, opportunities, and challenges are presented to encourage researchers in a related area.

Related Content