Chapter 22
Novel Approaches for Secure Data Packet Transmission in Public Spaces via GANs and Blockchain

M. Islabudeen
https://orcid.org/0000-0002-0811-450X
Vellore Institute of Technology, India

B. Lalithadevi
https://orcid.org/0000-0002-4491-4707
Sathyabama Institute of Science and Technology, India

S. Aruna
https://orcid.org/0000-0002-1052-3572
Dayananda Sagar College of Engineering, India

M. Mohamed Sithik
Mohamed Sathak Engineering College, India

K. Baskar
Kongunadu College of Engineering and Technology, India

ABSTRACT

In today's digitally connected world, giving secure data packet transmission in public spaces is paramount. Traditional encryption methods have limitations when it comes to protecting sensitive records from sophisticated cyber threats. This chapter proposes a novel approach leveraging generative adversarial networks (GANs) and block formed chain structured technology to enhance data packets security in public spaces. The proposed methodology, dubbed SecureGANChain, utilizes a machine learning-driven algorithm to encrypt and transmit data packets securely across public networks. SecureGANChain harnesses the power of GANs to generate encryption keys dynamically, making it extremely difficult for adversaries to intercept or decipher transmitted data packets. Additionally, block formed chain structured technology is employed to create a tamper-proof and immutable ledger, giving the integrity and authenticity of transmitted data packets.

DOI: 10.4018/979-8-3693-3597-0.ch022

INTRODUCTION

In today's digital age, the transmission of data packets plays a crucial role in our daily lives. Whether it's passing a message, sharing photos, or accessing records online, data packets transmission enables communication and interaction across the globe. In simple terms, data packets transmission refers to the process of passing and receiving records in digital form over various communication channels, such as the internet, mobile networks, or Wi-Fi. Every time we browse the web, make a phone call, or stream a video, data packets is being transmitted from one device to another. This process involves converting data packets into electronic signals, passing them through a medium like cables or wireless networks, and then decoding them back into usable records at the receiving end. From emails to social media updates, data packets transmission enables the seamless exchange of records that powers our interconnected world.

The importance of data packets transmission extends beyond personal communication. Businesses rely on it to conduct transactions, share documents, and collaborate with colleagues remotely. Governments use it to disseminate public records, monitor infrastructure, and provide essential services to citizens. Moreover, the rise of smart devices and the Internet of Things (IoT) has further increased the demand for efficient and secure data packets transmission, as these devices constantly exchange data packets to automate tasks and improve functionality.

However, with the convenience of digital communication also come concerns about data packets security and privacy. As data packets travels through various networks and devices, it becomes vulnerable to interception, manipulation, or un-authenticated access. Cyberattacks, data packets breaches, and surveillance are just some of the risks associated with data packets transmission in the digital age. Therefore, giving the security and integrity of data packets transmission is essential to protect sensitive records and maintain trust in the digital ecomethodology . In this way, we will explore the challenges and advancements in data packets transmission, as well as the technologies and strategies used to secure and optimize this critical process in our increasingly connected world. We will delve into the role of encryption, protocols, and emerging technologies such as block formed chain structured and machine learning in enhancing the reliability and security of data packets transmission. By understanding the complexities and implications of data packets transmission, we may better navigate the digital forms and harness its potential for innovation and progress.

Chances of Data Packets Threats

In today's digital world, data packets threats pose significant challenges to individuals, businesses, and governments alike. These threats encompass a wide range of malicious activities aimed at compromising the confidentiality, integrity, and availability of data packets. From cyberattacks to data packets breaches, the chances of encountering data packets threats are ever-present, necessitating constant vigilance and proactive measures to safeguard sensitive records. One of the most common data packets threats is malware, malicious software designed to infiltrate methodologys, steal data packets, or cause damage. Malware may take various forms, including viruses, worms, ransomware often spreads through infected emails, websites, or removable media. Once installed on a device, malware may compromise the security of data packets stored on the device or transmitted over networks, leading to financial loss, identity theft, or methodology disruptions. Another significant data packets threat is phishing, a deceptive technique used to trick individuals into revealing sensitive records such as login credentials, credit card numbers, or personal details. Phishing attacks typically involve fraudulent emails, messages, or