GROVE SCHOOL
OF ENGINEERING

CSE H0240: Law and Policy Issues in Cybersecurity

Position Paper On
Privacy, Security and Surveillance

Created By:

MD ABDUL KADIR

Submitted To:

Professor Benjamin Dynkin & Professor Barry Dynkin

CSE H0240 Course Instructor

Department of Cybersecurity (MS Program)

Grove School of Engineering

The City College of New York

Academic Session- Spring 2023

The surveillance video management system is rapidly expanding its scope of application at the request of citizens and the development of related technologies. In addition, as Cloud Computing and 5G networks are applied with AI, scope and function of surveillance systems are being enhanced to intelligent CCTV beyond simple monitoring. However, intelligent CCTV systems with Mobile Edge Computing and 5G, which have the risk of privacy infringement. Accordingly, it is necessary to identify various types of security threats that can occur through the cloud based surveillance system and to eliminate the risk of privacy and personal information breaches. There are increased demands for national security and public safety with intelligent surveillance systems. CCTV is one of the systems that monitors disaster and accidents. Recently, video monitoring through not only CCTV but also various mobile devices is rapidly increasing for city control. Moreover, the 5G network is deployed widely, large amounts of real-time video data can be processed quickly and various video analysis can be done through hierarchical cloud architecture.

Video surveillance cameras are pervasive in public places in response to growing security concerns. According to a report produced by IHS Markit, there are about 245 million surveillance cameras in operation today. London is the city with the highest number of cameras, where an average Londoner is estimated to be caught on camera 300 times a day. The number in China is expected to grow more than three times by the year 2020. Clearly individuals' privacy is at stake! People are being observed with or without their awareness almost wherever they go. This situation widely incurs concerns in the violation of individual's privacy.

The more powerful the modern surveillance cameras become, the more likely they are to be abused to gather private information. Authorized security personnel in charge of the surveillance system might abuse the cameras for voyeurism, cyber stalking, and unauthorized collection of data on activities or behaviors of individuals. Maneuverable cameras, like pan-tilt-zoom (PTZ) cameras, could be abused and directed to intrusively spy on other people in their apartments. For instance, there was an investigation launched after a security guard spied on the private apartment of the German Chancellor Angela Merkel using a museum's closed circuit television (CCTV) camera. Obviously, while the benefits of surveillance greatly outweigh the potential risks, surveillance and the privacy of people should be balanced out. There have been a number of efforts to address the privacy requirements through the introduction of smart cameras with embedded privacy curtailments in lieu of trying to abandon the practice of surveillance. However, a resource and bandwidth aware privacy-protection mechanism is still missing in most surveillance camera systems today.

Witnessing the increasingly pervasive deployment of security video surveillance systems(VSS), more and more individuals have become concerned with the issues of privacy violations. While the majority of the public have a favorable view of surveillance in terms of crime deterrence, individuals do not accept the invasive monitoring of their private life. To date, however, there is not a lightweight and secure privacy-preserving solution for video surveillance systems. The recent success of blockchain (BC) technologies and their applications in the Internet of Things (IoT) shed a light on this challenging issue. In this position paper, a lightweight blockchain-based privacy protection (Lib-Pri) scheme for smart surveillance at the edge I want to add as my opinion. It enables the construction of a privacy-aware smart surveillance system by integrating the advanced features of BC and smart contract with object detection (OD) technologies coupled with image scrambling techniques. The Lib-Pri system consists of three major parts in this privacy and resource aware service: smart cameras, BC nodes and users. The smart cameras are the edge devices with an embedded configurable set of privacy policies. The cameras capture videos and process them using the attached single board computer (SBC), e.g. the new Jetson Nano Module, a Tinker board or Raspberry Pi. Privacy-sensitive objects are detected and corresponding privacy protection measures are enforced. The BC network ensures authenticity. Users are assigned with different levels of access privileges to the videos, which are defined in the smart contracts. In addition, an isolated storage system is considered for the storage of reversibly scrambled images or videos for law enforcement purposes.

Security cameras are very easy to compromise due to the weak physical protection on-site. In some situations, the attacker is capable of capturing/damaging one or more cameras located in the target area. We call such a type of attacks *geo-range* attacks. *Geo-range* attacks pose a new challenge for developing a robust and privacy-preserving storage system for surveillance cameras.

I am aiming to find a general solution that can be used in both stationary cameras and mobile cameras. We assume that the cameras are connected via a wired or wireless network, and the security in the communication system is guaranteed by some existing solutions. Ideally, the camera system should have the following properties:

- **Robust**: Even if an attacker damages a subset of cameras, the video files from these cameras can still be recovered.
- **Privacy-preserving**: The attacker cannot view the content of a camera even if she has physical access to the camera and the local storage.