Chapter 20
Innovative Approaches to Public Safety: Implementing Generative Adversarial Networks (GANs) for Cyber Security Enhancement in Public Spaces

Anita Chaudhary
https://orcid.org/0009-0002-5815-5331
Eternal University, India

ABSTRACT

This book chapter examines cutting-edge tactics to improve public safety by using Generative Adversarial Networks (GANs) to improve cyber security in public areas. Conventional security solutions frequently fail to provide adequate protection against cyber-attacks in public settings in an era characterized by growing digital interconnection and changing security risks. Using GANs, a state-of-the-art machine learning method, offers a viable way to strengthen cyber security measures and reduce possible threats. The chapter explores the theoretical underpinnings of GANs and how they are used to identify and neutralize cyber threats in public areas. Through the utilisation of GANs to produce artificial intelligence-generated data and replicate cyber-attack scenarios, entities can anticipate weaknesses and develop resilient protection strategies in advance.

INTRODUCTION

Modern metropolitan landscapes would not be complete without public areas, which operate as centers of social interaction, business, and recreation. But as these areas become more digitalized, it is now crucial to ensure cyber security. Innovative solutions are required since traditional security measures are frequently insufficient to protect public places against cyber threats.

This chapter presents a new method for enhancing cyber security in public areas by using Generative Adversarial Networks (GANs). GANs are a state-of-the-art machine learning approach that provides

DOI: 10.4018/979-8-3693-3597-0.ch020

promising avenues to improve cyber security measures by simulating cyber-attack scenarios with data generated by artificial intelligence.

Novel approaches to successfully minimize potential threats are urgently needed in view of the growing cyber hazards and vulnerabilities in public spaces. This suggested approach seeks to address these issues and strengthen public space cyber security infrastructure by utilizing GANs, protecting vital resources and guaranteeing public safety.

GAN Architecture

A Generative Adversarial Network (GAN) is composed of two primary parts, which are the discriminator and the generator. To produce realistic data samples, these elements collaborate in a competitive way. An outline of the architecture is shown below:

Generator: Using random noise as input, the generator network creates synthetic data samples that closely mimic real data. Many neural network layers, such as fully linked or convolutional layers, are usually included. The generator has to figure out a way to link the space of realistic data samples to the random noise vector.

Discriminator: Distinguishing between actual data samples and those produced by the generator, the discriminator network functions as a binary classifier. It receives samples as input, both produced and real, and generates a probability score that represents the likelihood that the sample is real. The discriminator is made up of several layers of neural networks, just like the generator.

Literature Survey

The growing digitization of public areas in recent years has raised questions over cyber security flaws and its effects on public safety. In a thorough analysis titled "Cyber security Challenges in Public Spaces: A Comprehensive Review," (Wang et al., 2019) emphasized how constantly changing cyber threats affect vital infrastructure, including government buildings and transit hubs. The study underlined how novel

Figure 1. Architecture of generative adversarial network (GAN)