Cybersecurity Challenges in Net Energy Metering: Legal Frameworks and Practical Solutions

Sanika Wani[1]; Arya Shinde[2]
WIET, University of Mumbai

Rucha Patwardhan (Assistant Professor)
WIET, University of Mumbai

Abstract:- Net Energy Metering (NEM) has emerged as a key factor in Modern Energy Management, empowering consumers to produce their own electricity and return Net Excess Generation (NEG) to the grid. However, the increased usage of NEM has introduced significant network security challenges. As millions of electronic devices are interconnected through communication networks across critical power facilities cybersecurity has become a concerning factor, directly affecting the reliability of such extensive infrastructure. This paper gives an insight into the rising cyber offences associated with NEM systems, stipulates the legal framework, e-governance, and liabilities under the Information Technology (IT) Act, 2000. Categorization of potential cyber threats like Access control, database security and encryption, intrusion detection, malicious software, operating system vulnerabilities and security, application security has been highlighted. Evaluation of Time of Day (ToD) pricing mechanism focusing on real time monitoring and energy efficiency during peak and off-peak consumption. Incorporating Virtual Private Networks (VPNs) and other cybersecurity measures to safeguard the integrity and reliability of NEM systems. The paper illustrates the impact of cybercrimes on NEM, by exploring existing applications and case studies. It underscores the necessity of implementing robust cybersecurity practices to protect these systems. The objective of the paper is to raise awareness about the cybersecurity challenges encountered in NEM systems and to propose practical solutions to mitigate these risks, ensuring a safe and regulated environment for the functioning of smart grids in a progressively growing digital world.

Keywords:- *Net Energy Metering (NEM), Net Excess Generation (NEG), IT Act, VPN, Cyber Security, Time of Day (ToD), Integrity, Reliability, Advanced Metering Infrastructure(AMI), Supervisory Control and Data Acquisition (SCADA).*

I. INTRODUCTION

NEM has evolved as a vital component of modern energy management, enabling consumers to generate and contribute surplus electricity back to the grid. This decentralized approach to energy production has brought significant benefits, such as increased energy efficiency and reduced dependency on traditional power generation sources. NEM has transformed the traditional electrical grid by utilizing IT to gather data from network components, spanning from power producers to consumers, and effectively using this information to enhance the system's efficiency and reliability.

This system leverages communication and information technology for the generation, distribution, and consumption of energy. It fully integrates high-speed and bi-directional communication technologies. However, the widespread adoption of NEM systems has also introduced new cybersecurity challenges, as millions of interconnected devices within critical power infrastructure are exposed to potential cyberattacks, threatening the reliability and stability of the grid.

The critical infrastructure cyber security system mainly focuses on three key control systems such as Supervisory Control and Data Acquisition (SCADA), Process Control System (PCS) and Distributed Control System (DCS). SCADA act as the central nervous system of a wide- area control network, continuously collecting real-time data from remote units. PCS uses closed-loop control to manage ongoing tasks. A DCS combines the complexities of both SCADA and PCS.

The analog status data acquired by SCADA are utilized by an Energy Management System (EMS) in the control center to perform a wide range of system functions, including real-time control [2]. The communication system for wide-area protection and control of a power system can be compromised by component failures or communication delays.

The failure of a critical communication channel in the operational environment could hamper the ability to control or manage essential facilities, potentially leading to power outages. The development of SCADA systems has also led to concerns about cybersecurity vulnerabilities.

➢ *Cyberattacks on NEM Systems can take Various Forms such as*

- Unauthorized access to critical systems
- Exploitation of software vulnerabilities
- Manipulation of billing data

While legal frameworks like the IT Act, 2000, have been established to address these threats, some sophisticated attacks, particularly comprising advanced technologies such as VPNs, remain under-regulated. These gaps in the legal landscape pose significant risks, as attackers can use VPNs to conceal their actions, making detection and mitigation more challenging for authorities.

This paper aims to explore the cybersecurity challenges associated with NEM systems, focusing on the legal implications, penalties, and gaps in current regulations. It will analyze the advantages and disadvantages of various cyberattacks, evaluate the effectiveness of existing cybersecurity measures like VPNs, and propose practical solutions to enhance the protection of NEM systems. This study encourages a comprehensive understanding of the risks in NEM systems and offer actionable recommendations for improving their security and regulation.

II. OVERVIEW OF NET METERING SYSTEM

NEM system allows users to track and manage their electricity usage, either for residential or commercial purposes, using mobile devices. NEM offers several features such as offsetting the electricity consumption through the grid, significantly reduces consumption units.

➢ *Net Metering Model*

NEM system measures produced and consumed electricity at household or investor level. NEM is based on net banking approach. NEM is a full duplex communication system enabling real time monitoring and billing of the consumed as well as grid contributed units.

As per the provisions in India's Ministry of Power (MoP) electricity (Rights of consumer) Rules 2020 allows net metering for prosumers up to 500 kW or their sanctioned load, whichever is lower. Automation is crucial in a smart grid, utilizing advanced algorithms and control systems to monitor grid performance, detect faults, and optimize the flow of electricity. When an issue like a power outage or voltage fluctuation occurs, the system can swiftly respond, often resolving the problem before consumers are even aware.

➢ *This System Comprises of Rational Spheres:*

- Bulk Generation
- Transmission
- Distribution
- Customer
- Markets
- Service Provider
- Operations.

The first four spheres involve power and information bi-directional flow, while the last three focuses on information collection and power management. NEM is structured as a hybrid and hierarchical network, comprising both a backbone network and millions of local area networks.

The backbone network comprises of inter-domain communication and local area network is used for intra-domain communication.

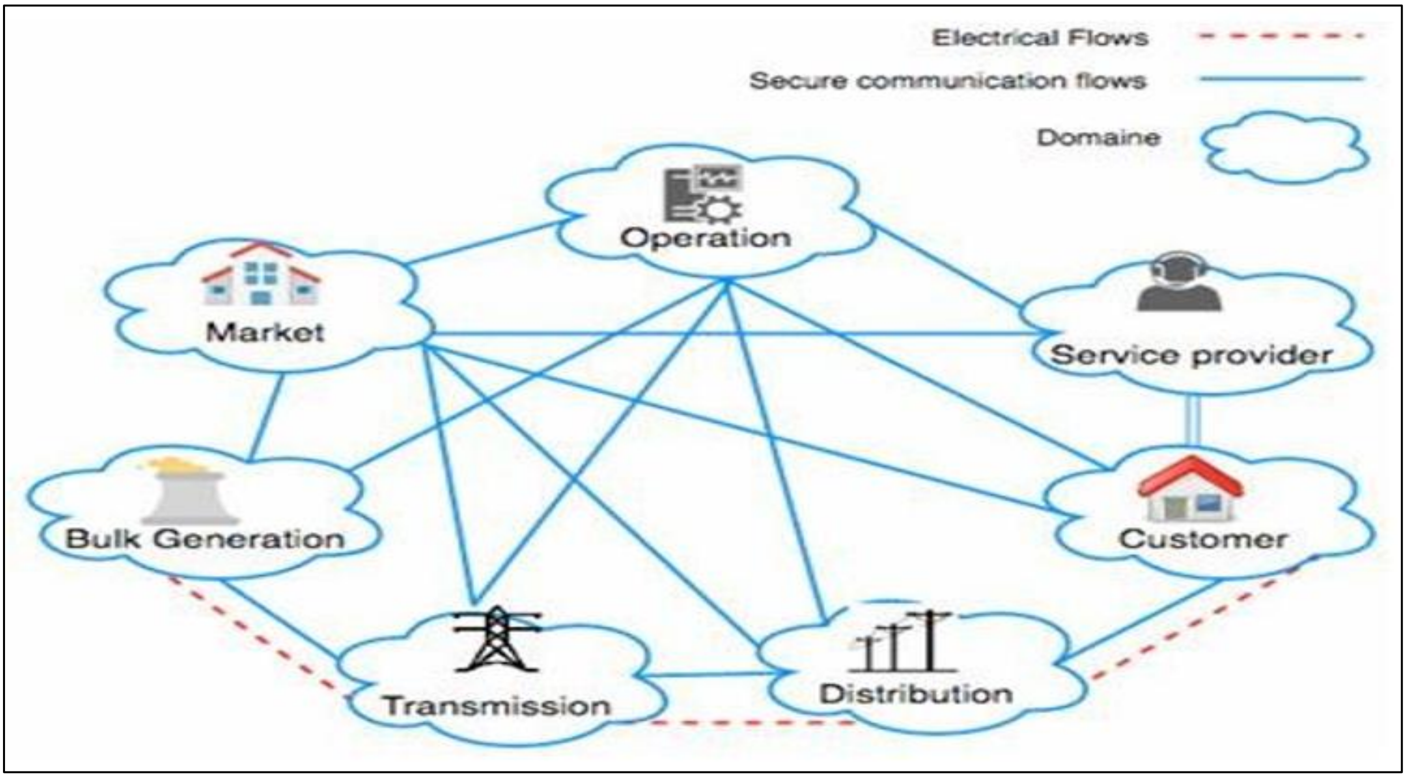


Fig 1 Seven Rational Spheres of NEM [3]

The customer domain consists of end users, they are generally of three types: home, commercial/building and industrial. In this domain the user can generate, store and manage the use of energy.

In this domain communication occurs between the distribution domain, service provider and the electricity market includes various participants who help maintain the balance between supply and demand this sector focuses on ensuring efficient and optimal operations in both transmission and distribution networks transmission operations use an EMS while distribution relies on a Distribution Management System (DMS), EMS employs SCADA to gather analog and status data whereas DMS uses Advanced Metering Infrastructure (AMI) for monitoring and controlling the distribution network.

- *NEM System*

Net metering encompasses a range of distributed and diverse applications, including AMI, substation automation, demand response, SCADA, Electric Vehicles (EV), and Home Energy Management (HEM) systems. Here, we will focus on two crucial and vulnerable applications within net metering: AMI and SCADA.

AMI integrates multiple technologies to fulfil its purpose. It includes smart meters installed at the customer's premises, a communication network, a Meter Data Management System (MDMS), and tools to incorporate the gathered data into a software application platform. Customers are equipped with advanced smart meters that collect real-time data and transmit it through the available local network to the AMI host system. This data is then forwarded to the MDMS, where it is stored, analyzed, and used to provide valuable insights to the utility service provider. AMI facilitates two-way communication between the customer and the utility [4].

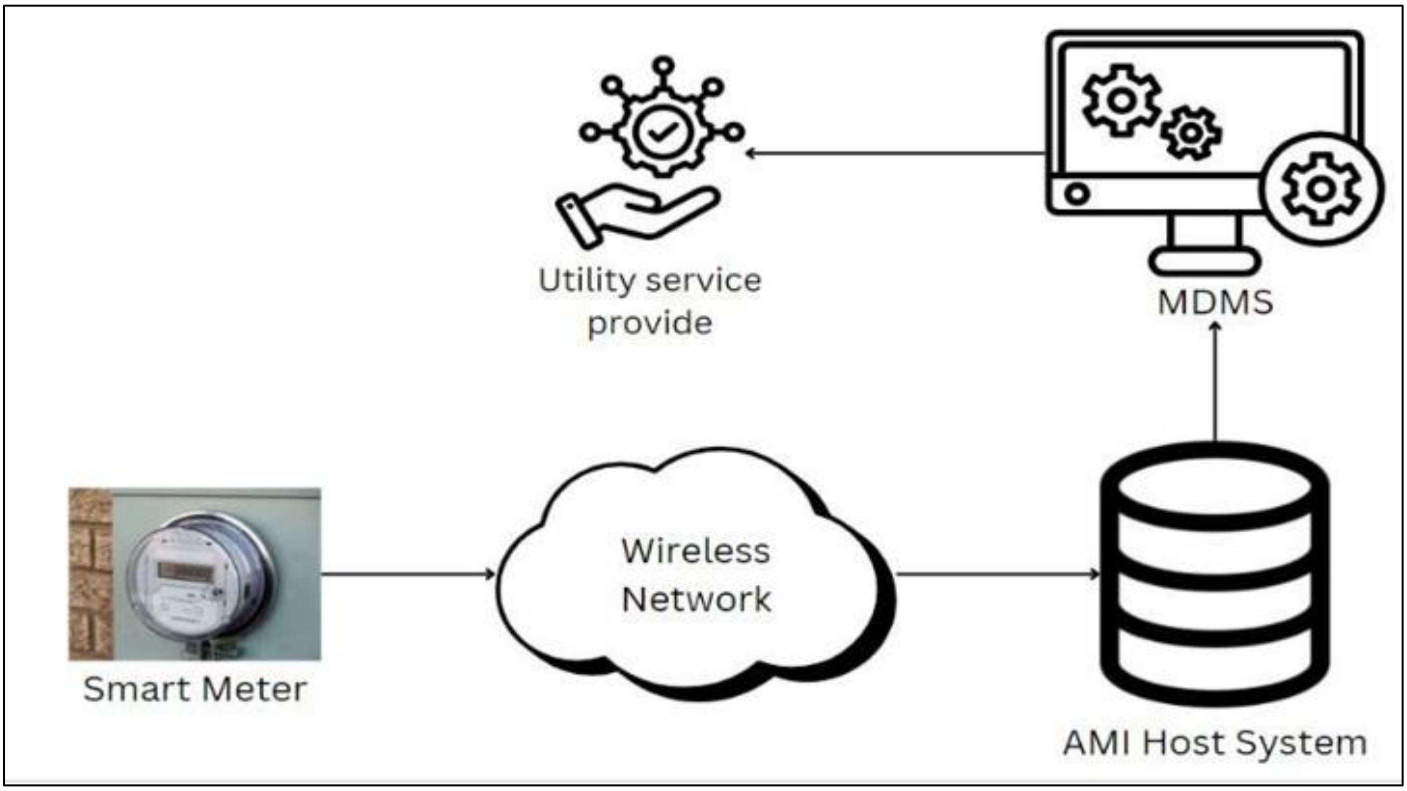


Fig 2 AMI Integration Pathway in NEM

SCADA systems, crucial for managing NEM systems, face significant cybersecurity challenges due to their use of protocols like DNP3, Modbus, and IEC 60870-5-104. These protocols, designed before modern cybersecurity threats emerged, often lack essential security features, making them vulnerable to attacks. Key risks include Man-in-the-Middle (MitM) attacks, where unencrypted data can be intercepted and altered, compromising the integrity of the system. To address these vulnerabilities, robust cybersecurity measures are needed. Encryption can protect data during transmission, while authentication using digital certificates ensures only trusted devices communicate. Regular software updates and patches are vital to closing security gaps, and real-time monitoring with AI and Machine Learning can help detect and respond to threats swiftly. As NEM adoption grows, prioritizing these security measures will be crucial for maintaining the resilience and reliability of energy systems

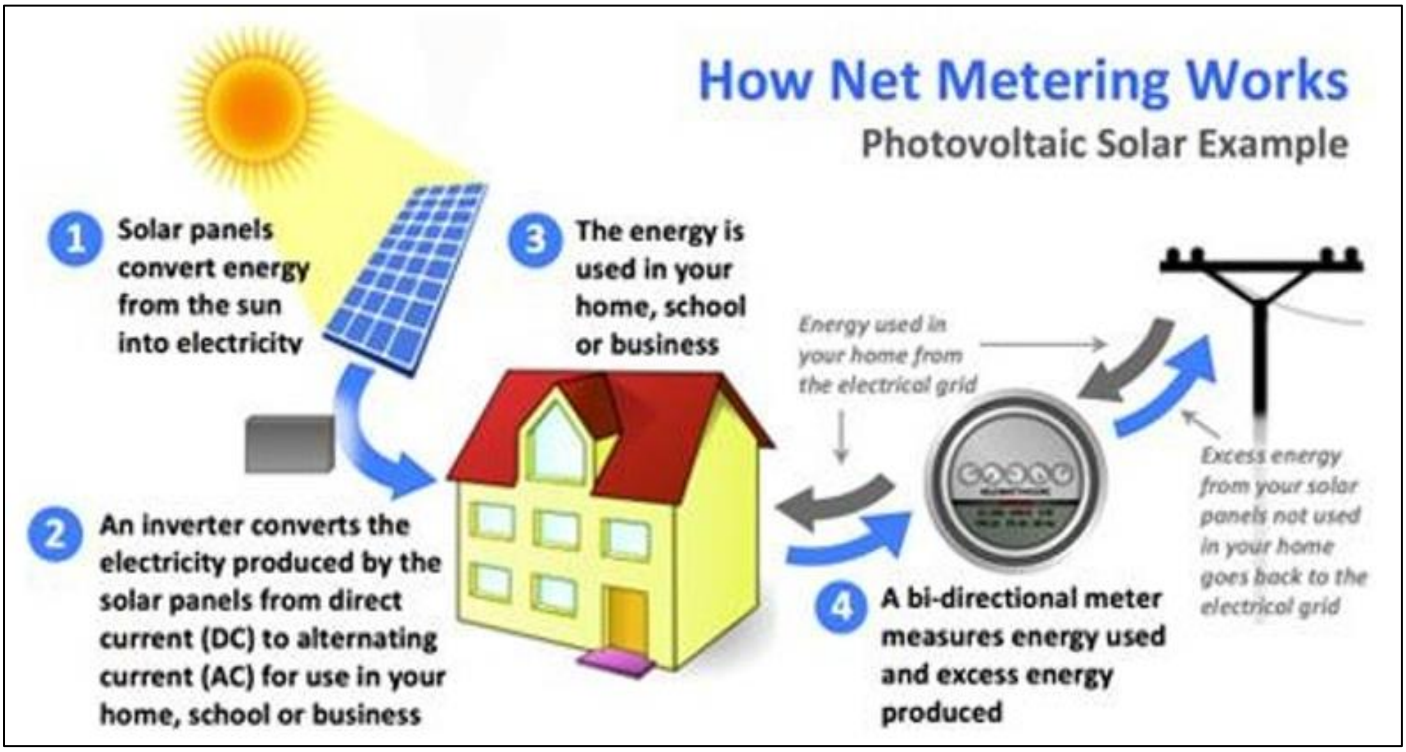

How Net Metering Works
Photovoltaic Solar Example
1 Solar panels convert energy from the sun into electricity
2 An inverter converts the electricity produced by the solar panels from direct current (DC) to alternating current (AC) for use in your home, school or business
3 The energy is used in your home, school or business
Energy used in your home from the electrical grid
4 A bi-directional meter measures energy used and excess energy produced
Excess energy from your solar panels not used in your home goes back to the electrical grid

Fig 3 NEM Functionality Overview [5]

III. CYBER-ATTACKS ON NEM SYSTEM

NEM system by nature is interconnected therefore the cyber-attacks can cause severe damage. A successful cyber-attack could manipulate or disable AMI, which includes smart meters that track energy consumption and production. This could result in inaccurate billing, allowing attackers to falsify energy credits or charges, causing financial losses for utilities and consumers.

A cyber-attack could disrupt SCADA systems, which are crucial for grid management. The cyber-attacks on NEM system violates the confidentiality, integrity and availability (CIA).

Table 1 CIA Triad of Cyber Security

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Confidentiality tracks sensitive information from unauthorized access, ensuring that only authorized individuals or entities can view or handle it.	Integrity assurance that data remains accurate, consistent, and unaltered during storage, transmission, and processing, ensuring the reliability of consumption unit.	Availability ensures that systems and data are consistently accessible to authorized users, preventing disruptions that could impact operation of net metering systems.
Threats violating CIA		
1.Cryptojacking It is a cyberattack where criminals secretly exploit a victim's computing resources to mine cryptocurrency, potentially slowing down the system.	**1.Insider Threat** An insider threat occurs when individuals within an organization intentionally or accidentally alter or manipulate data, compromising the integrity and security of critical information and systems.	**1.Drive-by Attacks** Drive-by attacks involve the automatic download of malware onto a system when a user visits a compromised or malicious website, potentially disrupting system availability and functionality.
2.Zero-DayExploit A zero-day exploit leverages unpatched vulnerabilities in software or systems, allowing attackers to gain unauthorized access and compromise data security before any defences are available.	**2.Fileless Malware** Fileless malware operates computer's memory without using traditional files, making it difficult to detect and allowing it to manipulate or corrupt data without leaving a trace on the system's storage.	**2.ATM Cash Out** ATM cash-out attacks involve manipulating banking systems to fraudulently withdraw large sums of money, with similar tactics potentially disrupting the availability and reliability of smart grid systems.
3.Watering Hole Attack A watering hole attack infects websites frequently visited by a targeted group to steal confidential information from users who visit the compromised sites.	**3.Supply Chain Attacks** Supply chain attacks involve inserting vulnerabilities or malicious code into software or hardware components during development or distribution, compromising the security.	**3.DNS Tunnelling** DNS tunnelling uses the Domain Name System to covertly transmit malicious traffic, potentially disrupting services and impacting the availability of systems like net metering and smart grids.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1839

4.Emotet Emotet is a sophisticated malware that steals sensitive information, posing a serious threat to the security and integrity of net metering and smart grid systems.	**4.Angler Phishing Attacks** Angler phishing attacks are advanced schemes that trick individuals into revealing sensitive information, compromising data integrity and system security in net metering and smart grid systems.	**4.Service Interruption** Service interruptions attacks disrupt access to systems or data, causing downtime and affecting the reliability of critical services.

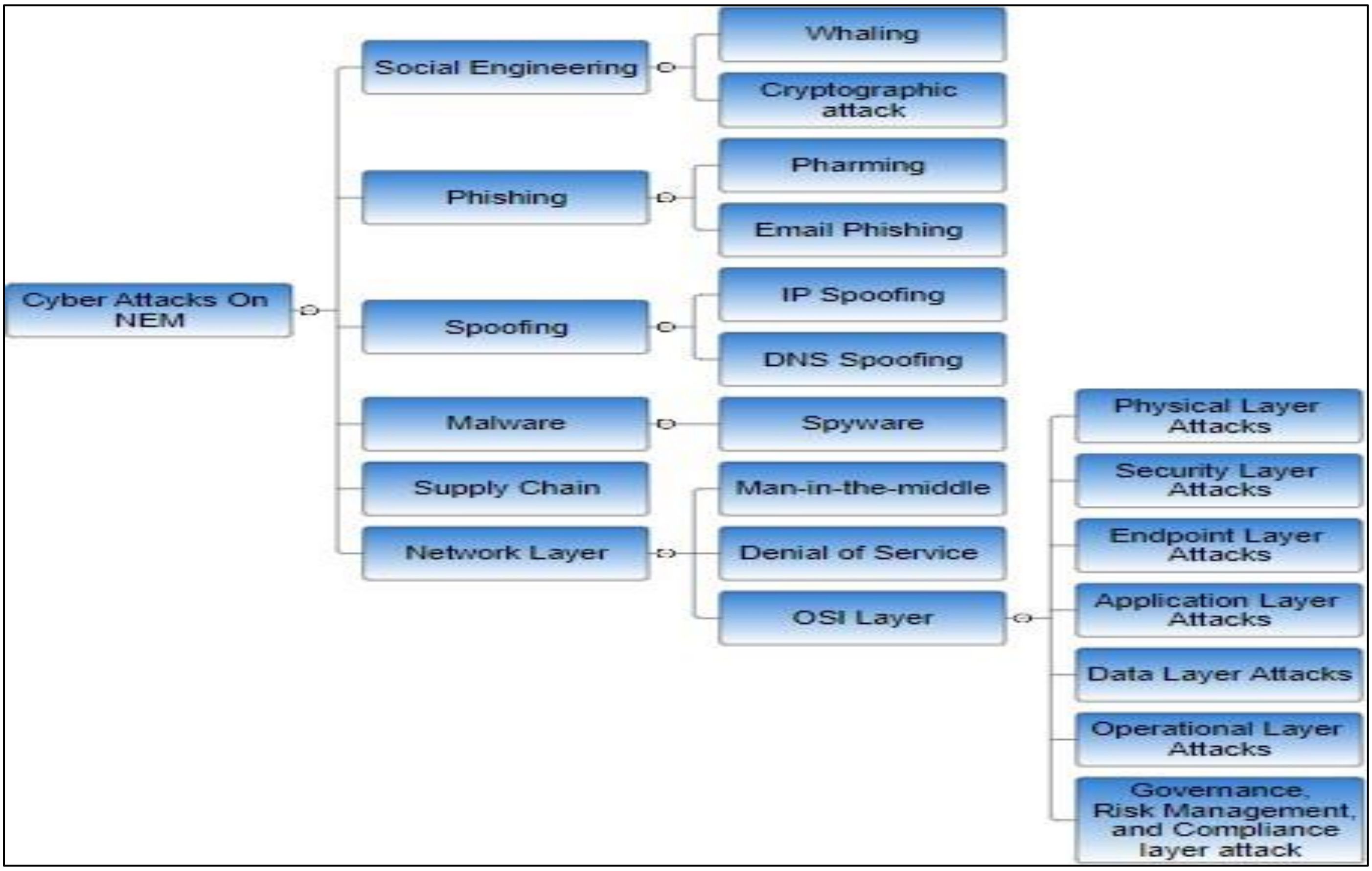


Fig 4 Types of Security Threats in NEM

A. *Social Engineering*

Social engineering is a designing tactic used in cybersecurity where attackers impose human psychology rather than technical vulnerabilities to gain illegitimate access to systems webs or confidential data.

- *Whaling*

In whaling hacker specifically choose high-profile individuals within an organization such as senior administrator or senior manager by pretending as trusted contacts or using personalized information.

- *Cryptographic Attack*

A cryptographic attack breaks the cryptologist system security by targeting a weak code, hashing method, protocol, or key management. For example, Attacker can attack on the PCS in SCADA and can get access over the complete system.

B. *Phishing*

Phishing is like a digital scam where attackers pretend to be someone you trust, such as a well-known company, to trick you into revealing sensitive information.

- *Pharming*

Pharming refers to a sneaky phishing. Pharming silently redirects browser to a bogus site, even after typing the correct web address. For example, the attacker can pretend to be an authorized customer’s service representative and solicit the customer to pay online electricity bill through their website and the attacker will provide a link to a bogus website which appears authorized and if the customer falls a bait to the attacker, then the money and banking credentials will be transferred to the attacker.

- *Email phishing*

Email phishing send emails that appear to come from reliable sources, like banks, colleagues or services when user clicks on a hyperlink or download copy in the email, they might be directed to a fake site that looks legitimate.

C. *Spoofing*

Spoofing is a deceitful trick used to make one thing look like another, usually to gain unauthorized access or information. In the digital world, it could involve faking a phone number, or website to trick people into sharing sensitive data or clicking on malicious links.

- *IP Spoofing*

IP spoofing is a cyber-attack where a malicious actor disguises their true identity by sending data packets with a forged IP address, making it appear as though the data is coming from a trusted source.

For example, in this the attacker can attack on the data packets which are being transferred from the customer's smart meter to AMI host system through locally available network.

- *Domain Name System (DNS) Spoofing*

DNS spoofing happens where an attacker tricks user computer into believing it is connecting to a legitimate website when, in fact, it's connecting to a fraudulent one. This is done by tampering with the DNS, which is like the internet's phone book, translating website names into IP addresses

D. Malware

It is a malicious software designed to harm, exploit, or compromise the integrity of a computer system. It encompasses various forms of malicious code, including viruses, worms, trojans, ransomware, and spyware. Attacks via malware can occur through multiple vectors, such as phishing emails, malicious websites, or infected software downloads.

- *Spyware*

Spyware designed to secretly gather information from a user's device without their consent. It can monitor and collect personal data, such as keystrokes, browsing habits, or sensitive information like login credentials and financial details.

E. Supply Chain

A supply chain is the network of organizations, people, and processes involved in the creation and delivery of a product or service. It attacks or exploits vulnerabilities within this network to compromise the security of an organization. For example, Solar winds supply chain attack where hackers infiltrated solar winds software updates to compromise thousands of organizations. By introducing malicious code into the company's Orion software, this is widely used for network management.

F. Network

A network attack is attempted by hacker to disrupt, intercept, or gain illegitimate access to a computer system or its resources. These attacks are typically carried out by exploiting vulnerabilities in network protocols or devices.

- *Man-in-the-Middle (MitM)*

It occurs when an attacker secretly intercepts and potentially alters communication between two parties without their knowledge. This type of attack exploits the communication channel, placing the attacker between the sender and receiver, and can occur in various scenarios, such as unsecured Wi-Fi networks or compromised websites.

- *Denial of Service (Dos)*

A DoS attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network. The goal of a DoS attack is to make the targeted service unavailable to its intended users, effectively causing downtime and disrupting business operations.

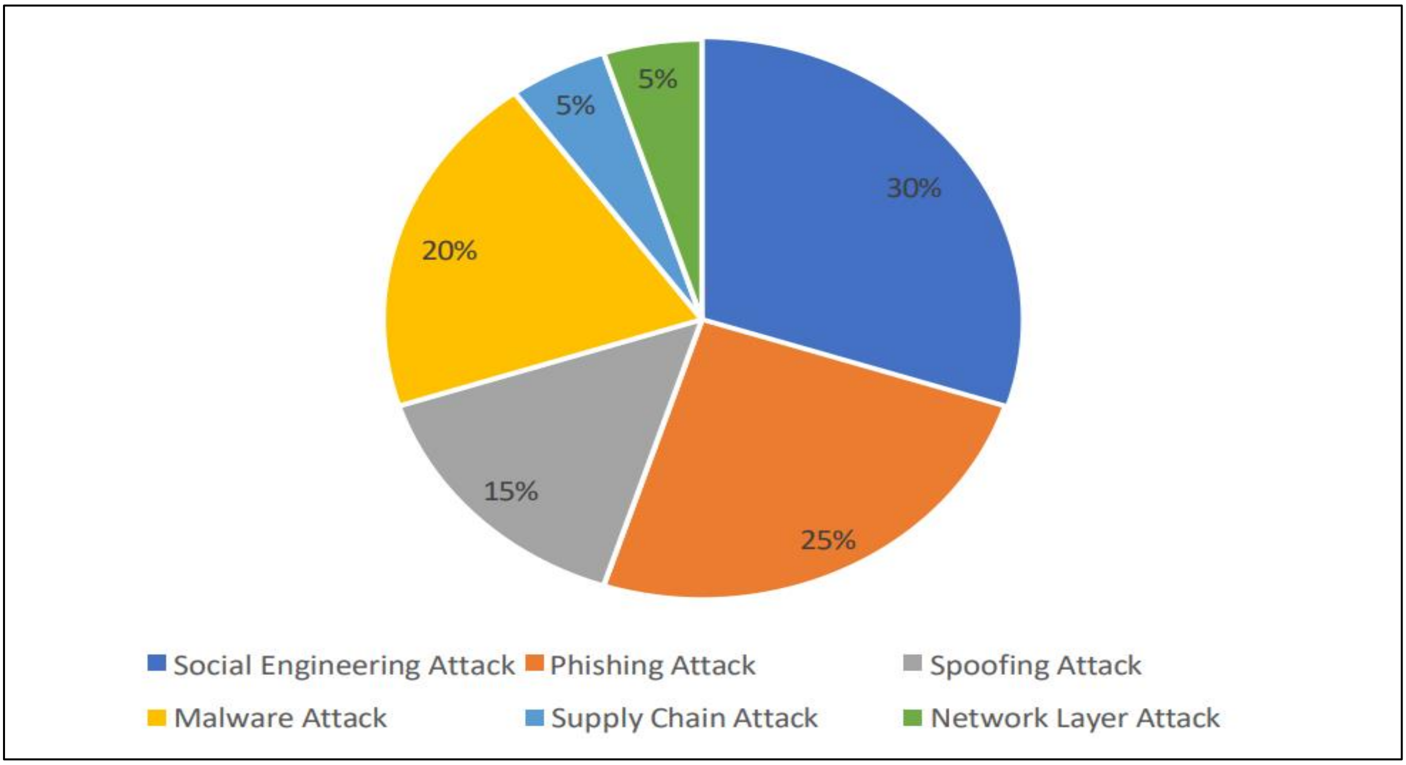


Fig 6 Frequency Distribution of Cyber Attacks

➢ *OSI Layer Attacks*

- *Physical Layer Attacks*

✓ Jamming Attacks: By interfering with the communication signals between net metering devices and the grid, attackers can prevent the data transmission, leading to potential disruptions in billing, energy credits, or grid stability.

✓ Hardware Insertion Attacks: Malicious hardware can be inserted into the system, such as rogue devices that intercept or manipulate data being sent to the grid, compromising the accuracy and reliability of energy measurements.

- *Security Layer Attacks*

✓ Man in the Middle Attacks: Attackers intercept communications between net metering devices and the grid, allowing them to alter or steal data without detection.

✓ Advanced Persistent Threat**:** Long-term, targeted undetected attacks that can alter or corrupt critical data, leading to significant operational risks over time.

- *Endpoint Layer Attacks*

✓ Ransomware: Attackers can encrypt data on endpoint devices, demanding payment to restore access. This can disrupt data collection and reporting in net metering systems.

✓ Fileless Malware: This type of malware operates in memory without traditional files, making it difficult to detect and allowing attackers to manipulate data or control devices remotely.

- *Application Layer Attacks*

✓ SQL Injection**:** This attack involves injecting malicious SQL code into an application's database query, potentially leading to unauthorized access, data manipulation, or data breaches.

✓ DoS: An attacker can overwhelm the application with excessive requests, rendering the service unavailable to legitimate users, disrupting operations and communication between net metering devices and the grid.

- *Data Layer Attacks*

✓ Data Breaches: Unauthorized access to sensitive data stored in the system can lead to the exposure of personal, financial, or operational information, potentially affecting user privacy and system integrity.

✓ Data Tampering: Attackers may alter stored data to manipulate billing, energy usage reports, or system configurations, leading to incorrect charges or operational issues.

- *Operational Layer Attacks*

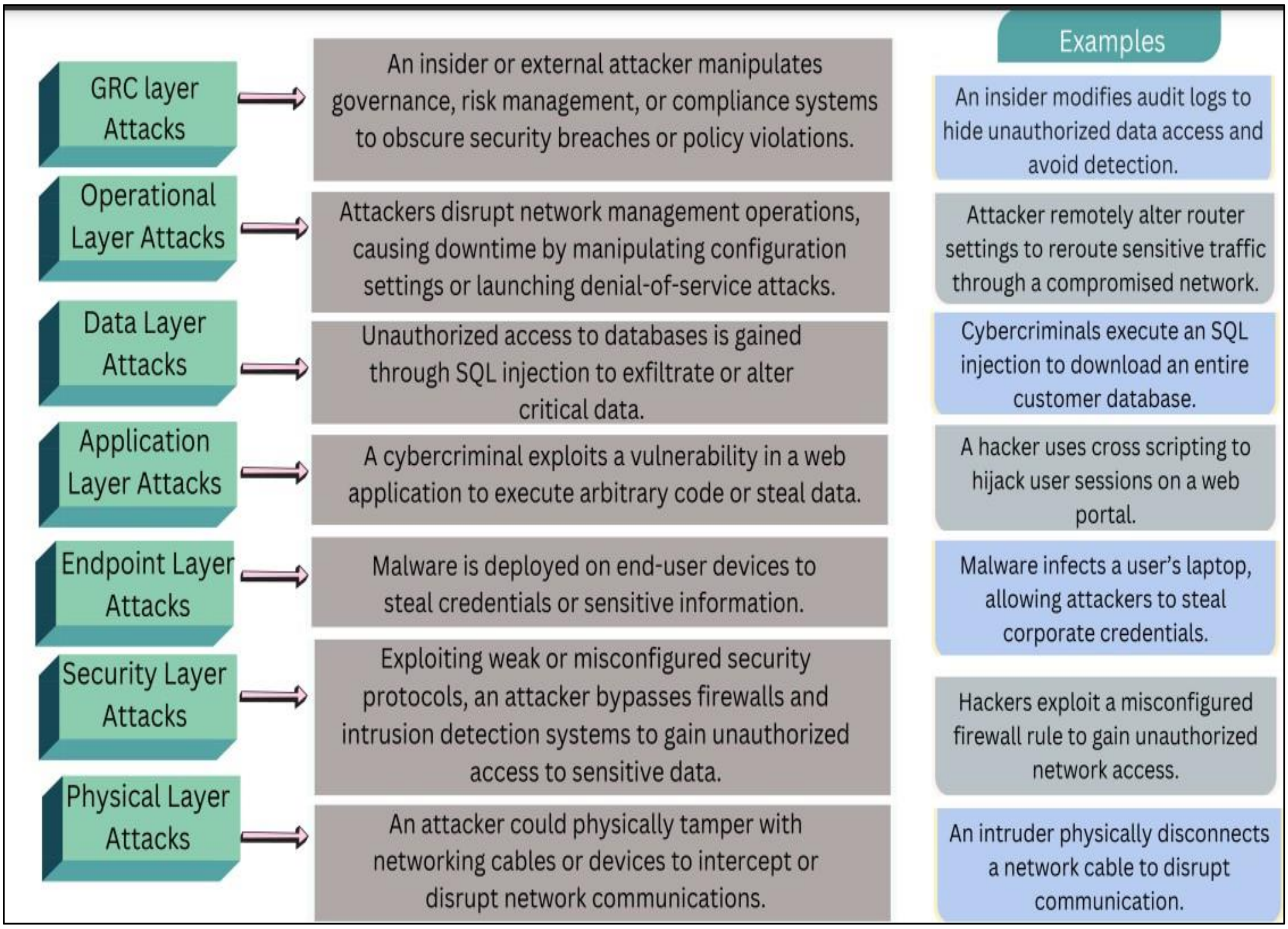
✓ Data Integrity Attacks: By corrupting or falsifying operational data, attackers can affect decision-making processes. This can lead to incorrect billing, improper energy distribution, or other operational issues.

✓ Configuration Manipulation: Attackers may exploit flaws in system configuration processes to alter critical settings. This can lead to mismanagement of energy resources and affect the overall performance and reliability of the net metering system.

- *Governance, Risk Management, and Compliance (GRC) layer Attacks*

✓ Credential Theft: Gaining unauthorized access to GRC systems through stolen credentials can provide attackers with the ability to manipulate risk assessments, bypass security controls, or tamper with compliance audits.

✓ Regulatory Non-Compliance: Attackers may manipulate or falsify compliance records, leading to non-compliance with regulations and potential legal repercussions. This can also result in financial penalties and damage to the organization's reputation



		Examples
GRC layer Attacks	An insider or external attacker manipulates governance, risk management, or compliance systems to obscure security breaches or policy violations.	An insider modifies audit logs to hide unauthorized data access and avoid detection.
Operational Layer Attacks	Attackers disrupt network management operations, causing downtime by manipulating configuration settings or launching denial-of-service attacks.	Attacker remotely alter router settings to reroute sensitive traffic through a compromised network.
Data Layer Attacks	Unauthorized access to databases is gained through SQL injection to exfiltrate or alter critical data.	Cybercriminals execute an SQL injection to download an entire customer database.
Application Layer Attacks	A cybercriminal exploits a vulnerability in a web application to execute arbitrary code or steal data.	A hacker uses cross scripting to hijack user sessions on a web portal.
Endpoint Layer Attacks	Malware is deployed on end-user devices to steal credentials or sensitive information.	Malware infects a user's laptop, allowing attackers to steal corporate credentials.
Security Layer Attacks	Exploiting weak or misconfigured security protocols, an attacker bypasses firewalls and intrusion detection systems to gain unauthorized access to sensitive data.	Hackers exploit a misconfigured firewall rule to gain unauthorized network access.
Physical Layer Attacks	An attacker could physically tamper with networking cables or devices to intercept or disrupt network communications.	An intruder physically disconnects a network cable to disrupt communication.

Fig 6 Security Breaches in the OSI Layer

IV. PROVISIONS ON CYBERATTACKS

Table 2 Legal Provisions in the IT Act for NEM Cyber Threats

Offence	Section	Punishment	Bail ability and Congizability
Social Engineering	66C	Imprisonment up to three years, or/and with fine up to ₹100,000	Non-bailable Cognizable
	66D	Imprisonment up to three years, or/and with fine up to ₹100,000	Non-bailable Cognizable
Whaling	66	Imprisonment up to three years, or/and with fine up to ₹500,000	Bailable Cognizable
	43	The Act does not specify a fixed amount for the penalty but indicates that the offender shall be liable to pay damages by way of compensation to the person affected by the act. The compensation amount can vary based on the extent of the damage or loss incurred by the affected party.	Bailable Cognizable
	66E	Imprisonment up to three years, or/and with fine up to ₹200,000	Bailable Cognizable
Cryptographic attack	43	The Act does not specify a fixed amount for the penalty but indicates that the offender shall be liable to pay damages by way of compensation to the person affected by the act. The compensation amount can vary based on the extent of the damage or loss incurred by the affected party.	Bailable Cognizable
	66	Imprisonment up to three years, or/and with fine up to ₹500,000	Bailable Cognizable

Phishing 1.Pharming 2.Email Phishing	66	Imprisonment up to three years, or/and with fine up to ₹500,000	Bailable Cognizable
	66D	Imprisonment up to three years, or/and with fine up to ₹100,000	Non-bailable Cognizable
	43	The Act does not specify a fixed amount for the penalty but indicates that the offender shall be liable to pay damages by way of compensation to the person affected by the act. The compensation amount can vary based on the extent of the damage or loss incurred by the affected party.	Bailable Cognizable
	66C	Imprisonment up to three years, or/and with fine up to ₹500,000	Bailable Cognizable
Spoofing 1.IP Spoofing 2.DNS Spoofing	43	The Act does not specify a fixed amount for the penalty but indicates that the offender shall be liable to pay damages by way of compensation to the person affected by the act. The compensation amount can vary based on the extent of the damage or loss incurred by the affected party.	Bailable Cognizable
	66	Imprisonment up to three years, or/and with fine up to ₹500,000	Bailable Cognizable
Malware 1.Spyware	66E	Imprisonment up to three years, or/and with fine up to ₹200,000	Bailable Cognizable
	43	The Act does not specify a fixed amount for the penalty but indicates that the offender shall be liable to pay damages by way of compensation to the person affected by the act. The compensation amount can vary based on the extent of the damage or loss incurred by the affected party.	Bailable Cognizable
Spyware	66C	Imprisonment up to three years, or/and with fine up to ₹500,000	Non-bailable Cognizable
	66D	Imprisonment up to three years, or/and with fine up to ₹100,000	Bailable Cognizable
Network 1.MitM 2.DoS 3.OSI Layer	66C	Imprisonment up to three years, or/and with fine up to ₹500,000	Non-bailable Cognizable
	66	Imprisonment up to three years, or/and with fine up to ₹500,000	Bailable Cognizable
	43	The Act does not specify a fixed amount for the penalty but indicates that the offender shall be liable to pay damages by way of compensation to the person affected by the act. The compensation amount can vary based on the extent of the damage or loss incurred by the affected party.	Bailable Cognizable

V. CASE STUDY

➢ *Ransom ware Attack on Solar Industries Limited (SIL)*

- Background**:** SIL, a major manufacturer of industrial and defence explosives based in Nagpur, India, serves crucial clients, including the Indian Army. Founded in 1995, the company has a significant presence in over 65 countries.
- Incident Overview**:** In 2024, the international hacking group BlackCat (ALPHV) launched a ransomware attack on SIL, stealing approximately 2TB of sensitive data from its servers. The stolen information included engineering specifications, blueprints for defence products like Pinaka rockets and BrahMos missiles, and confidential contracts with the Indian Army.
- Data Compromised**:** The compromised data encompassed critical details about warheads, explosives, surveillance footage, and audit reports, which were later auctioned on the dark web. The attack posed a severe threat to national security by exposing classified defence information.
- Response**:** After receiving four threatening emails from the hackers, SIL immediately alerted the Computer Emergency Response Team-India (CERT- In) and the Nagpur police. The case was subsequently handed over to the Central Bureau of Investigation (CBI) for a thorough investigation.
- Implications for Cybersecurity**:** This attack highlights the vulnerabilities of critical infrastructure to cyber threats, emphasizing the need for robust cybersecurity measures. Similar threats exist for NEM systems in smart grids, where a breach could lead to significant disruptions in energy distribution and security.

- Conclusion: The ransomware attack on SIL underscores the importance of enhancing cybersecurity across all critical sectors, including energy infrastructure. The ongoing CBI investigation aims to identify the perpetrators and mitigate the risks associated with such attacks.

VI. ARTIFICIAL INTELLIGENCE (AI) DRIVEN SOLUTION FOR CYBER-ATTACK ON NEM SYSTEM

AI is revolutionizing cybersecurity by providing innovative solutions to increasingly sophisticate threats. It can transform NEM systems by enhancing efficiency, security, and management. To safeguard NEM systems from cyberattacks, an AI-driven solution can be implemented that integrates predictive threat detection, deep learning- based anomaly detection, and automated response mechanisms.

By continuously monitoring network traffic and device behaviour, AI can predict and identify potential threats in real-time, isolating compromised devices and dynamically adjusting security protocols. AI-powered threat intelligence ensures the system remains updated against emerging threats, while behavioural analysis detects subtle manipulations of NEM devices. Additionally, adaptive multi-factor authentication enhances access control, and AI-driven risk assessment prioritizes high-risk areas for focused protection.

In cybersecurity, AI detects and responds to threats instantly by identifying anomalies in network traffic or device behaviour. Additionally, AI analyzes user behaviour to optimize energy usage, detects fraud, and facilitates peer-to-peer energy trading, ensuring efficient use of excess energy within the community.

Reinforcement learning further optimizes the system by continuously improving its defence strategies, ensuring a resilient and proactive cybersecurity framework for NEM systems.AI also supports dynamic energy pricing, adjusting rates in real-time based on demand and supply, and strengthens grid stability by managing electricity flow and preventing overloads.

VII. FUTURE SCOPE

As NEM systems become essential to modern energy infrastructure, enhancing cybersecurity is crucial. The expansion of smart meters, such as in Uttar Pradesh, underscores the need for robust security measures. Future advancements will likely include specialized VPN that offer stronger encryption, dynamic routing, and real-time threat adaptation, ensuring secure communication within NEM networks.

AI and Machine Learning (ML) will play a significant role in predicting and identifying vulnerabilities, enabling pre-emptive threat mitigation. AI can analyze smart meter data to detect anomalies and issue alerts for suspicious activities, thus reducing cyberattack risks.

Regulatory frameworks, including potential amendments to the IT Act, 2000, will need to evolve to mandate advanced cybersecurity measures. Regulations may require encrypted VPNs and AI-based monitoring for NEM systems and enforce strict standards for smart meter deployment and management.

Additionally, consumer-facing apps will empower users with insights into energy consumption, but these must be secured to protect data privacy. International collaboration will be vital for establishing global cybersecurity standards and responding to cross-border threats. Investing in these areas will ensure that NEM systems remain secure and capable of supporting the growing demand for efficient energy solutions.

VIII. CONCLUSION

NEM faces critical cyber security challenges, particularly in the application layer of smart grids. Key threats include social engineering, phishing, malware, and supply chain attacks, exemplified by the SolarWinds incident.

The IT Act, 2000, provides a legal framework, yet gaps in enforcement and adaptability persist. VPN and AI/ML offer potential solutions, enhancing security but requiring careful consideration of limitations.

As NEM adoption grows, proactive and adaptive cybersecurity measures are crucial, along with updated legal standards, international collaboration, and continuous technological advancements to safeguard these systems.

REFERENCES

[1]. Mohassel, R. R., Fung, A. S., Mohammadi, F., &Raahemifar, K. (2014, May). A survey on advanced metering infrastructure and its application in smart grids. In *2014 IEEE 27th Canadian conference on electrical and computer engineering (CCECE)* (pp. 1-8). IEEE.

[2]. Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defensemodeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(4), 853-865.

[3]. El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering, 67, 469- 482.

[4]. https://energycentral.com/c/iu/advanced-metering-infrastructure-ami-part-1-roots

[5]. Net Metering, Solar Net Metering, Dealer, Installation, Supplier (accuratesolar.in)

[6]. https://sci-hub.se/10.1109/SECON.2015.7132891

[7]. https://arxiv.org/pdf/2406.11716

[8]. https://arxiv.org/pdf/2407.07966