The Role of VPN in Network Security

Mukund Sharma (IIT Patna - 2101AI19)
Biswajit Sarkar (IIT Patna - 2101AI11)
Prakash Kumar (IIT Patna - 2101AI24)

April 21, 2025

Abstract

In an increasingly digital world, securing sensitive data in transit is paramount. Virtual Private Networks (VPNs) serve as critical tools for ensuring confidentiality, integrity, and availability of information across public and private networks. By encrypting data and masking user identities, VPNs help protect individuals and organizations from various cyber threats. This paper explores the role of VPNs in modern network security frameworks, describing how they work, their types, encryption protocols, applications, challenges, and emerging trends. Case studies and real-world examples illustrate their impact, while future directions discuss the integration of VPNs with evolving cybersecurity strategies.

1 Introduction

The rapid expansion of the internet, cloud services, and remote work has drastically altered the cybersecurity landscape. Today, individuals and organizations regularly exchange sensitive information over potentially insecure networks. This has increased the demand for tools that ensure secure data transmission. One such tool is the Virtual Private Network (VPN).

A VPN provides a secure communication channel over a public network by encrypting traffic and masking the user's IP address. Initially developed for corporate use, VPNs are now integral to personal and enterprise-level security systems. From employees accessing internal resources to individuals seeking online privacy, VPNs serve diverse roles. This paper outlines the technical and strategic significance of VPNs in network security.

2 How VPNs Work

A Virtual Private Network (VPN) works by creating a secure tunnel between the user's device and a VPN server over a public network, such as the internet. This tunnel ensures that any data exchanged between the device and the server is encrypted, making it unreadable to third parties who may attempt to intercept or monitor the traffic. The process of establishing a VPN connection involves several critical steps, each contributing to ensuring the privacy and integrity of the transmitted data. The main steps involved in how VPNs work are as follows:

2.1 Authentication

Authentication is the first step in establishing a secure connection between the user's device and the VPN server. This process verifies the identity of the client device to the VPN server. There are two main types of authentication methods used:

- **Username and Password:** This is the most common authentication method, where users provide their credentials (username and password) to access the VPN server. This form is typically used for personal or remote access VPNs.
- **Certificate-based Authentication:** This method uses digital certificates to verify the client's identity. Certificates are considered more secure and are widely used in corporate and enterprise environments, where security is critical. The certificate contains a public key that the VPN server uses to authenticate the device.

Once the authentication is successful, the VPN server grants access and allows the client to initiate the creation of the secure tunnel.

2.2 Tunneling Protocols

Tunneling protocols define how data is encapsulated and transmitted over the internet. These protocols are crucial because they ensure that data is safely transported through the secure tunnel. There are several types of tunneling protocols, each offering different features in terms of speed, security, and compatibility. Some commonly used protocols include:

- **IPsec (Internet Protocol Security):** IPsec is a suite of protocols used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session. It is commonly used for site-to-site VPNs and provides robust encryption and integrity checks. IPsec is typically paired with other protocols like L2TP (Layer 2 Tunneling Protocol) to form a complete secure solution.

- **OpenVPN:** OpenVPN is an open-source protocol that uses SSL/TLS for encryption, making it highly configurable and secure. OpenVPN is widely used for remote access VPNs, as it can operate over both UDP (User Datagram Protocol) and TCP (Transmission Control Protocol), allowing for flexibility in different network environments.

- **WireGuard:** WireGuard is a newer VPN protocol that offers excellent performance and security with a simpler and more efficient codebase. It uses modern cryptographic techniques, such as the Noise Protocol Framework, and aims to provide faster connection speeds and lower overhead compared to older protocols like OpenVPN and IPsec.

- **L2TP (Layer 2 Tunneling Protocol) over IPsec:** L2TP is often combined with IPsec for secure tunneling. L2TP by itself does not provide encryption, so it relies on IPsec to secure data transmission. L2TP/IPsec is often used for site-to-site and remote access VPNs.

Each protocol has its strengths, with the choice depending on the specific requirements of security, speed, and scalability for a particular network setup.

2.3 Encryption

Once the tunneling protocol establishes the tunnel, data encryption is applied to ensure that the information transmitted over the VPN is protected from unauthorized access. Encryption scrambles data so that only the intended recipient, who holds the correct decryption key, can read it. The most common encryption algorithms used in VPNs include:

- **AES (Advanced Encryption Standard):** AES-256 is one of the most widely used encryption standards in VPNs due to its high level of security. It uses a 256-bit key to encrypt data, making it virtually impossible to crack with current computing power. AES is used in protocols like IPsec and OpenVPN.

- **RSA (Rivest-Shamir-Adleman):** RSA is an asymmetric encryption algorithm used primarily for secure key exchange. It is commonly used in the initial stages of the VPN connection to securely exchange encryption keys before the actual data transmission begins.

- **ChaCha20:** ChaCha20 is a stream cipher used in modern VPN protocols like WireGuard. It provides excellent security and is faster than AES in some environments, particularly on mobile devices.

VPNs typically use a combination of symmetric (e.g., AES) and asymmetric (e.g., RSA) encryption techniques to maximize both security and performance. The combination of secure tunneling and strong encryption ensures that data is transmitted in a secure manner, even over insecure networks.

2.4 Transmission

Once encryption is applied, the data is ready for transmission through the secure VPN tunnel. This transmission occurs in two main stages:

- **Data Encapsulation:** The data, now encrypted, is encapsulated within an IP packet and sent through the VPN tunnel. The encapsulation ensures that the data is isolated from other traffic on the network and that only the encrypted data reaches the VPN server.

- **Decryption and Forwarding:** When the encrypted data reaches the VPN server, it is decrypted using the appropriate decryption keys. The server then forwards the data to its intended destination on the internet or internal network. Similarly, responses from the destination are encrypted by the server before being sent back through the tunnel to the user's device.

The entire process ensures that both the data's confidentiality and integrity are maintained, preventing unauthorized access or tampering.

2.5 End-to-End Encryption

End-to-end encryption ensures that the data remains encrypted during the entire journey—from the user's device to the final destination, passing through the VPN server. This process is critical, especially when using public networks like Wi-Fi hotspots or untrusted networks, where the risk of data interception is high. Even if attackers manage to intercept the data in transit, they will be unable to decrypt or tamper with it due to the encryption.

This makes VPNs highly effective in protecting sensitive information, such as login credentials, financial transactions, and personal communications, from prying eyes.

3 Types of VPNs

VPNs can be categorized based on their use case and configuration. Each type of VPN is designed to address specific needs in terms of security, scalability, and flexibility. The most common types of VPNs are as follows:

3.1 Remote Access VPNs

Remote Access VPNs enable individual users to securely connect to a private network from a remote location, typically over the internet. This type of VPN is essential for telecommuting, enabling employees to access company resources, databases, and files from outside the office while ensuring that sensitive data remains protected.

Remote Access VPNs can be configured for different levels of security based on the organization's needs. Some key features include:

- **Authentication Methods:** Remote Access VPNs usually employ user authentication methods such as passwords, certificates, or multi-factor authentication (MFA) to ensure that only authorized users can access the network.

- **Encryption:** Data transmitted over Remote Access VPNs is typically encrypted using strong encryption protocols such as AES-256 to prevent unauthorized access or eavesdropping on public networks like Wi-Fi.

- **Applications:** These VPNs are widely used by employees who work remotely or need secure access to corporate systems while traveling. They are commonly used in industries such as finance, healthcare, and technology, where data security is paramount.

This type of VPN is especially useful for businesses with a distributed workforce, offering flexibility and security while ensuring data integrity.

3.2 Site-to-Site VPNs

Site-to-Site VPNs, often referred to as *gateway-to-gateway* VPNs, connect two or more networks securely over a public network, such as the internet. These VPNs are typically used to link the networks of different offices, branches, or remote locations of a company, allowing them to communicate securely as if they were part of the same local network.

There are two main types of Site-to-Site VPNs:

- **Intranet VPN:** Connects multiple offices or branch locations of the same organization. This is typically used by large enterprises to connect geographically dispersed locations securely.
- **Extranet VPN:** Connects an organization's internal network with the network of a business partner or third-party vendor. Extranet VPNs facilitate secure data sharing and collaboration between organizations.

Key features of Site-to-Site VPNs include:

- **Network-Level Security:** Site-to-Site VPNs provide a high level of security as they encrypt traffic between entire networks. This means that all devices within a network can securely communicate without the need for individual VPN connections.
- **Scalability:** Site-to-Site VPNs are scalable, making them ideal for organizations with multiple locations or offices. New sites can be added to the network without significant configuration changes.
- **Tunneling Protocols:** Common protocols used in Site-to-Site VPNs include IPsec, GRE (Generic Routing Encapsulation), and MPLS (Multiprotocol Label Switching).

Site-to-Site VPNs are commonly used by medium and large organizations to connect multiple branches securely, ensuring seamless communication between locations.

3.3 Client-to-Site VPNs

Client-to-Site VPNs are a hybrid model that combines aspects of both Remote Access VPNs and Site-to-Site VPNs. This model allows a client device, such as a laptop or smartphone, to securely connect to an organization's network. Unlike Remote Access VPNs, where each user is individually authenticated, Client-to-Site VPNs can be used to connect a small number of devices to a larger network, often in a more centralized or enterprise-specific setup.

Key features include:

- **Secure Connection for Specific Devices:** This type of VPN is designed for organizations that want specific client devices (such as company-issued laptops) to have secure access to internal resources while maintaining a more controlled network perimeter.
- **Scalability for Smaller Deployments:** Client-to-Site VPNs are particularly useful for small or medium-sized enterprises (SMEs) that require secure connections for a limited number of users or devices. It is also beneficial for businesses that need to provide secure remote access to third-party contractors or partners.
- **Centralized Control:** Unlike Remote Access VPNs, which are often used on a per-user basis, Client-to-Site VPNs offer more control over the devices accessing the network. Network administrators can manage which devices are allowed to connect and can enforce stricter security policies for those devices.

This type of VPN provides a flexible solution for organizations that need to allow secure access to a limited number of remote users or client devices.

3.4 Cloud VPNs

Cloud VPNs provide secure, encrypted connections between local networks and cloud environments or between different cloud-based infrastructures. This type of VPN is especially useful for businesses that have hybrid infrastructures, combining on-premises data centers with cloud services, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud.

Key features of Cloud VPNs include:

- **Secure Cloud Access:** Cloud VPNs allow users to access cloud resources securely by establishing encrypted tunnels between on-premises networks and cloud platforms. This is particularly important for businesses that need to maintain sensitive data in the cloud while ensuring compliance with data protection regulations.

- **Integration with Cloud Services:** Cloud VPNs are tightly integrated with cloud infrastructure providers, allowing for seamless and secure access to cloud-based applications and data. Providers such as AWS, Azure, and Google Cloud offer native Cloud VPN solutions to facilitate secure connections.

- **Scalable for Cloud Environments:** Cloud VPNs are designed to scale with cloud environments, offering flexibility for growing businesses that rely heavily on cloud services. They can connect multiple cloud regions or data centers while maintaining security across distributed networks.

- **Dynamic IP Support:** Many Cloud VPN solutions are designed to work with dynamic IPs, ensuring seamless connectivity even when IP addresses change frequently.

Cloud VPNs are ideal for businesses with hybrid or multi-cloud infrastructures that need secure, encrypted connections between on-premises networks and cloud-based services.

4 VPN Protocols and Encryption

4.1 VPN Protocols

VPN protocols define how data is encapsulated, encrypted, and transmitted between the client and server, ensuring secure communication over untrusted networks. Common VPN protocols include:

- **IPsec:** The Internet Protocol Security (IPsec) protocol suite is widely used for securing IP communications by authenticating and encrypting each IP packet in a communication session. It is commonly employed in site-to-site VPNs, where it ensures the security of the connection between multiple network gateways. IPsec supports both transport and tunnel modes, offering flexibility for different network architectures.

- **OpenVPN:** OpenVPN is an open-source protocol that uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for encryption, making it highly flexible and customizable. It supports a range of encryption algorithms and can be used in both remote access and site-to-site VPNs. OpenVPN is popular for its robust security, extensive configurability, and ability to bypass network restrictions, such as firewalls.

- **WireGuard:** A newer VPN protocol, WireGuard has gained attention due to its simplicity, speed, and security. It features a lean codebase, which minimizes the potential for security vulnerabilities and offers faster performance compared to traditional protocols. WireGuard is designed to be easy to deploy and maintain, with a focus on modern cryptography standards.

- **L2TP/IPsec:** The Layer 2 Tunneling Protocol (L2TP) is commonly paired with IPsec for added security. While L2TP itself does not provide encryption, it establishes a tunnel for secure data transmission, and IPsec provides the encryption layer. This combination is often used in remote access VPNs and offers a high level of security for users, though it can be slower than some other protocols due to the double encapsulation of data.

4.2 Encryption Algorithms

Encryption algorithms are fundamental to VPN security, as they protect the confidentiality and integrity of transmitted data. Some of the most commonly used encryption algorithms in VPNs are:

- **AES-256:** The Advanced Encryption Standard (AES) with a 256-bit key is a symmetric encryption algorithm considered highly secure and efficient. It is widely used in VPNs due to its robustness against brute-force attacks and its performance, even on lower-powered devices. AES-256 is often the encryption standard of choice for securing sensitive data in both commercial and government applications.

- **RSA:** RSA is an asymmetric encryption algorithm used primarily for secure key exchange during the VPN handshake process. RSA relies on a pair of public and private keys, allowing secure transmission of keys over an untrusted network. It ensures that the keys used for encryption are shared securely between the client and server.

- **SHA-2:** The Secure Hash Algorithm 2 (SHA-2) family is used for ensuring data integrity and authenticity. It is a cryptographic hash function that produces a fixed-size output (the hash), which is unique for any given input. SHA-2 ensures that transmitted data has not been tampered with, offering protection against man-in-the-middle attacks.

Together, these protocols and encryption algorithms form the foundation of VPN security, providing data confidentiality, integrity, and authentication for users across the globe.

5 Applications and Benefits of VPNs

VPNs have widespread applications across various domains, offering both personal and organizational benefits. Some of the key applications include:

- **Secure Remote Work:** VPNs provide a secure method for employees to access internal systems and sensitive data from remote locations, such as their homes or while traveling. By establishing an encrypted connection, VPNs protect against data breaches and ensure that corporate resources remain secure, even when accessed over public or less secure networks. This has become increasingly important with the rise of telecommuting and hybrid work environments, where employees need to connect securely to the company's internal network from various locations.

- **Protection on Public Networks:** One of the most common uses of VPNs is securing data transmissions when connected to public Wi-Fi networks, such as those found in airports, cafes, or hotels. These networks are typically unsecured, making them vulnerable to eavesdropping and man-in-the-middle attacks. By encrypting data traffic, VPNs ensure that sensitive information, such as login credentials and financial transactions, remain protected from hackers and malicious actors on the same network.

- **Geo-restriction Bypass:** VPNs allow users to bypass geographical restrictions imposed by websites and streaming services. By masking the user's real IP address and routing the traffic through a server in a different country, VPNs make it appear as though the user is located in a region where the content is accessible. This is particularly useful for accessing geo-restricted services like Netflix, Hulu, or BBC iPlayer, enabling users to enjoy content that would otherwise be unavailable in their location.

- **Compliance:** Many industries and organizations are required to comply with strict data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the United States. VPNs help organizations meet these regulatory requirements by ensuring that sensitive data, such as personal health information or financial records, is transmitted securely. This is crucial for maintaining compliance with privacy laws and protecting customers' and clients' data from unauthorized access or breaches.

In addition to these applications, VPNs provide several key benefits, including:

- **Enhanced Privacy:** VPNs help users maintain privacy by masking their real IP address and encrypting their online activities. This prevents websites, ISPs, and even government agencies from tracking users' browsing behavior and identifying their geographical location. Enhanced privacy is particularly important for individuals who value anonymity or who live in countries with restrictive internet policies.
- **Encrypted Communication:** VPNs ensure that all data transmitted between the user's device and the VPN server is encrypted, making it unreadable to any third parties. This encryption ensures that sensitive communications, such as business transactions, personal correspondence, or confidential research, remain secure from hackers, cybercriminals, or other unauthorized entities.
- **Reduced Attack Surfaces:** By using a VPN, users can protect their devices from various cyber threats by reducing the potential attack surface. VPNs can shield users from targeted attacks by masking their IP addresses and protecting data in transit, thereby making it more difficult for attackers to launch successful cyberattacks. Additionally,

VPNs can prevent certain types of malware or spyware from compromising users' devices by encrypting the data and traffic before it reaches the target network.

6 Limitations and Challenges

Despite their significant advantages, VPNs are not without limitations and challenges. These issues can affect their performance, security, and ease of use. Some of the key limitations are:

- **Performance Issues:** The encryption and decryption processes involved in VPN usage can introduce overhead, potentially reducing connection speeds. This is particularly noticeable when using strong encryption algorithms like AES-256, which, while secure, require significant computational power. The geographical distance between the client and the VPN server can also contribute to latency and slower speeds. These performance issues can impact activities like video streaming, online gaming, and large file transfers, making it essential to choose VPN servers strategically to minimize speed degradation.

- **Single Point of Failure:** A VPN server acts as the central point for all encrypted traffic between the client and the destination. If the VPN server is compromised or experiences downtime, it could disrupt service and expose sensitive data. Attackers could target the VPN server to gain access to decrypted traffic or launch Denial of Service (DoS) attacks, thereby rendering the VPN ineffective. To mitigate this, organizations often deploy multiple VPN servers in different locations and ensure redundancy, but the risk remains a challenge.

- **Complex Setup:** Setting up a VPN can be technically challenging, especially for non-experts. Configuring the right tunneling protocols, encryption settings, and server options is crucial to ensure the VPN's security and performance. Incorrect configurations, such as weak encryption or exposed ports, can create vulnerabilities, potentially leaving the network open to attacks. Organizations often require dedicated IT support to ensure proper deployment and to handle any issues that arise. This complexity increases when scaling VPN usage across large organizations with diverse network needs.

- **Scalability:** Traditional VPNs may face difficulties when scaled to accommodate large numbers of users or devices. As the number of simultaneous connections grows, VPN servers may become overloaded, leading to performance degradation or connectivity issues. Additionally, in large-scale enterprise networks, VPNs may struggle to integrate with cloud infrastructures or multi-cloud environments. Newer technologies like Software-Defined WAN (SD-WAN) and Secure Access Service Edge (SASE) are emerging as alternatives that can address scalability challenges, but traditional VPNs may not be as effective in high-demand, large-scale deployments.

While these challenges exist, they can often be mitigated with careful planning, choosing appropriate protocols, optimizing server locations, and integrating VPNs into broader security frameworks that include monitoring, redundancy, and other protective measures.

7 Case Studies

7.1 COVID-19 and Remote Work

The COVID-19 pandemic led to an unprecedented surge in remote work, with companies worldwide shifting to online operations almost overnight. As a result, the demand for VPNs skyrocketed, as organizations sought secure methods for their employees to access corporate resources from home. VPNs played a crucial role in ensuring that employees could maintain secure connections to company networks, safeguarding sensitive data and business continuity.

The sudden transition to remote work exposed vulnerabilities in existing security frameworks, as many businesses had to quickly scale their VPN infrastructure to accommodate a larger remote workforce. This increased the pressure on IT departments to ensure that VPNs were properly configured to handle the increased load while maintaining security. VPNs enabled encrypted communications over public and private networks, protecting data from potential cyber threats such as man-in-the-middle attacks and unauthorized access to corporate systems. The pandemic highlighted the importance of VPNs in supporting a flexible, secure work environment and underscored the need for businesses to prioritize security as remote work became more prevalent.

7.2 NordVPN Breach (2018)

In 2018, NordVPN, one of the leading consumer VPN providers, suffered a significant breach involving a third-party data center. The breach occurred when an attacker gained unauthorized access to a server located in a data center in Finland that NordVPN used to host its infrastructure. The attacker exploited a vulnerability in the data center's physical security measures, allowing them to gain access to the server.

While no user data was compromised in the breach, the incident revealed critical weaknesses in VPN infrastructure, especially concerning third-party vendor management and data center security. NordVPN responded by severing ties with the affected data center provider and conducting a comprehensive audit of their infrastructure to ensure that similar vulnerabilities were not present elsewhere. The breach underscored the importance of securing not only the VPN software and network but also the underlying infrastructure and third-party partners.

This event also highlighted the need for VPN providers to implement rigorous security practices, such as regular independent security audits, multifactor authentication for internal systems, and improved physical security for data centers. As VPN services continue to grow in popularity, this breach served as a wake-up call for both providers and consumers, emphasizing the need for trust in the security practices of the VPN services they use.

8 Future Trends

The role of VPNs is continuously evolving as new technologies emerge and the cybersecurity landscape changes. Some of the key future trends in VPN technology include:

- **Integration with SASE (Secure Access Service Edge):** SASE is an emerging cybersecurity architecture that combines networking and security services into a single, cloud-delivered solution. This model integrates VPN functionality with additional services such as firewalls, secure web gateways, and zero trust network access (ZTNA). By merging these technologies, organizations can provide more comprehensive security and faster, more flexible access to applications and data. SASE simplifies network architecture by eliminating the need for separate security appliances and enables secure access from anywhere. VPNs will increasingly be a part of SASE frameworks, enhancing the overall security posture and simplifying the management of access policies across distributed networks and cloud environments.

- **Quantum-Resistant Encryption:** As quantum computing technology advances, traditional encryption algorithms like RSA and AES could become vulnerable to powerful quantum algorithms capable of breaking them. To address this potential threat, VPNs will likely adopt quantum-resistant encryption methods, which are designed to withstand the computational power of quantum computers. Research into post-quantum cryptography is already underway, with algorithms such as lattice-based cryptography showing promise in protecting data against future quantum attacks. The integration of quantum-resistant encryption into VPNs will ensure that sensitive data remains secure in the face of future computing advances, offering long-term protection against evolving threats.

- **AI-Driven Traffic Monitoring:** As VPN traffic increases and cyber threats become more sophisticated, traditional methods of monitoring and detecting network anomalies may become less effective. The future of VPN security will likely involve the integration of artificial intelligence (AI) and machine learning (ML) algorithms to enhance traffic monitoring and threat detection. AI-driven systems can analyze vast amounts of VPN traffic in real time, identifying patterns and behaviors that may indicate a potential threat, such as malware infections or unusual access patterns. By leveraging machine learning, VPNs can continuously adapt to evolving attack strategies and provide proactive defense mechanisms, making VPN security more dynamic and responsive.

These trends highlight the ongoing evolution of VPN technology and its integration with broader security frameworks. As cyber threats become more complex, VPNs will continue to adapt and provide critical protection for data transmission, ensuring their relevance in modern cybersecurity strategies.

9 Conclusion

VPNs are indispensable tools in the realm of network security. They provide encrypted communication, mask identities, and facilitate secure access to resources. Despite some challenges, their benefits far outweigh the drawbacks when implemented correctly. As cyber threats evolve, so too will VPN technology, adapting through new protocols, AI, and integration with broader security models like Zero Trust Architecture. Organizations must consider VPNs not as standalone tools but as integral components of a layered security strategy.

10 References

- National Institute of Standards and Technology (NIST)
- Cisco Systems: VPN Technology Overview
- OpenVPN Documentation
- Ponemon Institute: Cost of a Data Breach Report 2023
- Gartner Research: Emerging Trends in Network Security

11 Appendix

11.1 VPN Protocol Comparison

Protocol	Encryption Used	Speed	Security Level
OpenVPN	AES-256, SSL/TLS	Moderate	High
IPsec	AES-256	Moderate	High
WireGuard	ChaCha20	High	Very High
L2TP/IPsec	AES-256	Low to Moderate	Medium

11.2 VPN Usage Metrics

Metric	Value
Global VPN usage growth	27% YoY
Most-used VPN protocol	OpenVPN
Industries with highest VPN adoption	IT, Finance, Healthcare
Average number of users per org VPN	500+ (mid-size orgs)

12 Statutory Declaration

We, the undersigned authors, hereby declare that this paper titled **"Role of VPN in Network Security"** is an original work completed by us as part of our academic requirements at the Indian Institute of Technology Patna. All sources of information have been properly cited and acknowledged. The work has not been submitted for publication or evaluation elsewhere and does not contain any form of plagiarism.

We affirm that this submission adheres to the ethical guidelines of academic integrity, and we bear full responsibility for its content.

Signed:
Mukund Sharma
Roll No: 2101AI19
Indian Institute of Technology Patna

Biswajit Sarkar
Roll No: 2101AI11
Indian Institute of Technology Patna

Prakash Kumar
Roll No: 2101AI24
Indian Institute of Technology Patna

Date: April 21, 2025