Presentation Title: Fake Profile Detection on social media using Generative Adversarial Networks (GANs)

Presenting Student: Edidiong Akpan

T Number – T01327827

Program: Information Technology

Faculty/mentor name: Indira Dutta

Abstract: Generative Adversarial Networks (GANs) is an artificial intelligence framework used to make computers inventive. This has been applied in several areas of security such as intrusion detection systems. With the wave of globalization and increased social media presence, security has become a thing of concern. For instance, social media security breaches and faking has become one of the many things people are subjected to ranging from impersonation, cyberbullying, stalking, fraud, fleecing of personal assets, and issuing online threats behind fake profiles, these fake profiles are created either by hacking an existing account or by copying the lifestyle and events shared to create a duplicate in other to perpetuate their crimes. People of all backgrounds and genders are creating and making updates on social networks in growing numbers. Millions of individuals follow them across several profiles. However, the use of fake profiles to pollute online channels is becoming more prevalent. Fake profiles often spam regular users with offensive or illegal content. Several indicators might help you know a social media impersonator who is attempting to mislead you. It is no longer news that social media accounts of users can be accessed and used without the authority of the owner. These are done on users who use guessable passwords like date of birth, middle name, or the names of their pet. However, others go the length of using applications to develop a prototype of your account but for negative intentions by using the APP called FAKED. Common cybercrime attacks used include Service interruption, Ransomware, Malware, and Phishing. Leaked data most of the time end up in the dark web. This is where it is used for criminal purposes such as password cracking, credential stuffing, and phishing. Hackers

cause data breaches on social media to set up mirror profiles of unsuspecting victims to launch targeted phishing attacks. This information is also used by cybercriminals to send spam to email addresses and phone numbers, as well as brute-force credentials for social media accounts and email addresses. Identity fraud and theft occur because of a data breach that accumulates enough personally identifiable information (PII). Due to the increase in data breaches, these threats are becoming more prevalent online. This research applies GANs to detect fake profiles and combat the menace of social media crimes in the long run. The generator and discriminator models are used by GANs to train themselves using fake profiles. It will learn the algorithm of these fake profiles and the relationship that exists between the bio information, profile picture, messages sent out, and followers by repeatedly training generative models with replicated examples of the original counterfeit profiles. After generating these fake profiles, it then uses the technique to detect and classify profiles. The generator and discriminator models will be subjected to the performance of a system to determine the for accuracy detecting fake profiles.